

Symmetric and Quadratic Forms, with  
Applications to Coding Theory, Algebraic  
Geometry and Topology <sup>1</sup>

Chris Peters, Hans Sterk  
Eindhoven University of Technology

Version JUNE 2024

<sup>1</sup>September 16, 2024

# Contents

<b>Preface</b>	v
<b>Introduction</b>	1
List of Notation . . . . .	6
Interdependence of Chapters . . . . .	10
List of Basic Notions . . . . .	12
<b>1 Symmetric and Quadratic Forms, an Overview</b>	13
1.1 Quadratic Forms: a Review of Linear Algebra . . . . .	14
1.2 First Acquaintance with Integral Lattices . . . . .	17
1.3 Orthogonality . . . . .	20
1.4 Examples of Integral Lattices . . . . .	23
1.5 Isometry and Equivalence . . . . .	25
1.6 Discriminant Forms . . . . .	28
1.7 More Examples . . . . .	33
1.8 Lattice Embeddings . . . . .	40
1.9 On $p$ -Adic Lattices and the Genus . . . . .	41
1.10 Finiteness Results . . . . .	48
1.11 Excursion: Small Lattice Vectors and the Sphere Packing Problem	52
1.12 Positive Definite Lattices . . . . .	54
1.13 Outlook: Indefinite Lattices . . . . .	57
<b>2 Indefinite Unimodular Integral Lattices</b>	59
2.1 Reduction Modulo a Prime and Characteristic Elements . . . . .	59
2.2 Classification in Rank At Most Four . . . . .	61
2.3 Odd Indefinite Forms . . . . .	62
2.4 Even Indefinite Forms . . . . .	62
2.5 Applications to Topology . . . . .	64
<b>3 Quadratic Forms over <math>\mathbb{Q}</math> and <math>\mathbb{Q}_p</math></b>	69
3.1 The Hasse Invariant is Well Defined . . . . .	70
3.2 Representation by Forms . . . . .	73
3.3 Classification . . . . .	76
<b>4 Forms Related to Graphs</b>	79
4.1 Root Lattices Spanned by $(-2)$ -Roots . . . . .	79
4.2 Other Root Lattices . . . . .	88
4.3 Lattices Obtained From the Euclidean Algorithm . . . . .	92
4.4 Lens Spaces . . . . .	99
4.5 Surface Singularities, Surface Fibrations and Mordell–Weil Lattices	106

---

<b>5</b>	<b>Forms Related to Coding Theory and Number Theory</b>	119
5.1	Codes and Lattices . . . . .	119
5.2	Application to Nodes, K3 Surfaces and Nodal Quintics . . . . .	126
5.3	Lattices, Number Fields and Codes . . . . .	131
5.4	Lattices and Quaternions . . . . .	136
<b>6</b>	<b>Symmetric and Quadratic Forms Revisited</b>	143
6.1	Bilinear Forms on $R$ -Modules . . . . .	143
6.2	The Correlation Morphism . . . . .	149
6.3	Forms on Free $R$ -Modules . . . . .	150
6.4	Discriminant Forms . . . . .	156
6.5	Isometry Groups . . . . .	157
<b>7</b>	<b>Reflections and the Witt Decomposition</b>	162
7.1	Reflections . . . . .	162
7.2	The Theorems of Cartan–Dieudonné and Witt . . . . .	164
7.3	Excursion: The Witt Ring . . . . .	168
<b>8</b>	<b>Inner Product Spaces Over Fields</b>	170
8.1	Characteristic Different from Two . . . . .	170
8.2	Characteristic Two . . . . .	171
8.3	Classification of Quadratic Inner Product Spaces over Finite Fields	176
<b>9</b>	<b>Symmetric and Quadratic Torsion Groups</b>	180
9.1	Generalities on Symmetric and Quadratic Torsion Modules . . . . .	180
9.2	The Sylow Decomposition . . . . .	184
9.3	Jordan Splittings for $p$ -primary Torsion Groups . . . . .	185
9.4	Building Blocks For $p$ -Primary Torsion Forms . . . . .	192
<b>10</b>	<b><math>p</math>-adic Lattices</b>	194
10.1	Low Rank $p$ -adic Lattices . . . . .	194
10.2	Jordan Splitting of $p$ -adic Lattices . . . . .	198
10.3	Compatibility of Jordan Splittings . . . . .	202
10.4	Application: the Hasse Invariants of $p$ -adic Lattices . . . . .	205
<b>11</b>	<b>Normal Forms and the Genus</b>	207
11.1	Normal Form Decomposition for odd $p$ . . . . .	207
11.2	Normal Form Decomposition for $p = 2$ . . . . .	210
11.3	Characterizing the Genus of a Quadratic Lattice . . . . .	215
<b>12</b>	<b>Integral Lattices: the Discriminant Form</b>	217
12.1	Existence of Quadratic Integral Lattices with Given Discriminant Form . . . . .	217
12.2	Stable Equivalence and Discriminant Forms . . . . .	219
12.3	Calculation of the Index Mod 8 . . . . .	222
12.4	Applications to the Genus: Existence of Even Lattices . . . . .	227

---

12.5 Applications to Odd Lattices . . . . .	233
<b>13 The Spin Group</b>	243
13.1 The Clifford Algebra . . . . .	244
13.2 The Clifford Group . . . . .	249
13.3 The Spin Group and Spinor Norm . . . . .	251
13.4 The Spin Group: Lattice Aspects . . . . .	254
<b>14 Spinor Equivalence</b>	257
14.1 The Genus Revisited . . . . .	258
14.2 The Spinor Genus . . . . .	260
14.3 Strong Approximation for the Spin Group . . . . .	267
14.4 Genus, Spinor Genus and Equivalence . . . . .	268
14.5 Lifting Isometries of the Discriminant Group . . . . .	270
14.6 Uniqueness of $p$ -Elementary Lattices . . . . .	272
<b>15 Lattice Embeddings</b>	276
15.1 Primitive Embeddings of Lattices . . . . .	276
15.2 Primitive Embeddings into Unimodular Quadratic Lattices . . . . .	280
15.3 Primitive Embeddings Into Non-Unimodular Quadratic Lattices . . . . .	286
15.4 On Embeddings into Odd Unimodular Lattices . . . . .	289
<b>16 The Structure of Orthogonal Groups I, Vector spaces</b>	292
16.1 Vector Space Isometries and Sign Structures . . . . .	292
16.2 Orthogonal Groups in Characteristic Two . . . . .	296
16.3 Orthogonal Groups of Quadratic Spaces over Finite Fields . . . . .	299
16.4 Application: Theta Characteristics . . . . .	301
<b>17 The Structure of Orthogonal Groups II, Lattices</b>	307
17.1 An Overview of Lattice Isometries . . . . .	307
17.2 Root Lattices and Reflection Groups . . . . .	310
17.3 Eichler–Siegel Transformations . . . . .	317
<b>18 Applications to Singularities</b>	324
18.1 Generalized Dynkin Diagrams and Vanishing Lattices . . . . .	324
18.2 Application to the Monodromy of Singularities . . . . .	332
18.3 Application to Global Monodromy . . . . .	338
<b>19 Application to Moduli of K3 Surfaces</b>	342
19.1 Background On K3 Surfaces . . . . .	342
19.2 Period Domains, Néron–Severi lattices and Transcendental Lattices . . . . .	344
19.3 The Moduli Space of Marked K3 Surfaces . . . . .	349
19.4 Lattices and Compactifications of Moduli Spaces . . . . .	352
19.5 Supersingular K3 Surfaces . . . . .	356

---

<b>20 Automorphism Groups of K3 Surfaces</b>	363
20.1 The Automorphism Group of a Projective K3 Surface . . . . .	364
20.2 Finite Groups Acting On a K3 Surface . . . . .	368
20.3 The Mathieu Group $M_{23}$ . . . . .	372
20.4 Finite Abelian Groups Acting Symplectically . . . . .	373
20.5 Involutions on K3 Surfaces . . . . .	384
20.6 Kummer Surfaces Revisited . . . . .	388
20.7 Nikulin Involutions Revisited . . . . .	391
20.8 Shioda–Inose structures . . . . .	394
20.9 Appendix: On Surfaces Admitting an Action of a Finite Group . .	398
<b>21 Applications to Enriques Surfaces</b>	407
21.1 Enriques Surfaces: Moduli . . . . .	407
21.2 Automorphisms of Enriques Surfaces . . . . .	414
<b>A Background in Algebra and Number Theory</b>	420
A.1 Modules over Principal Ideal Domains . . . . .	420
A.2 The Field $\mathbb{Q}_p$ . . . . .	422
A.3 Approximation Theorems Related to Vector Spaces and Lattices .	423
A.4 Hilbert Symbols . . . . .	425
A.5 Symplectic Forms and Symplectic Groups . . . . .	428
A.6 Cohomology of Groups and Group Actions . . . . .	431
<b>B Background on Complex Surfaces</b>	434
B.1 Generalities on Kähler Geometry . . . . .	434
B.2 Basic Invariants of Surfaces . . . . .	435
B.3 Examples . . . . .	438
B.4 Period Domains . . . . .	442
B.5 Surface Classification . . . . .	443
<b>C Quadratic Forms: Specialized Topics</b>	447
C.1 On Witt’s Extension Theorem . . . . .	447
C.2 Index Invariants for Torsion Forms . . . . .	452
C.3 Normal Forms for 2-Primary Torsion Quadratic Forms . . . . .	456
<b>References</b>	461
<b>Index</b>	479

## *Preface*

Our main motivation to write the present monograph comes from the desire to make Nikulin's article [171] more accessible. In this article he rewrote the classical theory of integral quadratic forms in terms of the discriminant quadratic form. In geometry this is particularly useful since the input often comes from the discriminant form as demonstrated e.g. in [168, 169, 170, 172, 173].

The importance and scope of Nikulin's work [171] was immediately realized by the algebraic geometry community. At the same time a need was felt for an introductory exposition of the number theoretic aspects required to understand the details of Nikulin's densely written article. Unfortunately, to this date no such work exists in the literature, although the prepublication [156] of R. Miranda and D. Morrison serves this goal to some extent. Since they ultimately aimed at a full explanation of [154, 155] – which extends Nikulin's results considerably – their report, while starting out on an elementary level, quickly becomes technically involved.

Instead, we started on a more elementary level, developing the theory of integral quadratic forms gradually, with regular excursions to apply the theory developed so far to disparate fields such as topology, singularity theory and algebraic geometry, notably to K3 and Enriques surfaces. The reader we have in mind is an algebraic geometer or topologist without a broad background on quadratic forms. For this reason in the first few chapters several classical results concerning quadratic forms are explained in detail.

In this way we hope to have succeeded not only in making Nikulin's work more accessible, but that we also have shown that these results have applications in many different fields of mathematics.

Noordwijkerhout, Eindhoven,  
July 2024

C. Peters  
H. Sterk

TO DO: acknowledgments



# Introduction

## Brief Historical Remarks

The subject of quadratic forms is a very old one. It traces back to the problem of finding the Pythagorean triples, some of which were known to the Babylonians around 2000 BCE. A modern way of enumerating those triples starts from the rational points on the plane quadric curve  $x^2 + y^2 = z^2$ ; the latter admits a rational parametrization from which all Pythagorean triples can be written down. This old example shows the interplay between number theory and geometry.

Later other quadratic equations were investigated, notably by Brahmagupta who in 628 found a conditional method to solve the equation  $x^2 - ny^2 = 1$ , now called Pell's equation. Later Bhāskara II around 1150 solved Pell's equation unconditionally.

In Europe this equation was studied much later by Fermat, and a solution was published by the British mathematician Brouncker after Fermat in a 1657 letter announced he could solve the equation, and challenged others to do so. More than a century later, Gauss wrote his famous *Disquisitiones Arithmeticae* (1801) which contains a substantial part devoted to the theory of binary quadratic forms (i.e., quadratic forms in two variables) over the integers.

The algebraic theory of quadratic forms, that is, the study of quadratic forms over arbitrary commutative rings, only started in the 20th century. The main protagonists are E. Witt (cf. [251]) and M. Eichler (cf. [67]). Analytic theory also plays a major role for positive definite forms since there are strong relations to theta functions as explained by C.L. Siegel in [212, 213, 214].

The earliest monographs on integral quadratic forms are [112, 246, 177, 151] by B. Jones, G. Watson, O. O'Meara, respectively J. Milnor–D. Husemoller. The first three develop the classical theory in more or less detail, while the last reference provides a short original treatment of unimodular forms and is also devoted to applications to topology. The algebraic and analytic theory from that epoch is masterly explained in J. Cassels' book [36].

As mentioned in the preface, V. Nikulin's work [171] brings the classical algebraic theory in a new phase through his original and influential reformulation thereof in terms of the discriminant form associated to an integral quadratic form.

## Kaleidoscopic View of This Book

As is clear from the title of the book, symmetric and quadratic forms are intimately related. This relation should be well-understood from the start. An  $n$ -ary quadratic form over a commutative ring  $R$  is just a quadratic function in  $n$  variables  $x_1, \dots, x_n$ , say  $q = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j$  with coefficients  $a_{ij}$  in  $R$ . The associated upper



triangular matrix  $A = (a_{ij})$  defines a symmetric matrix  $B = A + A^T = (b_{ij})$  leading to a symmetric form, the polar form  $\sum_{1 \leq i, j \leq n} b_{ij} x_i y_j$  of  $q$ . Whenever we work in a situation where 2 is invertible, every symmetric matrix  $B$  can be decomposed as  $B = A + A^T$  with  $A$  upper-triangular and with entries in  $R$ . If this is the case, there is no essential difference between symmetric and quadratic forms. Unfortunately this does not apply to integral forms since a polar form of an integral symmetric form always has even diagonal elements. Such symmetric bilinear forms are called "even forms". Those that are not even are simply called "odd".

Our main objects of investigation are indeed the integral symmetric forms, and a long introductory chapter is devoted to these. The reader opting for a more general set-up might as well start right away with Chapter 6. However, since the general theory exposed in these later chapters is quite technical, Chapter 1 offers a more leisurely treatment of the central concepts along with several illustrative basic examples. For instance we explain the genus of a lattice which encapsulates local information. Alongside we give an inventory of basic  $p$ -adic lattices. We also introduce the discriminant form, both locally and globally.

Before embarking on the full classification, in Chapter 2 we first deal with indefinite unimodular forms since, as remarked by J. Milnor (cf. [151]), their classification is much simpler and can be explained using less advanced tools. This has also the advantage that this results in a classification of intersection lattices of compact manifolds, since by Poincaré duality these lattices are unimodular. Some topological applications thereof are given in Section 2.5.

Quadratic forms over the rational numbers play of course a central role. Their classification is explained in Chapter 3 where we largely follow Chapter IV in J. P. Serre's monograph [204]. After this somewhat abstract chapter we have inserted two chapters in which we discuss several constructions for lattices and apply these to coding theory and topology. More in detail, in Chapter 4 we turn to graphs related to the Euclidean algorithm and apply these considerations to lens spaces, (complex) surface singularities and surface fibrations. As a byproduct, following C.T.C. Wall in [245], a lattice is constructed whose discriminant form is a given cyclic torsion form, a result playing a decisive role in Chapter 12. Then, in Chapter 5 we investigate some lattices constructed by algebraic means (linear codes, number fields and quaternion algebras). These results are first applied to Kummer surfaces, following [168], and then following ideas [17] of A. Beauville, to surfaces with many nodes.

From Chapter 6 on, we broaden our perspective and reconsider quadratic and symmetric forms over an arbitrary commutative unital ring  $R$ , adding assumptions on  $R$  as we go from Chapter 6 to Chapter 10. In these chapters we develop the necessary fundamental theory. For instance, the later classification results are based on a splitting principle, proven in Chapter 6, which reduces classification to rank one and two. This is used in Chapter 8 to obtain the classification over fields. Furthermore, it leads in Chapters 9 and 10 to a classification of torsion quadratic forms and of symmetric  $p$ -adic lattices. Before this, in Chapter 7, we prove the more elementary, but fundamental results of Cartan–Dieudonné on reflections and those of E. Witt about splitting off isotropic subspaces. The importance of the

first result reveals itself later in the Chapters 13 and 14 where we show how it leads to the spinor norm and to spinor equivalence. The second leads to the concept of the Witt index which generalizes the notion of the index of a real quadratic form to forms over other fields. In our book this notion plays a less important role.

We point out that, contrary to the usual simplification in many elementary textbooks, characteristic two is incorporated in our treatment. This has a reason: many applications make essential use of this characteristic, for instance the description of supersingular K3 surfaces as discussed in Section 19.5, or in establishing the count of the number of elliptic fibrations on general Enriques surfaces (cf. Corollary 21.2.4). As examples of typical characteristic two concepts we mention the Arf invariant which comes up in Section 8.2, and the Dickson invariant which is treated in Section 16.2.

In Chapter 11 we start elaborating Nikulin's theory and show that the genus of an integral quadratic lattice<sup>1</sup> is completely determined by its index and discriminant quadratic form. Next, in Chapter 12, following the approach [56] of A. Durfee, we show that a torsion quadratic form is the discriminant form of some lattice. Provided some easily verifiable conditions are satisfied, the index and torsion quadratic form determine a unique genus of even integral lattices. In the last section of this chapter, Section 12.5, we derive analogous results for odd lattices.

If a genus is non-empty, how many isometry classes are there? This question is addressed in Chapter 14 and can be considered as the main technical pillar on which the classification of indefinite integral lattices rests. We observe in Section 1.12 of the introductory chapter that the number of isometry classes of a definite lattice in a genus grows enormously with the (absolute value of) its discriminant. Fortunately, for indefinite lattices the situation is drastically different and is much more manageable. The problem can be tackled by splitting it up into two problems of a very different nature:

- The first step is to investigate spinor-equivalence which is intermediate between equivalence(=isometry) and genus-equivalence. The number of spinor genera in a given genus is the order of a “computable” finite group. From the genus invariants one can often deduce that this group is trivial and so, by Nikulin's approach, this translates as a condition on the rank, index and discriminant form.
- The second step consists of finding conditions which imply that spinor-equivalent lattices are isometric. As we shall explain, this is a consequence of the strong approximation theorem. The surprising main result here is that a spinor genus of an indefinite lattice of rank at least 3 contains only one isometry class.

After these (elaborate) steps, we arrive at the final result, Theorem 14.4.2, which, in this formulation, is of course also due to Nikulin. In the remainder of Chapter 14 as well as in Chapter 15 the results obtained so far are used to derive several lattice-theoretic consequences that are useful for geometric applications such as

---

<sup>1</sup>In this introduction lattices are assumed to be non-degenerate.

criteria for embedding lattices in unimodular lattices and for extending isometries of sublattices to the entire lattice.

The next two chapters are devoted to isometry groups of quadratic vector spaces and of quadratic lattices respectively. In the first, Chapter 16, we also discuss some typical characteristic  $p$  topics such as counting the orders of the orthogonal groups over finite fields, the notion of a rotation in characteristic 2 using the Dickson invariant, and also the classical application of quadratic forms over the field  $\mathbb{F}_2$  to theta-characteristics. In the next chapter, Chapter 17, special attention is given to isometry groups generated by hyperplane reflections as well as to Eichler–Siegel transformations. The latter provide a powerful tool to investigate isometry groups of Lorentzian lattices. These also turn out to be useful in the study of monodromy groups of isolated singularities as illustrated in Chapter 18.

In the last 40 years the techniques developed in this book have been predominantly applied to K3 surfaces as well as to Enriques surfaces. Already in Nikulin’s fundamental article [171] several such applications were given; D. Morrison considered in [158] applications to special K3 surfaces, whereas W. Barth–C. Peters as well as I. Dolgachev applied these to Enriques surfaces (cf. [16, 51]). We also want to point out the applications to supersingular K3 surfaces as given by A. N. Rudakov and I. R. Šafarevič in [199]. These and several other applications find their place in Chapters 19–21.

In the first two appendices we have assembled some more or less well-known material which is used in the book, mainly for easy reference but also to give the non-expert a synoptic view of subject material on which several examples are based. The last appendix is devoted to technical results on quadratic forms, some of which are used in the main body of the text. It is worthwhile to mention that it contains some less known statements and proofs of Witt’s extension theorem and the Cartan–Dieudonné theorem over local rings in which 2 is not invertible. The appendix also contains proofs of some technical results on dyadic forms that are used in the main text but would divert the reader too much from the already involved line of reasoning.

## What Other Monographs on Quadratic Lattices Offer

As already mentioned, the present monograph on quadratic forms serves a limited goal. Consequently, some aspects of the theory have been barely touched upon whereas others have been completely ignored. Many classic articles can be found in the collected works of E. Witt [252] and of C.-L. Siegel [215, 216, 217, 218].

There are also several excellent monographs available. Apart from the ones already mentioned, we want to briefly discuss some older as well as some more recent standard books on quadratic forms.

To start, M. Eichler’s book [67] is a classic book focussing on orthogonal and spinor groups over several kinds of fields and requires basic knowledge of algebraic number theory. For forms over algebraic number fields one should also consult Y. Lam’s book [132] as well as the second rewritten edition [133]. Here the theory of

the Witt rings find their proper place; for instance, the formidable progress due to A. Pfister has been explained in these books. For the original work by A. Pfister see [188].

Next, in the more recent book [123] by M.-A. Knus the purely algebraic aspects of quadratic forms are treated, as well as those of Hermitian forms. Furthermore, extensive material on Clifford algebras, Azumaya algebras and the  $K$ -theory of quadratic and Hermitian forms can be found in this treatise.

The book [201] of W. Scharlau has a different flavour: non-commutative algebras equipped with an involution come up and also transcendental extensions play a role.

Readers interested in applications to cryptography and cryptoanalysis may consult L. Gerstein's book [84], and, finally, those interested in applications to algebraic geometry may want to read the exposition [70], written by R. Elman, N. Karpenko and A. Merkurjev. It requires ample understanding of algebraic geometry in a scheme-theoretic setting, the natural setting for arithmetic applications.

## List of Notation

Symbol	meaning	page
$\text{disc}(b)$	discriminant of $b$	15
$b_q$	polar form of $q$	14
$\oplus$	orthogonal direct sum	16
$L_{\mathbb{Q}}, L_{\mathbb{R}}$	$L \otimes_{\mathbb{Z}} \mathbb{Q}, L \otimes_{\mathbb{Z}} \mathbb{R}$	19
$\text{rad}(b)$	radical of $b$	20, 146
$\tau(L, b)$	index of $(L, b)$	23
$\langle a \rangle$	integral form $(x, y) \mapsto axy$	23
$[\frac{1}{2}a]$	integral quadratic form $x \mapsto \frac{1}{2}ax^2$	23
$L(m)$	lattice $L$ with form scaled by $m$	23
$U$	the hyperbolic plane	23
$(L_{\Gamma}, b_{\Gamma})$	lattice associated to a graph $\Gamma$	23
$E_8$	root lattice for the Dynkin graph $E_8$	23
$\Gamma_n$	pos. definite lattice of rank $n$ , $n \equiv 0 \pmod{8}$	25
$L \simeq L'$ or $b \simeq b'$	$L$ and $L'$ are isometric	25
$O(b)$ or $O(L)$	the orthogonal group of the lattice $(L, b)$	26, 158
$\sigma_x$	reflection in the vector $x$	26, 158
$W^{\epsilon}(L)$	the Weyl group of $L$	27
$W_{\tau}(V)$	Witt index of $V$	27, 167
$L^*$	$\text{Hom}_{\mathbb{Z}}(L, \mathbb{Z})$ , the dual of $L$	28
$b_L$	correlation morphism	28, 149
$\text{dg}_L$	discriminant group $L^*/L$	28
$\ell(G)$	length of the finite group $G$	28
$b_{\mathbb{Q}}, q_{\mathbb{Q}}$	extension of $b, q$ to $L_{\mathbb{Q}}$	30
$b_L^{\#}$	discriminant bilinear form	30
$q_L^{\#}$	discriminant quadratic form	30
$L^G, L_G$	$G$ -invariant, anti-invariant sublattice of $L$	36
$\mathbf{1}_n$	square identity matrix of size $n$	40
$L_p, p$ a prime	$L \otimes_{\mathbb{Z}} \mathbb{Z}_p$	41
$b_p$	the $\mathbb{Z}_p$ -bilinear extension of $b$	41
$D(R)$	the group $R^{\times}/(R^{\times})^2$	42
$\mathcal{P}$	the collection of places of $\mathbb{Q}$	43
$L_{\infty}$	$(L_{\mathbb{R}}, b_{\mathbb{R}})$ , $L_{\mathbb{R}} = L \otimes \mathbb{R}$ and $b_{\mathbb{R}} = b \otimes \mathbb{R}$	43
$b_{L_p}^{\#}$	discriminant bilinear form on $\text{dg}_{L_p}$	43
$q_{L_p}^{\#}$	discriminant quadratic form on $\text{dg}_{L_p}$	43
$\mathfrak{g}(L)$	the genus of $L$	43
$\langle up^k \rangle$	$p$ -adic form $up^kxy$ on $\mathbb{Z}_p$ ,	46
$\langle up^{-k} \rangle$	torsion form $up^{-k}xy$ on $\mathbb{Z}/p^k\mathbb{Z}$	46
$U_k$	quadratic $p$ -adic binary form $p^kxy$	47
$u_k$	torsion quadratic binary form $p^{-k}xy$	47

Symbol	meaning	page
$V_k$	binary dyadic form $2^k(x^2 + xy + y^2)$	47
$v_k$	torsion quadratic binary form $2^{-k}(x^2 + xy + y^2)$	47
$\Lambda_{K3}$	K3-lattice	57
$\Lambda_{\text{Enr}}$	Enriques-lattice	57
$\sigma(L)$	modulo 8-invariant of $L$	60
$H_X$	the middle cohomology (mod torsion) of an oriented compact manifold $X$	64
$S_X$	intersection form on $H_X$	64
$X \# X'$	connected sum of $X$ and $X'$	64
$w_k(X)$	$k$ -th Stiefel-Whitney class of $X$	66
$c_k(X)$	$k$ -th Chern class of $X$	67
$T_X$	holomorphic tangent bundle of $X$	67
$K_X$	canonical bundle of $X$	67
$\mathbb{P}^n$	complex projective $n$ -space	66
$Q$	$\mathbb{P}^1 \times \mathbb{P}^1$ as a differentiable manifold	66
$K3$	K3 surface as a differentiable manifold	67
$\varepsilon_v(q)$	Hasse invariant of $q$ at a place $v \in \mathcal{P}$	69
$(a, b)_v$	Hilbert symbol at a place $v \in \mathcal{P}$	69, 426
$A_n, D_n, E_n, \tilde{T}_{p,q,r}$	root lattices (Dynkin diagrams)	79–81
$\tilde{A}_n, \tilde{D}_n, \tilde{E}_n$	extended Dynkin diagrams	81
$\mathbb{Z}^{1,n}$	Lorentz lattice	84
$[b_0, b_1, \dots, b_m]$	continued fraction defined by the $b_j$	93
$\Gamma_a$	graph associated to $a$	92
$L(t, s)$	lens space of type $(t, s)$	99
$\ln c, c'$	linking number of $c$ and $c'$	101
$\tau_{16}(X)$	index mod 16 of the manifold $X$	102
$A_{t,s}$	Hirzebruch–Jung singularity	107
$\text{NS}(X)$	Néron–Severi group/lattice of $X$	107, 445
$\rho(X)$	Picard number of $X$	107, 445
$p_a(D)$	arithmetic genus of the curve $D$	108, 445
$[D]$	class of divisor $D$	110
$\text{MWL}(E_K)$	Mordell–Weil group/lattice	114
$\chi(\mathbb{O}_X)$	genus of a surface $X$	110, 434
$\Gamma_C$	lattice associated to a code $C \subset \mathbb{F}_q^n$	120
$C_{\text{Gol}}$	binary extended Golay code	123
$\Gamma_{24}$	Leech lattice	123
$M_{24}$	Mathieu group	123
$S^{\leq k}(W)$	$k$ -th order Reed–Muller code on $W$	124
$D_{m+1}$	Reed–Muller code $S^{\leq 1}(\mathbb{F}_2^m)$	125
$C_m$	Linear functions on $\mathbb{F}_2^m$ as a code	125
$\Lambda_{\text{Kum}}$	abstract Kummer lattice	128
$\Lambda_{\text{Nik}}$	Nikulin lattice	129
$N_{K/k}, \text{Tr}_{K/k}$	norm form, resp. trace form for $K/k$	131
$\left(\frac{a,b}{k}\right)$	quaternion algebra over $k$	137
$Q(R)$	fraction field of an integral domain $R$	143
$V^*, V_F^*$	duals of $R$ -module $V$	144
$O(V, b)$	isometry group of $(V, b)$	145
$\langle r \rangle_R$	form $(x, y) \mapsto rxy$ on $R$	145

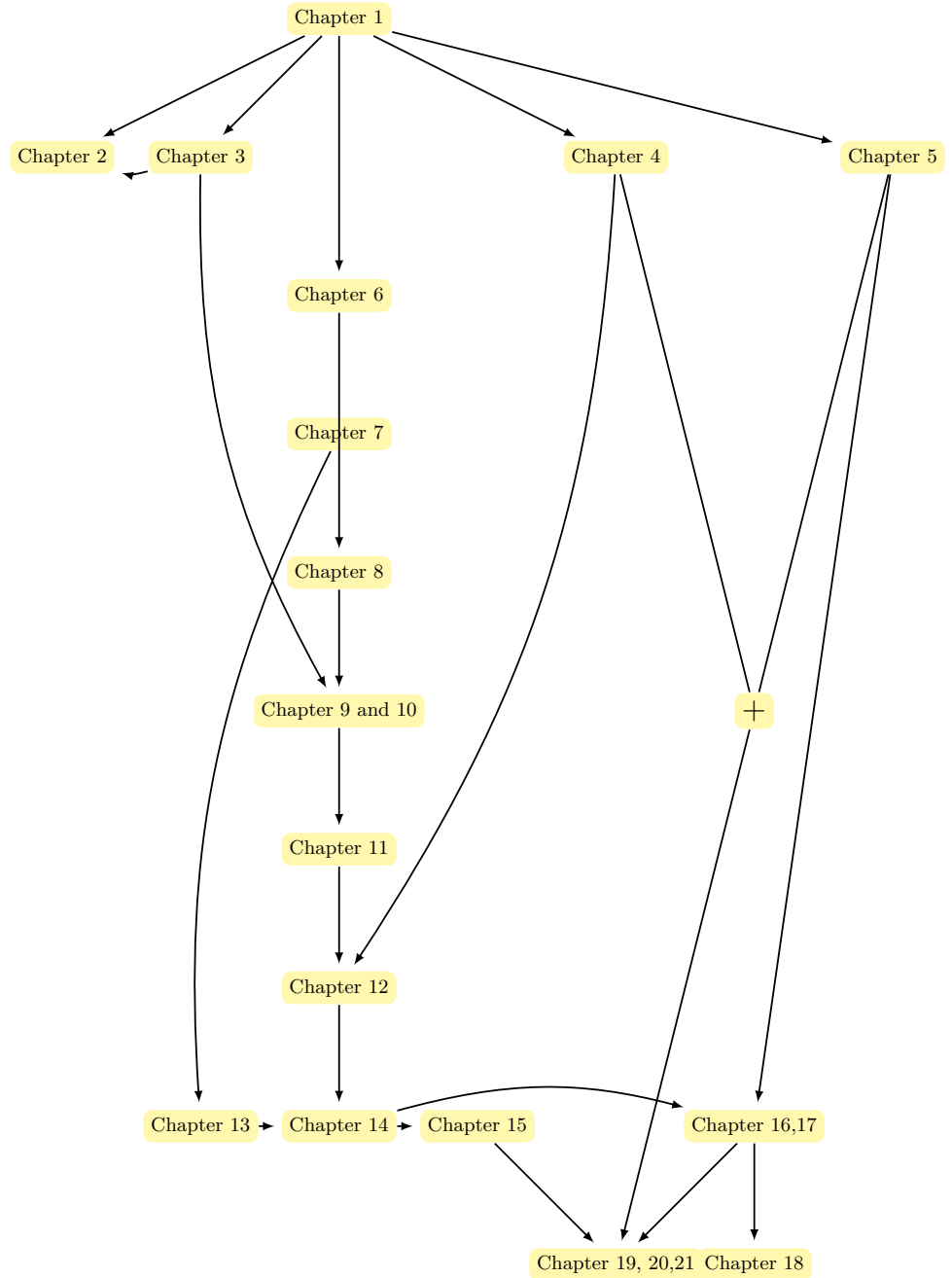
Symbol	meaning	page
$\text{rad}(b)$	radical of the symmetric form $b$	146
$\text{rad}(q)$	radical of the quadratic form $q$	146
$C_m$	cyclic group of order $m$	147
$\langle a^{-1}m \rangle$	torsion bilinear form on $\mathbb{Z}/m\mathbb{Z}$	147
$U_R$	hyperbolic $R$ -plane	153
$U_V$	hyperbolic module associated to $V$	155
$U_{L,q}$	split hyperbolic inner product space	155
$\wp$	Artin–Schreier map (in characteristic 2)	172
$\text{arf}(q)$	Arf invariant of $q$	172
$\text{SO}(L)$	group of rotations of the lattice $L$	158
$\sigma_S$	symmetry in the sublattice $S$	158
$r_L^b$	reduction map $\text{O}(L, b) \rightarrow \text{O}(b_L^\#)$ ,	159
$r_L = r_L^q$	— respectively, $\text{O}(L, q) \rightarrow \text{O}(q_L^\#)$	270
$W(R)$	Witt group/ring of $R$	168
$[V]$	class of the lattice $V$ in the Witt ring	168
$\delta(b), \delta(q)$	reduced discriminant	183
$\mu$	2-adic invariant	206
$(\frac{1}{2}G, \frac{1}{2}b)$	halving of a torsion bilinear form $b$ on $G$	191
$g(L)$	genus invariant of a lattice $L$	216, 238
$L_{r,u}$	$p$ -adic lattice $\langle u \rangle \oplus \oplus^{r-1} \langle 1 \rangle$	208
$L_{b^\#}$	normal form for $p$ -adic lattice, $p \neq 2$ with discriminant form $b^\#$	208
$L_{q^\#}^{(1)}, L_{q^\#}^{(2)}$	normal forms for dyadic lattices with discriminant quadratic form $q^\#$	213
$\tau_8$	index mod 8	222
$\omega(-)$	standard additive character	224
$\mathbb{C}(q), \mathbb{C}(L)$	Clifford algebra of $q$ or $L$	245, 256
$\mathbb{C}^0(q), \mathbb{C}^0(L)$	even Clifford algebra of $q$ or $L$	245, 256
$\text{Clif}(q), \text{Clif}^0(q)$	Clifford group, special Clifford group of $q$	249
$C_{p,q}$	real Clifford algebra	246
$\text{Mat}(n, K)$	$n \times n$ matrices over $K$	248
$\text{Nm}_{\text{spin}}(u)$	spinor norm of $u$	251
$\text{Spin}(q), \text{Pin}(q)$	(s)pin group of $q$	251
$\text{SO}^+(q)$	reduced orthogonal group of $q$	251
$S_V, S_L, S_{V_p}, S_{L_p}$	image of the spinor norm w.r. to $V, L, V_p, L_p$	254
$\text{Spin}(L), \text{Pin}(L)$	(s)pin group of $L$	256
$\text{O}^+(L), \text{SO}^+(L)$	reduced orthogonal groups of $L$	256
$\text{O}^\#(L)$	$\ker \left( r_L : \text{O}(L) \rightarrow \text{O}(q_L^\#) \right)$	270
$\text{SO}^\#(L)$	$\ker \left( r_L : \text{SO}(L) \rightarrow \text{SO}(q_L^\#) \right)$	270.
$\text{Nm}_{\text{spin}}^\epsilon$	$\epsilon$ -spinor norm	293
$\text{O}^\epsilon(L)$	$\{g \in \text{O}(L) \mid \text{Nm}_{\text{spin}}^\epsilon(g) = 1\}$	293
$C_V$	component of the light cone in $V$	295
$W^\epsilon(L)$	Weyl group of $L$	308
$\Delta_\epsilon(L), I_{\epsilon\text{-root}}$	set of $\epsilon$ -roots in $L$ and sublattice they span	308
$\text{O}^{\epsilon, \#}(L)$	$\text{O}^\epsilon(L) \cap \text{O}^\#(L)$	309
$\text{SO}(L) \xrightarrow{\rho_n} \text{Aut}(L/nL)$	group homomorphism induced by $L \rightarrow L/nL$	309

Symbol	meaning	page
$O(L)[n]$	$\ker(\rho_n)$	309
$\Delta(L), L_{\text{root}}$	$\Delta_\epsilon(L), L_{\epsilon\text{-root}}$ for $\epsilon = -1$	309
$\psi_{f,y}$	Eichler–Siegel transformation	317
$\psi_U(L')$	certain subgroup of $O(U \oplus L')$	321
$\Lambda$	orbit of $\Lambda$ under the reflection group for $\Lambda$	325
$T_{p,q,r}^1$	a certain Dynkin diagram	329
$\Lambda_{X,x}$	Milnor lattice of $(X, x)$	333
$\mu$	Milnor number of singularity	333
$D_{\mathbf{F}}$	discriminant locus for the family $\mathbf{F}$	334
$\nu$	Tjurina number of a singularity	334
$\text{Mon}(\Lambda_{X,x})$	monodromy group of $(X, x)$	336
$\text{Mon}(\Lambda_{n,d})$	monodromy for universal family of degree $d$ hypersurfaces in $\mathbb{P}^{n+1}$	338
$O_\ell(L)$	isometries of $L$ fixing $\ell \in L$	339
$C_X$ , resp. $C_X^{\text{Käh}}$	positive cone, resp. Kählercone of $X$	343, 436
$C_X^{\text{amp}}$	ample cone inside $\text{NS}(X)_{\mathbb{R}}$	344, 436
$\mathcal{M}$	moduli space of marked K3 surfaces	349
$\mathcal{M}_S$	moduli space of $S$ -marked K3 surfaces	351
$\text{Aut}_s(X)$	group of symplectic automorphisms of the K3 surface $X$	364
$G_C$	stabilizer of $C$ in the group $G$	364
$\phi$	The Euler totient function	366
$\mathcal{M}_G$	moduli space of $G$ -marked K3 surfaces	370
${}^t_{\text{Nik}}$	abstract Nikulin involution	391
$\hat{f}_i$	Gysin map in cohomology	399
${}^t_{\text{Enr}}$	lattice Enriques involution	407
$\text{Aut}_s(Y)$	group of semi-symplectic automorphisms of the Enriques surface $Y$	415
$C_n$	cyclic group of order $n$	421
$\left(\frac{x}{p}\right)$	Legendre symbol	426
$\varepsilon(-)$	standard character	426
$\  - \ _p$	$p$ -adic norm	422
$\nu_p$	$p$ -adic valuation	422
$\Omega_X^p$	sheaf of homomorphic $p$ -forms on $X$	434
$H^{p,q}(X)$	subspace of $H^{p+q}(X, \mathbb{C})$ of $(p, q)$ -classes	434
$h^{p,q}(X)$	$\dim H^{p,q}(X)$	434
$p_g(X)$	$\dim H^{2,0}(X)$ for a surface $X$	434
$q(X)$	$\dim H^{1,0}(X)$ for a surface $X$	434
$\mathbf{F}_n$	Hirzebruch surface	438
$D(L, b)$	period domain for $(L, b)$	443
$P_m(X)$	$m$ -th plurigenus of $X$	445
$\kappa(X)$	Kodaira dimension of $X$	445
$J_n$	standard symplectic form	429
$\text{Sp}(V)$	group of symplectic automorphisms of $V$	430



## Interdependence of Chapters

Lower level chapters require all chapters from higher levels except Chapter 1.



## List of Basic Notions

Adjoint map for $(V, b)$ : morphism $V \xrightarrow{b_V} V_F^*$ sending $x$ to $b(x, -)$	quadratic — : an even integral lattice
Binary form: symmetric or quadratic form in 2 variables	non-degenerate — : a lattice with non-zero discriminant
Correlation map: <i>see</i> Adjoint map	unimodular — : a lattice with discriminant $= \pm 1$
Discriminant of $R$ -bilinear form $b$ : value of $\det(B_E)$ modulo squares, where $B_E$ is the Gram matrix with respect to a basis $E$	isometry between $R$ -symmetric modules: bijective $R$ -linear map preserving the bilinear forms
discriminant bilinear form: the torsion form given by $(\bar{x}, \bar{y}) \mapsto b_{Q(R)}(x, y) \bmod R$	Jordan decomposition of a $p$ -primary module: direct sum decomposition into homogeneous summands
discriminant quadratic form: the torsion quadratic form given by $q_L^\#(\bar{x}) = q_{Q(R)}(x) \bmod R$	Jordan splitting of a $p$ -primary module: orthogonal direct sum decomposition into homogeneous summands
discriminant group of $(L, b)$ : torsion group $L^*/b_L(L)$ where $b_L$ is the correlation morphism	Jordan splitting of a $p$ -adic lattice $L$ : $L = \bigoplus_{k=1}^m L_k(p^k)$ with $L_k$ unimodular
dyadic lattice, — symmetric/quadr. form: $\mathbb{Z}_2$ -lattice, 2-adic symmetric/quadr. form	Length of finite abelian group $G$ : minimal number of generators of $G$
Equivalent lattices: sublattices of an inner product space $V$ related by an isometry of $V$	Non-degenerate form: form whose correlation morphism is an injection
exponent of the torsion group $R/p^e R$ : the integer $e$	Quadratic $F$ -valued $R$ -module: $R$ -module endowed with an $F$ -valued quadratic form
Gram matrix of a symmetric form $b$ : the matrix $(b(e_i, e_j))$ w.r. to a basis $\{e_1, \dots, e_n\}$	quadratic $R$ -module: a quadratic $R$ -valued $R$ -form
Inner product space over $R$ : a unimodular symmetric free $R$ -module of finite rank	quadratic inner product space over $R$ : unimodular free quadratic $R$ -module of finite rank
integral lattice: a free $\mathbb{Z}$ -module $L$ of finite rank equipped with a symmetric bilinear form	quadratic torsion $R$ -module: $Q(R)/R$ -valued quadratic form over $R$
	quadratic torsion group: torsion group endowed with a $\mathbb{Q}/\mathbb{Z}$ -valued quadratic form

---

Radical of a quadratic $R$ -module $(V, q)$ $V^\perp \cap \{x \in V \mid q(x) = 0\}$	valued symmetric form
radical of a symmetric $R$ -module $V: V^\perp$	symmetric $R$ -module: symmetric $R$ -valued $R$ -module
root (vector): $x \in L$ primitive, non-isotropic, s.t. $L$ is preserved by the reflection $\sigma_x$	symmetric torsion $R$ -module: $Q(R)/R$ -valued $R$ -bilinear symmetric form
root lattice: integral lattice spanned by its roots	symmetric torsion group: torsion group endowed with a $\mathbb{Q}/\mathbb{Z}$ -valued symmetric form
Split hyperbolic inner-product space: lattice $L \oplus L^*$ with form $(x, f) \mapsto q(x) + f(x)$	Ternary form: quadratic form in 3 variables
Sylow decomposition of torsion module $T$ : $T = \oplus_p T_p$ with $T_p$ a $p$ -primary module	Unimodular form: form whose correlation morphism is an isomorphism
symmetric $F$ -valued $R$ -module: $R$ -module endowed with an $F$ -	

# Symmetric and Quadratic Forms, an Overview

## Introduction

This longer chapter is meant as an overview of all the themes that will be treated in depth in later chapters. It focusses on the special case of integral lattices after we have reviewed the pertinent linear algebra in Section 1.1. The general theory over arbitrary rings is postponed until Chapter 6.

There are a few basic concepts and ideas that play a major role in this book. Among these are the notions of discriminant, orthogonality, decomposability, index and signature, treated in Sections 1.1, 1.2 and 1.3. A first set of examples of lattices are introduced in Section 1.4. These come up later as building blocks.

What it means to say that two lattices are the same, and what automorphisms of lattices are, is explained in Section 1.5. Here the theorems of Witt and Dieudonné-Cartan are promoted.

A further central concept is the discriminant form and Section 1.6 is devoted to its basic properties. With help of this tool, in Section 1.7 we can give further elementary examples: neighbouring lattices,  $p$ -elementary lattices and overlattices. We return to these examples in later chapters, for example in Chapter 15 in which we consider the embedding problem for lattices: can a given lattice be embedded in another given lattice and if so, is the embedding unique? In Section 1.8 we introduce the reader to this circle of ideas.

To classify lattices it is often helpful to “localize”. This leads to  $p$ -adic lattices and the concept of genus. Section 1.9 offers a comprehensive introduction. From the list of examples of  $p$ -adic lattices we present here, all others can be constructed as will be shown in later chapters. A genus contains only finitely many equivalence classes of lattices as we show in Section 1.10. We furthermore point out the innovative approach to the genus initiated by Nikulin. This approach gives the discriminant form a central place which is one more reason to explain this notion in more detail in this introductory chapter.

In Sections 1.12, 1.13 we point out the drastically different behaviour of lattices with a “form of a fixed sign” (definite lattices) and the indefinite ones.

We have interspersed this chapter with (sub)sections called “outlook”. These are meant as beacons shining light on central results to which we return later in the book.

Finally, Section 1.11, headed “excursion” contains further results mostly without proofs but which mention interesting related developments, a full treatment of which would lead us too far afield.

## 1.1 Quadratic Forms: a Review of Linear Algebra

Before we pass to lattices we review some concepts from linear algebra. So we start with a finite dimensional vector space  $V$  over any field  $k$  and select some basis  $\mathbf{E} = \{e_1, \dots, e_n\}$ . A **symmetric bilinear form** on  $V$  is given by a function

$$b : V \times V \longrightarrow k$$

such that

1.  $b$  is linear in each of its two arguments, that is  $b(\alpha x + \beta y, z) = \alpha b(x, z) + \beta b(y, z)$  for all  $\alpha, \beta \in k$ ,  $x, y, z \in V$ , and similarly for the second argument;
2.  $b(x, y) = b(y, x)$  for all  $x, y \in V$ .

Such a form is uniquely determined by the symmetric matrix

$$B_{\mathbf{E}} = (b_{ij}) \in k^{n \times n}, \quad b_{ij} = b(e_i, e_j),$$

the **Gram matrix** of  $b$  with respect to  $\mathbf{E}$ . Indeed, writing  $x = \sum x_i e_i$  and  $y = \sum y_i e_i$  we find

$$b(x, y) = (x_1, \dots, x_n) \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

The function  $x \mapsto b(x, x)$  is an example of a **quadratic form**, that is, a function  $q : V \rightarrow k$  for which

1.  $q(\alpha x) = \alpha^2 q(x)$ ,  $\alpha \in k$  and  $x \in V$ ;
2. the form  $b_q(x, y) = q(x + y) - q(x) - q(y)$  is a symmetric bilinear form on  $V$ , the **polar form** of  $q$ . In particular, setting  $y = x$ , we find

$$b_q(x, x) = 2q(x).$$

Using these properties and starting for instance with

$$q(x_1 e_1 + \cdots + x_n e_n) = q(x_1 e_1 + \cdots + x_{n-1} e_{n-1}) + q(x_n e_n) + b_q(x_1 e_1 + \cdots + x_{n-1} e_{n-1}, x_n e_n),$$

the quadratic form  $q$  can be expressed in matrix form as follows:

$$q(x) = (x_1, \dots, x_n) \overbrace{\begin{pmatrix} q_{11} & \cdots & \cdots & q_{1n} \\ 0 & q_{22} & \cdots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & q_{nn} \end{pmatrix}}^Q \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad (1.1)$$

where  $q_{ii} = q(e_i)$  and  $q_{ij} = b_q(e_i, e_j)$  if  $i < j$ . We observe two things:

1. The matrix  $Q$  is not always determined by the polar form  $b_q$ . To see this, observe that  $b_q$ 's Gram matrix is  $B_E = Q + Q^T$ , so that  $q_{ij} = b_{ij}$  if  $i < j$ ,  $q_{ij} = b_{ji}$  if  $i > j$ , and  $b_{ii} = 2q_{ii}$ . Hence  $q_{ii}$  can only be recovered if the characteristic is different from 2.
2. Given a bilinear form  $b$ , the polar form of the quadratic form  $x \mapsto b(x, x)$  equals  $2b$  and so in characteristic 2 this is zero.

These observations show that characteristic 2 is special. For the remaining characteristics we may divide by 2 and there is a perfect correspondence between quadratic forms and symmetric bilinear forms.

*Remark 1.1.1.* **1.** If we don't insist on  $Q$  being upper triangular, the Gram matrix  $B_E$  of the polar form of a quadratic form can be written in many ways as  $B_E = S + S^T$ , while still  $xSx^T = xQx^T$  for all vectors  $x \in k^n$ . Indeed, in characteristic  $\neq 2$  the matrix  $Q$  can be replaced by any matrix  $S = Q + A$ , where  $A$  is anti-symmetric, and in characteristic 2 we can take  $S = Q + A$ , where  $A$  is symmetric and has zeros on the diagonal. We leave the easy verification as an exercise.

**2.** There are analogous definitions for the above notions for  $R$ -valued forms on a finite rank free  $R$ -module over a commutative ring  $R$ . This will be treated extensively in Chapter 7. The case  $R = \mathbb{Z}$  is the topic of the remainder of the chapter.

**3.** Since 2 is not invertible in  $\mathbb{Z}$  there is again a difference between integral bilinear forms and polar forms of integral quadratic forms. We shall see (cf. Proposition 1.2.5) that the latter correspond to so-called even forms.

We list some basic properties of symmetric bilinear forms. Similar properties hold for quadratic forms by considering their polar forms. We say that the form  $b$  is *non-degenerate* if and only if  $\det(B_E) \neq 0$ . This does not depend on the choice of basis. Indeed, in another basis  $F$ , say  $f_j = \sum_k c_{kj}e_k$ ,  $k = 1, \dots, n$ , we readily find

$$B_F = C^T B_E C, \quad C = (c_{ij}), \quad (1.2)$$

and so  $\det B_F = (\det C)^2 \det B_E$ . For a non-degenerate form the determinant of the Gram matrix is well defined up to multiplication with non-zero squares. This gives the *discriminant* of  $b$ , denoted

$$\text{disc}(b) = \det B_E \cdot (k^\times)^2 \in k^\times / (k^\times)^2.$$

A pair  $(V, b)$  of a finite dimensional vector space equipped with a non-degenerate symmetric bilinear form is also called an *inner product space*. An equivalent intrinsic way of phrasing non-degeneracy follows from

**Proposition 1.1.2.** *The form  $b$  is non-degenerate if and only if for any non-zero  $x \in V$  there exists  $y \in V$  with  $b(x, y) = 1$  (equivalently:  $y \mapsto b(x, y)$  is non-trivial).*

*Proof.* Let  $e_1 = x$  be the first vector of the basis  $E = \{e_1, \dots, e_n\}$  and let  $B_E$  be the Gram matrix of  $b$ . Suppose  $b(x, V) = 0$ , then  $(1, 0, \dots, 0) B_E (y_1, \dots, y_n)^T = 0$  for all  $(y_1, \dots, y_n) \in k^n$  and so  $(1, 0, \dots, 0) B_E = 0$ , which means that  $B_E$  is not invertible,

contrary to the assumption. Hence, there exists  $z \in V$  with  $b(x, z) = a \neq 0$  and we can take  $y = a^{-1}z$ .

Conversely, let  $E = \{e_1, \dots, e_n\}$  be a basis of  $V$  and suppose  $\det B_E = 0$ . Then there exists a non-zero vector  $(x_1, \dots, x_n) \in k^n$  with  $(x_1, \dots, x_n)B_E = 0$ , so that  $(x_1, \dots, x_n)B_E(y_1, \dots, y_n)^T = 0$  for all  $(y_1, \dots, y_n) \in k^n$ . This translates into  $b(x, y) = 0$  for all  $y \in V$ , where  $0 \neq x = x_1e_1 + \dots + x_n e_n$ , contradicting the assumption.  $\square$

Related to the usual direct sums in vector space theory (which we assume known), in the setting of symmetric bilinear forms a central role is played by orthogonality: we say that two sets  $S, T \subset V$  are (mutually) orthogonal if  $b(s, t) = 0$  for all  $s \in S, t \in T$ . If, moreover,  $S$  is a subspace and  $T = \{x \in V \mid b(x, S) = 0\}$ , we write  $T = S^\perp$  and call  $T$  the **orthogonal complement** of  $S$ . It is a linear subspace of  $V$ . The subspace  $V^\perp$  is called the **radical** of  $b$ . We state an important (well-known) splitting principle.

**Lemma 1.1.3.** *Let  $S$  be a subspace of  $V$  and let  $b$  be a symmetric bilinear form on  $V$ .*

1.  *$b$  is non-degenerate if and only if the radical of  $b$  is  $\{0\}$ . In the case  $b$  is non-degenerate,  $\dim S^\perp + \dim S = \dim V$ . Moreover,  $(S^\perp)^\perp = S$ .*
2. *If  $b$  and  $b|_S$  are non-degenerate, then  $S \oplus S^\perp = V$  and  $b|_{S^\perp}$  is non-degenerate. Conversely, if  $b$  is non-degenerate and  $V = S \oplus S^\perp$ , then  $b$  restricts non-degenerately to  $S$  and  $S^\perp$ .*

*Proof.* 1. If  $x \in V^\perp$ , then  $b(x, y) = 0$  for all  $y \in V$ , and conversely. In other words,  $x \in V^\perp$  if and only if the coordinate vector of  $x$  belongs to the kernel of the Gram matrix  $B_E$ , where  $E$  is a basis. So the radical of  $b$  is  $0$  precisely if  $B_E$  is invertible, that is,  $\text{disc}(b) \neq 0$ . If  $b$  is non-degenerate and  $\{e_1, \dots, e_n\}$  is a basis of  $V$  extending a basis  $\{e_1, \dots, e_s\}$  of  $S$ , then from the chain  $V \supset e_1^\perp \supset e_1^\perp \cap e_2^\perp \supset \dots \supset e_1^\perp \cap \dots \cap e_n^\perp = V^\perp = \{0\}$  we infer that  $\dim S^\perp = \dim(e_1^\perp \cap \dots \cap e_s^\perp) = n - s = \dim V - \dim S$ .

To show that  $(S^\perp)^\perp = S$ , observe that clearly  $S \subset (S^\perp)^\perp$  and that  $S$  and  $(S^\perp)^\perp$  have the same dimension by the formula just derived.

2. The intersection  $S \cap S^\perp$  equals the radical of  $(S, b|_S)$ , and so is trivial by the previous part of the lemma. By the dimension formula and part 1 we obtain  $\dim(S + S^\perp) = \dim S + \dim S^\perp = \dim V$  so that  $V = S + S^\perp$ . Using a basis of  $V$  consisting of a basis of  $S$  and one of  $S^\perp$  the non-zero determinant of the resulting Gram matrix is the product of the corresponding Gram matrices for  $b|_S$  and  $b|_{S^\perp}$ . Hence the latter is non-zero so that  $b|_{S^\perp}$  is non-degenerate. The same argument can be used for the last statement.  $\square$

An orthogonal direct sum decomposition  $V = S \oplus T$  as in the above lemma will be denoted

$$V = S \oplus T.$$

**Proposition 1.1.4.** *Let  $k$  have characteristic different from 2. Then every inner product space  $(V, b)$  of positive dimension has a basis in which the Gram matrix is diagonal.*

*Proof.* We claim that there exists a vector  $u$  with  $b(u, u) \neq 0$ . Indeed, if not, the quadratic form  $x \mapsto b(x, x)$  would be zero and hence so would be its polar form  $2b$ . Using the assumption on the characteristic we deduce that  $b = 0$ , contrary to our assumption.

Consequently, by Lemma 1.1.3 one has an orthogonal direct sum decomposition  $V = ku \oplus u^\perp$  with  $b|_{u^\perp}$  non-degenerate. We conclude by induction on the dimension.  $\square$

*Remark 1.1.5.* The technique used in the proof of the preceding proposition shows that every quadratic form in characteristic different from 2 is diagonalizable; if there is a non-zero radical, say of dimension  $n$ , all diagonalized forms have precisely  $n$  zeros on the diagonal. If  $k$  is a field of characteristic 2, this is no longer true. Consider for example the so-called **hyperbolic plane** over  $k$ ,  $U = k \cdot e \oplus k \cdot f$  with bilinear form given by  $b(e, e) = b(f, f) = 0$ ,  $b(e, f) = 1$ . Since  $b(x, x) = 0$  for all  $x \in U$ , this form is not diagonalizable.

Finally a word about the comparison of forms. A metric linear map between two  $k$ -vector spaces  $V, V'$  equipped with symmetric bilinear forms, say  $(V, b)$  and  $(V', b')$ , is a linear map  $f$  for which  $b'(f(x), f(y)) = b(x, y)$  for all  $x, y \in V$ . If  $b$  is non-degenerate,  $f$  is injective. If, moreover,  $f$  is bijective, then  $b'$  is also non-degenerate and  $f$  is called an **isometry**. Two inner product spaces are said to be **isometric** if there exists an isometry between them.

## 1.2 First Acquaintance with Integral Lattices

By an **integral (symmetric) lattice** we mean a pair  $(L, b)$  consisting of a free  $\mathbb{Z}$ -module  $L$  of finite rank and a symmetric bilinear form  $b$  on  $L$  with integral values. Since a free  $\mathbb{Z}$ -module  $L$  of rank  $n$  admits a basis  $\mathbf{E} = \{e_1, \dots, e_n\}$ , an integer valued form  $b$  on  $L$  is completely determined by its Gram matrix  $\mathbf{B_E} = (b(e_i, e_j)) \in \mathbb{Z}^{n \times n}$  as in the case of vector spaces equipped with a symmetric bilinear form. If we change to the basis  $\mathbf{F}$  of  $L$ , by (1.2) we have  $\mathbf{B_F} = \mathbf{C^T B_E C}$ , where  $\mathbf{C}$  is the transition matrix. Since  $\mathbf{C}$  is invertible and integral, we have  $\det \mathbf{C} = \pm 1$  and hence  $\det \mathbf{B_E} = \det \mathbf{B_F}$ . We conclude that the discriminant of  $b$  is a well-defined integer.

*Remark 1.2.1.* 1. If  $(L, b)$  is an integral lattice of rank two, the form  $b$  is also called a **binary form**.

2. If instead of being  $\mathbb{Z}$ -valued,  $b$  has values in  $\mathbb{Q}$ , the above argument shows that the determinant of a Gram matrix for  $b$  is still independent of the choice of a basis for  $L$ . This rational number will also be called “discriminant” of  $b$  and denoted as  $\text{disc}(b) \in \mathbb{Q}$ . For the sake of simplicity we prefer to work with  $\mathbb{Z}$ -valued forms. This restriction occasionally necessitates however to adapt an argument slightly.



As for forms on vector spaces, a lattice  $(L, b)$  (or its form  $b$ ) is called **non-degenerate** if  $\text{disc}(b) \neq 0$ . If  $\text{disc}(b) = \pm 1$  it is called **unimodular**. These notions can be defined intrinsically as in Lemma 1.6.1.

There are two basic types of symmetric forms, the **even** forms  $b$  characterized by  $b(x, x)$  being even for all  $x \in L$ , and the remaining ones which are called **odd** forms. The **parity of a lattice** is the property of being even or odd.

Submodules  $S$  of  $L$  give new lattices by restricting the symmetric form to  $S$ . We call such a submodule a **sublattice** of  $L$ . If  $S$  has the same rank as  $L$ , the **index**  $e = [L : S] = |L/S|$  is finite (and conversely). Hence, if  $x \in L$ , then  $e \cdot x \in S$ . For such sublattices there is an important observation:

**Lemma 1.2.2.** *If  $L$  is a non-degenerate lattice and  $L' \subset L$  a sublattice of finite index, then*

$$\text{disc}(L') = [L : L']^2 \cdot \text{disc}(L).$$

*Proof.* Using the theory of elementary divisors (cf. Lemma A.1.1) there is a basis  $\mathbf{E} = \{e_1, \dots, e_n\}$  for the  $\mathbb{Z}$ -module  $L$  such that for some positive integers  $d_1, \dots, d_n$  the set  $\mathbf{E}' = \{d_1 e_1, \dots, d_n e_n\}$  is a basis for  $L'$ . Then

$$\begin{aligned} \text{disc}(L') &= \det(B_{\mathbf{E}'}) \\ &= (d_1 \cdots d_n)^2 \det(B_{\mathbf{E}}) \\ &= [L : L']^2 \text{disc}(L). \quad \square \end{aligned}$$

*Remark 1.2.3.* One can also use matrices to describe sublattices. For instance, if  $\{e_1, \dots, e_n\}$  is a basis of  $L$ , then a sublattice  $L'$  of finite index can be described as the span of  $v_1, \dots, v_n$ , where  $v_i = \sum_{j=1}^n a_{ij} e_j$ ,  $i = 1, \dots, n$ , and where the matrix  $A = (a_{ij})$  has integer entries and non-zero determinant. Using the basis  $\mathbf{E}'$  as in the proof of the lemma, one derives that  $[L : L'] = |\det(A)|$ .

A proper sublattice  $L' \subsetneq L$  of maximal rank is never primitive in the following sense.

**Definition 1.2.4.** A submodule or sublattice  $S$  of  $L$  is called **primitive**<sup>1</sup> if one of the following equivalent assertions is true.

1. For  $x \in L$ , if the non-zero integral multiple  $nx$  belongs to  $S$ , then  $x$  belongs to  $S$ ;
2.  $L/S$  is free of torsion;
3. Any basis for  $S$  can be extended to a basis for  $L$ ;
4. For some submodule  $S'$  of  $L$  one has  $L = S \oplus S'$ .

A non-zero vector  $x \in L$  is called primitive, if the sublattice  $\mathbb{Z}x$  it generates is primitive, that is, if  $x = n \cdot y$  for some  $y \in L$ , then  $n = \pm 1$ .

<sup>1</sup> $S$  is automatically free

Let us check the equivalence. Clearly 1 and 2 are equivalent, and so are 3 and 4. To see the equivalence of 2 and 3, first of all, if a basis  $\{e_1, \dots, e_m\}$  of  $S$  can be extended to a basis  $\{e_1, \dots, e_n\}$  of  $L$ , the span of  $\{e_{m+1}, \dots, e_n\}$  is a free submodule of rank  $n-m$  isomorphic to  $L/S$  and hence  $L/S$  is free of torsion. Conversely, if  $L/S$  is a free module of rank  $n-m$  with basis  $\{f_{m+1}, \dots, f_n\}$ , we may write  $f_j = e_j \bmod S$  for  $e_j \in L$ ,  $j = m+1, \dots, n$ . If  $\{e_1, \dots, e_m\}$  is a basis for  $S$ , then  $\{e_1, \dots, e_n\}$  gives a basis for  $L$ .  $\square$

If  $S \subset L$  is any free submodule, its *primitive closure*<sup>2</sup> is the smallest primitive submodule of  $L$  containing  $S$ , i.e.

$$S_{\mathbb{Q}} \cap L = \{x \in L \mid nx \in S \text{ for some } n \in \mathbb{Z}\},$$

where  $S_{\mathbb{Q}} = S \otimes_{\mathbb{Z}} \mathbb{Q}$  is the associated rational vector space. In particular, if  $S$  has the same rank as  $L$ , then its primitive closure is  $L$ .

Quadratic forms have been discussed in the context of vector spaces. In the lattice case we have a similar notion: an *integral quadratic form* is a function  $q : L \rightarrow \mathbb{Z}$  that satisfies the same two conditions as we had for vector spaces:

1.  $q(\alpha x) = \alpha^2 q(x)$  for all  $\alpha \in \mathbb{Z}$  and all  $x \in L$ ;
2. The polar form  $b_q(x, y) := q(x+y) - q(x) - q(y)$  is a symmetric bilinear form on  $L$ .

The pair  $(L, q)$  is called an *integral quadratic lattice*. Note that  $b_q(x, x) = 2q(x)$ , so that the polar form is even. Conversely, if  $(L, b)$  is an even lattice, the quadratic form  $q(x) = \frac{1}{2}b(x, x)$  is integral and  $b$  is the polar form of  $q$ . Summarizing:

**Proposition 1.2.5.** *The polar form of an integral quadratic form is even and, conversely, every even form  $b$  is the polar form of the integral quadratic form  $q(x) = \frac{1}{2}b(x, x)$ .*

*Remark 1.2.6.* If  $B = (b_{ij})$  is a real symmetric matrix of size  $n \times n$ , there is a corresponding symmetric form  $b(x, y)$  defined by  $\sum_{i,j=1}^n b_{ij}x_i y_j$ . Note that  $b(x, x) = \sum_{i,j=1}^n b_{ij}x_i x_j$  has integral values on  $\oplus^n \mathbb{Z}$  precisely if  $b_{ii} \in \mathbb{Z}$ ,  $2b_{ij} \in \mathbb{Z}$  if  $i \neq j$ .

Unfortunately,  $\det B$  then need not be integral. For instance the matrix  $\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$  having determinant  $3/4$  would then represent the quadratic form  $x^2 + xy + y^2$ . In cases where a matrix will be used to define an integral lattice, we shall therefore adhere to Kneser's convention from [122], i.e., as in formula (1.1) a quadratic form  $(x_1, \dots, x_n) \mapsto \sum_{1 \leq i \leq j \leq n} q_{ij}x_i x_j$  corresponds to the upper triangular matrix  $Q = (q_{ij})$  and conversely. Then the quadratic form is integral if and only if  $Q$  has integral entries and its polar form corresponds to  $B = Q + Q^T$ , a form with

<sup>2</sup>Other terminology sometimes found in the literature: saturation of  $S$  or saturated overlattice of  $S$ .

even integral entries on the diagonal and with  $\det B$  integral. Thus  $x^2 + xy + y^2$  corresponds to a polar form with Gram matrix  $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ .

One could also consider quadratic forms  $\sum_{i,j=1}^n q_{ij}x_ix_j$ , starting from a symmetric integral matrix  $(q_{ij})$ . J.W. Cassels [36] calls such forms *classically integral* after Gauß. However, this excludes forms like  $x^2 + xy + y^2$ .

### 1.3 Orthogonality

For lattices, the concept of orthogonality is as for vector spaces. Let  $(L, b)$  be a lattice. If  $S \subset L$  is a sublattice, its *orthogonal complement*

$$S^\perp = \{x \in L \mid b(x, S) = 0\}$$

is a sublattice. The *null-space* or *radical* of  $b$ ,

$$\text{rad}(b) = L^\perp = \{x \in L \mid b(x, y) = 0 \quad \forall y \in L\}$$

is the sublattice orthogonal to all of  $L$ . By extending scalars, i.e.,  $L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$ , various results in the vector space case carry over to the case of lattices. For instance, the null-space of  $b$  corresponds to the kernel of the Gram matrix  $B_{\mathbf{E}}$  and  $(L, b)$  is non-degenerate if and only if its null-space is 0.

Since the radical is a primitive sublattice, we can always write  $(L, b) = (L', b|_{L'}) \oplus \text{rad}(b)$  with  $b|_{L'}$  non-degenerate. This occasionally enables us to restrict to non-degenerate lattices. However, note that, even if  $b$  is non-degenerate, its restriction to a sublattice may have a non-zero radical. For instance, this happens if  $L$  contains *isotropic vectors*, that is vectors  $x \in L - \{0\}$  with  $b(x, x) = 0$ . If the restriction of  $b$  to a non-trivial subspace of  $L$  is identically zero, then this subspace is called an *isotropic subspace*. If  $b$  is even, e.g.,  $b$  is the polar form of  $q$ , it suffices that  $q(x) = 0$  for all  $x$  belonging to the subspace.

The relation between sublattices and their orthogonal complements is as follows.

**Lemma 1.3.1.** *Let  $(L, b)$  be a non-degenerate lattice.*

1. *If  $S_1 \subset S_2 \subset L$ , then  $S_1^\perp \supset S_2^\perp$ .*
2. *The orthogonal complement  $T = S^\perp$  of any sublattice  $S$  is primitive and  $T^\perp$  is the primitive closure of  $S$ . Furthermore,*
  - (a)  *$\text{rank}(S) + \text{rank}(T) = \text{rank}(L)$  and if  $b|_S$  is non-degenerate then  $S \cap T = \{0\}$ .*
  - (b) *If  $b|_S$  is non-degenerate, then  $S \oplus T$  is a sublattice of  $L$  of finite index, say  $e$ . If, moreover,  $S$  is primitive and  $0 < \text{rank}(S) < \text{rank}(L)$ , then*

there are integers  $c_S, c_T$  such that

$$\begin{aligned}\operatorname{disc}(S) &= e \cdot c_S \\ \operatorname{disc}(T) &= e \cdot c_T \\ \operatorname{disc}(L) &= c_S c_T.\end{aligned}$$

In particular,  $L$  is unimodular if and only if  $|\operatorname{disc}(S)|$  and  $|\operatorname{disc}(S^\perp)|$  are equal to  $e = [L : S \oplus S^\perp]$ .

*Proof.* 1. If  $x \in S_2^\perp$  we have  $b(x, y) = 0$  for all  $y \in S_2$  and hence a fortiori for all  $y \in S_1$ .

2. If for some non-zero integer  $n$  the vector  $nx$  is orthogonal to  $S$ , then so is  $x$ . Clearly  $S \subset T^\perp$  and since  $b$  is non-degenerate,  $\operatorname{rank}(T^\perp) = \operatorname{rank}(S)$ . Since  $T^\perp$  is primitive it must be the primitive closure of  $S$ .

- (a) The first assertion follows from the linear algebra assertion Lemma 1.1.3.1. Suppose next that  $b|_S$  is non-degenerate. If  $x \in S \cap T$ , then  $b(x, y) = 0$  for all  $y \in S$  and since  $b|_S$  is non-degenerate,  $x = 0$ .
- (b) The first assertion is a direct consequence of (a). One would like to prove the remaining assertions by directly comparing Gram matrices for suitable bases for  $S$ ,  $T$  and  $L$ , but this seems hard. Instead, following [122, Satz 14.5], we enlarge  $L$  to  $\tilde{L} := L \oplus S(-1)$  and let  $\tilde{S} = \{(x, x) \in L \oplus S(-1) \mid x \in S\}$ . Observe that the form on  $L \oplus S(-1)$  restricts to 0 on this sublattice. In this enlarged lattice  $T$  and  $\tilde{S}$  are orthogonal, just as  $S$  and  $T$ . Next, we make use of the primitivity of  $T$  inside  $L$  to choose a direct sum splitting  $L = M \oplus T$ . Since  $\tilde{S} \cap L = \{0\}$  in  $\tilde{L}$ , this gives a direct sum decomposition

$$\tilde{L} = M \oplus T \oplus \tilde{S}.$$

Let  $\mathbf{E} = \{\mathbf{E}_M, \mathbf{E}_T, \mathbf{E}_{\tilde{S}}\}$  be a basis of  $\tilde{L}$  adapted to this splitting. Our construction is such that the matrix for the symmetric form adapted to this basis is of the form

$$\mathbf{b}_{\mathbf{E}} = \begin{pmatrix} * & * & C^\top \\ * & \mathbf{b}_{\mathbf{E}_T} & 0 \\ C & 0 & 0 \end{pmatrix}.$$

Hence

$$\operatorname{disc}(\tilde{L}) = (-1)^k c_S^2 \operatorname{disc}(T), \quad c_S = \det(C), \quad k = \operatorname{rank}(M) = \operatorname{rank}(S).$$

On the other hand, since  $\tilde{L} = L \oplus S(-1)$ , we find

$$\operatorname{disc}(\tilde{L}) = (-1)^k \operatorname{disc}(L) \operatorname{disc}(S),$$

and hence  $\operatorname{disc}(L) \operatorname{disc}(S) = c_S^2 \operatorname{disc}(T)$ .

Because  $S$  is primitive, in  $L$  we have  $S = T^\perp$  and we can do the same for  $T$  resulting in  $\text{disc}(L) \cdot \text{disc}(T) = c_T^2 \text{disc}(S)$ . Multiplying the results, one gets  $\text{disc}(L) = \pm c_S \cdot c_T$ . Now use Lemma 1.2.2 to conclude that

$$c_S^2 \text{disc}(T) \text{disc}(S) = c_S^2 \text{disc}(S \oplus T) = c_S^2 e^2 \text{disc}(L).$$

Since also  $c_S^2 \text{disc}(T) \text{disc}(S) = \text{disc}(L)(\text{disc}(S))^2$ , we find  $\text{disc}(S) = \pm(e \cdot c_S)$  and – similarly –  $\text{disc}(T) = \pm(e \cdot c_T)$ . We replace  $c_S$  by  $\pm c_S$ , where the sign is the same as in the expression  $\text{disc}(S) = \pm(e \cdot c_S)$ , and similarly for  $c_T$ . Then we must have  $\text{disc}(L) = c_S c_T$ .

□

*Remark 1.3.2.* Let  $S \subset L$  be a non-degenerate sublattice of a non-degenerate lattice  $L$ . Instead of  $T = S^\perp$ , suppose  $T \subset L$  is only known to be orthogonal to  $S$ . Then  $S \cap T = \{0\}$ , since  $S$  is non-degenerate. Suppose that in addition  $S \oplus T$  has finite index in  $L$ . Then  $T = S^\perp$  if and only if  $T$  is primitive in  $L$ , and a similar assertion holds for  $T$ .

Contrary to what happens for inner product spaces, a non-degenerate sublattice does not always split off orthogonally.

**Example 1.3.3.** The hyperbolic lattice is the rank two  $\mathbb{Z}$ -module  $\mathbb{Z}^2$  equipped with the form with Gram matrix  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Take for  $S$  the lattice spanned by the non-isotropic vector  $(1, 1)$  with orthogonal complement  $\mathbb{Z} \cdot (1, -1)$ . The vectors  $(k, 0)$  and  $(0, \ell)$  for  $k$  and  $\ell$  odd do not belong to  $S \oplus S^\perp$ .

As shown by the preceding example, if  $S$  is a non-degenerate sublattice, the sum  $S \oplus S^\perp$  need not be equal to the full lattice, but is merely a sublattice of finite index. If this index is 1 then we do have a direct sum splitting  $L = S \oplus S^\perp$ , and if  $S \neq 0$  we say that  $S$  *splits off* and that  $L$  is *decomposable*. If such a sublattice does not exist,  $L$  is called *indecomposable*. For classification purposes it suffices to enumerate the indecomposable ones.

We mention one important case where we do have a splitting:

**Corollary 1.3.4.** *If  $S$  is a unimodular sublattice of a non-degenerate lattice  $L$ , then  $L = S \oplus S^\perp$ . If, moreover,  $L$  is unimodular, then  $S^\perp$  is unimodular.*

*Proof.* Since  $\text{disc}(S) = e \cdot c_S = \pm 1$  we must have  $e = 1$  which means exactly that  $L = S \oplus S^\perp$ . If  $L$  is unimodular, then  $\pm 1 = \text{disc}(L) = \text{disc}(S) \text{disc}(S^\perp)$  so that  $\text{disc}(S^\perp) = \pm 1$ . □

Apart from the discriminant there is a further basic lattice invariant which comes from considering the extension  $(L_{\mathbb{R}}, b_{\mathbb{R}})$  of  $(L, b)$  to the real numbers. As we have seen (cf. Proposition 1.1.4 and Remark 1.1.5), we can diagonalize  $b_{\mathbb{R}}$  and, adapting the orthogonal basis, a diagonal form can be written as  $x_1^2 + \dots + x_r^2 - x_{r+1}^2 - \dots - x_{r+s}^2$  with only 1 and  $-1$  as coefficients. A similar expression can also be realized in other bases. It turns out that the pair of non-negative integers  $(r, s)$

is unique; it is called the *signature* of  $b$ . This is the content of *Sylvester's law* which we prove later (see Corollary 8.1.3). For non-degenerate lattices, instead of the signature, one may equivalently give the *index*  $\tau(b) = r - s$ .

The lattice  $L$  is called positive (negative) semi-definite if  $s = 0$  (respectively,  $r = 0$ ) and positive (negative) definite if moreover  $r + s = n$ . Otherwise we speak of an *indefinite lattice*. Note that a positive (negative) definite lattice is automatically non-degenerate.

**Outlook.** For definite lattices the way a lattice splits into indecomposable ones, is unique. See Theorem 1.12.3. For indefinite ones, this is in general not the case. See for example Lemma 4.1.5 where we deal with the so-called Enriques lattice.

## 1.4 Examples of Integral Lattices

The most basic examples of such lattice are rank one lattice. These are of the form

$$\langle a \rangle = \text{lattice } \mathbb{Z} \text{ with symmetric form } (x, y) \mapsto axy.$$

Note that, according to this convention, for any even integer  $a$  the polar form of the integral quadratic form on  $\mathbb{Z}$  given by  $x \mapsto \frac{1}{2}ax^2$  is the symmetric form  $\langle a \rangle$ . We usually denote this quadratic form also by  $\langle a \rangle$ , but by  $[\frac{1}{2}a]$  in case confusion might be possible.<sup>3</sup>

If  $L$  is a lattice with form  $b$  and  $m \in \mathbb{Z}$ , we put

$$L(m) = L \text{ with form } (x, y) \mapsto m \cdot b(x, y).$$

In the examples we often use a dot to denote symmetric bilinear forms and so, instead of  $b(v, w)$ , we write  $v \cdot w$ .

1. The **hyperbolic plane**  $U$ . We have encountered this lattice before in Example 1.3.3. It is the lattice  $U = \mathbb{Z}e \oplus \mathbb{Z}f$  for which  $e \cdot f = 1$  and  $e \cdot e = f \cdot f = 0$ . We have  $\text{disc}(U) = -1$ . The polar form of the quadratic lattice endowed with the quadratic form

$$x_1e + x_2f \mapsto x_1x_2$$

is the form  $U$ . The hyperbolic plane is an even lattice.

2. **Lattices associated to graphs.** Given an undirected graph  $\Gamma$  without loops and no multiple edges, one defines a symmetric bilinear form  $b_\Gamma$  on the

<sup>3</sup>Many sources, such as [156], use a different convention, e.g. the quadratic form  $ax^2$  and the bilinear form  $axy$  are both denoted by  $\langle a \rangle$ .

free abelian group on the set of vertices  $V$  by setting for  $v, w \in V$

$$b_\Gamma(v, w) = \begin{cases} -2 & \text{if } v = w \\ 1 & \text{if } v \text{ and } w \text{ are connected by an edge} \\ 0 & \text{otherwise.} \end{cases}$$

The lattice is denoted  $L_\Gamma$ , an example of a so-called **root lattice**, by definition a lattice having a basis consisting of roots. In the present setting a root, or  $(-2)$ -root is just a vector  $e$  with  $b_\Gamma(e, e) = -2$  (see Section 1.5 below for more on roots). In particular, such lattices are always even. The graph  $\Gamma$  is the **Dynkin diagram** of the lattice  $L_\Gamma$ . For classification purposes the Dynkin diagram  $E_8$  below plays a central role: The associated lattice  $E_8(-1)$

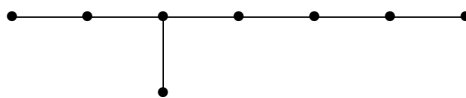


Figure 1.4.1: The Dynkin diagram  $E_8$

is even and negative definite. We have  $\text{disc}(E_8(-1)) = 1$ . See the detailed calculations in Section 4.1. Of course, for  $E_8$ , we take the same underlying module, but reverse the sign in the bilinear form.

3. **The lattices  $\Gamma_n$ .** These are the positive definite lattices of rank  $n$  divisible by 4 constructed as follows. Start from the standard lattice  $E^{(1)} = \mathbb{Z}^n$  in the vector space  $\mathbb{Q}^n$  equipped with the dot-product, that is, the standard euclidean product. Let  $E^{(0)} \subset E^{(1)}$  be the sublattice consisting of vectors  $x \in E^{(1)}$  with  $x \cdot x$  even. This is equivalent to demanding that  $\sum x_j$  be even. Clearly, the index of  $E^{(0)}$  in  $E^{(1)}$  is 2 and so by Lemma 1.2.2,  $\text{disc}(E^{(0)}) = 4$ . Now take

$$\Gamma_n = \mathbb{Z} \underbrace{\left(\frac{1}{2}, \dots, \frac{1}{2}\right)}_e + E^{(0)} \subset \mathbb{Q}^n \text{ so that } \begin{array}{c} E^{(1)} \\ \swarrow \searrow \\ E^{(0)} \\ \swarrow \searrow \\ \Gamma_n \end{array}$$

Some explanation is in order. Note that  $e \cdot e = \frac{1}{4}n$  is integral since  $n$  is divisible by 4 and it is even if and only if  $n$  is divisible by 8. Secondly,  $2e = (1, \dots, 1) \in E^{(0)}$  since  $n$  is even and so  $E^{(0)}$  has also index 2 in  $\Gamma_n$ . Hence, since  $\text{disc}(E^{(0)}) = 4$ , again by Lemma 1.2.2, also  $\Gamma_n$  is unimodular.

Summarizing: for all  $n$  divisible by 4, the lattice  $\Gamma_n$  is unimodular. If  $n$  is divisible by 8, it is even and unimodular.

## 1.5 Isometry and Equivalence

Homomorphisms between integral lattices are module homomorphisms that respect the bilinear forms. Such homomorphisms need not be injective. To see this, if  $\varphi : (L, b) \rightarrow (L', b')$  preserves the forms and  $\varphi(x) = 0$ , then  $b(x, y) = b'(\varphi(x), \varphi(y)) = 0$  for all  $y \in L$  and so  $x \in \ker(b)$ . If on the contrary  $b$  is non-degenerate,  $\varphi$  is always injective and then we have an *isometric embedding*. As for inner product spaces, two lattices  $(L, b)$  and  $(L', b')$  are said to be *isometric*, written as  $L \simeq L'$  or  $b \simeq b'$ , if there is an *isometry*  $f : L \rightarrow L'$ , that is, an isomorphism of free  $\mathbb{Z}$ -modules such that  $b'(f(x), f(y)) = b(x, y)$  for all  $x, y \in L$ . The forms  $b$  and  $b'$  are then said to be isometric or *integrally equivalent*.

In the special case  $(L, b) = (L', b')$  and  $f$  has an inverse, linear algebra tells us that  $\det(f) = \pm 1$ . Then  $f$  is called a *rotation*, respectively a *reflection*, if  $\det(f) = 1$ , respectively  $-1$ .

Let  $f : L \rightarrow L'$  be an isomorphism,  $\mathbf{E}$  a basis for  $L$ ,  $\mathbf{E}'$  a basis for  $L'$ . If  $F$  is the matrix of the isomorphism  $f : L \rightarrow L'$  with respect to  $\mathbf{E}$  and  $\mathbf{E}'$ , then

$$f \text{ is an isometry} \iff F^\top B_{\mathbf{E}'} F = B_{\mathbf{E}},$$

where  $B_{\mathbf{E}}, B_{\mathbf{E}'}$  is the Gram matrix of  $b$  with respect to a basis  $\mathbf{E}$  of  $L$ , respectively of  $b'$  with respect to  $\mathbf{E}'$  of  $L'$

Similarly, if  $L$  is a non-degenerate lattice, taking a basis  $\mathbf{F}$  of a sublattice  $S$  (with Gram matrix  $B_{\mathbf{F}}$ ), we have:

$$f : S \hookrightarrow L \text{ is an isometric embedding} \iff F^\top B_{\mathbf{E}'} F = B_{\mathbf{F}}. \quad (1.3)$$

**Examples 1.5.1. 1.** The lattice  $\Gamma_8$  is isometric to  $E_8$ . To see this, one takes as a basis for  $\Gamma_8$  the roots

$$\begin{aligned} \alpha_0 &= (1, 1, 0, 0, 0, 0, 0, 0), \\ \alpha_1 &= \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right), \\ \alpha_2 &= (-1, 1, 0, 0, 0, 0, 0, 0), \\ \alpha_3 &= (0, -1, 1, 0, 0, 0, 0, 0), \\ \alpha_4 &= (0, 0, -1, 1, 0, 0, 0, 0), \\ \alpha_5 &= (0, 0, 0, -1, 1, 0, 0, 0), \\ \alpha_6 &= (0, 0, 0, 0, -1, 1, 0, 0), \\ \alpha_7 &= (0, 0, 0, 0, 0, -1, 1, 0) \end{aligned}$$

and checks that these give the Dynkin diagram  $E_8$  (see Fig. 1.4.1) discussed earlier.

**2.** The two unimodular positive definite lattices  $E_8 \oplus E_8$  and  $\Gamma_{16}$  of rank 16 are not isometric. Indeed,  $E_8 \oplus E_8$  is a root lattice, but this is not the case for  $\Gamma_{16}$ . To see this, observe that the function  $\sum_{i=1}^{16} (x_i + \frac{1}{2})^2 = 2$  has no solution since the minimum of the left-hand side is 4, hence the only roots are  $\pm e_j \pm e_k$ ,  $j \neq k$ , where  $\{e_1, \dots, e_{16}\}$  is the standard basis of  $\mathbb{Q}^{16}$ . However, the vector  $e = (\frac{1}{2}, \dots, \frac{1}{2})$  is not in the sublattice generated by these roots. A similar statement is true for all lattices  $\Gamma_{8m}$  with  $m \geq 2$ : for  $m \geq 2$  the lattice  $\Gamma_{8m}$  is not a root lattice.

One of the purposes of lattice theory is to classify lattices up to isometry. To this end we need isometry invariants. Here are the most obvious ones:



**Lemma 1.5.2.** *For non-degenerate lattices the discriminant, index and parity are isometry invariants.*

*Proof.* The discriminant has been defined using a basis of the underlying  $\mathbb{Z}$ -module. An isometry sends a basis of the source lattice to a basis of the target, and so preserves the discriminant. Two isometric lattices remain isometric under ring-extension and so are isometric over  $\mathbb{R}$  and thus have the same index. As to parity: this can be tested on a basis and as we have remarked, an isometry sends a basis to a basis of the target lattice.  $\square$

**Corollary 1.5.3.** *Let  $a, a' \in \mathbb{Z}$ . The lattices  $\langle a \rangle$  and  $\langle a' \rangle$  are isometric if and only if  $a = a'$ .*

Automorphisms of a lattice  $L$  preserving the bilinear form  $b$  form the **isometry group** of  $(L, b)$ , denoted

$$\mathbf{O}(b) \text{ (or } \mathbf{O}(L)) = \{\varphi \in \text{Aut}_{\mathbb{Z}}(L, L) \mid b(\varphi(x), \varphi(y)) = b(x, y) \forall x, y \in L\}.$$

Isometric lattices have isomorphic isometry groups. More precisely, if  $f : L \rightarrow L'$  is an isometry, and  $\varphi \in \mathbf{O}(L)$  an auto-isometry of  $L$ , then  $f \circ \varphi \circ f^{-1}$  is an auto-isometry of  $L'$  and the homomorphism which sends  $\varphi \in \mathbf{O}(L)$  to  $f \circ \varphi \circ f^{-1} \in \mathbf{O}(L')$  is an isomorphism.

Since we can multiply the equation  $b(\varphi(x), \varphi(y)) = b(x, y)$  by a non-zero integer, we have:

**Lemma 1.5.4.** *If  $L$  is an integral lattice, then for all  $k \in \mathbb{Z}$ ,  $k \neq 0$ , the lattice  $L(k)$  has the same automorphism group as  $L$ .*

*Remark 1.5.5.* If  $b$  is an even integral form, then  $b$  is the polar form of an integral quadratic form  $q$ . A lattice automorphism preserving  $q$  of course preserves  $b$ , but the converse is also true: an isometry (an automorphism preserving  $b$ ) also preserves  $q$  since  $q(x) = \frac{1}{2}b(x, x)$ . So we can and shall use the notation  $\mathbf{O}(b)$  and  $\mathbf{O}(q)$  interchangeably.

A lattice always has the isometries  $\text{id}_L$  and  $-\text{id}_L$ . If  $L$  has even rank,  $-\text{id}_L$  is a rotation and otherwise it is a reflection. Recall that euclidean vector spaces admit **hyperplane reflections** which are examples of reflections since they have determinant  $-1$  as one verifies by choosing a suitable basis. Not all lattices admit such hyperplane reflections. To see this, it is convenient to view a lattice  $L$  as sitting in  $L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$ . A hyperplane reflection exists if the vector  $x$  normal to the hyperplane does not belong to it, i.e.,  $x$  is non-isotropic. For vector spaces there is a well-known formula for the reflection defined by  $x$ :

$$L_{\mathbb{Q}} \xrightarrow{\sigma_x} L_{\mathbb{Q}}, \quad y \mapsto y - \frac{2b(x, y)}{b(x, x)}x. \quad (1.4)$$

Observe that the image of  $L_{\mathbb{Q}}$  under  $\sigma_x - \text{id}$  is the line  $\mathbb{Q} \cdot x$  and if  $\sigma_x L = L$ , the image of  $L$  is a lattice in this line. Because  $\sigma_x = \sigma_{a \cdot x}$  for all  $a \in \mathbb{Q}^{\times}$  we may thus

scale  $x$  so that  $x \in L$ . We also may assume that  $x$  is primitive. The formula then tells us that  $\sigma_x$  preserves  $L \subset L_{\mathbb{Q}}$  if and only if

$$2b(x, y) \in b(x, x) \cdot \mathbb{Z} \text{ for all } y \in L. \quad (1.5)$$

A primitive  $x \in L$  with  $b(x, x) = k \neq 0$  satisfying this condition is called a ***k-root***. For example, if  $k = \pm 1$  or  $k = \pm 2$  the condition (1.5) is automatically true. Let us set this apart.

**Lemma 1.5.6.** *Let  $(L, b)$  be a lattice. The reflection in a hyperplane orthogonal to a vector  $x \in L$  with  $b(x, x) = \pm 1$  or with  $b(x, x) = \pm 2$  preserves the lattice. All such vectors  $x$  are roots.*

An isometry  $\varphi$  of  $L$  preserves  $k$ -roots and since

$$\sigma_{\varphi(x)} = \varphi \sigma_x \varphi^{-1},$$

the group generated by reflections in  $k$ -roots (for fixed  $k$ ) is a normal subgroup of the isometry group of  $L$ . In an even lattice we mostly consider those roots for which  $q(x) = \frac{1}{2}b(x, x) = \pm 1$  and often refer to these simply as ***roots***,  ***$\pm 2$ -roots***, or also ***roots of type  $\epsilon \in \{+, -\}$*** . The corresponding group of reflections is denoted

$$W^{\epsilon}(L) := \{\text{group generated by } \sigma_x \mid x \in L, q(x) = \epsilon\}$$

and will be referred to as the ***Weyl group*** of  $L$ . This is somewhat ambiguous, but the context makes clear whether  $\epsilon = 1$  or  $-1$ . If the lattice is definite, there is of course no confusion about signs. A lattice spanned by its  $k$ -roots (for all possible  $k$ ) is called a ***root lattice***. Examples of root lattices can be found in Sections 4.1 and 4.2.

**Outlook.** From linear algebra we know that the orthogonal group of a real inner product space is generated by reflections, and the Cartan–Dieudonné theorem, which we prove in Section 7.2, implies that this is also true for the orthogonal group  $O(b_{\mathbb{Q}})$  where  $b$  is possibly indefinite. Indeed, this holds over any field of characteristic distinct from 2.

The theorems of Witt treated in Section 7.2 focus on the role of the isotropic vectors in vector spaces such as  $L_{\mathbb{Q}}$ . In our situation these theorems state that there is an orthogonal decomposition

$$L_{\mathbb{Q}} = \widehat{U} \oplus S, \text{ (Witt decomposition),}$$

where  $\widehat{U}$  is an even-dimensional space which contains the isotropic vectors while  $S$  contains none. This decomposition is unique up to isometry. In particular, half the dimension of  $\widehat{U}$  is an invariant of  $L_{\mathbb{Q}}$ , the ***Witt index***,  $W_{\tau}(L_{\mathbb{Q}})$ . This invariant can be defined for  $L_{\mathbb{R}}$  as well. Here  $W_{\tau}(L_{\mathbb{R}})$  is related to the signature  $(r, s)$ :  $W_{\tau}(L_{\mathbb{R}}) = \min(r, s)$ .

## 1.6 Discriminant Forms

If  $(L, b)$  is an integral lattice, the collection of the  $\mathbb{Z}$ -linear functions on  $L$  taking values in  $\mathbb{Z}$  constitute a  $\mathbb{Z}$ -module, the **dual of  $L$** ,

$$L^* = \text{Hom}_{\mathbb{Z}}(L, \mathbb{Z}).$$

It is a free  $\mathbb{Z}$ -module of the same rank as  $L$  and we can compare the two using the **correlation morphism**

$$b_L : L \rightarrow L^*, \quad x \mapsto b_L(x), \quad b_L(x)y = b(x, y). \quad (1.6)$$

Observe that the matrix representation of  $b_L$  with respect to a basis  $\mathbf{E} = \{e_1, \dots, e_n\}$  of  $L$  and the dual basis  $\mathbf{E}^* = \{e_1^*, \dots, e_n^*\}$  of  $L^*$  is just the Gram matrix:

$$b_L(e_i) = \sum_j b(e_i, e_j) e_j^*. \quad (1.7)$$

Consequently, one deduces:

**Lemma 1.6.1.** *For an integral lattice the correlation morphism  $b_L$  is injective if and only if  $L$  is non-degenerate, and  $b_L$  is an isomorphism if and only if  $L$  is unimodular.*

Let  $S \subset L$  be a sublattice of  $L$ . The map  $\beta_S : L \rightarrow S^*$  which assigns to  $x \in L$  the linear map on  $S$  given by  $y \mapsto b(x, y)$ ,  $y \in S$ , extends the correlation map  $b_S : S \rightarrow S^*$  on  $S$  to  $L$ . Since  $\ker \beta_S = S^\perp$ , there is an induced injective homomorphism  $\bar{\beta}_S : L/S^\perp \rightarrow S^*$ .

**Lemma 1.6.2.** *Let  $S \subset L$  be a sublattice. If  $S$  is primitive and  $L$  unimodular, the morphism  $\bar{\beta}_S : L/S^\perp \rightarrow S^*$  is an isomorphism of  $\mathbb{Z}$ -modules.*

*Proof.* Assume that  $S$  is primitive and that  $L$  is unimodular. To show that  $\bar{\beta}_S$  is an isomorphism, it suffices to show that  $\beta_S$  is surjective. Since  $L$  is unimodular, first of all  $b_L$  is onto. Secondly, since  $S$  is primitive, the restriction map  $r_S : L^* \rightarrow S^*$  is surjective. Indeed, write  $L = S \oplus S'$ , then  $f : S \rightarrow \mathbb{Z}$  extends to  $\tilde{f} : L \rightarrow \mathbb{Z}$  by setting  $\tilde{f}(s, s') = f(s)$  for  $s \in S, s' \in S'$ . Consequently  $\beta_S = r_S \circ b_L$  is surjective as well.  $\square$

*Remark.* The variant  $\beta_S$  of the correlation morphism is to be discussed in generality in Section 6.2.

Since  $b_L$  is an injection if and only if  $b$  is non-degenerate, we can and shall identify  $b_L(L)$  with its image in  $L^*$  in the case of a non-degenerate  $L$ . In that case the quotient  $L^*/L$  is a finite group, the **discriminant group**

$$\text{dg}_L := L^*/L.$$

From the theory of elementary divisors (cf. Lemma A.1.1) it follows that the free  $\mathbb{Z}$ -module  $L^*$  has a basis  $\{\varepsilon_1^*, \dots, \varepsilon_n^*\}$  such that for some positive integers  $d_1, \dots, d_n$ ,

the vectors  $d_1\epsilon_1^*, \dots, d_n\epsilon_n^*$  form a basis for  $L$ . In these bases, the matrix of the correlation morphism is diagonal with the  $d_j$  on the diagonal and so has determinant equal to  $d_1 \cdots d_n$ . Up to sign this equals  $\text{disc}(b)$ . As  $L$  is non-degenerate,  $d_1 \cdots d_n$  is the index of  $L$  in  $L^*$ , and so

$$|\text{dg}_L| = [L^* : L] = |\text{disc}(L)|. \quad (1.8)$$

We make a few elementary observations concerning the discriminant group. In our setting  $\text{dg}_L = L^*/L \simeq \bigoplus_{j=1}^n \mathbb{Z}/d_j\mathbb{Z}$  where we may discard those  $d_j$  for which  $d_j = 1$ . Since  $\ell(\text{dg}_L)$ , the minimal number of generators of  $\text{dg}_L$ , is the number of non-trivial elementary divisors (see e.g. A.1.3), one has

$$\ell(\text{dg}_L) \leq \text{rank}(L). \quad (1.9)$$

If  $b$  is non-degenerate, the injective correlation map  $b_L : L \rightarrow L^*$  extends to  $L_{\mathbb{Q}}$  and then gives a  $\mathbb{Q}$ -linear isomorphism. Via this isomorphism the  $\mathbb{Q}$ -bilinear extension  $b_{\mathbb{Q}}$  of  $b$  can be transported to give a non-degenerate  $\mathbb{Q}$ -bilinear form  $b_{\mathbb{Q}}$  on  $L_{\mathbb{Q}}$ . For the form  $b_{\mathbb{Q}}$  on  $L_{\mathbb{Q}}$  we also have a correlation map, say  $b_{L_{\mathbb{Q}}}^* : L_{\mathbb{Q}}^* \rightarrow (L_{\mathbb{Q}}^*)^*$ . Recall that there is a natural identification

$$\lambda : L_{\mathbb{Q}} \xrightarrow{\simeq} (L_{\mathbb{Q}}^*)^* \quad (1.10)$$

which associates to  $x \in L_{\mathbb{Q}}$  the function  $\lambda_x$  on  $L_{\mathbb{Q}}^*$  given by  $f \mapsto f(x)$ . The correlation maps turn out to be compatible with the isomorphism  $\lambda$  and preserve the lattice structure as well, as we show now together with some other basic facts.

**Lemma 1.6.3.** *Let  $L$  be a non-degenerate integral lattice.*

1. *If one identifies  $L_{\mathbb{Q}}$  with  $L_{\mathbb{Q}}^*$  using the correlation map, then  $L^*$  is the free  $\mathbb{Z}$ -module inside  $L_{\mathbb{Q}}$  consisting of those  $y \in L_{\mathbb{Q}}$  for which  $b_{\mathbb{Q}}(y, L) \subset \mathbb{Z}$ .*
2. *If  $A = b_{\mathbf{E}}$  is the Gram matrix of  $b$  with respect to the basis  $\mathbf{E}$ , then  $A^{-1}$  is the Gram matrix of  $b_{\mathbb{Q}}$  with respect to the dual basis  $\mathbf{E}^*$ .*
3. *Under the identification of  $L_{\mathbb{Q}} = L_{\mathbb{Q}}^*$  given by the correlation map,  $A$ , respectively  $A^{-1}$ , is also the matrix expressing the  $\mathbb{Q}$ -basis  $\mathbf{E}$  in  $\mathbf{E}^*$ , or the other way around.*
4.  *$b_{L_{\mathbb{Q}}}^* \circ b_{L_{\mathbb{Q}}} = \lambda$ . Under this map  $L$  and  $(L^*)^*$  become identified.*

*Proof.* 1. Since the correlation map induces an isomorphism  $L_{\mathbb{Q}} \xrightarrow{\simeq} L_{\mathbb{Q}}^*$ , every  $\mu \in L_{\mathbb{Q}}^*$  is of the form  $\mu = b_L(x)$  for some  $x \in L_{\mathbb{Q}}$ . Then the functional  $\mu = b_L(x)$  belongs to  $L^*$  if and only if

$$\mu(L) \subset \mathbb{Z} \iff b_{\mathbb{Q}}(x, L) \subset \mathbb{Z}.$$

2. We have seen (cf. (1.7)) that the matrix of the correlation map with respect to  $\mathbf{E}$  and  $\mathbf{E}^*$  is the Gram matrix  $A$ . Let  $C$  be the Gram matrix of  $b_{\mathbb{Q}}$  with respect to  $\mathbf{E}^*$ . By definition

$$b_{\mathbb{Q}}(b_L x, b_L y) = b(x, y) \quad (1.11)$$

which translates as  $A^T C A = A$  and hence  $C = A^{-1}$ .

3. The correlation map being given by the matrix  $A$  with respect to the bases  $\mathbf{E}, \mathbf{E}^*$ , this means exactly that the column vectors of  $A$  express the basis vectors of  $\mathbf{E}$  in the basis  $\mathbf{E}^*$ .

4. Since

$$\begin{aligned} \lambda_x(b_{L_{\mathbb{Q}}}(y)) &= b_{L_{\mathbb{Q}}}(y) \text{ evaluated in } x \\ &= b_{\mathbb{Q}}(y, x) = b_{\mathbb{Q}}(x, y) \\ &= b_{\mathbb{Q}}(b_{L_{\mathbb{Q}}}(x), b_{L_{\mathbb{Q}}}(y)) \text{ by (1.11)} \\ &= b_{L_{\mathbb{Q}}^*}(b_{L_{\mathbb{Q}}}(x)) \text{ evaluated in } b_{L_{\mathbb{Q}}}(y), \end{aligned}$$

we see that under the composition of the correlation maps,  $x \in L_{\mathbb{Q}}$  corresponds to  $\lambda_x$  and hence  $b_{L_{\mathbb{Q}}^*} \circ b_{L_{\mathbb{Q}}} = \lambda$ . If  $x \in L$ ,  $\lambda_x$  is integral on  $L^*$  and so  $\lambda(L) = (L^*)^*$ .  $\square$

We now come to an important construction, that of a torsion form on the discriminant group. First we discuss the bilinear version.

**Definition 1.6.4.** Let  $(L, b)$  be a non-degenerate integral lattice. The *discriminant bilinear form* is the  $\mathbb{Q}/\mathbb{Z}$ -valued bilinear form on the discriminant group of  $L$  given by

$$b_L^{\#} : \text{dg}_L \times \text{dg}_L \rightarrow \mathbb{Q}/\mathbb{Z}, \quad (\bar{x}, \bar{y}) \mapsto b_{\mathbb{Q}}(x, y) \bmod \mathbb{Z}. \quad (1.12)$$

Since  $b_{\mathbb{Q}}(x+u, y+v) \equiv b_{\mathbb{Q}}(x, y) \bmod \mathbb{Z}$  for  $x, y \in L^*$ ,  $u, v \in L$ ,  $b_L^{\#}$  is well defined. The form is non-degenerate in the sense that  $b_L^{\#}(\bar{x}, \text{dg}_L) = 0$  precisely if  $\bar{x} = 0$ . To see this, note that  $b_L^{\#}(\bar{x}, \text{dg}_L) = 0$  translates as  $b(x+L, L^*) \in \mathbb{Z}$  implying  $x+L = L$ , i.e.,  $\bar{x} = 0$ .

Secondly, we introduce a version for integral quadratic forms:

**Definition 1.6.5.** Let  $q$  be a non-degenerate quadratic form with polar form  $b$ . Extending  $q$  in a  $\mathbb{Q}$ -quadratic fashion to  $L_{\mathbb{Q}}$ , we have the *discriminant quadratic form*:

$$q_L^{\#} : \text{dg}_L \rightarrow \mathbb{Q}/\mathbb{Z}, \quad \bar{x} \mapsto q_{\mathbb{Q}}(x) \bmod \mathbb{Z}. \quad (1.13)$$

Since

$$\begin{aligned} q_{\mathbb{Q}}(x+u) &= q_{\mathbb{Q}}(x) + q_{\mathbb{Q}}(u) + b_{\mathbb{Q}}(x, u) \\ &\equiv q_{\mathbb{Q}}(x) \bmod \mathbb{Z} \text{ for } x \in L^* \text{ and } u \in L, \end{aligned}$$

this is well defined. Even forms  $b$  have a discriminant quadratic form relative to the integral quadratic form  $q(x) = \frac{1}{2}b(x, x)$ , since  $b$  then is the polar form of  $q$ .

The pair  $(\text{dg}_L, b_L^{\#})$  is an example of a *symmetric torsion group* (and  $(\text{dg}_L, q_L^{\#})$  is an example of a *quadratic torsion group*).

*Remark 1.6.6.* In the literature (e.g. in [171]) often a different convention is used, namely  $q_L^{\#}(x) = b_{\mathbb{Q}}(x, x) \bmod 2\mathbb{Z}$ , i.e., we get a  $\mathbb{Q}/2\mathbb{Z}$ -valued form instead of a  $\mathbb{Q}/\mathbb{Z}$ -valued form. This is equivalent to our approach since multiplication by 2 induces an isomorphism  $\mathbb{Q}/\mathbb{Z} \xrightarrow{\sim} \mathbb{Q}/2\mathbb{Z}$  which links the two.

**Definition 1.6.7.** A non-zero subgroup of a torsion group is called *isotropic* with respect to a symmetric bilinear form (respectively a quadratic form) if the bilinear form (quadratic form) is identically zero on the subgroup.

**Examples 1.6.8. 1.** Let us consider the rank one module  $\mathbb{Z}e$  with form given by  $b(e, e) = a$ ,  $a \neq 0$ , i.e.,  $\langle a \rangle$ . The dual module is generated by  $\varepsilon^* = a^{-1}e$  and  $b_{\mathbb{Q}}(\varepsilon^*, \varepsilon^*) = a^{-2} \cdot a = a^{-1}$ . Hence the discriminant group  $a^{-1}\mathbb{Z}e/\mathbb{Z}e \simeq \mathbb{Z}/a\mathbb{Z}$  is equipped with the bilinear form which takes the value  $a^{-1} \pmod{\mathbb{Z}}$  on the pair  $(\varepsilon^*, \varepsilon^*)$ .

For the quadratic form  $q$  associated with the rank one forms  $\langle a \rangle$  with  $a$  even, this goes as follows. With  $e$  and  $\varepsilon^*$  as before, one has  $q(e) = \frac{1}{2}a$  since  $q(e) = \frac{1}{2}b(e, e)$ , and so  $q(\varepsilon^*) = q(a^{-1}e) = a^{-2} \cdot \frac{1}{2}a = \frac{1}{2}a^{-1} = \frac{1}{2}b_{\mathbb{Q}}(\varepsilon^*, \varepsilon^*)$ . On the level of the discriminant group  $a^{-1}\mathbb{Z}e/\mathbb{Z}e$  this equality induces the equality  $q(\varepsilon^*) = \frac{1}{2}b_{\mathbb{Q}}(\varepsilon^*, \varepsilon^*)$  in the value group  $\mathbb{Q}/\mathbb{Z}$ .

**2.** If  $L$  is any non-degenerate lattice, then the dual module of  $L(k)$  equals  $k^{-1}L^*$ . Indeed, for  $x \in L_{\mathbb{Q}}$  we have

$$\begin{aligned} x \in L(k)^* &\iff k \cdot b(x, y) \in \mathbb{Z} \quad \forall y \in L \\ &\iff b(k \cdot x, y) \in \mathbb{Z} \quad \forall y \in L \\ &\iff k \cdot x \in L^*. \end{aligned}$$

Suppose that  $L$  is in addition unimodular of rank  $n$ . Then  $L = L^*$ , hence  $L(k)^* = k^{-1}L$ . Hence all elementary divisors of the discriminant group of  $L(k)$  are equal to  $k$  so that  $\text{dg}_{L(k)} = k^{-1}L/L \simeq \oplus^n \mathbb{Z}/k\mathbb{Z}$ . In this case, all entries of the Gram matrix of  $\text{dg}_{L(k)}$  are in  $k^{-1}\mathbb{Z}/\mathbb{Z}$  and so the discriminant form of  $L(k)$  is  $k^{-1}\mathbb{Z}/\mathbb{Z}$ -valued.

Let us next explain how to find the discriminant group from the Gram matrix  $A$  of  $L$  with respect to an  $L$ -basis  $\mathbf{E}$ . We just observed that the rows (and columns, by symmetry) of  $A^{-1}$  express the dual basis  $\mathbf{E}^*$  for  $L^*$  in the basis  $\mathbf{E}$  for  $L$ . Elementary row and column operations that are unimodular correspond to new bases for  $L$  and for  $L^*$  (viewed as  $\mathbb{Z}$ -modules). Hence suitable bases can be found so that  $A$  is equivalent to a diagonal form. We shall show that using elementary row and column operations carefully, the diagonal elements give the elementary divisors of  $L^*/L$ :

**Step 1:** since  $A$  is non-singular, no column is zero and by a row operation we move a non-zero entry  $A_1$  to place  $(1, 1)$ . Using integral row and column addition, replace the other entries in the first column and row by 0 or by a non-zero element with absolute value  $< |A_1|$ .

**Step 2:** repeat step 1 with such a non-zero element, and so on until all entries in the first column and row are 0 except the (new) entry  $A_{1,1}$ .

**Step 3:** if there is a non-zero entry  $A_{i,j}$ ,  $i, j \geq 2$ , that is not divisible by  $A_{1,1}$  we add the  $i$ -th row to the first and start step 1 and 2 anew. Repeating this step makes all entries  $A_{1,j}$ ,  $j \geq 2$ ,  $A_{i,1}$ ,  $i \geq 2$  zero, and makes the entries  $A_{i,j}$ ,  $i, j \geq 2$ , divisible by  $A_{1,1}$ .

**Step 4:** repeat steps 1–3 with the matrix  $(A_{i,j})$ ,  $i, j \geq 2$ .

**Example 1.6.9.** On  $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$  consider the even form  $b_A$  given by the Gram matrix  $A = \begin{pmatrix} -2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & -2 \end{pmatrix}$ . The form  $b_A$  is also the polar form of an integral quadratic form  $q_A$ . It is best to exchange rows 1 and 2 so that the first column and row can be handled quickly, yielding  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 2 \\ 0 & 1 & -2 \end{pmatrix}$ . Now we repeat the steps

for  $\begin{pmatrix} 5 & 2 \\ 1 & -2 \end{pmatrix}$  by first exchanging rows 1 and 2. Finally we arrive at  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 12 \end{pmatrix}$

so that  $\text{dg}_L \simeq \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . The third column of the inverse matrix  $A^{-1} = \frac{1}{12} \begin{pmatrix} -5 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & -5 \end{pmatrix}$  represents a vector  $e_3^* \in L^*$  which is obviously of order 12 modulo  $L$  and so must generate  $\text{dg}_L$ . Then the discriminant forms are given by  $b_{A,\mathbb{Q}}(e_3^*, e_3^*) = \frac{7}{12} \pmod{\mathbb{Z}}$  and  $q_{A,\mathbb{Q}}(e_3) = \frac{7}{24} \pmod{\mathbb{Z}}$ .

Generalizing the previous example, we consider any non-degenerate integral lattice  $(L, b)$  and let  $A = b_E$  be the Gram matrix of  $b$  with respect to a basis  $E$  for  $L$ . Since the Gram matrix of  $b_{\mathbb{Q}}$  with respect to the dual basis  $E^*$  equals  $A^{-1}$ , considering its entries in  $\mathbb{Q}/\mathbb{Z}$ , we obtain a matrix representing  $b_L^\#$ . As in that example, we may choose a basis  $\{\varepsilon_1^*, \dots, \varepsilon_n^*\}$  of  $L^*$  which is adapted to the elementary divisors  $\{d_1, \dots, d_r\}$  of the torsion group  $\text{dg}_L$ , that is,

- $\{e_1 = d_1\varepsilon_1^*, \dots, e_r = d_r\varepsilon_r^*, e_{r+1} = \varepsilon_{r+1}^*, \dots, e_n = \varepsilon_n^*\}$  is a basis of  $L$ ;
- the classes of  $\{\varepsilon_1^*, \dots, \varepsilon_r^*\}$  modulo  $L$  give a set  $\mathbf{S}$  of generators for the discriminant group  $\text{dg}_L$ .

The set  $\mathbf{S}$  is called an *ordered basis of  $\text{dg}_L$*  and we shall investigate the shape of the Gram matrix  $B_{\mathbf{S}}$  of the discriminant form on such a basis  $\mathbf{S}$ . First note that since  $b_{\mathbb{Q}}(e_i, \varepsilon_j^*) \in \mathbb{Z}$ ,  $b_{\mathbb{Q}}(\varepsilon_i^*, \varepsilon_j^*) = d_i^{-1}b_{\mathbb{Q}}(e_i, \varepsilon_j^*) \in d_i^{-1}\mathbb{Z}$  for  $i, j = 1, \dots, r$ . Secondly, all  $d_i$  divide  $d_r$  and so  $B_{\mathbf{S}}$  is  $d_r^{-1}\mathbb{Z}/\mathbb{Z}$ -valued and, by the preceding remarks, is represented by the  $\mathbb{Q}$ -valued matrix

$$B' = \begin{pmatrix} \frac{\beta_{11}}{d_1} & \frac{\beta_{12}}{d_1} & \dots & \frac{\beta_{1r}}{d_1} \\ \frac{\beta_{21}}{d_1} & \frac{\beta_{22}}{d_2} & \dots & \frac{\beta_{2r}}{d_2} \\ \vdots & \ddots & \vdots & \vdots \\ \frac{\beta_{r1}}{d_1} & \frac{\beta_{r2}}{d_2} & \dots & \frac{\beta_{rr}}{d_r} \end{pmatrix} \quad \text{for certain } \beta_{ij} = \beta_{ji} \in \mathbb{Z}. \quad (1.14)$$

In other words, the first row and column belong to  $d_1^{-1}\mathbb{Z}$ , the remaining entries in the second row and column to  $d_2^{-1}\mathbb{Z}$ , etc. The corresponding entries of  $B_{\mathbf{S}} = B' \pmod{\mathbb{Z}}$  then are well defined in  $\mathbb{Q}/\mathbb{Z}$ .

A non-degenerate even form  $b$  has Gram matrix  $A = Q + Q^T$  where  $Q$  is an integral valued upper triangular matrix and the corresponding discriminant quadratic form (with values in  $\mathbb{Q}/\mathbb{Z}$ ) is then represented by an upper triangular  $\mathbb{Q}$ -valued matrix  $Q' = (q'_{ij})$  such that  $Q' + Q'^T = B'$  as in (1.14). So modulo  $\mathbb{Z}$  the diagonal elements  $q'_{ii} = \frac{1}{2}B'_{ii} = \frac{1}{2}d_i^{-1} \cdot b_{\mathbb{Q}}(e_i, \varepsilon_i^*)$  take values in  $(2d_r)^{-1}\mathbb{Z}/\mathbb{Z}$  instead of in  $d_r^{-1}\mathbb{Z}/\mathbb{Z}$ . This generalizes what we saw in Example 1.6.8.1 for cyclic discriminant groups.

*Remark 1.6.10.* Of course, the form  $b_{\mathbb{Q}}$  on  $L_{\mathbb{Q}}^*$  does not in general assume integral values on  $L^*$ , but, as we have seen, if  $d$  is the largest elementary divisor of  $\text{dg}_L$ , then  $d \cdot b_{\mathbb{Q}}|L^*$  is integer valued. More generally, if  $\rho \in \mathbb{Z}$ ,  $\rho > 0$ , is such that  $\rho \cdot b_{\mathbb{Q}}|L^*$  assumes integral values, we can consider the lattice  $L^*(\rho)$ , that is,  $L^*$  equipped with  $\rho \cdot b_{\mathbb{Q}}$ . Example 1.6.8.2 can be generalized to this situation by expressing the elementary divisors of the discriminant group of  $L^*(\rho)$  in terms of the elementary divisors  $d_1, \dots, d_r$  of  $\text{dg}_L$ , where these satisfy the usual divisibility relations  $d_1|d_2|\dots|d_r$ . To start with, the dual module of  $L^*(\rho)$  equals  $1/\rho \cdot (L^*)^*$ . There is a basis  $\{\varepsilon_1^*, \dots, \varepsilon_n^*\}$  for  $L^*$  such that

$$E = \{\varepsilon_1 = d_1\varepsilon_1^*, \dots, \varepsilon_r = d_r\varepsilon_r^*, \varepsilon_{r+1}^*, \dots, \varepsilon_n^*\}$$

is a basis for  $L \subset L^*$ . We identify  $L$  and its double dual using the composition  $b_{L_{\mathbb{Q}}^*} \circ b_{L_{\mathbb{Q}}}$  of the correlation maps. (So  $L^*(\rho)^*/L^*(\rho)$  is isomorphic to  $\frac{1}{\rho}L/L^*(\rho)$ .) Since  $1/\rho \cdot E$  is a basis of  $(L^*(\rho))^* = 1/\rho \cdot L \subset 1/\rho \cdot L^*$ , we see that  $d_1^* = \rho/d_1, \dots, d_r^* = \rho/d_r, d_{r+1}^* = \rho, \dots, d_n^* = \rho$  yield the elementary divisors of  $\text{dg}_{L^*(\rho)}$  by leaving out terms for which  $d_j = \rho$ . The discriminant quadratic form of  $b$  takes values in  $(2d)^{-1}\mathbb{Z}/\mathbb{Z}$ , while the discriminant quadratic form for the lattice  $L^*(\rho)$  takes values in  $(2\rho)^{-1}\mathbb{Z}/\mathbb{Z}$ .

## 1.7 More Examples

Making use of the dual of a lattice, we can now discuss several important concepts that come up later. We first claim that if we have an inclusion  $M \subset N$  of non-degenerate lattices of the same rank, then  $N^* \subset M^*$  and  $[M^* : N^*] = [N : M]$ . This can be seen by taking a basis  $\{e_1, \dots, e_n\}$  for  $N$  as in the proof of Lemma 1.2.2, ensuring the existence of positive integers  $d_1, \dots, d_n$ , such that  $\{d_1e_1, \dots, d_n e_n\}$  is a basis for  $M$ . This proves the claim since then  $\{d_1^{-1}e_1^*, \dots, d_n^{-1}e_n^*\}$  is a basis for  $M^*$ .

**1.7.A Neighbouring Lattices.** Two lattices  $E^{(1)}$  and  $E^{(2)}$  are *neighbours* if they contain a common index 2 sublattice  $E^{(0)}$ , that is:

$$E^{(1)} \text{ neighbour of } E^{(2)} \iff \exists E^{(0)} \text{ with } \begin{array}{c} \xrightarrow{\text{index } 2} E^{(1)} \\ E^{(0)} \subset \\ \xrightarrow{\text{index } 2} E^{(2)}. \end{array}$$



Lemma 1.2.2 implies that neighbouring lattices have the same discriminant, but we can say more. Recall that the discriminant group is a torsion group and so has a Sylow decomposition into  $p$ -primary parts.

**Lemma 1.7.1.** *Neighbouring lattices of a non-degenerate lattice  $N$  have the same discriminant. For odd primes  $p$  the  $p$ -primary part of the discriminant group of a neighbour of  $N$  is isomorphic to the  $p$ -primary part of  $N^*/N$ . In particular, discriminant groups of neighbouring lattices with odd discriminant are all isomorphic.*

*Proof.* Let  $L$  be a lattice with  $[N : L] = 2$ . We already remarked that  $\text{disc}(L) = 4 \text{disc}(N)$  and so  $\text{disc}(L)$  only depends on  $N$ .

From the sequence of inclusions  $L \subset N \subset N^* \subset L^*$  one derives two exact sequences of torsion abelian groups

$$0 \rightarrow N/L \rightarrow L^*/L \rightarrow L^*/N \rightarrow 0, \quad 0 \rightarrow N^*/N \rightarrow L^*/N \rightarrow L^*/N^* \rightarrow 0.$$

Since  $[N : L] = 2 = [L^* : N^*]$ , both  $N/L$  in the first sequence and  $L^*/N^*$  in the second sequence are isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ . These sequences are stable under taking  $p$ -primary parts. Assume that  $p$  is an odd prime. Then the first sequence shows that the  $p$ -primary part of  $L^*/L$  is isomorphic to the  $p$ -primary part of  $L^*/N$  and the second that the  $p$ -primary part of  $L^*/N$  is isomorphic to the  $p$ -primary part of  $N^*/N$ .  $\square$

If, in the situation of the proof of the lemma, the order of  $N^*/N$  is odd, the second sequence splits. If the first sequence splits, then

$$L^*/L \simeq N^*/N \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

and so the 2-primary part of  $L^*/L$  is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . If it does not split, the 2-primary part of  $L^*/L$  is isomorphic to the non-split extension of  $\mathbb{Z}/2\mathbb{Z}$  by  $\mathbb{Z}/2\mathbb{Z}$ , i.e.,  $\simeq \mathbb{Z}/4\mathbb{Z}$ . For unimodular neighbours  $L^*/L$  is 2-primary and both cases may occur as shown by the following examples.

1. Let  $n > 0$  be an odd integer. Start with the index 2 sublattice  $E^{(0)}$  of  $\mathbb{Z}^n$  consisting of vectors such that  $x \cdot x$  is even; equivalently, the vectors  $x$  whose coordinate sum  $x_1 + \dots + x_n$  is even. As for the dual we find the two index 2 inclusions

$$E^{(0)} \stackrel{2}{\subset} \mathbb{Z}^n \stackrel{2}{\subset} (E^{(0)})^*.$$

Let  $(x_1, \dots, x_n) \in E^{(0)}$ . By subtracting suitable integral multiples of the vectors  $(1, -1, 0, \dots, 0), \dots, (0, \dots, 1, -1)$  we then get an element of the shape  $(0, \dots, 0, d)$  in  $E^{(0)}$ . So  $d$  must be even, showing that  $e_1 - e_2, \dots, e_{n-1} - e_n, 2e_n$  spans  $E^{(0)}$ . Clearly, they are independent.

Now  $f = \frac{1}{2} \sum_i e_i$  takes integral values on  $E^{(0)}$ , is not in  $\mathbb{Z}^n$ , and satisfies  $2f \in \mathbb{Z}^n - E^{(0)}$  since  $n$  is odd. So  $f$  determines an element of order 4 in the discriminant group  $(E^{(0)})^*/E^{(0)}$ . Hence this group is cyclic of order 4.

In case  $n > 0$  is even, the non-zero elements in the discriminant group are the classes of  $e_1, f = \frac{1}{2} \sum_i e_i, e_1 + f$ , all of order 2.

2. Let  $L$  be an odd unimodular lattice so that  $x \cdot x$  is odd for at least one vector  $x \in L$ . Let  $L^{(0)}$  be the subset of vectors  $y \in L$  for which  $y \cdot y$  is even. This is a sublattice, since  $(y_1 + y_2) \cdot (y_1 + y_2) \equiv y_1 \cdot y_1 + y_2 \cdot y_2 \pmod{2}$ . Moreover, if  $x, y \notin L^{(0)}$ , then  $x + y \in L^{(0)}$ , so that  $[L : L^{(0)}] = 2$ . In fact  $L^{(0)}$  is the kernel of the surjective homomorphism  $L \rightarrow \mathbb{Z}/2\mathbb{Z}$  which sends  $x \in L$  to  $x \cdot x$ . Consider  $(L^{(0)})^* = \text{Hom}_{\mathbb{Z}}(L^{(0)}, \mathbb{Z})$ . Recall that for unimodular lattices such as  $L$  we have  $L = L^*$ . So, since  $L$  has index 2 in  $(L^{(0)})^*$ , we obtain a chain of inclusions of lattices, each of index 2 in the next:

$$L^{(0)} \subset L = L^* \subset (L^{(0)})^*.$$

Since  $(L^{(0)})^*/L^{(0)}$  is a group of order 4, there are at most 3 integral lattices strictly contained between  $L^{(0)}$  and its dual, one of these being  $L$ . Any other intermediate submodule gives a lattice, precisely if the  $\mathbb{Q}$ -valued form restricts to an integer valued form. In that case it is a (unimodular) neighbour of  $L$ .

We give an easy example. Consider  $W = \langle 1 \rangle \oplus \langle -1 \rangle$  with basis  $\{e, f\}$ . Then  $W^{(0)}$  is spanned by  $e + f$  and  $e - f$  and so is isometric to  $U(2)$ . The dual lattice is spanned by  $\frac{1}{2}(e + f)$  and  $\frac{1}{2}(e - f)$ . So the discriminant group in this case is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .

The two neighbours of  $W$  are  $U' = \mathbb{Z}(e + f) \oplus \mathbb{Z}(\frac{1}{2}(e - f))$  and  $U'' = \mathbb{Z}(e - f) \oplus \mathbb{Z}(\frac{1}{2}(e + f))$ , both isometric to  $U$ . So from the three unimodular lattices that contain  $W^{(0)}$  precisely one is odd, namely  $W$ .

**1.7.B  $p$ -Elementary Lattices.** Given a prime number  $p$ , a  $p$ -elementary lattice is a non-degenerate integral lattice  $(L, b)$  such that  $pL^* \subset L$ . Hence, if  $x \in L^*$ , then  $px \in L$  which is equivalent to  $\text{dg}_L = L^*/L$  being a  $\mathbb{Z}/p\mathbb{Z}$ -module. These come up naturally:  $L$  is  $p$ -elementary in case  $\text{disc}(L) = \pm p$ , or, if  $L$  is unimodular, then  $L(p)$  is  $p$ -elementary. Furthermore, orthogonal sums of  $p$ -elementary lattices are again  $p$ -elementary.

Note that if  $pL^* \subset L$ , then the form on  $pL^*$  is divisible by  $p$ . To see this, take  $x, y \in pL^*$ . Then  $y \in L$  and  $x \in pL^*$ , so  $x \cdot y \in p\mathbb{Z}$ . In particular, if  $p = 2$ ,  $2L^*$  is even.

As we have seen, the discriminant form  $b_L^\#$  is the non-degenerate form on  $\text{dg}_L$  induced by  $b_{\mathbb{Q}}$  and is *a priori*  $\mathbb{Q}/\mathbb{Z}$ -valued. In our situation,  $\text{dg}_L$  is  $p$ -torsion and so  $b_L^\#$  now has values in  $p^{-1}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ . Equivalently, we may view  $(\text{dg}_L, b_L^\#)$  as an  $\mathbb{F}_p$ -vector space equipped with a non-degenerate  $\mathbb{F}_p$ -valued form and write the latter as

$$W_L = (L^*/L, \cdot_{w_L}).$$

The inclusions  $pL^* \subset L \subset L^*$  suggest a second quotient,

$$V_L = (L/pL^*, \cdot_{v_L}),$$

where  $\bar{x} \cdot_{v_L} \bar{y} = b(x, y) \pmod{p}$ ,  $\bar{x}, \bar{y} \in L/pL^*$ . Since  $V_L \subset L^*/pL^*$ , it is a  $\mathbb{F}_p$ -vector space in a natural way and  $\cdot_{v_L}$  is non-degenerate since  $b$  is. Indeed, if  $b(x, L) \in p\mathbb{Z}$  then  $x/p \in L^*$  and so the class of  $x$  in  $L/pL^*$  is zero.

So a  $p$ -elementary lattice comes associated with two  $\mathbb{F}_p$ -spaces  $V_L$  and  $W_L$  equipped with non-degenerate forms. As to their dimensions, one has

$$\text{rank}(L) = \dim W_L + \dim V_L. \quad (1.15)$$

This is implied by the short exact sequence of groups

$$0 \rightarrow L^*/L \cong pL^*/pL \rightarrow L/pL \rightarrow L/pL^* \rightarrow 0.$$

The situation for quadratic forms and their discriminant quadratic forms is different however, since the latter takes values in  $(2p)^{-1}\mathbb{Z}/\mathbb{Z}$ . For  $p \neq 2$  the values are of the form  $a/2p \pmod{\mathbb{Z}}$  with  $a = 0$  or  $(a, p) = 1$  and so, if  $2^{-1}$  is the inverse of 2 in  $\mathbb{F}_p$  we can replace  $a/2p \pmod{\mathbb{Z}}$  with  $a \cdot 2^{-1} \in \mathbb{F}_p$ . For  $p = 2$  this is no longer possible. We distinguish two cases:

**Definition 1.7.2.** A 2-elementary even lattice is a *type I lattice* if its discriminant quadratic form is  $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ -valued and it is a *type II lattice otherwise, i.e., its discriminant quadratic form takes at least one value in  $\frac{1}{4}\mathbb{Z}/\mathbb{Z} - \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ .*

Type I lattices have non-degenerate polar forms and then  $\dim W_L$  is even. Using the isomorphism  $\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2$ , the vector space  $W_L$  gets the structure of an  $\mathbb{F}_2$ -inner product space. For type II this does not make sense. Moreover, for a type II lattice, neither  $\dim V_L$  nor  $\dim W_L$  need to be even.

The hyperbolic form  $U(2)$  with discriminant form  $u(2)$  is an example of a type I form. An example of a type II lattice is the lattice  $\langle 2 \rangle$ , with corresponding quadratic form [1] and the discriminant quadratic form takes the value  $\frac{1}{4}$  on the generator.

**Example 1.7.3.** Suppose that a finite group  $G$  acts through isometries on a non-degenerate lattice  $(L, b)$ . Two sublattices canonically associated to this action are:

$$L^G = \{x \in L \mid gx = x \text{ for all } g \in G\}, \quad L_G = (L^G)^\perp.$$

Both lattices are primitive sublattices of  $L$ . We claim that they are also non-degenerate. To see this, by Lemma 1.1.3.2, it suffices to remark that writing any  $x \in L$  as

$$x = \frac{1}{n}t_G(x) + \left(x - \frac{1}{n}t_G(x)\right), \quad t_G := \sum_{g \in G} g \in \mathbb{Z}[G], \quad n = |G|,$$

one obtains an orthogonal direct sum decomposition  $L_{\mathbb{Q}} = L_{\mathbb{Q}}^G \oplus L_{G, \mathbb{Q}}$  as we show now. Each element in the first summand is  $G$ -invariant. Since  $b(t_G(x), t_G(x)) = nb(x, t_G(x))$  for all  $x \in L$ , it is orthogonal to  $(x - \frac{1}{n}t_G(x))$ . Finally, if  $y \in L^G \cap L_G$ , then  $b(y, \frac{1}{n}t_G(x) + (x - \frac{1}{n}t_G(x))) = 0$  for all  $x$  and so  $y = 0$  and the above writing gives a direct sum splitting. It follows that  $L^G \oplus L_G$  is a finite index sublattice of  $L$ . Moreover, the decomposition also shows that  $nL \subset L^G \oplus L_G$ .

Suppose next that  $L$  is unimodular. From the inclusion  $nL \subset L^G \oplus L_G$  we obtain

$$\frac{1}{n}L = \frac{1}{n}L^* = (nL)^* \supset (L^G \oplus L_G)^*,$$

which implies

$$n(L^G)^* \oplus n(L_G)^* \subset L$$

and so, since  $t_G = n \cdot \text{id}$  on the first summand and  $t_G = 0$  on the second summand (since  $t_G^2 = nt_G$ ), we get inclusions  $n(L^G)^* \subset L^G$  and  $n(L_G)^* \subset L_G$ . So, if  $n$  is a prime number,  $L^G$  and  $L_G$  are  $n$ -elementary.

We observed that, for any  $n$ , prime or not,  $L_G \oplus L^G$  has finite index in  $L$ . This means that  $L$  is an example of an overlattice of  $L_G \oplus L^G$ , a concept we treat next.

**1.7.C Overlattices.** An *overlattice* of a non-degenerate symmetric lattice  $(N, b)$  is an integral lattice  $L$  containing  $N$  as a finite index sublattice. In particular  $b_{\mathbb{Q}}|L$  is integer valued. If the latter form is even, we say that  $L$  is a *quadratic overlattice*.

Observe that since the index  $[L : N]$  is finite, one has  $N \subset L \subset L^* \subset N^*$ , leading to the chain of inclusions

$$L/N \subset L^*/N \subset N^*/N = \text{dg}_N.$$

The discriminant form  $b_N^{\#}$  restricts to zero on  $L/N$  since  $b_{\mathbb{Q}}|L$  is integer valued. In other words,  $L/N$  is an isotropic subgroup of  $b_N^{\#}$ . If  $N$  is even, replacing  $b_N^{\#}$  with  $q_N^{\#}$  (derived from  $q(x) = \frac{1}{2}b(x, x)$ ), we obtain a subgroup isotropic for the quadratic torsion form. The converse also holds:

**Proposition 1.7.4.** *1. The overlattices  $L$  of a non-degenerate lattice  $(N, b)$  are in one-to-one correspondence with the isotropic subspaces  $H$  of  $(\text{dg}_N, b_N^{\#})$ . The correspondence is given by*

$$\begin{aligned} L &\longmapsto H_L := L/N \\ H &\longmapsto L_H := \{y \in N^* \mid y \bmod N \in H\}. \end{aligned}$$

*2. The discriminant group of an overlattice  $L$  is  $(L/N)^{\perp}/(L/N)$  with discriminant form induced by the form  $b_N^{\#}$  on  $N^*/N$  (observe that  $b_N^{\#}|_{L/N} = 0$ ). Unimodular overlattices  $L$  correspond to maximal isotropic subspaces of  $(\text{dg}_N, b_N^{\#})$ , that is, overlattices  $L$  for which  $(L/N)^{\perp} = L/N$ .*

*3. If  $b$  is even and  $q(x) = \frac{1}{2}b(x, x)$ , there is a one-to-one correspondence between subspaces isotropic with respect to the discriminant quadratic form on the one hand and even overlattices of  $N$  on the other hand.*

*Proof.* 1. We have seen the first correspondence. To see the second correspondence, it suffices to show that the form  $b_{\mathbb{Q}}$  on  $L_H$  is integer valued. Suppose  $x, y \in N^*$  such that  $\bar{x} = x \bmod N, \bar{y} = y \bmod N \in H$ . Since  $b_N^{\#}(\bar{x}, \bar{y}) = 0$  by assumption,  $b(x, y) \in \mathbb{Z}$ .

That the two correspondences are each other's inverse is immediate. For instance, one has

$$L_{L/N} = \{y \in N^* \mid y \bmod N \in L/N\} = L.$$

2. First we show that  $(L/N)^\perp = L^*/N$  in  $N^*/N$ . Fix  $\bar{x} \in N^*/N$ , with  $x \in N^*$ . Then  $\bar{x} \in (L/N)^\perp$  if and only if  $b_N^\#(\bar{x}, \bar{y}) = 0 \pmod{\mathbb{Z}}$  for all  $\bar{y} \in L/N$ . This is equivalent to  $\bar{x} \in L^*/N$ . So  $L^*/N = (L/N)^\perp$ . Since the form  $b_N^\#$  vanishes on  $L/N$ , the quotient  $(L/N)^\perp/(L/N)$  comes with a form induced by  $b_0$ . But this quotient is naturally isomorphic to  $(L^*/N)/(L/N) \cong L^*/L$  which also inherits its form from  $b_0$ .
3. For quadratic overlattices the proof is the same, replacing the discriminant bilinear form with the discriminant quadratic form.  $\square$

We illustrate the above technique with two examples.

**Examples 1.7.5. 1.** We return to the lattice  $U(2)$  in example 2 on page 34. The bilinear form is denoted  $b$ . Retaining the notation used there,  $U(2) = \mathbb{Z}(e+f) + \mathbb{Z}(e-f)$ , where  $b(e,e) = 1$ ,  $b(f,f) = -1$ , and  $b(e,f) = 0$ . Now  $U(2)^*/U(2) = \frac{1}{2}U(2)/U(2)$  with the induced discriminant symmetric form  $b^\#$  has three isotropic subspaces (of order 2):  $\langle \bar{e} \rangle$ ,  $\langle \frac{1}{2}(\bar{e} - \bar{f}) \rangle$ ,  $\langle \frac{1}{2}(\bar{e} + \bar{f}) \rangle$ . These correspond to the three overlattices  $W = \mathbb{Z}e + \mathbb{Z}f$ ,  $U' = \mathbb{Z}(e+f) + \mathbb{Z}(\frac{1}{2}(e-f))$ , and  $U'' = \mathbb{Z}(e-f) + \mathbb{Z}(\frac{1}{2}(e+f))$ , respectively. With respect to the discriminant quadratic form  $q^\#$  induced by the quadratic form  $q(x) = \frac{1}{2}b(x,x)$  on  $U(2)$ , however, only  $\langle \frac{1}{2}(\bar{e} - \bar{f}) \rangle$  and  $\langle \frac{1}{2}(\bar{e} + \bar{f}) \rangle$  are isotropic (note that  $q^\#(\bar{e}) = \frac{1}{2} \pmod{\mathbb{Z}}$ ). So the quadratic form ‘detects’ the even overlattices  $U'$  and  $U''$ .

**2.** Consider the quadratic lattice  $N = \mathbb{Z}^8(2)$ . In  $N^*/N$  take the span of the vectors  $\frac{1}{2}(1, 1, 1, 1, 0, 0, 0, 0)$ ,  $\frac{1}{2}(1, 1, 0, 0, 1, 1, 0, 0)$ ,  $\frac{1}{2}(1, 1, 0, 0, 0, 0, 1, 1)$ ,  $\frac{1}{2}(1, 0, 0, 1, 1, 0, 0, 1)$ . This is an isotropic subspace of dimension 4. This leads to an even overlattice  $L$  in which  $N$  is a sublattice of index  $2^4$ . By Lemma 1.2.2  $\text{disc}(L) = 1$  and so  $L \simeq E_8$  since up to isometry  $E_8$  is the only positive definite quadratic lattice of rank 8 (see Section 1.12 for further background). Lemma 4.1.6 gives an alternative explanation of this embedding by looking at roots.

Taking the span of  $\frac{1}{2}(1, 1, 1, 1, 0, 0, 0, 0)$ ,  $\frac{1}{2}(0, 0, 0, 0, 1, 1, 1, 1)$ ,  $\frac{1}{2}(0, 0, 1, 1, 1, 1, 0, 0)$  in  $N^*/N$  we obtain in a similar way an even overlattice isometric to  $D_8$  studied in Section 4.1.A. Indeed, a basis consisting of roots is given by the vectors in  $N^*$  (corresponding to the roots  $\alpha_1, \dots, \alpha_8$  of the corresponding Dynkin diagram on page 81)

$$\begin{aligned} \alpha_1 &= (0, 0, 0, 0, -\frac{1}{2}, -\frac{1}{2} - \frac{1}{2}, -\frac{1}{2}), & \alpha_2 &= (0, 0, 0, 0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}), \\ \alpha_3 &= (0, 0, 0, 0, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}), & \alpha_4 &= (0, 0, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, 0, 0), \\ \alpha_5 &= (-\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, 0, 0, 0, 0), & \alpha_6 &= (\frac{1}{2}, -\frac{1}{2} - \frac{1}{2}, -\frac{1}{2}, 0, 0, 0, 0), \\ \alpha_7 &= (-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0, 0, 0, 0), & \alpha_8 &= (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0, 0, 0, 0). \end{aligned}$$

Proposition 1.7.4 also leads to the next result:

**Lemma 1.7.6.** *Let  $S$  be a non-degenerate primitive sublattice of a unimodular lattice  $L$  and  $T = S^\perp$  its orthogonal complement. Then there is a natural isometry  $\text{dg}_S \xrightarrow{\cong} \text{dg}_T(-1)$  of discriminant bilinear forms. If  $L$  is even it is an isometry of discriminant quadratic forms.*

*Proof.* The lattice  $N = S \oplus T$  has finite index in  $L$  and so  $L$  is an overlattice of  $N$ . There are inclusions of free  $\mathbb{Z}$ -modules  $N \hookrightarrow L = L^* \hookrightarrow N^*$ , giving an inclusion

$L/N \hookrightarrow N^*/N = \text{dg}_S \oplus \text{dg}_T$ . If we compose this injection with the projections on the two factors, two morphisms of finite abelian groups result,  $\pi_S : L/N \rightarrow \text{dg}_S$  and  $\pi_T : L/N \rightarrow \text{dg}_T$ . Since  $S$  and  $T$  are primitive, Lemma 1.3.1 implies that  $[L : N] = |\text{dg}_S| = |\text{dg}_T|$  so that the above torsion groups  $L/N, \text{dg}_S$  and  $\text{dg}_T$  all have the same cardinality. We shall argue that they are in fact canonically isomorphic. We start with the observation that the maps  $L = L^* \rightarrow S^* \rightarrow S^*/S$  and  $L = L^* \rightarrow T^* \rightarrow T^*/T$  have their kernels in  $N$ . To see this, suppose that, for  $x \in L$ , the functional  $x \mapsto b(x, -)|_S$  is of the form  $b(s, -)|_S$  for some  $s \in S$ . Then  $x - s \in S^\perp = T$  and consequently  $x \in S \oplus T = N$ . A similar argument holds for  $T$ . This implies that  $\pi_S$  and  $\pi_T$  are injective and hence isomorphisms, whence the announced natural identification  $\psi = \pi_T \circ \pi_S^{-1} : \text{dg}_S \xrightarrow{\sim} \text{dg}_T$  under which  $L/N$  becomes the graph of  $\psi$ . The isomorphism  $\psi$  is an anti-isometry in the sense that it sends the discriminant form on  $\text{dg}_S$  to the negative of the one on  $\text{dg}_T$ . Indeed, Proposition 1.7.4 implies that  $L/N$  is a (maximal) isotropic subspace of the discriminant group  $\text{dg}_S \oplus \text{dg}_T$ .  $\square$

Next, we discuss a criterion for extending isometries  $\lambda : N \rightarrow N'$  to overlattices  $L$  of  $N$  and  $L'$  of  $N'$  respectively. The  $\mathbb{Q}$ -extension  $\lambda_{\mathbb{Q}} : N_{\mathbb{Q}} \xrightarrow{\sim} N'_{\mathbb{Q}}$  sends  $N^*$  to  $(N')^*$  and so there is an induced isometry of the discriminant forms

$$r_{N,N'}(\lambda) : (\text{dg}_N, b_N^\#) \xrightarrow{\sim} (\text{dg}_{N'}, b_{N'}^\#).$$

Clearly  $\lambda$  extends to the overlattices if and only if  $\lambda_{\mathbb{Q}}$  sends  $L$  to  $L'$ . This implies that in the commutative diagram

$$\begin{array}{ccc} N^* & \xrightarrow{\lambda_{\mathbb{Q}}} & (N')^* \\ \downarrow & & \downarrow \\ N^*/N = \text{dg}_N & \xrightarrow[r_{N,N'}(\lambda)]{\sim} & \text{dg}_{N'} = (N')^*/N' \\ \uparrow & & \uparrow \\ L/N & \dashrightarrow & L'/N', \end{array}$$

the dashed arrow exists, that is,  $r_{N,N'}(\lambda)$  sends  $L/N$  to  $L'/N'$  if and only if  $\lambda$  extends. A similar argument applies to quadratic lattices. In other words, we have shown:

**Proposition 1.7.7** (Extending isometries). *Let  $L, L'$  be overlattices of non-degenerate symmetric (or quadratic) lattices  $N, N'$  respectively. An isometry  $\lambda : N \xrightarrow{\sim} N'$  extends to an isometry  $L \xrightarrow{\sim} L'$  if and only if the isomorphism induced by  $\lambda$  on the discriminant groups sends  $L/N$  to  $L'/N'$ . In particular,  $\lambda \in \text{O}(N)$  extends to an isometry of  $L$  if and only if  $r_{N,N'}(\lambda)$  preserves  $L/N$ .*

## 1.8 Lattice Embeddings

To be able to embed a given integral lattice  $S$  in another lattice  $L$  there is an obvious restriction, namely  $\text{rank}(S) \leq \text{rank}(L)$ . Even more specifically, if  $(s_+, s_-)$  is the signature of  $S$  and  $(\ell_+, \ell_-)$  that of  $L$  we must have  $s_+ \leq \ell_+$  and  $s_- \leq \ell_-$ .

By way of example we show that, surprisingly, *all* even lattices can be embedded in an orthogonal sum of hyperbolic planes, provided the above conditions are satisfied.

**Lemma 1.8.1.** *Every even lattice  $(S, b)$  of rank  $s \leq a$  can be isometrically embedded in*

$$L = \underbrace{U \oplus \cdots \oplus U}_{a \text{ copies}}$$

as a primitive sublattice such that  $S^\perp \simeq S(-1) \oplus \oplus^{(a-s)}U$ , where we view  $S$  as embedded in  $L$ .

*Proof.* We provide an explicit embedding of  $S$  in  $L$ .<sup>4</sup> It is no restriction to assume that  $S$  has rank  $s = a$ . Let  $\{e_j, f_j\}$  be a basis of the  $j$ -th copy of  $U$  in  $L$  and choose  $\mathbf{E} = \{e_1, \dots, e_a, f_1, \dots, f_a\}$  as basis for  $L$ , so that the Gram matrix of the form on  $L$  with respect to  $\mathbf{E}$  becomes

$$\begin{pmatrix} 0 & \mathbf{1}_a \\ \mathbf{1}_a & 0 \end{pmatrix}.$$

Pick any basis  $\{c_1, \dots, c_a\}$  of  $S$  and let  $s_{ij} = b(c_i, c_j)$ . As in (1.1) let

$$s = \begin{pmatrix} \frac{1}{2}s_{11} & s_{12} & \cdots & \cdots & s_{1a} \\ 0 & \frac{1}{2}s_{22} & s_{23} & \cdots & s_{2a} \\ 0 & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \frac{1}{2}s_{a-1,a-1} & s_{a-1a} \\ 0 & \cdots & \cdots & 0 & \frac{1}{2}s_{aa} \end{pmatrix}$$

be the matrix of the associated quadratic form, so that  $s + s^\top$  is the matrix of the symmetric form on  $S$ . We define a primitive embedding  $i : S \hookrightarrow L$  on the coordinate level by sending the coordinate column vector  $\underline{u}$  corresponding to  $\sum u_i c_i$  to the coordinate vector  $A\underline{u}$ , where  $A = \begin{pmatrix} I_a \\ s^\top \end{pmatrix}$  (the presence of the block  $I_a$  guarantees that  $i(S)$  is primitive). Then we have

$$A^\top \begin{pmatrix} 0 & I_a \\ I_a & 0 \end{pmatrix} A = s + s^\top.$$

Hence formula (1.3) tells that  $i$  is an isometric primitive embedding. Put  $B = \begin{pmatrix} I_a \\ -s \end{pmatrix}$ . Since

$$B^\top \begin{pmatrix} 0 & I_a \\ I_a & 0 \end{pmatrix} B = -(s + s^\top),$$

<sup>4</sup>We prove a more general statement in Section 6.2.

this defines a primitive embedding  $j : S \hookrightarrow L$  with  $j(S)$  isometric to  $S(-1)$ . On the other hand,

$$A^T \begin{pmatrix} 0 & I_a \\ I_a & 0 \end{pmatrix} B = 0$$

and so  $j(S)$  is the orthogonal complement of  $i(S)$  in  $L$  (here we also use that  $\text{rank}(S) = \text{rank}(S^\perp)$ ). Hence we conclude  $i(S)^\perp \simeq S(-1)$ .  $\square$

**Outlook.** We give a glimpse of what can be found in Section 15.2, especially about the role which the discriminant form plays in embedding questions. Suppose we have a primitive embedding of a non-degenerate lattice  $S$  into an even unimodular lattice  $L$ . In Lemma 1.7.6 we proved by means of the technique of overlattices that  $S$  and  $T = S^\perp$  have isomorphic discriminant groups and opposite discriminant quadratic forms. Reversing the procedure, suppose that  $S$  and  $T$  are two non-degenerate even lattices together with an abstract isomorphism  $\psi : \text{dg}_S \xrightarrow{\cong} \text{dg}_T$  inducing opposite discriminant quadratic forms. It turns out that there is an even unimodular overlattice  $L$  of  $S \oplus T$  which induces  $\psi$  as in the cited example. In favorable situations the isometry class of  $L$  is uniquely determined. This is for instance the case if  $S$  is indefinite as stated by Theorem 2.4.1. In that case, using Nikulin's results, this ultimately leads to the criteria enumerated in Theorem 15.2.3 which ensure that  $S$  is embeddable in  $L$ . Uniqueness of a given embedding  $S \hookrightarrow L$  is a more difficult question. See Theorem 15.2.6.

A related problem is the extension problem for isometries: suppose that we have a sublattice  $S \subset L$ ,  $L$  unimodular, and two isometries  $\sigma \in \text{O}(S)$ , respectively  $\tau \in \text{O}(T)$ ,  $T = S^\perp$ . When can one extend the isometry  $\sigma \oplus \tau$  of  $S \oplus T$  to  $L$ ? Of course it extends as an isometry of  $L_\mathbb{Q}$ , so the question is: under which condition does the latter preserve the lattice  $L$ ? Theorem 15.1.7 tells us that this is the case if and only if the isometries  $\bar{\sigma}, \bar{\tau}$  induced by  $\sigma$ , respectively  $\tau$  on the discriminant groups satisfy the relation  $\psi \circ \bar{\sigma} = \bar{\tau}$ . We shall use this criterion in several examples.

## 1.9 On $p$ -Adic Lattices and the Genus

To classify an integral lattice  $(L, b)$ , one traditionally passes to its localizations  $L_p$  at primes  $p$ . By definition,  $L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ , where  $\mathbb{Z}_p$  is the ring of  $p$ -adic integers.<sup>5</sup> One extends the form  $b$  in a  $\mathbb{Z}_p$ -linear fashion which results in a symmetric form  $b_p$  on  $L_p$ . Summarizing, we have

$$L_p := L \otimes_{\mathbb{Z}} \mathbb{Z}_p, \quad b_p \text{ the } p\text{-adic bilinear extension of } b.$$

If, instead, one starts with a quadratic lattice  $(L, q)$ , an analogous process yields the pair  $(L_p, q_p)$ .

<sup>5</sup>We invite the reader to recall the basics on  $p$ -adic numbers as assembled in Appendix A.2.



The pair  $(L_p, b_p)$  is an example of a *p-adic lattice*. Abstractly, a *p-adic lattice* is a free finite rank  $\mathbb{Z}_p$ -module equipped with a  $\mathbb{Z}_p$ -valued  $\mathbb{Z}_p$ -bilinear symmetric form. So this resembles the definition of an integral lattice given in Section 1.2: one just replaces  $\mathbb{Z}$  everywhere by the *p-adic integers*  $\mathbb{Z}_p$ . Similar remarks apply to quadratic forms. The notion of isometry also extends in the obvious way.

The definition of the discriminant proceeds in an analogous fashion: it is the determinant of a matrix representing the form in a basis. As for forms on *k*-vector spaces, the resulting number  $\text{disc}(b_p)$  is only well defined up to multiplication with a square of a *p-adic unit*. Writing the discriminant of a non-degenerate form  $b_p$  as  $\text{disc}(b_p) = u \cdot p^k$  for some unit  $u$ , this means that  $u$  should be viewed in the factor group  $\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2$ , and thus interpreted it is an isometry invariant. The same type of group comes up when we shall consider forms on *R*-modules where *R* is an arbitrary commutative ring *R* with unit. This motivates to introduce the shorthand

$$D(R) := R^\times / (R^\times)^2. \quad (1.16)$$

As for forms on vector spaces and on free  $\mathbb{Z}$ -modules, we say that the lattice  $(L_p, b_p)$  is *non-degenerate* if  $\text{disc}(b_p) \neq 0$  and *unimodular* if  $\text{disc}(b_p)$  is itself a unit up to squares, i.e., belongs to  $D(\mathbb{Z}_p)$ .

Recall the structure of the group  $D(\mathbb{Z}_p)$  as described in Appendix A.2: if *p* is an odd prime, this group is cyclic of order two and has representatives 1 and any non-square unit  $\varepsilon$ . So the discriminant of a non-degenerate *p-adic lattice* has a representative of the form  $p^k$  or  $\varepsilon \cdot p^k$ , where *k* is a non-negative integer; unimodularity then means  $k = 0$ . Also, for every *k* there are exactly two isometry classes of rank one lattices,  $\langle p^k \rangle$  and  $\langle \varepsilon p^k \rangle$ . For the prime 2 this is slightly more involved as we explain below in Example 1.9.5.2.

As for integral lattices, the correlation morphism  $x \mapsto b_p(x, -)$  for the *p-adic lattice*  $(L_p, b_p)$  is injective (an isomorphism) precisely if the lattice is non-degenerate (respectively unimodular), and similarly for quadratic lattices. The proof is the same. So in the non-degenerate situation  $L_p$  embeds in the dual  $L_p^* = \text{Hom}_{\mathbb{Z}_p}(L_p, \mathbb{Z}_p)$  via the correlation morphism. The quotient  $\text{dg}_{L_p} = L_p^*/L_p$  is a finite *p*-primary group, i.e., a finite group for which all elements are annihilated by a suitable power of *p*. We observe also that the relation (1.8), which relates the index to the discriminant, has a *p-adic analog*:

$$|\text{dg}_{L_p}| = [L_p^* : L_p] = p^v, \quad \text{if } \text{disc}(L_p) = \text{unit} \cdot p^v. \quad (1.17)$$

To see this, remark that  $\mathbb{Z}_p$  is a principal ideal domain (the only non-trivial ideals are  $(p^k)$ , *k* a positive integer) so that the theory of elementary divisors (cf. Lemma A.1.1) is applicable. Here the principal divisors are no longer integers, but ideals in  $\mathbb{Z}_p$  and the argument leading to (1.8) gives (1.17).

The form  $b_p$  induces a  $\mathbb{Q}_p/\mathbb{Z}_p$ -valued discriminant symmetric form  $b_{L_p}^\#$  and  $(L_p, q_p)$ , using the polar form  $b_{\mathbb{Q}_p}$  to define  $L_p^*$ , leads to a discriminant quadratic form  $q_{L_p}^\#$  on  $\text{dg}_{L_p}$ :

$$\begin{aligned} b_{L_p}^\# : \text{dg}_{L_p} \times \text{dg}_{L_p} &\longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \\ q_{L_p}^\# : \text{dg}_{L_p} &\longrightarrow \mathbb{Q}_p/\mathbb{Z}_p. \end{aligned}$$

The pair  $(\mathrm{dg}_{L_p}, b_{L_p}^\#)$  is an example of a *symmetric  $p$ -primary torsion group* and  $(\mathrm{dg}_{L_p}, q_{L_p}^\#)$  is an example of a *quadratic  $p$ -primary torsion group*. These will be examined in more detail in Section 10.2.

As we just said,  $p$ -adic lattices arise naturally when one localizes an integral lattice at a prime. More generally, we can localize at a so called “place”. A finite place is just a prime number, but in addition there is a place at  $\infty$ :

$$L_\infty = L_{\mathbb{R}} = L \otimes \mathbb{R} \text{ equipped with the } \mathbb{R}\text{-bilinear extension } b_{\mathbb{R}} \text{ of } b.$$

The set of all places of  $\mathbb{Q}$  is denoted by  $\mathcal{P}$ . This can be generalized to number fields where there are more places at infinity corresponding to embeddings of the field in the real or complex numbers. Except in Chapter 5.1 we won’t make use of this.

Two isometric lattices have isometric localizations. The converse need not be true, as indicated in the outlook at the end of this section. This motivates the concept of the genus of a lattice:

**Definition 1.9.1.** The *genus*  $\mathfrak{g}(L)$  of a lattice  $L$  is the set of isometry classes of lattices  $L'$  such that  $L'_v \simeq L_v$  for all places  $v \in \mathcal{P}$ . We then say that the lattices  $L$  and  $L'$  *belong to the same genus*, or, that they are *genus-equivalent*.

As we just said, a genus may contain several isometry classes. However, passing to the level of  $\mathbb{Q}$ -vector spaces, isometry is the same as genus-equivalence. We shall prove this in Chapter 3.

If  $L$  is non-degenerate, then so are its localizations, and likewise for unimodularity, and taking the discriminant commutes with localization:

$$\mathrm{disc}(L_v) = \mathrm{disc}(L)_v. \quad (1.18)$$

This requires some explanation, since the two discriminants belong to different groups. Indeed, for the local lattices  $\mathrm{disc}(L_p) \in \mathrm{D}(\mathbb{Z}_p)$  and  $\mathrm{disc}(L_\infty) \in \mathrm{D}(\mathbb{R})$ , while  $\mathrm{disc}(L) \in \mathbb{Z}$  which explains the right-hand side. Since there are natural embeddings  $\mathbb{Z} \subset \mathbb{Z}_p$ ,  $\mathbb{Z} \subset \mathbb{R}$ , we can write the right-hand side also as a multiplicative factor class  $\mathrm{disc}(L) \cdot (\mathbb{Z}_p^\times)^2$ , respectively  $\mathrm{disc}(L) \cdot (\mathbb{R}^\times)^2$ . The equality states that this procedure gives the localized discriminants. As a side remark, consistent with what we just said, we shall usually take  $\pm 1$  as values for  $\mathrm{disc}(L_\infty)$ .

We wish to point out that we can figure out the value of  $\mathrm{disc}(L)$  from the local discriminants. Here one needs one more ingredient (cf. Appendix A.1): any finite abelian group  $G$  decomposes into a direct product of its  $p$ -primary subgroups  $G_p$  and so  $|G| = \prod_p |G_p|$ . Combined with equation (1.8) on page 29 and (1.17) this gives the following formula

$$\begin{aligned} \mathrm{disc}(L) &= \mathrm{disc}(L_\infty) \cdot \prod_p |\text{\textit{p-primary part of } } \mathrm{dg}_L | \\ &= \underbrace{\mathrm{disc}(L_\infty)}_{\pm 1} \prod_p p^{v(p)}. \end{aligned} \quad (1.19)$$

The right-hand side up to sign corresponds exactly to the prime power decomposition of  $|\text{disc}(L)|$ ; and the sign is indeed  $\text{disc}(L_\infty)$ . We give a direct application.

**Proposition 1.9.2.** *1. The discriminant is a genus-invariant: all lattices of the same genus have the same discriminant.*

*2. The parity of a lattice is a genus-invariant: lattices of the same genus are either all even or all odd.*

*Proof.* 1. This is clear, since by uniqueness of the prime power decomposition of  $|\text{disc}(L)|$ , giving  $\text{disc}(L)$  is equivalent to giving the set of local discriminants.

2. A form is even if  $b(x, x) \in 2\mathbb{Z}$  for all  $x \in L$ , which is the case if and only if  $L_2$  is even, that is if  $b(x, x) \in 2\mathbb{Z}_2$  for all  $x \in L_2$ .  $\square$

**Example 1.9.3.** Suppose that  $L$  has discriminant  $-2^2 \cdot 3^2 \cdot 7^4$ . Then the local discriminants at the places  $\infty, 2, 3, 7$  are  $-1, 7 \cdot 2^2, 2 \cdot 3^2, 6 \cdot 7^4$ . This is clear for the place at  $\infty$ . For the prime 2 one observes that  $-3^2 \cdot 7^4 \equiv 7 \pmod{8}$  and Theorem A.2.1 tells us that the units in  $\mathbb{Z}_2$  modulo squares of units are represented modulo 8 by one of the four numbers 1, 3, 5, 7. For the primes 3 and 7 we observe that  $-2^2 \cdot 7^4 \equiv 2 \pmod{3}$  respectively  $-2^2 \cdot 3^2 \equiv 6 \pmod{7}$ .

Conversely, given local discriminants  $-1, 7 \cdot 2^2, 2 \cdot 3^2, 6 \cdot 7^4$  at the places  $\infty, 2, 3, 7$  and 1 elsewhere, we retrieve the global discriminant  $-2^2 \cdot 3^2 \cdot 7^4$ . Note that apart from the sign of  $L_\infty$ , only the  $p$ -adic orders of the local discriminants are relevant in determining the global discriminant.

Taking the discriminant form of  $L$  also commutes with localization. This requires some explanation as well, since the forms  $b_L^\#$  and  $b_{L_p}^\#$  take values in different rings: the discriminant form  $b_L^\#$  restricted to the  $p$ -primary part  $[\text{dg}_L]_p$  of the discriminant group can be seen to take values in  $\mathbb{Q}^{(p)}/\mathbb{Z}$ , where  $\mathbb{Q}^{(p)}$  is the set of rational numbers of the form  $q/p^r$ ,  $q \in \mathbb{Z}, \gcd(p, q) = 1$ . Via the canonical isomorphism  $\mathbb{Q}^{(p)}/\mathbb{Z} \simeq \mathbb{Q}_p/\mathbb{Z}_p$  (cf. Section A.2) we get a  $\mathbb{Q}_p/\mathbb{Z}_p$ -valued form. This is the discriminant form of the localization  $L_p$ . We summarize all this in the commutative diagram

$$\begin{array}{ccc}
 \text{integral lattice } (L, b) & \xrightarrow{\text{localization in } p} & p\text{-adic lattice } (L_p, b_p) \\
 \downarrow \text{discriminant bil. form} & & \downarrow \text{discriminant bil. form} \\
 \text{symmetric torsion} & \xrightarrow{p\text{-primary part}} & p\text{-primary symmetric} \\
 \text{group } b_L^\# & & \text{torsion group } b_{L_p}^\#
 \end{array} \tag{1.20}$$

The lower arrow for general torsion groups is to be interpreted as follows. Let  $(G, b)$  be a symmetric torsion group and  $G_p$  the subgroup of elements of  $G$  annihilated by some power of  $p$ . Then the values of the form  $b|_{G_p}$  are annihilated by a power

of  $p$  and so  $b|_{G_p}$  has values in  $\mathbb{Q}^{(p)}/\mathbb{Z} \simeq \mathbb{Q}_p/\mathbb{Z}_p$ . Hence  $(G_p, b|_{G_p})$  is a  $p$ -primary symmetric torsion group.

A similar story holds for even lattices  $(L, b_q)$  if we replace the discriminant bilinear form by the discriminant quadratic form. We shall see later (cf. Section 10.3) that every torsion form splits orthogonally into its  $p$ -primary parts, and so we have:

**Lemma 1.9.4.** *Two integral symmetric forms of the same genus have isometric discriminant bilinear forms and two quadratic forms of the same genus have isometric discriminant quadratic forms.*

Next we exhibit several basic examples of  $p$ -adic lattices. We shall prove in Chapter 9 that a  $p$ -adic lattice decomposes into direct sums with each summand isometric to one of the lattices in the examples below. We shall moreover show that symmetric and quadratic torsion forms decompose accordingly. We want to remark however that finding such a decomposition for a localization of a given integral lattice, e.g. for the root lattice  $E_8$  or the other root lattices to be discussed in Section 4.1, is not obvious. See e.g. Example 11.1.5.2 and Examples 11.2.5.3 and 4.

**Examples 1.9.5. 1.** Let  $p$  be an odd prime. Every non-zero  $p$ -adic integer is of the form (unit  $u$ ) $\cdot p^k$ ,  $k \geq 0$ , and this leads to the forms  $\langle up^k \rangle$  on  $\mathbb{Z}_p$ , explicitly given by

$$(x, y) \mapsto u \cdot p^k \cdot xy, \quad x, y \in \mathbb{Z}_p.$$

Note that  $\langle up^k \rangle \simeq \langle ua^2p^k \rangle$  for any  $a \in \mathbb{Z}_p^\times$  through  $x \mapsto a^{-1}x$  and  $\langle up^k \rangle \simeq \langle vp^k \rangle$  implies  $u = a^2v$  for some  $a \in \mathbb{Z}_p^*$ . The discriminant takes values in the group  $D(\mathbb{Z}_p)$  and so, since for an odd prime  $p$  this group is cyclic of order two generated by a non-square modulo  $p$ , the two lattices  $\langle p^k \rangle$  and  $\langle \epsilon \cdot p^k \rangle$  with  $\epsilon$  a non-square modulo  $p$  are not isomorphic. These represent all possible isometry classes for bilinear or quadratic such forms, since obviously a rank 1 form is classified by its discriminant.

A rank one quadratic form  $q$  is determined by  $q(1) = up^k$ ,  $k \geq 0$ . Replacing  $u$  by  $u + p$  one does not change its isometry class since by Theorem A.2.1.1  $u^{-1}(u + p) \equiv 1 \pmod{p}$  is a square and so  $\langle (u + p)p^k \rangle \simeq \langle up^k \rangle$ . Hence we may assume that  $u$  is an even unit. Then the polar form of  $x \mapsto \frac{1}{2}u \cdot p^k x^2$  is the form  $(x, y) \mapsto up^k xy$ . This quadratic form is denoted by  $\langle up^k \rangle$  - or - if confusion is likely, by  $[\frac{1}{2}up^k]$ .

As for discriminant forms, a complete classification will be given in Section 6.1. In our case  $L = \langle u \cdot p^k \rangle$  and then  $L^* = p^{-k}\mathbb{Z}_p$  so that the discriminant group is  $L^*/L = p^{-k}\mathbb{Z}_p/\mathbb{Z}_p \simeq \mathbb{Z}/p^k\mathbb{Z}$ . The induced  $\mathbb{Q}^{(p)}/\mathbb{Z}$ -valued form on  $L^*/L$  can then be identified with the symmetric form  $(x, y) \mapsto u \cdot p^{-k}xy$  on  $\mathbb{Z}/p^k\mathbb{Z}$ , denoted  $\langle u \cdot p^{-k} \rangle$ .

For a non-degenerate quadratic lattice  $(L, q)$  we define  $L^*$  using the form  $b_q$ . Then in a similar way we identify the quadratic form on  $L^*/L$  with the quadratic form<sup>6</sup>  $\langle u \cdot p^{-k} \rangle = [\frac{1}{2}u \cdot p^{-k}]$  on  $\mathbb{Z}/2p^k\mathbb{Z}$  given by  $x \mapsto \frac{1}{2}up^{-k}x^2$ . The isometry

<sup>6</sup>Both the Miranda–Morrison notation [156] as well as C.T.C. Wall’s notation [245] is completely different.

class of the form depends on  $\bar{u} \in D(\mathbb{Z}_p)$ . Hence we have two non-isometric forms, depending on  $u$  being a square or not.

2. Now let  $p = 2$ . Usually a 2-adic lattice is called a *dyadic lattice* and the underlying symmetric (quadratic) form a *dyadic symmetric (quadratic) form*. For a fixed  $k \geq 0$  we get four dyadic symmetric forms  $\langle u \cdot 2^k \rangle$  given by

$$(x, y) \mapsto u \cdot 2^k xy, \quad u \in \{\pm 1, \pm 3\}.$$

Indeed, by Theorem A.2.1, the group  $D(\mathbb{Z}_2)$  of units modulo squares of units in  $\mathbb{Z}_2$  is represented by one of these numbers modulo 8. This gives the complete classification of rank one dyadic lattices. For the dyadic quadratic forms  $\langle u \cdot 2^k \rangle = [u \cdot 2^{k-1}]$  given by

$$x \mapsto u \cdot 2^{k-1} x^2, \quad k \geq 1,$$

the situation is similar.<sup>7</sup>

The corresponding discriminant forms are the  $\mathbb{Q}^{(2)}/\mathbb{Z}$ -valued symmetric forms on  $\mathbb{Z}/2^k\mathbb{Z}$  denoted  $\langle u \cdot 2^{-k} \rangle$ . These give the polar forms of the quadratic forms  $[u \cdot 2^{-k-1}]$  on  $\mathbb{Z}/2^k\mathbb{Z}$ ,  $u \in \{\pm 1, \pm 3\}$ ,  $k \geq 1$ , and are given by

$$(x, y) \mapsto u \cdot 2^{-k} xy.$$

In Section 6.1 we shall discuss the classification of these torsion forms. In contrast to the lattice case, for low values of  $k$ , units  $u, u'$  that are different modulo squares might give rise to isometric symmetric or quadratic torsion forms.

3. The  $p$ -adic hyperbolic plane  $U = U_0$  and  $U_k = U(p^k)$ ,  $k \geq 1$ , give rank two symmetric  $p$ -adic lattices as follows, regardless whether  $p$  is an odd prime or  $p = 2$ . By definition, the Gram matrix of  $U_k$  in the standard basis of  $\mathbb{Z}_p^2$  is

$$U_k = \begin{pmatrix} 0 & p^k \\ p^k & 0 \end{pmatrix} = \begin{pmatrix} 0 & p^k \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ p^k & 0 \end{pmatrix}.$$

We have  $\text{disc}(U_k) = -p^{2k}$ . Observe that  $U_k$  is the polar form of the quadratic form

$$(x_1, x_2) \mapsto p^k x_1 x_2.$$

We shall denote this form also by  $U_k$ . Its discriminant group  $p^{-k}U_k/U_k \simeq \oplus^2(\mathbb{Z}/p^k\mathbb{Z})$  carries the quadratic form given by

$$(\bar{x}_1, \bar{x}_2) \mapsto p^{-k} \bar{x}_1 \bar{x}_2 \in \mathbb{Q}^{(p)}/\mathbb{Z}, \quad (\bar{x}_1, \bar{x}_2) \in \oplus^2(\mathbb{Z}/p^k\mathbb{Z}).$$

Its polar form has Gram matrix

$$u_k = \begin{pmatrix} 0 & p^{-k} \\ p^{-k} & 0 \end{pmatrix} = \begin{pmatrix} 0 & p^{-k} \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ p^{-k} & 0 \end{pmatrix}.$$

The discriminant quadratic form of  $U_k$  is also denoted  $u_k$ .

<sup>7</sup>Nikulin's notation differs between the symmetric and quadratic forms which we denote  $u_k, v_k$ , but does not change notation for the forms on  $\mathbb{Z}/2^k\mathbb{Z}$ . The Miranda–Morrison notation is completely different.

4. For  $p = 2$  the rank 2 bilinear dyadic lattice  $V_k$ ,  $k \geq 0$ , is given by the matrix  $2^k V$ , where

$$V = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

So  $V_k$  has discriminant  $3 \cdot 2^{2k}$ . In particular,  $V_0 = V$  is unimodular. The decomposition of  $V$  indicates that  $V_k$  is the polar form of the corresponding quadratic form (also denoted  $V_k$ ) given by

$$(x_1, x_2) \mapsto 2^k(x_1^2 + x_1x_2 + x_2^2).$$

The dyadic quadratic torsion form given by

$$(\bar{x}_1, \bar{x}_2) \mapsto 2^{-k}(\bar{x}_1^2 + \bar{x}_1\bar{x}_2 + \bar{x}_2^2), \quad (\bar{x}_1, \bar{x}_2) \in (\mathbb{Z}/2^k\mathbb{Z})^{\oplus 2} \quad (1.21)$$

is isometric to the discriminant quadratic form of  $V_k$ . To see this, note that the length of  $\text{dg}_{V_k}$  equals the rank of  $V_k$  and then the Gram matrix of the bilinear discriminant form with respect to the dual basis is given by  $(V_k)^{-1} \equiv 2^{-2k}V_k \equiv v_k \pmod{\mathbb{Z}}$ . This is the Gram matrix of the polar form of (1.21) over  $\mathbb{Q}^{(2)}/\mathbb{Z}$  since

$$v_k = \begin{pmatrix} 2^{-k+1} & 2^{-k} \\ 2^{-k} & 2^{-k+1} \end{pmatrix} = \begin{pmatrix} 2^{-k} & 2^{-k} \\ 0 & 2^{-k} \end{pmatrix} + \begin{pmatrix} 2^{-k} & 0 \\ 2^{-k} & 2^{-k} \end{pmatrix}.$$

As in the case of  $u_k$ , we shall denote the quadratic discriminant form of  $V_k$  also by  $v_k$ .

Observe that while the quadratic forms  $u_1$  and  $v_1$  are not isometric (just consider their values on non-zero vectors), there is no difference between the symmetric torsion forms  $u_1$  and  $v_1$  since the Gram matrix of  $v_1$  has the integer  $2 \cdot 2^{-1} = 1$  on the diagonal which is zero in  $\mathbb{Q}^{(2)}/\mathbb{Z}$  as is the case for  $u_1$ .

**Outlook.** Two  $\mathbb{Q}$ -vector spaces equipped with non-degenerate forms, say  $(V, b)$  and  $(V', b')$  that have isometric localizations  $V_v \simeq V'_v$  at all places  $v \in \mathcal{P}$  are themselves isometric. This is also called the **Hasse principle** and will be shown in Chapter 3. It follows that integral forms of the same genus are rationally equivalent. However, a genus of an integral lattice can have more than one isometry class. For instance, it turns out that the non-isometric lattices  $\Gamma_{16}$  and  $\Gamma_8 \oplus \Gamma_8$  that we considered in Example(4) in Section 1.4 belong to the same genus. However, the genus of an even indefinite unimodular lattice contains only one isometry class. This follows for example from an important (non-classical) characterization of the genus:

*Theorem (Characterization of the genus, [171, Cor. 1.9.4]). The genus of an even non-degenerate lattice  $L$  is determined by its signature and its discriminant quadratic form. In particular, an even unimodular lattice  $L$  belongs to a unique genus determined by its signature.*

This result will be proven in Section 11.3 but the unimodular case is, as

we said, much simpler and is treated in Chapter 2.

Clearly, we also want an existence result. Here a new concept enters the scene:  $\tau_8(q^\#)$ , **the index modulo 8** of a torsion quadratic group  $(G, q^\#)$ . This is by definition the index modulo 8 of any even form whose discriminant form equals a given non-degenerate torsion quadratic group. In Chapter 12 we show that this is a well-defined concept and that it can be calculated effectively. We can now formulate a simplified version of Nikulin's existence result (the full version is Theorem 12.4.4):

*Theorem (Existence of even lattices, [171, Th. 1.10.1]). Given a pair of non-negative integers  $(r_+, r_-)$  and a non-degenerate torsion quadratic group  $(G, q^\#)$  with  $\tau_8(q^\#) \equiv r_+ - r_- \pmod{8}$ . Then there exists a non-degenerate even lattice  $L$  of rank  $r = r_+ + r_-$ , signature  $(r_+, r_-)$  and with discriminant form  $(G, q^\#)$  if  $\ell(G) < r$ , where  $\ell$  is the minimal number of generators of  $G$ .*

*Example 1.9.6.* Consider the form  $q^\# = \langle -3 \cdot 2^{-1} \rangle = [-3 \cdot 2^{-2}]$ , i.e., the form on  $\mathbb{Z}/2\mathbb{Z}$  sending a generator to  $\frac{-3}{4} \in \mathbb{Q}/\mathbb{Z}$ . We find  $\tau_8(q^\#) = 1$  (cf. Proposition 12.3.3) and thus there exists a negative definite even lattice of rank 7 whose discriminant form equals  $q^\#$ . Indeed,  $E_7(-1)$  is such a lattice (cf. Table 4.1.1).

The analogous results (characterization of the genus and existence) in the odd case are discussed in Section 12.5.

## 1.10 Finiteness Results

We have seen that the discriminant of a lattice is a basic isometry invariant. We prove a classical finiteness result which involves this invariant:

**Theorem 1.10.1** (Eisenstein–Hermite). *Fix positive integers  $n, d$ . There are only finitely many isometry classes of non-degenerate integral lattices  $L$  of rank  $n$  and  $|\text{disc}(L)| \leq d$ .*

We shall show that this theorem is in fact a consequence of a classical bound on discriminants which uses a further invariant of a lattice  $L$ :

$$m_L = \min_{y \in L - \{0\}} |b(y, y)|. \quad (1.22)$$

Since  $b$  is integer valued, this minimum exists and it is equal to zero if and only if  $L$  has isotropic vectors.

**Proposition 1.10.2.** *Let  $(L, b)$  be a non-degenerate integral lattice of rank  $n$ . Either  $m_L = 0$ , which means that  $L$  contains an isotropic vector, or we have*

$$0 < m_L \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \cdot d_L^{\frac{1}{n}}, \quad d_L = |\text{disc}(L)|.$$

*Proof.* We may assume that  $L$  does not contain isotropic vectors. Let  $e \in L$  be such that

$$m_L = |b(e, e)|.$$

Then  $e$  is primitive and can be completed to a basis  $\mathbf{E} = \{e = e_1, e_2, \dots, e_n\}$  of  $L$ . The proof is by induction on  $n$ . The case  $n = 1$  is clear. For the induction step we use the orthogonal projection defined by  $e$ . To make sense of this, we embed  $L$  in the vector space  $V = L_{\mathbb{Q}}$  equipped with the  $\mathbb{Q}$ -linear extension of the form  $b$  which we continue to denote  $b$ . The orthogonal projection

$$\pi : V \rightarrow W = e^{\perp}, \quad x \mapsto x - \frac{b(x, e)}{b(e, e)}e \quad (1.23)$$

then maps  $L$  to a (non-integral) lattice  $L'$  of rank  $n - 1$  with basis  $\mathbf{E}' = \pi(\mathbf{E} - \{e\})$ . The form  $b$  restricts to  $L'$  as a form having values in  $b(e, e)^{-1} \cdot \mathbb{Z}$  because of the formula (1.23) for the projection. So there is an invariant  $m_{L'}$ , which is positive since  $L' \subset V$  and  $V$  does not contain isotropic vectors. We show next that

$$\begin{aligned} d_L &= |b(e, e)| \cdot d_{L'} \\ &= m_L \cdot d_{L'}. \end{aligned} \quad (1.24)$$

Since the (non-integral) lattice  $\tilde{L} = L + \frac{1}{b(e, e)}\mathbb{Z} \cdot e$  contains  $L$  as a sublattice of index  $|b(e, e)|$ , we have  $d_L = [\tilde{L} : L]^2 d_{\tilde{L}} = b(e, e)^2 d_{\tilde{L}}$ . On the other hand,  $\tilde{L} = \frac{1}{b(e, e)}\mathbb{Z} \cdot e \oplus L'$  and so  $d_{\tilde{L}} = \frac{1}{|b(e, e)|} d_{L'}$ . Combining the two expressions we obtain  $d_L = |b(e, e)| \cdot d_{L'}$ .

Every  $x' \in L'$  is by construction “close” to a point of the lattice  $L$ : write

$$x' = \pi(u) = u + \lambda \cdot e, \quad \lambda \in \mathbb{Q}, \quad b(x', e) = 0,$$

and choose  $k \in \mathbb{Z}$  such that

$$x' = \underbrace{u + k \cdot e}_{x \in L} + \underbrace{(\lambda - k)}_t \cdot e, \quad |t| \leq \frac{1}{2}.$$

Now apply this to a vector  $x' \in L'$  for which  $|b(x', x')| = m_{L'}$  so that

$$m_L \leq b(x, x) = b(x', x') + t^2 b(e, e) \quad (1.25)$$

$$= m_{L'} + t^2 m_L \quad (1.26)$$

$$\leq m_{L'} + \frac{1}{4} m_L \quad (1.27)$$

and so  $m_L \leq \frac{4}{3} m_{L'}$ . The induction procedure can be applied to  $L'$ , even if  $b$  is not integer valued on  $L'$  because first of all the form  $b(e, e) \cdot b$  restricts to an integer valued form on  $L'$  and, secondly, the desired inequality is insensitive to scaling  $b$ . The induction hypothesis states

$$m_{L'} \leq \left(\frac{4}{3}\right)^{\frac{n-2}{2}} \cdot d_{L'}^{\frac{1}{n-1}}.$$



By (1.24), we have  $d_L = m_L d_{L'}$  and so

$$m_L \leq \left(\frac{4}{3}\right)^{\frac{n}{2}} \left(\frac{d_L}{m_L}\right)^{\frac{1}{n-1}}$$

which implies

$$m_L^n \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}} d_L,$$

another expression of the desired inequality.  $\square$

*Remark 1.10.3.* The absolute value of the discriminant  $d_L$  of a lattice  $L$  can be related to the volume of a fundamental domain for  $L$  in  $V = L_{\mathbb{R}}$ . To explain this, observe that there exists an orthogonal basis  $\mathbf{B} = \{b_1, \dots, b_n\}$  of  $V$  with respect to  $b$  in which the Gram matrix for  $b$  reads

$$I_{p,n-p} = \text{diag}(\underbrace{1, \dots, 1}_p, \underbrace{-1, \dots, -1}_{n-p}).$$

We put a euclidean structure on  $V$  by declaring  $\mathbf{B}$  to be an orthonormal basis. The parallelepiped in  $V$  determined by the basis  $\mathbf{E}$  for  $L$  defined by

$$P_L = \{x_1 e_1 + \dots + x_n e_n \mid 0 \leq x_j \leq 1, j = 1, \dots, n\} \quad (1.28)$$

is a fundamental domain for  $L$ . Let the matrix  $E = (e_{ij})$  relate the bases  $\mathbf{B}$  and  $\mathbf{E}$ , that is  $e_i = \sum_j e_{ji} b_j$ . The volume of  $P_L$  with respect to the euclidean metric in which  $\mathbf{B}$  is an orthonormal basis equals  $|\det E|$ . Now we use the change of basis formula (1.2) to relate the Gram matrices  $B_{\mathbf{E}}$  for  $b$  with respect to  $\mathbf{E}$  and  $I_{p,n-p}$  with respect to  $\mathbf{B}$ . We find

$$B_{\mathbf{E}} = E^T I_{p,n-p} E$$

and so, taking determinants, this gives

$$d_L = (\det E)^2 = \text{vol}^2(P_L).$$

*Proof of Theorem 1.10.1.* The proof is by induction on the rank  $n$  of  $L$ . For  $n = 1$  the assertion is clear. We use the invariant  $m_L$  defined by (1.22) and first construct a finite set of isometry classes of auxiliary lattices  $S$  of rank 1 or 2 that may occur as a sublattice of  $L$ .

**Case 1** Suppose that  $m_L \neq 0$  and that  $x_0 \in L$  satisfies  $|x_0 \cdot x_0| = m_L$ . Put  $S = \mathbb{Z}x_0$ . Since  $S$  has rank 1 there are at most two possible isometry classes for  $S$ .

**Case 2** If  $m_L = 0$  pick a primitive isotropic vector  $e_1$  and define  $S \subset L$  as follows. The set of integers  $e_1 \cdot L$  is an ideal in  $\mathbb{Z}$ , generated by, say,  $k > 0$ . So in a basis  $\mathbf{E} = \{e_1, \dots, e_n\}$  the entries of the first row and column of the matrix  $B_{\mathbf{E}}$  are all divisible by  $k$  and since  $n \geq 2$  we have that  $k^2$  is a divisor of  $d_L$  and hence we have

$$k^2 \leq d_L \leq d. \quad (1.29)$$

Let  $e'_2 \in L$  be such that  $e_1 \cdot e'_2 = k$ . Since

$$\begin{aligned} (e'_2 + te_1) \cdot (e'_2 + te_1) &= e'_2 \cdot e'_2 + 2te_1 \cdot e'_2 \\ &= e'_2 \cdot e'_2 + 2tk, \end{aligned}$$

we may add to  $e'_2$  a suitable integral multiple of  $e_1$  to achieve the inequality  $|e'_2 \cdot e'_2| \leq k$ . In this situation we set  $S = \mathbb{Z}e_1 + \mathbb{Z}e'_2$ . Then  $|\text{disc}(S)| = k^2 \leq d$  by (1.29) and so  $d_S = |\text{disc}(S)|$  is bounded. Hence there are only finitely many possibilities for the isometry classes of the lattice  $S$ .

We want to apply the induction hypothesis to  $T = S^\perp$  by showing that  $d_T = |\text{disc}(T)|$  is bounded as well. We do this by applying Lemma 1.3.1, but we first need to see that in both cases  $S$  is primitive. In case 1 this is clear since by minimality  $x_0$  is primitive. Otherwise we have  $S = \mathbb{Z}e_1 + \mathbb{Z}e'_2$  with  $e_1$  primitive and  $e'_2$  chosen such that  $e_1 \cdot e'_2 = k$  generates  $e_1 \cdot L$ . So, if  $z = ae_1 + be'_2 \in L_\mathbb{Q} \cap S$ , then  $bk = z \cdot e_1 \in k\mathbb{Z}$  and so  $b \in \mathbb{Z}$  and then, by primitivity of  $e_1$ , also  $a \in \mathbb{Z}$ . This shows that  $S$  is primitive in this case too. Since we assume that  $|\text{disc}(L)| \leq d$ , Lemma 1.3.1, 2(b) implies:

$$d_T \leq d_S \cdot d_L \leq d_S \cdot d$$

and thus  $d_T$  is bounded. Since  $\text{rank}(T) < n$ , the induction hypothesis applies and we conclude that there are finitely many isometry classes for  $T$ .

To conclude, observe that

$$S \oplus T \subset L \subset L^* \subset S^* \oplus T^*.$$

This implies that for  $L$  there are only finitely many possible isometry classes, since up to isometry  $L$  is a lattice between two  $\mathbb{Q}$ -valued  $\mathbb{Z}$ -modules from a finite list.  $\square$

By Proposition 1.9.2.1 all lattices of the same genus have the same discriminant, and so the following consequence is immediate.

**Corollary 1.10.4** (Finiteness of isometry classes in a genus). *Every genus contains at most finitely many isometry classes of lattices.*

This motivates:

**Definition 1.10.5.** The *class number of a genus* is the number of isometry classes of that genus.

**Example 1.10.6** ([36, Ch. 9.3]). The estimate of Proposition 1.10.2 can in some cases be used to show that the class number is 1 for a given genus. As an example consider the odd form  $b$  in  $\mathbb{Z}^3$  whose Gram matrix is the diagonal matrix  $\text{diag}(1, 1, -3)$ . There are no isotropic vectors since  $x^2 + y^2 = 3z^2$  has no non-trivial integral solution. As we announced in the outlook at the end of Section 1.9, by the Hasse principle to be shown in Chapter 3, a form  $b'$  of the same genus as  $b$  is rationally equivalent to  $b$ . In particular,  $b'$  has no isotropic vectors (over  $\mathbb{Q}$  and integrally) and then the estimate of Proposition 1.10.2 shows that there exists a

non-isotropic vector  $a$  with  $b'(a, a) \leq \frac{4}{3} \cdot 3^{\frac{1}{3}} < 2$ . In other words,  $b'(a, a) = \pm 1$  and by Corollary 1.3.4 we can split off  $\mathbb{Z}a$ . Then  $b'$  is equivalent to  $\langle \pm 1 \rangle \oplus b''$  where  $b''$  is either an even or an odd binary form with discriminant  $\pm 3$  (use that the discriminant is a genus invariant). The binary form  $b''$  contains an element  $c$  such that  $b''(c, c) = \pm 1$  in the odd case and an element  $e$  such that  $b''(e, e) = \pm 2$  in the even case. The existence of such elements is again based on the estimate in Proposition 1.10.2 for the rank 2 case: if the lattice contains no isotropic vectors (as in the situation at hand), then there exists a non-zero element  $x$  in our rank two lattice such that

$$0 < |b''(x, x)| \leq \left(\frac{4}{3}\right)^{1/2} \cdot d_{L''}^{1/2} = \frac{2}{\sqrt{3}} \cdot \sqrt{3} = 2.$$

In the odd case, respectively even case, this provides us with the elements  $c, e$  as desired.

- We first consider the case of an odd  $b''$ , i.e., there is a vector  $c$  with  $b''(c, c) = \pm 1$  and so  $\langle \pm 1 \rangle$  splits off from  $b''$ . Since the index is a genus invariant we find that  $b'$  is either equivalent to  $b$ , or to  $\text{diag}(1, -1, 3)$ . But the latter has an isotropic vector and hence can be discarded. Concluding, in this situation the form  $b'$  is isometric to  $b$ .
- In the even case, there is an element  $e$  with  $b''(e, e) = \pm 2$ . The Gram matrix with respect to a basis  $\{e, f'\}$  is of the form  $\pm \begin{pmatrix} 2 & \beta \\ \beta & \gamma \end{pmatrix}$  with  $\gamma$  even. Using  $\text{disc}(b'') = \pm 3$  we get  $2\gamma - \beta^2 = \pm 3$  and it follows that  $\beta$  is odd. By looking at the equation modulo 4 we conclude that the case  $-3$  does not occur. In the basis  $\{e, f = f' - \frac{1}{2}(\beta + 1)e\}$  the form has Gram matrix  $\pm A_2$  where  $A_2 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ . This is the matrix for the Dynkin diagram  $A_2$  which will come up again in Section 4.1. To complete the argument, first note that in this case the condition on the signature forces  $b' \simeq \langle -1 \rangle \oplus A_2$  and, finally, remark that the Gram matrix of  $b$  in the basis  $\{(1, 1, 1), (1, -1, 0), (1, 2, 1)\}$  is indeed  $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$  and so also in this case  $b'$  is isometric to  $b$ .

Note that this argument also shows that a positive even definite form of rank 2 with discriminant 3 is isometric to  $A_2$ .

### 1.11 Excursion: Small Lattice Vectors and the Sphere Packing Problem

For a lattice  $L$  without isotropic vectors there is an alternative approach to bound the invariant  $m_L = \min_{y \in L - \{0\}} |b(y, y)|$  as explained in [151, II.1]. See also [36, Ch. 5.3]. It gives a much sharper bound than the one of Theorem 1.10.1.

Let us outline this method. As in Remark 1.10.3 one starts by embedding  $L$  in the real vector space  $V = L_{\mathbb{R}}$  and then one chooses an orthogonal basis  $\mathbf{E}$  such that the matrix for  $\mathbf{b}_{\mathbb{R}}$  becomes the diagonal matrix  $I_{p,n-p}$ . The inner product  $\mathbf{b}$  is then (up to  $n - p$  minus signs) the same as the standard (positive definite) euclidean metric in which  $\mathbf{E}$  becomes an orthogonal basis. In particular, comparing  $\mathbf{b}$  and the euclidean norm  $\|\cdot\|^2$  we have  $|\mathbf{b}(\mathbf{x}, \mathbf{x})| \leq \|\mathbf{x}\|^2$ . So, if a ball of radius  $r$  contains a lattice point  $\mathbf{x} \neq 0$ , then  $0 < \|\mathbf{x}\|^2 \leq r^2$  and so if  $\mathbf{x}$  is non-isotropic, we also have  $0 < |\mathbf{b}(\mathbf{x}, \mathbf{x})| \leq r^2$ .

Next, to obtain a bound for  $r$ , instead of Proposition 1.10.2, one invokes Minkowski's theorem. This result tells us that if a symmetric convex body  $K$  in euclidean  $n$ -space satisfies the volume estimate  $\text{vol}(K) > 2^n \cdot \text{vol}(P_L)$ , with  $P_L$  the fundamental domain as described in (1.28), then  $K$  must contain a non-zero lattice point. Following [151, II, Cor. 1.5], if we apply Minkowski's theorem to balls  $K = B(r)$  of varying radius  $r$ , an optimal value for  $r$  is found which yields a much better estimate for the invariant  $m_L$  (cf. (1.22)):

$$m_L \leq 4 \left( \frac{1}{\omega_n} \right)^{2/n} \cdot d_L^{1/n}, \quad \omega_n = \text{vol}(B(1)) = \frac{\pi^{n/2}}{\Gamma(1 + \frac{n}{2})}.$$

Here  $\Gamma$  is the Gamma function. To see that this is indeed a better estimate, observe that Stirling's formula, which states that  $\Gamma(1 + x)$  is asymptotic to  $x^x e^{-x} \sqrt{2\pi x}$ , implies

$$\omega_n^{-\frac{2}{n}} \sim \frac{1}{e\pi} \cdot n.$$

So the coefficient of  $d_L^{1/n}$  grows linearly in contrast with the exponential coefficient in Proposition 1.10.2. In fact, for small  $n$  one finds the following table. Cf. [151, II.1].

$n$	1	2	3	4	5	6	7	8	9
$4 \left( \frac{1}{\omega_n} \right)^{2/n}$	1	1,27..	1,54..	1,80..	2,06..	2,31..	2,57..	2,82..	3,07..

Applications to the *sphere packing problem* are given in [151, II.7]. This problem asks to find the maximal possible density

$$\rho(P) = \lim_{r \rightarrow \infty} \text{vol}(P \cap Q_r) / \text{vol}(Q_r), \quad Q_r = \{\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n \mid |x_i| \leq r, i = 1, \dots, n\}$$

for sphere packings in  $\mathbb{R}^n$ , that is, unions  $P$  of non-overlapping balls of a fixed radius in  $\mathbb{R}^n$ . A positive definite lattice  $L$  gives rise to a sphere packing, say  $P(L)$ , by centering a ball of radius  $r$  at each lattice point where  $(2r)^2 = m_L$ . Its density turns out to be given by the formula

$$m_L = 4 \left( \frac{\rho(P(L))}{\omega_n} \right)^{2/n} \cdot d_L^{1/n}.$$

Note that Minkowski's inequality translates into  $\rho(P(L)) \leq 1$ .

We further point out some related references. Many record densities for higher ranks are discussed in the monograph [44]. In Chapter 13 of [202] one finds an overview of algebro-geometric constructions leading to many record densities in low rank. Finally, [233, 41] contains recent optimality results concerning  $E_8$ , respectively the Leech lattice. We treat this lattice of rank 24 in some detail in Chapter 5, § 5.1.B, after we explain the relation between codes and lattices.

## 1.12 Positive Definite Lattices

**1.12.A Low rank lattices, and mass formulas.** In Section 1.4 we have seen a few examples of indecomposable positive definite unimodular lattices<sup>8</sup>: the lattice  $\langle 1 \rangle$ , the root lattice  $E_8$  and the lattices  $\Gamma_n$  for  $n$  divisible by 8. M. Kneser [119] has shown that all unimodular lattices of rank  $n \leq 13$  are orthogonal sums of these lattices, and that for  $n = 14, 15, 16$  an indecomposable odd unimodular lattice of rank  $n$  exists and no other one of that rank (up to isometry). Although for larger  $n$  there is no classification, there is a formula for the number of isometry classes of rank  $n$  lattices in terms of  $n$ , the Siegel–Minkowski formula [212, 153]. This formula is a weighted count of the isometry classes  $[\Gamma]$ , counted with weight  $1/|\mathcal{O}(\Gamma)|$ . This is a non-zero rational number since the isometry group of a definite lattice is finite.

Let us consider this for unimodular lattices. For those, as we have seen in the “outlook” on page 48, the rank and parity alone determine the genus. So the genus  $M_n$  of an even unimodular rank  $n$  lattice  $L$  depends on  $n$  alone and gives the “restricted” mass<sup>9</sup>

$$m_n = \text{mass}(M_n) := \sum_{\Gamma \in M_n, n=8k} \frac{1}{|\mathcal{O}(\Gamma)|}.$$

Following [204, Ch. V.2.3], the Siegel–Minkowski formula in this case then states

$$m_n = \frac{B_{2k}}{8k} \prod_{j=1}^{4k-1} \frac{B_j}{4^j},$$

where

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} t^k, \quad B_1 = \frac{1}{6}, B_2 = \frac{1}{30}, B_3 = \frac{1}{30}, B_5 = \frac{5}{66}.$$

The numbers  $B_k$  are the *Bernoulli numbers*. From this formula, after (tedious) calculations (see [204, Ch. V.2.3] and [152, end of Ch. II.9]), we get estimates on the number of isometry classes in  $M_n$ , resulting in Table 1.12.1.

We already remarked on the examples of positive definite lattices of row rank given in Section 1.4. The table integrates M. Kneser’s results we just mentioned

<sup>8</sup>Indecomposable: not the orthogonal sum of non-trivial sublattices.

<sup>9</sup>We shall prove in Chapter 2, that the rank of an even unimodular lattices is divisible by 8 (see Theorem 2.4.2).

Table 1.12.1: Number  $\#M_n$  of isometry classes of even unimodular lattices of given rank  $n$ 

$n = 8k$	8	16	24	32	40
$\#M_n$	1	2	24	$\geq 10^7$	$\geq 10^{51}$

and we see that  $E_8$  is the only rank 8 unimodular quadratic lattice and that the only two rank 16 unimodular quadratic lattices are the two lattices  $E_8 \oplus E_8$  and  $\Gamma_{16}$  (these are non-isometric, as we have seen in Example 1.5.1.2). In the outlook that follows we discuss the case  $n = 24$ .

**Outlook.** From Table 1.12.1 we see that there are 24 classes of unimodular positive definite even lattices of rank 24. Such a lattice is called a **Niemeier lattice** named after H. Niemeier who was the first to investigate these systematically. Among their many properties we quote:

*Theorem 1.12.1 ([167],[44, Ch. 16]).* *The 24 isometry classes of Niemeier lattices are classified by their root sublattice, i.e., the sublattice spanned by the 2-roots. The latter is either 0 (no roots present) or of maximal rank 24.*

There is a complete list of such lattices (loc. cit.). As examples we mention  $\oplus^3 E_8$ ,  $\Gamma_{16} \oplus E_8$  and  $\Gamma_{24}$ . Another example is the Leech lattice  $\Lambda_{24}$  which is to be dealt with in § 5.1.B. It is the unique Niemeier lattice without roots. In the same subsection one also finds the relation between the Golay code and the (unique) Niemeier lattice with root lattice  $A_1^{24}$ .

We shall revisit these lattices in Section 20.3 where they are seen to play a special role in the study of finite groups which act on K3-surfaces.

We have mentioned before that in the unimodular case the genus of an even lattice is determined by its rank. This need not be so in the non-unimodular situation. The mass in this situation is a sum over the isometry classes of forms within a fixed genus:

$$\text{mass}(\mathfrak{g}(L)) := \sum_{\Gamma \in \mathfrak{g}(L)} \frac{1}{|\mathcal{O}(\Gamma)|}.$$

The full Minkowski–Siegel mass formula has many ingredients and is too complicated to state here. Its derivation uses analytic tools and falls outside the scope of this book. For a modern treatment see e.g. [43].

**1.12.B Theta functions and isospectral non-isometric manifolds.** For details on this subject, see [204, Ch. VII.6.5] and [149]. The crucial observation here is that one can associate a theta function to every even non-degenerate positive

definite lattice  $L$  given by

$$\theta_L(z) := \sum_{x \in L} q^{\frac{1}{2}x \cdot x}, \quad q := e^{2\pi iz}.$$

The above series converges on the upper half plane (see loc. cit.). It is called the **theta function of the lattice  $L$** . The theta function encodes the eigenvalues of the Laplace operator on the flat torus  $V/L^*$ , where  $V$  is the real vector space  $L_{\mathbb{R}}$ . Indeed, for each  $x \in L$ , there is a corresponding eigenfunction  $y \mapsto q^{x \cdot y}$  with eigenvalue  $(2\pi)^2 x \cdot x$ . This has an interesting geometric consequence, first remarked by J. Milnor [149]:

**Theorem 1.12.2.** *The two flat tori  $V/L_1$  and  $V/L_2$ ,  $L_1 = \Gamma_{16}$ ,  $L_2 = E_8 \oplus E_8$ , are not isomorphic as Riemannian manifolds but they are isospectral, that is, they have the same spectrum for the Laplace operator.*

*Sketch of the proof.* We should comment on the statement of the theorem. By construction, the two lattice structures are induced from  $V = \mathbb{R}^{16}$  with the euclidean norm and so the induced metric on the tori comes from the standard euclidean metric. In particular, the induced Riemannian structures cannot be isomorphic, since there is no orthogonal transformation of  $\mathbb{R}^{16}$  sending  $L_1$  to  $L_2$  because  $\Gamma_{16}$  and  $E_8 \oplus E_8$  are not isometric as we have seen in Example 1.5.1.2.

As to the spectra of the two Laplace operators, we saw that these are encoded in the associated theta functions. As shown in [204, Ch. VII.6.5], the two theta functions are equal to the unique cusp form  $E_4$  of weight 8, i.e.  $E_4 = 1 + 480 \sum_{m=1}^{\infty} \sigma_7(m) q^m$ , where  $\sigma_k(m) = \sum_{d|m} d^k$ . Since the two lattices  $L_i$ ,  $i = 1, 2$ , are unimodular,  $L_i^* = L_i$  and so, by the definition of the theta functions, the two corresponding tori are isospectral.  $\square$

Theta functions have also been employed in relation to codes. See Chapter II of W. Ebeling's monograph [64]. As will be explained in Section 5.1, codes define lattices and the theta functions in loc. cit. are precisely associated to these lattices. In Section 16.4 we shall discuss the relation between quadratic forms and the Riemann theta function and its cousins. These are theta functions in several variables and are crucial in the study of compact Riemann surfaces.

**1.12.C Unique decomposition.** We finish this section by showing a remarkable property of positive definite lattices which is not valid in the indefinite situation:

**Theorem 1.12.3** ([66], Unique splitting of definite lattices). *A definite lattice can be written in a natural (hence unique) way as an orthogonal sum of indecomposable lattices.*

*Proof.* (Compare [117]) Let  $L$  be a positive definite lattice. A non-zero vector  $x \in L$  is called minimal if it is not the sum  $x = y + z$  of two vectors  $y, z \in L$  whose lengths are strictly shorter than that of  $x$ . Since the procedure of writing vectors as sums of shorter and shorter vectors must stop,  $L$  is spanned by its collection of minimal

vectors. If  $L$  is an orthogonal sum, every minimal vector belongs to just one of the summands.

Let us say that two minimal vectors  $x, x'$  can be connected if there is a finite sequence  $x = x_0, x_1, \dots, x_m = x'$  of minimal vectors with  $x_{j-1} \cdot x_j \neq 0$  for  $1 \leq j \leq m$ . This defines an equivalence relation. Obviously, every equivalence class spans an indecomposable sublattice of  $L$ , and distinct equivalence classes span mutual orthogonal sublattices. As the minimal vectors span  $L$ , these orthogonal sublattices produce the required splitting of  $L$ .  $\square$

### 1.13 Outlook: Indefinite Lattices

Indefinite lattices behave completely differently when compared to the definite case. For example, often there is only one isometry class in a genus. This is in particular true for indefinite unimodular lattices where there is a complete classification which we shall examine in Chapter 2. Recall that there are two types of lattices distinguished by their parity: the even and the odd lattices. In both (unimodular) cases the genus is completely specified by giving the rank and the index. In fact, this also determines the isometry class. We shall state the resulting classification result and illustrate it with a few examples.

**Theorem.** *The isometry class of an indefinite unimodular lattice is uniquely determined by its parity, rank and index. Moreover, even unimodular lattices have index divisible by 8. Indefinite odd unimodular forms are diagonalizable over the integers (hence isometric to orthogonal direct sums of  $\langle 1 \rangle$  and  $\langle -1 \rangle$ ). Indefinite even unimodular lattices of any rank exist as long as the index is divisible by 8.*

**Examples 1.13.1.** 1. Let  $L$  be a unimodular lattice of rank 7 and index  $-1$ . Then  $L$  must be odd and the form is diagonalizable,  $L \simeq \langle 1 \rangle^{\oplus 3} \oplus \langle -1 \rangle^{\oplus 4}$ .

2. A unimodular even lattice of rank 22 and signature  $(3, 19)$  is isometric to

$$\Lambda_{K3} := U^{\oplus 3} \oplus E_8(-1)^{\oplus 2}.$$

This is the so-called *K3 lattice*.

3. An even unimodular lattice of rank 10 and signature  $(1, 9)$  is isometric to the *Enriques lattice*

$$\Lambda_{\text{Enr}} := U \oplus E_8(-1).$$

4. (Rank 2 indefinite unimodular lattices.) Let  $L = \mathbb{Z}e_1 + \mathbb{Z}e_2$  with Gram matrix  $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}$ . We claim that if  $a$  is even then  $L \simeq U$ , and if  $a$  is odd, then  $L \simeq \langle 1 \rangle \oplus \langle -1 \rangle$ . Indeed, if  $a$  is even, use the basis  $\{e_1, e_2 - \frac{1}{2}ae_1\}$ , while if  $a = 2k + 1$  is odd, use the basis  $\{e_2 - ke_1, e_2 - (k + 1)e_1\}$ . This



confirms the classification theorem in the case of unimodular rank 2 lattices of signature  $(1, 1)$ .

Indefinite but non-unimodular lattices also often have a unique isometry class in their genus. See Corollary 14.4.3 which states:

**Theorem 1.13.2** ([171, 1.13.3], [118]). *Let  $L$  be an even non-degenerate indefinite lattice of rank  $r$ . Assume that the discriminant group of  $L$  can be generated by at most  $r - 2$  elements. Then the genus of  $L$  consists of one isometry class.*

**Example 1.13.3.** As soon as  $L$  is even, indefinite, and splits off an even unimodular lattice (this is always a lattice of rank  $\geq 2$ ) the assumption of the above theorem is satisfied. For example, using Example 1.6.8.2, the lattices  $U \oplus E_8(s)$  as well as  $\Gamma_{4k}(s) \oplus \underbrace{U \oplus \cdots \oplus U}_{t \text{ copies}}$ ,  $s \neq 0, k, t \geq 1$  are unique in their genus.

**Historical and Bibliographical Notes.** Most of this Chapter's material is very classical and can be found for instance in the books by J. Cassels [36] and M. Kneser [122]. We especially mention our debt to M. Kneser for the proof of Proposition 1.3.1.2 as well as for the proofs in Section 1.10 (cf. Satz 14.5, respectively §20 in [122]). Less classical is the concept of discriminant form, which figures predominantly in V. Nikulin's works [171]. The thesis [56] of A. Durfee which predates Nikulin's work also introduces and investigates properties of the discriminant form in the guise of "induced form". The reader may further consult Chapter II of the preprint [156] by R. Miranda and D. Morrison which inspired some of our proofs. The procedure to calculate the elementary divisors we gave in Section 1.6 is modeled on the lucid explanation given in § 87 of Seifert–Threlfall's opus [203].

In Sections 1.11 and 1.12 somewhat more recent topics are discussed and there we have given ample references to the literature. Here we only mention the origin of some of the terminology used in these sections. Firstly, Niemeier lattices have been named after the author of [167]. Next, the term "Enriques lattice" is named after the Italian geometer F. Enriques (1871–1946), famous for his work [71] on the classification of algebraic surfaces. Finally, K3 surfaces have been so named by A. Weil in his "Final report on contract AF 18(603)-57", c.f. [248] after the three mathematicians Kummer, Kodaira and Kummer as well as after the mountain K2 in Kashmir which is notably hard to climb.

---

## Indefinite Unimodular Integral Lattices

### Introduction

In this chapter  $(L, b)$  denotes an integral lattice. We shall often write  $x \cdot y$  in place of  $b(x, y)$ . The goal is to give a short and elementary proof of the classification result for indefinite unimodular lattices as announced in Section 1.13:

**Theorem.** *An indefinite unimodular lattice is uniquely determined by its parity, rank and index.*

For odd lattices the proof is easy (see Section 2.3), and in Section 2.4 we use the technique of neighbouring lattices (see Section 1.4) to reduce the even case to the odd case. The proof uses the classification of unimodular lattices in rank  $\leq 4$ , indefinite or not (cf. Theorem 2.2.1), and the  $\sigma$ -invariant which is the "index mod 8". This is explained in Section 2.1. The only deep result on which the proof depends is Meyer's theorem which we shall discuss in Section 3.3 of the next chapter.

In Section 2.5 we describe some applications to the topology of compact manifolds.

### 2.1 Reduction Modulo a Prime and Characteristic Elements

We need a few concepts and results that apply to lattices that are not necessarily indefinite or unimodular. Below we shall make use of reduction modulo 2 which is a special case of reduction modulo a prime  $p$ , which we now explain.

**Definition 2.1.1.** Let  $(L, b)$  be an integral lattice and  $p$  a prime number. Its *reduction modulo  $p$*  consists of the  $\mathbb{F}_p$ -vector space  $L/pL$  equipped with the symmetric  $\mathbb{F}_p$ -bilinear form induced by  $b$ .

If  $\bar{b}$  is the bilinear form induced by  $b$ , then  $\text{disc}(\bar{b}) \in \mathbb{F}_p$ . This discriminant can be zero, even if  $b$  is non-degenerate. However, if  $b$  is non-degenerate with discriminant prime to  $p$ , then  $\bar{b}$  is non-degenerate and so, by definition,  $(L/pL, \bar{b})$  is an inner product space. Let us consider the special case  $p = 2$ .

**Lemma 2.1.2.** *Let  $(L, b)$  be an even integral lattice with  $\text{disc}(b)$  odd. The inner product space  $V = (L/2L, \bar{b})$  has even dimension and the rank of  $L$  is also even.*

*Proof.* Since  $\text{disc}(b)$  is odd, the form  $\bar{b}$  is non-degenerate. We show that  $V$  has even dimension. Let  $x \in V$  be any non-zero vector. Since the product is non-degenerate, by Proposition 1.1.2 there exists  $y \in V$ ,  $y \neq x$ , with  $\bar{b}(x, y) = 1$  and

$\{x, y\}$  spans a non-degenerate plane  $U$  (here we use that  $L$  is even). Then  $U^\perp$  is a non-degenerate subspace of  $V$  and by induction it has even dimension.  $\square$

*Remark 2.1.3.* An inner product space in characteristic 2 such as  $V$  is a symplectic space. These are treated from a general point of view in Appendix A.5.

We use reduction modulo 2 to define so-called characteristic elements:

**Definition 2.1.4.** Let  $L$  be an integral lattice with odd discriminant. We say that  $u \in L$  is a *characteristic* element if  $u \cdot x \equiv x \cdot x \pmod{2}$  for every  $x \in L$ .

**Example 2.1.5.** For an even integral lattice with odd discriminant  $x \cdot x$  is even by definition, and so  $u = 0$  is a characteristic element.

The basic result is as follows.

**Lemma 2.1.6.** *Every lattice  $L$  with odd discriminant has a characteristic element  $u \in L$ . Moreover, its so-called  $\sigma$ -invariant*

$$\sigma(L) := u \cdot u \pmod{8}$$

*does not depend on the choice of the characteristic element. It is an additive invariant, that is, for all lattices  $L$  and  $M$  with odd discriminant we have  $\sigma(L \oplus M) = \sigma(L) + \sigma(M)$ .*

*Proof.* As before we consider the inner product space  $V = L/2L$ . We shall denote the image of  $x$  in  $V$  by  $\bar{x}$ . For simplicity we write  $x \cdot y$  instead of  $b(x, y)$  and similarly for  $\bar{b}(\bar{x}, \bar{y})$ . The function  $\bar{x} \mapsto \bar{x} \cdot \bar{x}$  is linear:

$$\begin{aligned} \overline{\alpha x + \beta y} \cdot \overline{\alpha x + \beta y} &= \bar{\alpha}^2 \bar{x} \cdot \bar{x} + \bar{\beta}^2 \bar{y} \cdot \bar{y} \\ &= \bar{\alpha} \bar{x} \cdot \bar{x} + \bar{\beta} \bar{y} \cdot \bar{y}, \end{aligned}$$

because we are in characteristic 2. Since the correlation map  $\bar{x} \mapsto \bar{x} \cdot -$  is an isomorphism, this function, like every linear function on  $V$ , is of the form  $\bar{u} \cdot x$  for a unique  $\bar{u} \in V$ . Any preimage  $u \in L$  then satisfies

$$u \cdot x \equiv x \cdot x \pmod{2},$$

and so  $u$  is a characteristic element.

We note that  $u \cdot u \pmod{8}$  is indeed an invariant of  $L$ . Since  $\bar{u}$  is unique, any other characteristic element is of the form  $u' = u + 2x$  and we have

$$\begin{aligned} u' \cdot u' &= u \cdot u + 4 \underbrace{(u \cdot x + x \cdot x)}_{\equiv 0 \pmod{2}} \\ &\equiv u \cdot u \pmod{8}. \end{aligned}$$

Characteristic elements are clearly additive.  $\square$

*Remark 2.1.7.* The above concerns only lattices with odd discriminant, the only cases we need later on.

**Example 2.1.8.** • Let  $L$  be the symmetric lattice  $L = \oplus^p \langle 1 \rangle \oplus \oplus^q \langle -1 \rangle$ . Since  $\pm e$  is characteristic for the unimodular lattice  $\mathbb{Z} \cdot e$  with  $e \cdot e = \pm 1$  and because of additivity,  $\sigma(L) \equiv p - q = \tau(L) \pmod{8}$ , where, we recall,  $\tau(L)$  is the index of  $L$ .

- For an even lattice the zero vector is a characteristic element and so for even lattices we have  $\sigma(L) \equiv 0 \pmod{8}$ .

## 2.2 Classification in Rank At Most Four

To prove the classification result mentioned in the introduction to this chapter we first need a classification result for small rank.

**Theorem 2.2.1** (Classification in rank  $\leq 4$ ). *Let  $L$  be a unimodular lattice of rank at most 4. Then either  $L$  is odd and diagonalizable, or, if  $L$  is even,  $L \simeq U$ , or  $L \simeq U \oplus U$ .*

*Proof.* We use induction on the rank  $n$ . The assertion being obvious for  $n = 1$  we assume  $n > 1$ . We first apply the estimate of Proposition 1.10.2, which in this case states that  $L$  contains either an isotropic vector or a vector  $x$  with  $0 < |x \cdot x| \leq (4/3)^{3/2} < 2$ . So there are two possibilities:

**First case** There is a vector  $x \in L$  with  $x \cdot x = \pm 1$ . Then by Corollary 1.3.4,  $L = \mathbb{Z}x \oplus x^\perp$ . If  $L' = x^\perp$  is odd, it has an orthogonal basis and we are done. Otherwise, by induction  $L' = U$  with basis  $\{y, z\}$  for which  $y \cdot y = z \cdot z = 0$  and  $y \cdot z = 1$ . Then  $\{x + y, x \mp z, x + y \mp z\}$  forms an orthogonal basis for  $L$ .

**Second case** In this case we assume there is no vector  $x \in L$  with  $x \cdot x = \pm 1$ . Then there is a primitive vector  $x_1 \neq 0$  with  $x_1 \cdot x_1 = 0$ . It is part of a basis  $\{x_1, \dots, x_n\}$  for  $L$ . Let  $\{x_1^*, \dots, x_n^*\}$  be the dual basis. Since  $L$  is unimodular this is a basis for  $L$ . The sublattice  $L_1 = \mathbb{Z}x_1 + \mathbb{Z}x_1^*$  has Gram matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}.$$

Example 1.13.1.5 determines the isometry class of  $L_1$  according to the parity of  $a$ . If  $a$  is odd,  $L_1$  is diagonalizable and there is a vector  $x$  with  $x \cdot x = \pm 1$ , which we have excluded. So  $a$  is even and  $L_1 \simeq U$ . By Corollary 1.3.4,  $L \simeq U \oplus L_1^\perp$ . Since  $L_1^\perp$  is unimodular and does not contain a vector with  $x \cdot x = \pm 1$ ,  $L_1^\perp$  is either 0 or of rank 2 and not diagonalizable. In that case  $L_1^\perp \simeq U$  by induction.  $\square$

**Corollary 2.2.2.** *Let  $L$  be an indefinite unimodular lattice, then*

- $L$  contains an isotropic vector, that is, a non-zero vector  $x$  with  $x \cdot x = 0$ ;
- $L$  is isometric to either  $U \oplus L'$  or to  $W \oplus L''$  where  $L'$  as well as  $L''$  are unimodular,  $U$  is the hyperbolic plane and  $W = \langle 1 \rangle \oplus \langle -1 \rangle$ .

*Proof.* For rank at most 4 the first statement follows from the preceding theorem. For larger rank Meyer's theorem, Corollary 3.3.4, guarantees the existence of an isotropic vector.

Once we have a primitive  $x \in L$  with  $x \cdot x = 0$ , examining the last part of the proof of Theorem 2.2.1 we see that the second assertion is true.  $\square$

### 2.3 Odd Indefinite Forms

The lattices  $\oplus^p \langle 1 \rangle \oplus \oplus^q \langle -1 \rangle$  with  $p, q \geq 1$  provide examples of odd indefinite unimodular lattices. The next theorem shows that these are all.

**Theorem 2.3.1.** *Every odd indefinite unimodular lattice is diagonalizable, that is, isometric to an orthogonal direct sum of copies of  $\langle 1 \rangle$  and  $\langle -1 \rangle$ . In particular, such lattices are classified by their rank and index.*

*Proof.* We use induction with respect to the rank. Let  $L$  be an odd lattice. For rank at most 4 the assertion follows from Theorem 2.2.1. Next, apply the representability result Corollary 2.2.2 to find a non-zero primitive  $x_1 \in L$  with  $x_1 \cdot x_1 = 0$ . Complete this to a basis  $\{x_1, \dots, x_n\}$  of  $L$  and form the dual basis  $\{x_1^*, \dots, x_n^*\}$  of  $L$  (since  $L$  is unimodular this is also a basis for the lattice). Since  $L$  is odd, there is an index  $j$  such that  $x_j^* \cdot x_j^*$  is odd. If  $x_1^* \cdot x_1^*$  happens to be odd, we let  $L_1 = \mathbb{Z}x_1 + \mathbb{Z}x_1^*$ . If however  $x_1^* \cdot x_1^*$  is even but  $x_k^* \cdot x_k^*$  odd for some  $k > 1$ , then set  $L_1 = \mathbb{Z}x_1 + \mathbb{Z}(x_1^* + x_k^*)$ . In both cases  $L_1$  is a sublattice of  $L$  such that the Gram matrix with respect to the given basis is  $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}$  with  $a$  odd. From Example 1.13.1.5, we know that  $L_1 \simeq \langle 1 \rangle \oplus \langle -1 \rangle$  since  $a$  is odd. So  $L \simeq \langle 1 \rangle \oplus \langle -1 \rangle \oplus L_1^\perp$ . Now choose a sign so that  $\langle \pm 1 \rangle \oplus L_1^\perp$  is indefinite and apply the induction hypothesis to this odd unimodular indefinite lattice.  $\square$

### 2.4 Even Indefinite Forms

**Theorem 2.4.1.** *Two even indefinite unimodular lattices with the same rank and index are isometric.*

*Proof.* Let  $L$  be an even indefinite unimodular lattice. By Corollary 2.2.2,  $L$  is isometric to  $L' \oplus U$  where  $L'$  is an even unimodular lattice. Note that  $L'$  might be definite so that a simple induction argument is not possible.

Instead, we employ the technique of neighbouring lattices to link even and odd unimodular lattices so that we can use our previous classification for odd lattices. To be specific, we use the construction detailed in Example 1.7.A and start with the odd lattice  $L' \oplus W$ ,  $W = \langle 1 \rangle \oplus \langle -1 \rangle$ . The sublattice consisting of vectors  $x \in L' \oplus W$  with  $x \cdot x$  even is isometric to  $L' \oplus U(2)$ . The even neighbours of  $L' \oplus W$  all contain this lattice and are contained in  $L'^* \oplus \frac{1}{2}U(2) \simeq L' \oplus \frac{1}{2}U(2)$ . So  $L'$  does

not play a role in the argument of Example 1.7.A.2 (where  $L' = 0$ ) and this shows that there are two even neighbours, both isometric to  $L' \oplus U = L$ . Now suppose we have another even indefinite unimodular lattice  $\Lambda$  with the same rank and index as  $L$ . We may write it again as  $\Lambda' \oplus U$ , and consider  $\Lambda' \oplus W$ . As for  $L' \oplus W$ , the even neighbours of  $\Lambda' \oplus W$  are isometric to  $\Lambda$ . Now the two odd unimodular lattices  $L' \oplus W, \Lambda' \oplus W$  are indefinite and have the same rank and index. So, by the classification in the odd case, Theorem 2.3.1, they are isometric. Hence so are their neighbours. It follows that  $L$  and  $\Lambda$  are isometric.  $\square$

What is missing is an exhaustive list of even indefinite unimodular lattices. We have seen that  $E_8$  is an even unimodular lattice and so is  $E_8(-1)$ . So any orthogonal direct sum of copies of hyperbolic planes and copies of  $E_8$  or  $E_8(-1)$  must belong to the list. To see that the list is complete we need a property of the index.

**Theorem 2.4.2.** *For every unimodular lattice  $L$ , indefinite or not, we have  $\sigma(L) = \tau(L) \pmod{8}$ , that is, the index modulo 8 is the  $\sigma$ -invariant. If, moreover,  $L$  is even, the index is divisible by 8.*

*Proof.* Recall from Lemma 2.1.6 that every unimodular lattice  $L$  has an invariant  $\sigma(L) \in \mathbb{Z}/8\mathbb{Z}$  and we saw in Example 2.1.8 that  $\sigma(L) \equiv \tau(L)$  for unimodular lattices  $L$  that are diagonalizable. By the classification result for odd lattices this comprises all odd unimodular indefinite lattices. If  $L$  is even,  $M = L \oplus \langle 1 \rangle \oplus \langle -1 \rangle$  is odd and by additivity  $\sigma(L) = \sigma(M) \equiv \tau(M) = \tau(L) \pmod{8}$ . On the other hand, for even  $L$  we have seen (again in Example 2.1.8) that  $\sigma(L) = 0$  and so  $\tau(L) \equiv 0 \pmod{8}$ .  $\square$

According to Lemma 2.1.2 the rank  $r$  of any even unimodular lattice is even. Theorem 2.4.2 states that the index  $\tau$  is divisible by 8. Using the pairs  $(r, \tau)$  with  $r > 0$  even and  $|\tau| < r$  divisible by 8, the lattices  $\oplus^a E_8(\pm 1) \oplus^b U$  with  $a = \frac{1}{8}|\tau|$  and  $b = \frac{1}{2}(r - |\tau|)$  realize all possible ranks and indices for even indefinite unimodular lattices. If we combine the above two theorems, we deduce the following final classification result.

**Corollary 2.4.3** (Existence and uniqueness for indefinite even unimodular lattices). *Let  $L$  be an even unimodular and indefinite lattice of (necessarily even) rank  $r$  and index  $\tau = 8a\varepsilon$ , where  $a$  is a non-negative integer and  $\varepsilon = \pm 1$ . Then  $L$  is isometric to*

$$\underbrace{(E_8 \oplus \cdots \oplus E_8)(\varepsilon)}_{a \text{ summands}} \oplus \underbrace{U \oplus \cdots \oplus U}_{b \text{ summands}}, \quad b = \frac{1}{2}(r - |\tau|).$$

**Example 2.4.4.** Applying this to the lattice  $E_8 \oplus E_8(-1)$  a lattice of rank 16 and index 0, we obtain  $E_8 \oplus E_8(-1) \simeq \oplus^8 U$ .

## 2.5 Applications to Topology

**2.5.A The intersection form on manifolds.** Consider a compact connected oriented topological manifold  $X$  of dimension  $4d$  with cohomology ring  $H^*(X, \mathbb{Z})$ . The orientation gives an isomorphism  $H^{4d}(X, \mathbb{Z}) \simeq \mathbb{Z}$  so that the cup-product form on the middle cohomology group modulo torsion

$$H_X := H^{2d}(X, \mathbb{Z})/\text{torsion},$$

becomes a bilinear pairing

$$S_X : H_X \times H_X \longrightarrow \mathbb{Z}, \tag{2.1}$$

which, by Poincaré duality, is unimodular. It is called the *intersection form* of  $X$ .<sup>1</sup> The intersection form is symmetric since  $2d$  is even. Any form  $b$  with  $b = S_X$  for an oriented topological or differentiable manifold  $X$  is said to be topologically, respectively differentiably *represented*. If  $b$  and  $b'$  are represented, then so is  $b \oplus b'$ . To see this, one uses the connected sum construction: if  $X$  and  $X'$  are two manifolds of the same dimension, say  $d$ , their *connected sum*  $X \# X'$  is constructed by taking out a  $d$ -disc from  $X$  and  $X'$  and glueing  $X$  and  $X'$  along the boundary spheres. This can be done differentiably if  $X$  and  $X'$  are smooth manifolds. See e.g. [150].

The result we are referring to reads as follows.

**Lemma 2.5.1.** *If  $X, X'$  are two four-manifolds, then we have  $S_{X \# X'} = S_X \oplus S_{X'}$ .*

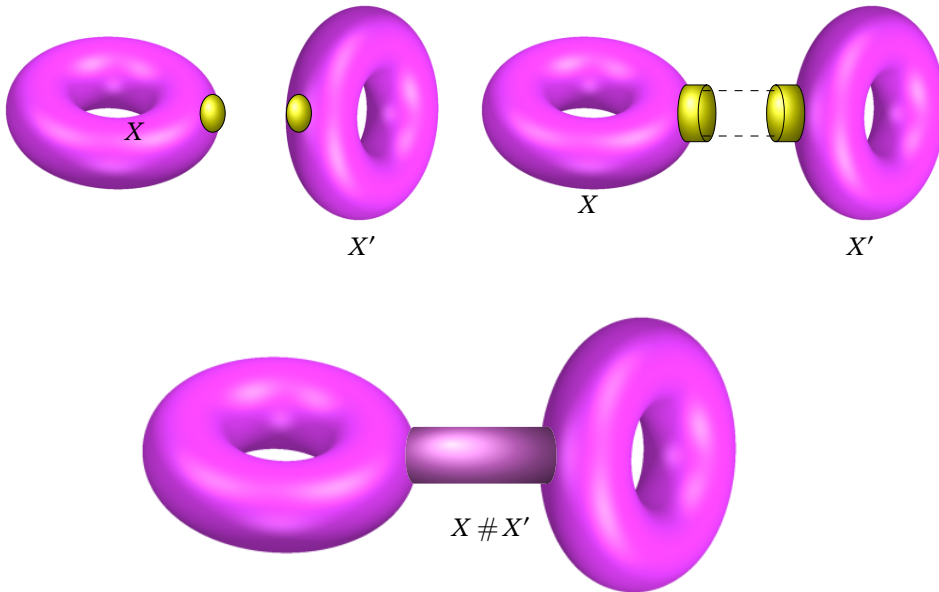
Write the signature of the intersection form  $S_X$  as  $(b_X^+, b_X^-)$ . If  $S_X$  happens to be indefinite, its isometry class is completely determined by the parity (even or odd) and the index of  $S_X$ . We want to apply this to simply connected manifolds of dimension 4. In that case the cohomology has no torsion anyway (see Example 2.5.5).

For such four-manifolds we have a celebrated result of Freedman [73] which – in simplified form – states:

**Theorem 2.5.2.** *The oriented homeomorphism type of a simply connected four-manifold  $X$  is completely determined by  $S_X$  and, moreover, any unimodular form can occur in this way as the intersection form of some simply connected four-manifold.*

Now as we have seen in Section 1.12, the number of non-isomorphic definite forms goes up quite drastically with the rank and so this holds also for the number of non-isomorphic four-manifolds with definite intersection form. However, the situation changes dramatically for the subclass of differentiable four-manifolds. Indeed, Donaldson obtained a striking result:

<sup>1</sup>Topologists usually say that the intersection form is non-degenerate which means that the form  $S_X$  with respect to a chosen integral basis for  $H_X$  gives an invertible matrix, which is equivalent to unimodularity. Under Poincaré-duality cup product of cohomology classes translates into intersection of homology classes. In the middle homology this gives the intersection numbers of two (oriented) transversely intersecting cycles. This explains the terminology.

Connected sum of  $X$  and  $X'$ 

**Theorem 2.5.3** (Donaldson [54]). *If a simply connected differentiable four-manifold  $X$  has a definite intersection form it is diagonalizable over  $\mathbb{Z}$  and so*

$$S_X = \langle 1 \rangle \oplus \cdots \oplus \langle 1 \rangle \text{ or } S_X = \langle -1 \rangle \oplus \cdots \oplus \langle -1 \rangle.$$

*In particular, it cannot be an even form.*

Hence, in a sense "most" topological four-manifolds with definite intersection form do not admit differentiable structures. Together with the classification results for indefinite unimodular forms in this chapter, it follows that the only forms that can possibly be differentiably represented are the diagonal forms, or else, forms isometric to direct sums of the hyperbolic plane and the forms  $E_8(\pm 1)$ . To find out which, will be investigated in the next subsection.

**2.5.B Representability by differentiable four-manifolds.** A word of warning here. Freedman's theorem 2.5.2 tells us that for any simply connected four-manifold  $X$  its intersection form  $S_X$  is a complete invariant and so, if for two such manifolds the intersection forms are isometric, the manifolds are oriented homeomorphic. However, if these manifolds have a differentiable structure, the homeomorphism need not be realizable by a diffeomorphism. Indeed, there are counterexamples. See [15, Ch. IX].

Let us now go down the list of allowable unimodular forms. As explained in Appendix B.3.(1), the form  $\langle 1 \rangle$  is the intersection form of the complex projec-



tive plane  $\mathbb{P}^2$  and then  $\langle -1 \rangle$  is the one of the plane with the opposite orientation. Lemma 2.5.1 then implies that by taking connected sums all odd unimodular diagonal lattices can be represented differentiably.

The hyperbolic plane  $U$  is represented by a product of two 2-spheres, or, what is the same, by  $Q = \mathbb{P}^1 \times \mathbb{P}^1$  where  $\mathbb{P}^1$  is the complex projective line (or Riemann sphere). Note also that  $Q$  is isomorphic to a smooth complex quadric surface in  $\mathbb{P}^3$ . See loc. cit. What about other even forms? One might first ask about topological restrictions. There are classical topological invariants, e.g., the Stiefel–Whitney classes  $w_k(X) \in H^k(X, \mathbb{F}_2)$ , where the coefficient field is  $\mathbb{F}_2$ , the field of two elements. See e.g. [152] for their definition and properties. For us the second Stiefel–Whitney class turns out to be pertinent. As shown in loc. cit., for four-dimensional manifolds  $X$  satisfies

$$b'(x, x) = b'(w_2(X), x) \text{ for all } x \in H^2(X, \mathbb{F}_2).$$

**Proposition 2.5.4** (Criterion for even forms). *Let  $X$  be a compact differentiable four-manifold such that  $H^*(X, \mathbb{Z})$  has no 2-torsion. Then  $S_X$  is even if and only if the second Stiefel–Whitney class  $w_2(X)$  vanishes.*

*Proof.* Let us relate  $w_2$  to the integral intersection form. To do this, consider the short exact sequence of groups

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

and the following portion of the long exact sequence in cohomology

$$\cdots \rightarrow H^2(X, \mathbb{Z}) \xrightarrow{\times 2} H^2(X, \mathbb{Z}) \xrightarrow{\pi} H^2(X, \mathbb{Z}/2\mathbb{Z}) \rightarrow \cdots \quad (2.2)$$

This becomes a short exact sequence if the integral cohomology has no 2-torsion and then there is an element in  $H^2(X, \mathbb{Z})$  that maps to  $w_2(X)$ . This element is then an integral characteristic element and so, if  $w_2(X) = 0$ , the intersection form is even and conversely.  $\square$

**Example 2.5.5.** Let  $X$  be a simply connected four-manifold. For these  $H_1(X, \mathbb{Z}) = 0$  and then  $0 = \text{Tors}(H_1(X, \mathbb{Z})) = \text{Tors}(H^2(X, \mathbb{Z}))$ , by the universal coefficient theorem and Poincaré duality (cf. for example [86, Ch. 28]). Hence there is no torsion at all in the cohomology. So, if  $w_2(X) = 0$ , the intersection form is even.

If  $w_2 = 0$  there is a well-known restriction on the index:

**Theorem 2.5.6** (Rohlin [196]). *For a compact differentiable four-manifold  $X$  with  $w_2(X) = 0$ , the index is divisible by 16.*

Proposition 2.5.4 and Theorem 2.5.6 have the following consequence.

**Corollary 2.5.7.** *Let  $X$  be a simply connected compact differentiable four-manifold with even intersection form. Then the index of  $S_X$  is divisible by 16.*

**2.5.C Representability using complex surfaces.** Let us consider what happens for complex surfaces, that is four-manifolds  $X$  which admit a complex structure. In that case, there are invariants in integral cohomology refining the Stiefel–Whitney classes, the Chern classes  $c_i(X) \in H^{2i}(X, \mathbb{Z})$ . The class  $w_2(X)$  is just the modulo 2 restriction of  $c_1(X)$ . Hence if  $H^*(X, \mathbb{Z})$  has no 2-torsion,  $c_1(X)$  is an integral characteristic element.

**Corollary 2.5.8.** *Let  $X$  be a simply connected complex manifold of dimension 2 such that  $c_1(X)$  is 2-divisible in  $H^2(X, \mathbb{Z})$ . Then  $S_X$  is an even form. Examples include K3 surfaces (see below) and smooth hypersurfaces in  $\mathbb{P}^3$  of even degree. See Table B.3.1.*

For complex surfaces  $X$  the class  $-c_1(X)$  admits an alternative description as the cohomology class of the canonical line bundle  $K_X = \Lambda^2 T_X^*$  since  $c_1(X) = c_1(T_X) = c_1(\Lambda^2 T_X) = -c_1(\Lambda^2 T_X^*)$ . Holomorphic sections of  $K_X$  are exactly the holomorphic 2-forms. So, if for example  $X$  admits a nowhere vanishing holomorphic 2-form, the bundle  $K_X$  is trivial and  $c_1(X) = 0$ .

The invariant  $c_2(X) \in H^4(X, \mathbb{Z}) \simeq \mathbb{Z}$  is "purely topological": it can be identified with the Euler number  $e(X)$ . The index of the intersection form  $S_X$  can be expressed in terms of  $c_1(X)$  and  $c_2(X)$ <sup>2</sup> as follows.

$$\tau(X) = \frac{1}{3}(c_1^2(X) - 2c_2(X)) = \frac{1}{3}(K_X \cdot K_X - 2e(X)).$$

Hence, if  $K_X$  is the trivial line bundle, the index is determined by the Euler number  $e(X)$ .

As we have seen, an even indefinite lattice of index  $\pm 16b$ ,  $b \geq 0$ , is of the form

$$E_{a,\pm b} := \oplus^a U \oplus \oplus^{2b} E_8(\pm 1), \quad a \geq 1.$$

The simplest indefinite forms of index 16 are  $E_{1,\pm 1} = U \oplus E_8 \oplus E_8$  and it is not known whether these are representable by differentiable manifolds and neither is this known for  $E_{2,\pm 1}$ . However  $E_{3,-1}$  does occur: it is isometric to the intersection lattice  $S_{K3}$  where K3 is a K3-surface. See Appendix B.3.(4). A K3 surface with its opposite orientation,  $-K3$  represents  $E_{3,1}$  and so, using connected sums we can represent  $E_{3m,\pm m}$ . Since  $U = E_{1,0}$  is represented by the quadric  $Q = \mathbb{P}^1 \times \mathbb{P}^1$ , for any pair of integers  $(m, n)$  with  $m \geq 0$  and  $n \geq 1$  we can thus represent  $E_{3m+n,\pm m}$  by the differentiable four-manifold

$$X(\pm m, n) = \pm \underbrace{[K3 \# \cdots \# K3]}_{m \text{ copies}} \# \underbrace{Q \# \cdots \# Q}_{n \text{ copies}}. \quad (2.3)$$

The following classical conjecture would imply that these cover all (differentiably) representable lattices.

**Conjecture** (The 11/8 Conjecture). For every simply connected oriented differentiable four-manifold  $X$  with even intersection form we have the inequality

$$b_2(X) \geq \frac{11}{8} |\tau(X)|.$$

<sup>2</sup>cf. Appendix B.2 for some further details and references.

Indeed, we show that any  $X$  as in the conjecture must then be homeomorphic to one of the manifolds  $X(\pm m, n)$  of (2.3). First of all, by Donaldson's result, Theorem 2.5.3, the form must be indefinite. Next, Rohlin's theorem shows that its index is divisible by 16 so that  $\pm m = \tau(X)/16$  is an integer. Moreover,

$$n = \frac{1}{16}(8b_2(X) - 11|\tau(X)|)$$

is an integer since an even unimodular intersection form is isometric to a direct sum of copies of  $U$  and  $\pm E_8$  so that  $b_2$  is even. The 11/8 Conjecture just says that this number is non-negative. It follows that  $X$  is oriented homeomorphic to  $X(\pm m, n)$ .

The conjecture is true for complex surfaces. For a proof see e.g. [15, Ch. IX.3] where also the representability of indefinite forms by complex and almost complex surfaces is discussed. In particular, any such surface is oriented homeomorphic to some  $X(m, n)$  and the two forms  $E_{1,1}$  or  $E_{2,1}$  can only be represented, if at all, by non-algebraic differentiable four-manifolds.

**Historical and Bibliographical Notes.** This chapter is based on Milnor's approach from [151]. The application to the homotopy classification of four-manifolds [151, Thm. V.1.5] has been superseded by Freedman's groundbreaking work [73] and, in the differentiable setting, by Donaldson's results [54, 55]. This leads to the applications we present here. It is an extract from [15, Chapter IX]. See als [183]. For more on the topology of surfaces, see [184].

## Quadratic Forms over $\mathbb{Q}$ and $\mathbb{Q}_p$

### Introduction

In this chapter we discuss the classification of non-degenerate quadratic forms over the rationals. We have seen (cf. Proposition 1.1.4) that such forms are diagonalizable. However, it is not straightforward to decide effectively whether two given diagonal forms are isometric as illustrated by the following calculation. Consider the quadratic form in two variables  $2x^2 + 3y^2$ . We claim that it is isometric to  $\frac{6}{5}x^2 + 5y^2$ . This can be shown as follows.

$$\begin{aligned} 2x^2 + 3y^2 &= 2u^2 + 4uv + 5v^2, & x &= u + v, y = v, \\ &= 2u^2 + 5\left(v + \frac{2}{5}u\right)^2 - \frac{4}{5}u^2 \\ &= \frac{6}{5}u^2 + 5w^2, & w &= v + \frac{2}{5}u. \end{aligned}$$

Let us sketch how to solve the classification problem for (diagonalized) rational forms effectively.

**Step 1: Local classification.** The basic local invariant is the *Hasse invariant*  $\varepsilon_v(q)$  of  $q$ , obtained from the Hilbert symbols  $(a, b)_v$ ,  $a, b \in \mathbb{Q}_v^\times$ , discussed in Appendix A.4:

$$\varepsilon_v(q) := \prod_{i < j} (a_i, a_j)_v, \text{ with } q(x) = \sum a_j x_j^2, \quad (3.1)$$

where we tacitly use the convention that an empty product is 1 so that  $\varepsilon_v(q) = 1$  for a rank one form.

We shall show (Proposition 3.1.3) that this is indeed an invariant of  $q_v$ . Then, for a finite place  $p$  we derive the following classification result (cf. Theorem 3.3.1):

$$q \text{ and } q' \text{ are isometric over } \mathbb{Q}_p \iff \begin{cases} \text{rank}(q) = \text{rank}(q') \\ \text{disc}(q) = \text{disc}(q') \text{ (up to squares)} \\ \varepsilon_p(q) = \varepsilon_p(q'). \end{cases}$$

As to the place at infinity, one knows from linear algebra that real quadratic forms are classified by their rank and index (cf. also Theorem 8.1.5):

$$q \text{ and } q' \text{ are isometric over } \mathbb{R} \iff \begin{cases} \text{rank}(q) = \text{rank}(q') \\ \tau(q) = \tau(q'). \end{cases}$$

**Step 2: Global classification.** In Section 3.3 we take up the classification over  $\mathbb{Q}$  where we show the *Hasse principle* which states that two non-degenerate forms

$q, q'$  over  $\mathbb{Q}$  are isometric if and only if  $q_v \simeq q'_v$  for all places  $v \in \mathcal{P}$ . We deduce this important principle from the Hasse-Minkowski theorem which states that a rational form represents 0 if and only if it does so at all places. We shall not prove this theorem, but refer to [204, IV.3.2]. So the Hasse principle and the local classification imply the classification result over the rationals. Explicitly, we have for non-degenerate forms  $q$  and  $q'$  :

$$q \text{ and } q' \text{ are isometric over } \mathbb{Q} \iff \begin{cases} \text{rank}(q) = \text{rank}(q') \\ \tau(q) = \tau(q') \\ \text{disc}(q) = \text{disc}(q') \text{ (up to squares)} \\ \varepsilon_p(q) = \varepsilon_p(q') \text{ for all primes } p. \end{cases}$$

Let us finish this introduction by calculating the Hasse invariants for the forms at the start of this introduction. These two forms,  $2x^2 + 3y^2$  and  $\frac{6}{5}x^2 + 5y^2$ , are manifestly positive definite, have the same discriminant, and so, to show that they are isometric it suffices to prove that  $(2, 3)_p = (\frac{6}{5}, 5)_p$  for all prime numbers  $p$ . First note that by Theorem A.4.4 we have  $(2, 3)_p = 1$  for  $p \neq 2, 3$ , and  $(2, 3)_2 = -1$  and  $(2, 3)_3 = (\frac{2}{3}) = -1$ . Let us check that we get the same values for the other Hilbert symbol, using the standard rules:

$$\begin{aligned} (\frac{6}{5}, 5)_p &= (5, \frac{6}{5})_p \text{ by (A.7)} \\ &= (5, -6)_p \text{ by (A.11)} \\ &= (-6, 5)_p \text{ by (A.7)} \\ &= (-2, 5)_p(3, 5)_p \text{ by (A.10)}. \end{aligned}$$

Again by Theorem A.4.4 this equals 1 unless  $p = 2, 3, 5$ . For  $p = 2$  we get  $(-2, 5)_2(3, 5)_2 = (-1) \cdot 1 = -1$ , for  $p = 3$  one gets  $(-2, 5)_3(3, 5)_3 = 1 \cdot (\frac{5}{3}) = -1$ , and finally  $(-2, 5)_5(3, 5)_5 = (\frac{-2}{5}) \cdot (\frac{3}{5}) = 1$ . So indeed, for this example the two sets of local invariants are the same.

### 3.1 The Hasse Invariant is Well Defined

In this section  $(V, q)$  is a quadratic space over a field  $k$  of characteristic  $\neq 2$ .

We introduce a bilinear form by the formula

$$x \cdot y = \frac{1}{2}(q(x+y) - q(x) - q(y)) \quad (3.2)$$

so that  $x \cdot x = q(x)$ .<sup>1</sup> Occasionally we shall speak of the *hyperbolic plane*  $ke+kf$ . As for integer lattices, this means that  $e \cdot e = f \cdot f = 0$  and  $e \cdot f = 1$ .

<sup>1</sup>Note that the polar form  $b_q$  differs from this form by a factor 2.

The concept of a *contiguous chain of orthogonal bases* will be used to show that the Hasse invariant does not depend on the particular diagonalization. By definition, such a chain starts from a given orthogonal basis and at each step one forms a new orthogonal basis by replacing a finite number of vectors of the basis, making sure that at least one vector stays the same.

**Example 3.1.1.** Take  $\mathbb{R}^3$  with the standard euclidean metric. Let  $\{e_1, e_2, e_3\}$  be orthonormal. Take a rotation in the plane spanned by  $\{e_2, e_3\}$  giving  $\{e_1, e'_2, e'_3\}$  followed by a rotation in the plane  $\{e_1, e'_2\}$  giving  $\{e'_1, e''_2, e'_3\}$ . This gives the contiguous chain

$$\{e_1, e_2, e_3\} \rightarrow \{e_1, e'_2, e'_3\} \rightarrow \{e'_1, e''_2, e'_3\}.$$

Returning to the operation of contiguity, we have the following result:

**Proposition 3.1.2.** *Suppose that  $\dim V \geq 3$ . Then any two orthogonal bases are connected by a contiguous chain of orthogonal bases.*

*Proof.* Let  $\mathbf{E} = \{e_1, \dots, e_n\}$  and  $\mathbf{E}' = \{e'_1, \dots, e'_n\}$  be two orthogonal bases. We distinguish three situations.

**1:** *the vectors  $e_1, e'_1$  span a plane  $P$ ,  $q|_P$  is non-degenerate and  $V = P \oplus P^\perp$ .* In this case we can find  $f_1, f'_1 \in P$  such that  $P = ke_1 \oplus kf_1 = ke'_1 \oplus kf'_1$ . If  $g_3, \dots, g_n$  is an orthogonal basis of  $P^\perp$ , the following is a contiguous chain

$$\mathbf{E} \rightarrow (e_1, f_1, g_3, \dots, g_n) \rightarrow (e'_1, f'_1, g_3, \dots, g_n) \rightarrow \mathbf{E}'.$$

**2:**  *$\{e_1, e'_2\}$  span a non-degenerate plane.* After interchanging  $e'_1$  and  $e'_2$  in  $\mathbf{E}'$ , we can apply the argument from case (1).

**3:** *the remaining case, i.e.*

$$\det \begin{pmatrix} q(e_1) & e_1 \cdot e'_j \\ e_1 \cdot e'_j & q(e'_j) \end{pmatrix} = 0 \text{ for } j = 1, 2. \quad (3.3)$$

If this is the case, the idea is to find a vector  $e = e'_1 + ae'_2$ ,  $a \neq 0$ , such that

- the plane  $ke_1 + ke$  is non-degenerate,
- $e$  is not isotropic.

Assuming the existence of such a vector  $e$ , the plane spanned by  $\{e'_1, e'_2\}$  has a second orthogonal basis  $\{e, e''_2\}$  since  $e$  is not isotropic. Now

$$\mathbf{E}'' = \{e, e''_2, e'_3, \dots, e'_n\}$$

is an orthogonal basis of  $V$  and  $\mathbf{E}' \rightarrow \mathbf{E}''$  is a contiguous chain. By assumption,  $ke_1 + ke$  is a plane to which  $q$  restricts non-degenerately and as in case 1 there is a contiguous chain from  $\mathbf{E}$  to  $\mathbf{E}''$ , hence also from  $\mathbf{E}$  to  $\mathbf{E}'$ .

Let us check that there indeed exists a vector  $e = e'_1 + ae'_2$  as desired. The first condition reads

$$\det \begin{pmatrix} q(e_1) & e_1 \cdot e'_1 + a(e_1 \cdot e'_2) \\ e_1 \cdot e'_1 + a(e_1 \cdot e'_2) & q(e'_1) + a^2q(e'_2) \end{pmatrix} \neq 0.$$

Using (3.3) this is seen to simplify into  $-2a(e_1 \cdot e'_1)(e_1 \cdot e'_2) \neq 0$ . The second condition,  $q(e) = q(e'_1 + ae'_2) \neq 0$ , translates into  $a^2 \neq -\frac{q(e'_1)}{q(e'_2)}$ . Since (3.3) implies that  $e_1 \cdot e'_j \neq 0$  for  $j = 1, 2$ , we can find a vector  $e$  satisfying the requirements if and only if there exists an  $a \neq 0$  with  $a^2 \neq -\frac{q(e'_1)}{q(e'_2)}$ . These conditions eliminate at most three values of  $a$  and so  $a$  can be found if  $k \neq \mathbb{F}_3$ . For the field  $\mathbb{F}_3$  the equations (3.3) for  $j = 1, 2$  read

$$\begin{aligned} q(e_1)q(e'_1) &= (e_1 \cdot e'_1)^2 = 1 \\ q(e_1)q(e'_2) &= (e_1 \cdot e'_2)^2 = 1, \end{aligned}$$

and hence  $q(e'_1)/q(e'_2) = 1$ . So if we take  $a = 1$ , then  $a \neq 0$  and  $a^2 \neq -q(e'_1)/q(e'_2)$ .  $\square$

We turn now to vector spaces over  $\mathbb{Q}_v$ ,  $v \in \mathcal{P}$ , and show:

**Proposition 3.1.3.** *The Hasse invariant is well defined, i.e., independent of the choice of orthogonal basis.*

*Proof.* Let  $n$  be the rank of the form and let us compare two diagonal forms

$$q = \sum a_j x_j^2 = \sum a'_j y_j^2.$$

For  $n = 1$  both invariants are 1. For  $n = 2$ , observe that by definition  $(a_1, a_2)_p = 1$  if and only if  $z^2 = a_1 x_1^2 + a_2 x_2^2$  has a non-trivial solution in  $\mathbb{Q}_p$ . This is the case if and only if  $q(x_1, x_2)$  represents 0 or 1 =  $q(x_1, x_2)$  for some  $(x_1, x_2) \in \mathbb{Q}_p$ . But this is independent of the representation of  $q$  as a linear combination of two squares.

For  $n \geq 3$  we use induction on  $n$ . By Proposition 3.1.2 it suffices to consider two bases in a contiguous chain having one basis vector in common. We show that the Hasse invariant is the same for two such bases. Symmetry of the Hilbert symbol implies that we may permute the elements of the basis at will. Hence we may suppose that the first vectors of the bases are the same. Hence  $a'_1 = a_1 = q(e_1)$ . Since  $\text{disc}(q) = a_1 \cdots a_n = a_1 \cdot a'_2 \cdots a'_n$ , using equations (A.8) and (A.10) we have

$$\begin{aligned} \prod_{i < j} (a_i, a_j)_p &= (a_1, a_2 \cdots a_n)_p \prod_{2 \leq i < j} (a_i, a_j)_p \\ &= (a_1, \text{disc}(q)a_1)_p \prod_{2 \leq i < j} (a_i, a_j)_p \end{aligned}$$

and

$$\begin{aligned} \prod_{i < j} (a'_i, a'_j)_p &= (a_1, a'_2 \cdots a'_n)_p \prod_{2 \leq i < j} (a'_i, a'_j)_p \\ &= (a_1, \text{disc}(q)a_1)_p \prod_{2 \leq i < j} (a'_i, a'_j)_p. \end{aligned}$$

Now by induction applied to  $e_1^\perp$  we have  $\prod_{2 \leq i < j} (a_i, a_j)_p = \prod_{2 \leq i < j} (a'_i, a'_j)_p$  and the result follows.

For  $v = \infty$  the result is a consequence of Sylvester's law (cf. Corollary 8.1.3).  $\square$

### 3.2 Representation by Forms

$V$  is a vector space over a field  $k$  of characteristic different from 2,  $q$  a non-degenerate quadratic form on  $V$ . Conform (3.2) one sets  $x \cdot y = \frac{1}{2}[q(x+y) - q(x) - q(y)]$ .

We say that  $q$  **represents**  $a \in k$ , or  $a$  is represented by  $q$  if for some non-zero  $x \in V$  one has  $q(x) = a$ . Note that 0 is represented if and only if there is an isotropic vector. If this is the case we claim :

**Lemma 3.2.1.** *If  $x \in V$  is isotropic, then  $q$  represents all elements in  $k$ .*

*Proof.* Let  $y \in V$  be a vector with  $x \cdot y \neq 0$ . Such a vector exists since the bilinear form is non-degenerate. One may assume that  $x \cdot y = 1$  and, replacing  $y$  with  $y - \frac{1}{2}q(y)x$ , we may assume that in addition  $y$  is isotropic. Then the plane  $P$  spanned by  $x$  and  $y$  is a hyperbolic plane and  $V = P \oplus P^\perp$ . Clearly,  $q(\frac{1}{2}ax + y) = a$ .  $\square$

*Remark 3.2.2.* See also Lemma 6.3.8 where we prove the result in a more general setting.

**Lemma 3.2.3** (Representability criterion (characteristic  $\neq 2$ )). *Let  $a \in k^\times$ . Then the following conditions are equivalent:*

1.  $q$  represents  $a$ ;
2.  $q \simeq q' \oplus [a]$  where  $q'$  has rank  $n - 1$ ;
3.  $q \oplus [-a]$  represents 0.

*Proof.* We only prove the non-trivial implications (1)  $\implies$  (2) and (3)  $\implies$  (1). Suppose (1) holds: for some  $x \in V$  one has  $q(x) = a \neq 0$ . Then  $V = [a] \oplus x^\perp$  and (2) follows.

Suppose that (3) holds, i.e.  $q \oplus [-a]$  has a non-trivial zero, say  $q(x + \alpha e) = 0$  where  $e$  generates the summand  $[-a]$ . So  $q(x) - \alpha^2 \cdot a = 0$ . If  $\alpha = 0$ , that is,  $x$  is an isotropic vector, we apply Lemma 3.2.1. If not, then  $q(x/\alpha) = q(x)/\alpha^2 = a$ . In both cases (1) follows.  $\square$

Next we investigate representability of 0 in  $p$ -adic fields. Let

$$q(x_1, \dots, x_n) = a_1x_1^2 + \dots + a_nx_n^2, \quad a_j \in \mathbb{Q}_p, \quad j = 1, \dots, n,$$

be a non-degenerate form in  $n$  variables. Depending on the dimension  $n$ , we derive criteria for representability in terms of the discriminant and various Hilbert symbols as follows.

**Dimension  $n = 2$ .** We have a non-trivial solution for  $q(x_1, x_2) = 0$  precisely when  $-a_1/a_2$  is a square, but modulo squares this equals  $-a_1a_2 = -\text{disc}(q)$ . Hence a non-degenerate form  $q(x_1, x_2)$  represents 0  $\iff \text{disc}(q) = -1 \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ .



**Dimension  $n = 3$ .** Multiplying with  $-a_3$  and replacing  $x_3$  with  $a_3x_3$  we see that we may replace  $q(x_1, x_2, x_3)$  with  $-(a_1a_3x_1^2 + a_3a_2x_2^2 + x_3^2)$ . By the definition of the Hilbert symbol this form represents zero if and only if  $(-a_3a_1, -a_3a_2)_p = 1$  (see Section A.4). Using the bilinearity of the Hilbert symbol we may expand this equation

$$\begin{aligned}
1 &= (-1, -a_3a_2)_p (a_3, -a_3a_2)_p (a_1, -a_3a_2)_p \\
&= (-1, -a_3a_2)_p (a_3, -a_3a_2)_p (a_1, -1)_p \underbrace{(a_1, a_3)_p (a_1, a_2)_p}_{\varepsilon_p(q)} \\
&\stackrel{(A.11)}{=} (-1, -a_3a_2)_p (a_1, -1)_p \underbrace{(a_3, a_2)_p (a_1, a_3)_p (a_1, a_2)_p}_{\varepsilon_p(q)} \\
&\stackrel{(A.7)}{=} (-1, -\underbrace{a_1a_2a_3}_{\text{disc}(q)})_p \cdot \varepsilon_p(q) \\
&= (-1, -\text{disc}(q))_p \cdot \varepsilon_p(q).
\end{aligned}$$

Hence a non-degenerate form  $q(x_1, x_2, x_3)$  represents 0  $\iff \varepsilon_p(q) = (-1, -\text{disc}(q))_p$ .

We first note a consequence:

$$a \neq 0 \text{ is represented by } a_1x_1^2 + a_2x_2^2 \iff (a, -a_1a_2)_p = (a_1, a_2)_p. \quad (3.4)$$

This follows from Lemma 3.2.3 which states that the above representability is equivalent to  $-ax_0^2 + a_1x_1^2 + a_2x_2^2$  having an isotropic vector. By what we just said, this occurs if and only if  $\varepsilon_p(q) = (-1, -\text{disc}(q))_p$ , i.e.,  $(-a, a_1)_p (-a, a_2)_p (a_1, a_2)_p = (-1, aa_1a_2)_p$ . This can indeed be rewritten as  $(a, -a_1a_2)_p = (a_1, a_2)_p$ .

**Dimension  $n = 4$ .** Here we have

$$\text{a non-degenerate form } q(x_1, x_2, x_3, x_4) \text{ represents 0} \iff \begin{cases} \text{either } \text{disc}(q) \neq 1 \\ \text{or } \text{disc}(q) = 1 \text{ and} \\ \varepsilon_p(q) = (-1, -1)_p. \end{cases} \quad (3.5)$$

To show this, observe first that by writing  $q(x_1, x_2, x_3, x_4) = \sum a_i x_i^2$  as  $q = q_1 - q_2$ , where  $q_1 = a_1x_1^2 + a_2x_2^2$  and  $q_2 = -a_3x_3^2 - a_4x_4^2$ , we will be able to use (3.4). First observe that  $q$  represents 0 if and only if there exists an  $x \neq 0$  modulo squares represented by  $q_1$  and  $q_2$ . The ‘if’ part is trivial, so we turn to the ‘only if’ part. Suppose  $q(y_1, y_2, y_3, y_4) = 0$  with  $(y_1, y_2, y_3, y_4) \neq (0, 0, 0, 0)$ . Either  $q_1(y_1, y_2) \neq 0$  and we are done, or  $q_1(y_1, y_2) = 0$  and  $(y_1, y_2) \neq (0, 0)$ , or  $q_2(y_3, y_4) = 0$  and  $(y_3, y_4) \neq (0, 0)$ . In the case  $q_1(y_1, y_2) = 0$  Lemma 3.2.1 implies that  $q_1$  represents all elements in  $\mathbb{Q}_p^*$  and we can take for  $x$  any non-zero value of the form  $q_2$ . The case  $q_2(y_3, y_4) = 0$  is similar.

To rephrase the existence of an  $x \neq 0$  modulo squares represented by  $q_1$  and  $q_2$ , note that changing a representing vector by a non-zero scalar multiple multiplies the value of its quadratic form by its square, and so we may work at the level of  $D(\mathbb{Q}_p) = \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ . A similar remark applies to Hilbert symbols. Invoking (3.4)

the condition is equivalent to the existence of a solution of the following system of equations in  $D(\mathbb{Q}_p)$ :

$$\begin{aligned}(x, -a_1 a_2)_p &= (a_1, a_2)_p \\ (x, -a_3 a_4)_p &= (-a_3, -a_4)_p.\end{aligned}$$

We let  $A$  and  $B$  be the subset of  $D(\mathbb{Q}_p)$  consisting of the solutions of the first and second equation, respectively. The existence of a simultaneous solution is then equivalent to  $A \cap B \neq \emptyset$ . Since  $A$  and  $B$  are non-empty (e.g.,  $a_1 \in A$ ,  $-a_3 \in B$ ), by Lemma A.4.5  $A \cap B = \emptyset$  if and only if

$$a_1 a_2 = a_3 a_4 \text{ and } (a_1, a_2)_p = -(-a_3, -a_4)_p.$$

So the system has a solution precisely if not both equalities hold. This happens if and only if  $a_1 a_2 \neq a_3 a_4$  (which comes down to  $\text{disc}(q) \neq 1$ ) or  $a_1 a_2 = a_3 a_4$  and  $(a_1, a_2)_p = (-a_3, -a_4)_p$ . Now  $a_1 a_2 = a_3 a_4$  is equivalent to  $\text{disc}(q) = a_1 a_2 a_3 a_4 = (a_1 a_2)^2 = 1$ . Using  $a_1 a_2 = a_3 a_4$ ,  $(a_1, a_2)_p = (-a_3, -a_4)_p$ , and the rules for the Hilbert symbol we rewrite the condition  $(a_1, a_2)_p = (-a_3, -a_4)_p$  as

$$\begin{aligned}\varepsilon_p(q) &= \prod_{i < j} (a_i, a_j)_p = (a_1, a_2)_p (a_1 a_2, a_3 a_4)_p (a_3, a_4)_p \\ &= (a_1, a_2)_p (a_3, a_4)_p (a_3 a_4, a_3 a_4)_p = (a_1, a_2)_p (a_3, a_4)_p (-1, a_4)_p (-1, a_3)_p \\ &= (-a_3, -a_4)_p (-a_3, a_4)_p (-1, a_3)_p = (-a_3, -1)_p (-1, a_3)_p \\ &= (-1, -1)_p.\end{aligned}$$

So  $a_1 a_2 = a_3 a_4$  and  $(a_1, a_2)_p = (-a_3, -a_4)_p$  are equivalent to  $\text{disc}(q) = 1$  and  $\varepsilon_p(q) = (-1, -1)_p$ . Hence there exists a solution to the system if and only if  $\text{disc}(q) \neq 1$  or  $\text{disc}(q) = 1$  and  $\varepsilon_p(q) = (-1, -1)_p$ .

**Dimension  $n \geq 5$ .** Here we always have representability:

**Theorem 3.2.4.** *Any quadratic form  $q$  of rank  $\geq 5$  over  $\mathbb{Q}_p$  represents zero.*

*Proof.* The proof is a bit roundabout. We first search  $a \in \mathbb{Q}_p^\times$  such that  $a$  is represented by  $a_1 x_1^2 + a_2 x_2^2$  by making use of the criterion (3.4). In other words, we want to solve the equation

$$(x, -a_1 a_2)_p = \varepsilon_p(q') = \pm 1, \quad q' := a_1 x_1^2 + a_2 x_2^2,$$

in  $D(\mathbb{Q}_p)$ . The latter can be viewed as an  $\mathbb{F}_2$ -vector space of dimension  $r = 2$  if  $p$  is odd and of dimension  $r = 3$  if  $p = 2$ . Lemma A.4.5 states that  $(x, b)_p = \varepsilon$  has either  $2^{r-1}$  or  $2^r$  solutions unless  $b = 1$  and  $\varepsilon = -1$ . Apply this to  $b = -a_1 a_2$  and  $\varepsilon = \varepsilon_p(q')$ . Now note that we cannot at the same time have  $-a_1 a_2 = 1$  and  $(a_1, a_2)_p = -1$  since  $-a_1 a_2 = 1$  would lead to  $(a_1, a_2)_p = (a_1, -a_1 a_2)_p = (a_1, 1)_p = 1$  by formulas (A.11) and (A.8) and so the exception of "no solutions" is excluded. Hence there are  $\geq 2^{r-1}$  elements  $a \in D(\mathbb{Q}_p)$  represented by  $q'$ .

A fortiori this holds for any form of rank  $\geq 2$ , in particular for a form  $q$  of rank 5. Since  $2^{r-1} \geq 2$ , we can assume that  $a \neq \text{disc}(q)$  in  $D(\mathbb{Q}_p)$ . Then by Lemma 3.2.3 one has

$$q \simeq \tilde{q} \oplus [a],$$

with  $\tilde{q}$  of rank 4. Now  $\text{disc}(\tilde{q}) = a^{-1} \cdot \text{disc}(q) \neq 1$  and so, by the criterion for the existence of an isotropic vector for forms of rank 4 which we stated above, we see that  $\tilde{q}$  represents 0. But then also  $q$  represents 0. If a rank 5 form represents 0, then every form of higher rank does.  $\square$

As we just noticed, by Lemma 3.2.3 the preceding results have an immediate consequence for representation of  $q$  by non-zero numbers. Indeed, the form

$$q_a = a_1x_1^2 + \cdots + a_nx_n^2 - az^2,$$

isometric to  $q \oplus \langle -a \rangle$ , represents 0 if and only if  $q$  represents  $a \in k^*$ . The relation between the basic invariants is as follows.

$$\begin{aligned} \text{disc}(q_a) &= -a \cdot \text{disc}(q), \\ \varepsilon_p(q_a) &= \varepsilon_p(q) \prod_j (a_j, -a)_p \\ &= (-a, a_1 \cdots a_n)_p \varepsilon_p(q) \\ &= (-a, \text{disc}(q))_p \varepsilon_p(q). \end{aligned}$$

So the preceding results have the following consequence:

**Theorem 3.2.5** (Representability criterion (over  $\mathbb{Q}_p$ )). *Let  $q$  be a non-degenerate quadratic form over  $\mathbb{Q}_p$  of rank  $n$  and  $a \in \mathbb{Q}_p^\times$ . In order that  $a$  be represented by  $q$ , depending on its rank  $n$ , the necessary and sufficient condition is*

- for  $n = 1$ :  $a = \text{disc}(q)$ ;
- for  $n = 2$ :  $(a, -\text{disc}(q))_p = \varepsilon_p(q)$ ;
- for  $n = 3$ : either  $a \neq -\text{disc}(q)$ , or  $a = -\text{disc}(q)$  and  $(-1, -\text{disc}(q))_p = \varepsilon_p(q)$ ;
- for  $n \geq 4$ : no condition ( $a$  is always represented by  $q$ ).

*Remark 3.2.6.* If  $q$  is the localization of a non-degenerate ternary form over  $\mathbb{Q}$ , this implies that  $q$  assumes all values of  $\mathbb{Q}_p^\times$  with one possible exception,  $e_p := -\text{disc}(q)$ , but this happens at most for the finite set of primes  $p$  for which  $\varepsilon_p(q) \cdot (-1, e_p)_p = -1$ .

### 3.3 Classification

#### 3.3.A Local classification.

**Theorem 3.3.1.** *Two non-degenerate quadratic forms over  $\mathbb{Q}_p$  are isometric if and only if they have the same rank, discriminant and Hasse invariant.*

*Proof.* Isometric forms have the same invariants. Indeed, this is clear for the rank and discriminant. For the Hasse invariant this is Proposition 3.1.3.

The converse is proved by induction. Let  $q_1, q_2$  be two quadratic forms with the same invariants. By Theorem 3.2.5 these forms represent the same elements

in  $\mathbb{Q}_p^\times$ . Choose such an element  $a$ , for instance the value taken by  $q_1$  on some arbitrary non-zero vector, and apply Lemma 3.2.3 which implies

$$q_1 = q'_1 \oplus [a], \quad q_2 = q'_2 \oplus [a]$$

for forms  $q'_1, q'_2$  of rank one less. Let us calculate their invariants.

$$\begin{aligned} \text{disc}(q'_1) &= a^{-1} \text{disc}(q_1) \\ &= a^{-1} \text{disc}(q_2) \\ &= \text{disc}(q'_2), \\ \varepsilon_p(q'_1) &= \varepsilon_p(q_1)(a, \text{disc}(q'_1))_p \\ &= \varepsilon_p(q_2)(a, \text{disc}(q'_2))_p \\ &= \varepsilon_p(q'_2). \end{aligned}$$

By the induction hypothesis  $q'_1 \simeq q'_2$  and hence  $q_1 \simeq q_2$ .  $\square$

### 3.3.B Global results.

**Theorem 3.3.2** (Hasse–Minkowski). *A non-degenerate form  $q$  over  $\mathbb{Q}$  represents 0 if and only if  $q_v$  represents zero for all places  $v \in \mathcal{P}$ .*

We do not give a proof of this result since the proof uses techniques that are foreign to the main theme of this book. We refer to [204, IV.3.2]. Let us deduce some consequences of the Hasse–Minkowski result.

**Corollary 3.3.3.** *A rational non-zero number  $a$  is represented by a non-degenerate form  $q$  over  $\mathbb{Q}$  precisely if for all  $v \in \mathcal{P}$  the number  $a$  is represented over  $\mathbb{Q}_v$  by the non-degenerate form  $q_v$ .*

*Proof.* By Lemma 3.2.3 the form  $q$  represents  $a$  if and only if  $\tilde{q} = q \oplus \langle -a \rangle$  represents 0. Now apply the theorem to  $\tilde{q}$ .  $\square$

**Corollary 3.3.4** (Meyer’s theorem). *A non-degenerate rational quadratic form of rank  $\geq 5$  represents 0 if and only if it is indefinite.*

*Proof.* This follows from Theorems 3.2.4, 3.3.2, and the fact that a real form represents 0 precisely if it is indefinite.  $\square$

Now we are ready to prove the main classification result.

**Theorem 3.3.5** (Hasse Principle). *Two non-degenerate quadratic forms over  $\mathbb{Q}$  are isometric if and only if this is so locally, that is over each  $\mathbb{Q}_v$ ,  $v \in \mathcal{P}$ .*

*In other words: if  $L_1$  and  $L_2$  are two quadratic spaces over  $\mathbb{Q}$ , then an isometry  $L_1 \xrightarrow{\sim} L_2$  exists if and only if isometries  $L_{1,v} \xrightarrow{\sim} L_{2,v}$  exist for all places  $v \in \mathcal{P}$ .*

*Proof.* We need to see that local equivalence implies global equivalence. Let  $q_1, q_2$  be two locally equivalent quadratic forms over  $\mathbb{Q}$  of rank  $n \geq 1$ . We use induction

on  $n$ . Pick  $a \in \mathbb{Q}^\times$  represented by  $q_1$ . Then also  $q_2$  represents  $a$  by Corollary 3.3.3. This covers the case  $n = 1$ . For  $n \geq 2$  we now have by Lemma 3.2.3

$$\begin{aligned} q_1 &\simeq q'_1 \oplus [a] \\ q_2 &\simeq q'_2 \oplus [a]. \end{aligned}$$

The local assumption implies that  $q'_1 \oplus [a] \simeq q'_2 \oplus [a]$  over every  $\mathbb{Q}_v$ . This implies that  $q'_1 \simeq q'_2$  over any  $\mathbb{Q}_v$ . This is a consequence of a general result, Witt's cancellation theorem 7.2.7, which we prove in a later chapter. Assuming this, by induction there is a global isometry sending  $q'_1$  to  $q'_2$  and so also  $q_1$  is isometric to  $q_2$ .

In the present situation we may avoid an appeal to Witt's cancellation theorem as follows. Let  $e_1 \in L_1$ , respectively  $e_2 \in L_2$  span the summand  $[a]$  and let  $\phi_v : L_{1,v} \rightarrow L_{2,v}$  be an isometry. It sends  $e_1$  to a vector  $e \in L_{2,v}$  with  $q_{2,v}(e) = q_{2,v}(e_2) = a$ . The two vectors  $e + e_2$  and  $e - e_2$  cannot both be isotropic (otherwise their sum  $2e$  would be isotropic). Say  $x = e - e_2$  is non-isotropic. Then the reflection  $\tau = \sigma_x$  is defined and permutes  $e$  and  $e_2$ . If  $y = e + e_2$  is not isotropic, we use  $\tau = -\sigma_y$  to permute  $e$  and  $e_2$ . In either situation the isometry  $\tau$  permutes  $e$  and  $e_2$ , so that  $\tau \cdot \phi_v(e_1) = e_2$ . But then the isometry  $\tau \cdot \phi_v$  sends  $e_1^\perp$  with the form  $q'_1$  isometrically to  $e_2^\perp$  equipped with  $q'_2$ . Since this works for any place  $v$ , we conclude that  $q'_1 \simeq q'_2$ .  $\square$

*Remark 3.3.6.* 1. If for all  $v \in \mathcal{P}$  we have isometries  $\phi_v : q_{1,v} \rightarrow q_{2,v}$ , the above theorem states that a global isometry exists. However its localization at  $v \in \mathcal{P}$  need not be equal to  $\phi_v$ .

2. A non-degenerate real form  $q$  is classified by its signature,  $(s, t)$ . Since  $\text{disc}(q_\infty) = (-1)^t$  and  $\varepsilon_\infty(q) = (-1)^{t(t-1)/2}$ , the Hasse invariants and the discriminant don't suffice for the classification at  $\infty$ .
3. The Hilbert product formula (Theorem A.4.6) implies that

$$\prod_v \varepsilon_v(q) = 1, \tag{3.6}$$

which makes sense since for almost all  $v \in \mathcal{P}$  one has  $\varepsilon_v(q) = 1$ . See Section 12.4 for further existence conditions.

**Historical and Bibliographical Notes.** The topic of this chapter is classical. We follow largely J.-P. Serre's book [204, Ch. IV].

## Forms Related to Graphs

### Introduction

In Section 1.4 we have seen how to associate an integral lattice  $L_\Gamma$  to a finite simple graph  $\Gamma$ , the Dynkin diagram of the lattice. The corresponding lattices are root lattices by construction. In this case  $L_\Gamma$  has a basis consisting of  $(-2)$ -roots. In Section 4.1 we introduce various examples of this kind of root lattice and calculate the discriminant form. In Section 4.2 we extend the construction to weighted graphs and discuss the other classical semi-definite lattices.

In Section 4.3 we explain how the euclidean algorithm and a variant of it leads to graphs. The discriminant forms of the associated lattices realize all cyclic quadratic torsion forms and this will be made use of in Section 12.3.

In Section 4.4 we relate continued fractions to the topology of lens spaces. Then, in Section 4.5 we discuss an application to resolution of surface singularities, to elliptic fibrations and to Mordell–Weil lattices.

### 4.1 Root Lattices Spanned by $(-2)$ -Roots

In this section we use the labels to denote the roots. This is useful when we show how various geometrically relevant lattices are related.

**4.1.A Basic root lattices.** We introduce the following root lattices that will play a role in various applications. Note that all lattices are even.

1. **The root lattice  $A_n(-1)$ .** The graph for this lattice is as follows



with negative definite form given by the matrix

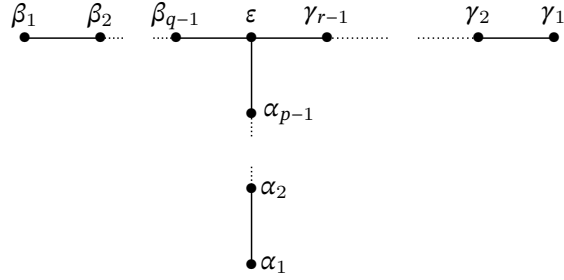
$$b_{A_n(-1)} = \begin{pmatrix} -2 & 1 & 0 & \cdots & \cdots & 0 \\ 1 & -2 & 1 & 0 & \cdots & 0 \\ 0 & 1 & -2 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \cdots & \vdots & \\ 0 & \cdots & & 1 & -2 & 1 \\ 0 & \cdots & \cdots & 0 & 1 & -2 \end{pmatrix} \in \mathbb{Z}^{n \times n}.$$

This presentation makes it possible to calculate the discriminant recursively:

$$\text{disc}(A_n(-1)) = (-1)^n(n+1). \quad (4.1)$$

We now show that this implies that the form  $b_{A_n}$  is indeed negative definite. Clearly  $b_{A_1}$  is negative definite, and adding a vertex at a time changes the sign of the discriminant as we see from (4.1). But since the form can be successively diagonalized (over the real numbers) each time we add a variable, every eigenvalue is negative and so the form is negative definite.

**2. The lattices  $\tilde{T}_{p,q,r}$ .** Here  $p, q, r$  are positive integers. These are of rank  $p+q+r-2$  and are defined by  $T$ -shaped graphs of the form



The lattice  $\tilde{T}_{p,q,r}$

Again, one can recursively find the discriminant:

$$\text{disc}(\tilde{T}_{p,q,r}) = (-1)^{p+q+r+1} pqr \left(1 - \frac{1}{p} - \frac{1}{q} - \frac{1}{r}\right). \quad (4.2)$$

This shows first of all, that the form is semi-negative definite if  $p^{-1} + q^{-1} + r^{-1} \geq 1$  and negative definite if strict inequality holds. Indeed, starting with the case  $p = q = r = 1$  we have a negative definite form and as long as strict inequality holds, the discriminant alters sign if we add a vertex. Since the form can be diagonalized inductively, this shows that the form remains negative definite until we attain the limit situation where  $p^{-1} + q^{-1} + r^{-1} - 1 = 0$  and then the form is degenerate. This occurs for one of the three triples  $(p, q, r) = (3, 3, 3), (2, 4, 4), (2, 3, 6)$ . These define the root lattices

$$\tilde{E}_6(-1) = \tilde{T}_{3,3,3},$$

$$\tilde{E}_7(-1) = \tilde{T}_{2,4,4},$$

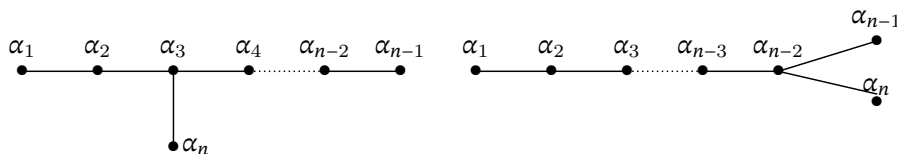
$$\tilde{E}_8(-1) = \tilde{T}_{2,3,6}.$$

Continuing, for  $p^{-1} + q^{-1} + r^{-1} < 1$  the graphs  $\tilde{T}_{p,q,r}$  define lattices of signature  $(1, p+q-3)$ .

It is customary to set

$$E_n(-1) = \tilde{T}_{2,3,n-3}, \quad n \geq 4, \quad \text{with } \text{disc}(E_n(-1)) = (-1)^{n+1}(n-9),$$

$$D_n(-1) = \tilde{T}_{2,2,n-2}, \quad n \geq 3, \quad \text{with } \text{disc}(D_n(-1)) = (-1)^n 4.$$

The lattices  $E_n(-1)$  and  $D_n(-1)$ 

Note that in particular,  $\tilde{E}_8(-1) = \tilde{T}_{2,3,6} = E_9(-1)$ . From formula (4.2) we also see which of the  $\tilde{T}_{p,q,r}$  are unimodular (if  $p \leq q \leq r$ , it is easy to see that  $p \geq 3$  leads to no solutions). We find the lattices

$$E_8(-1) = \tilde{T}_{2,3,5}, \quad E_{10}(-1) = \tilde{T}_{2,3,7}.$$

The second lattice turns out to be isometric to the Enriques lattice (see Example 1.13.1.4.) to which we come back in Lemma 4.1.5. The lattices  $E_n$  have another description as sublattices of the Lorentz lattice. See § 4.1.C below. The lattices  $D_n$  also have another description which we now give.

**Lemma 4.1.1.** *Let  $\mathbb{Z}^n = \mathbb{Q}^n \langle 1 \rangle$  be the standard euclidean lattice. The sublattice consisting of the integral vectors  $(x_1, \dots, x_n) \in \mathbb{Z}^n(-1)$  for which  $\sum_{j=1}^n x_j \equiv 0 \pmod{2}$  is isometric to  $D_n(-1)$ .*

*Proof.* Let  $\{e_1, \dots, e_n\}$  be the standard basis of  $\mathbb{Z}^n(-1)$  and consider the roots  $\alpha_j = e_j - e_{j+1}$ ,  $j = 1, \dots, n-1$ , and  $\alpha_0 = -e_1 - e_2$ . It is easily seen that these roots form a diagram of type  $D_n(-1)$ . The lattice spanned by these roots contains all roots of the form  $e_i \pm e_j$ ,  $i \neq j$ , and all vectors  $2e_j$ , and all of these vectors have even coordinate sum. Conversely, writing

$$\begin{aligned} x_1 e_1 + \dots + x_n e_n &= x_1(e_1 - e_2) + (x_1 + x_2)(e_2 - e_3) + \\ &\quad \dots + (x_1 + \dots + x_{n-1})(e_{n-1} - e_n) + \\ &\quad + \frac{1}{2} \underbrace{(x_1 + \dots + x_n)}_{\text{even}} 2e_n, \end{aligned}$$

one sees that all vectors with even coordinate vectors are in the lattice  $D_n(-1)$ .  $\square$

Well-known properties of so-called irreducible root systems for which we refer to [103, Ch. III], especially §10.4 therein, imply the following useful observation:

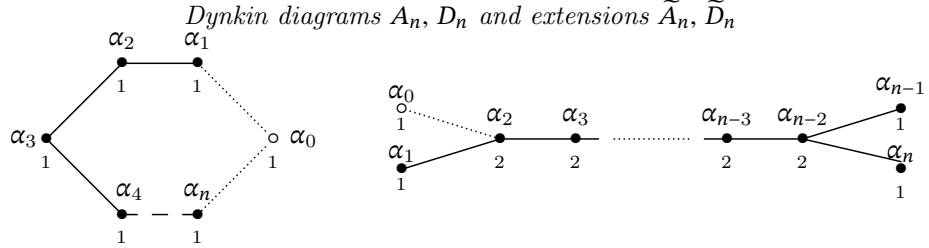
**Observation 4.1.2.** *Two 2-roots in each of the indecomposable root lattices  $A_n$ ,  $D_n$ ,  $E_6$ ,  $E_7$ ,  $E_8$  are conjugate under the Weyl group of the lattice.*

We come back to these root lattices in Section 17.2.A.

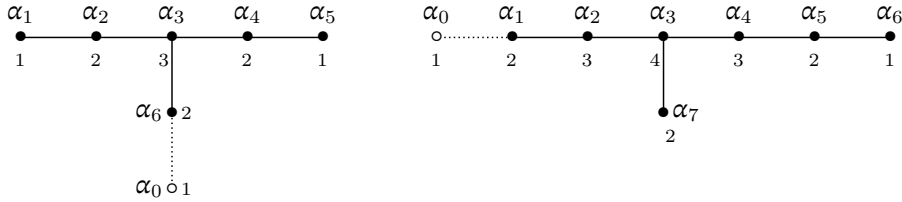
**3. Semi-definite root lattices spanned by  $-2$ -roots.** These consist of the so-called  $A$ - $D$ - $E$ -series and their extensions. These come up in many contexts, as we



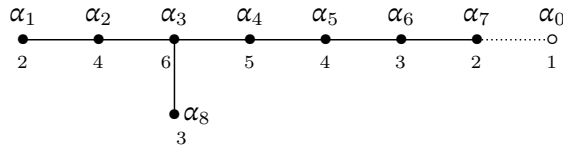
shall see later. We first introduce them, and in Proposition 4.1.4 we show that the list is complete. From the extended graphs (which give semi-definite forms with a non-trivial null-space) the corresponding definite Dynkin diagrams are obtained by omitting the white vertex.



*Dynkin diagrams  $E_6(-1), E_7(-1)$  and extensions  $\tilde{E}_6(-1), \tilde{E}_7(-1)$*



*Dynkin diagram  $E_8(-1)$  and its extension  $\tilde{E}_8(-1)$*



The null-space of the lattice of the extended graph is one-dimensional and spanned by the linear combination of all of the indicated roots with the coefficients written below the roots. For example the root  $\alpha_0 + \dots + \alpha_n$  spans the null-space of  $\tilde{A}_n$  and  $\alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + \alpha_5 + 2\alpha_6 + \alpha_0$  spans the one of  $\tilde{E}_6$ . We leave the (easy) verification of this to the reader. These calculations also yield:

**Lemma 4.1.3.** *The sublattice of  $E_8(-1)$  orthogonal to the root  $\beta = 2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 5\alpha_4 + 4\alpha_5 + 3\alpha_6 + 2\alpha_7 + 3\alpha_8$  is isometric to  $E_7(-1)$ . Consequently, the orthogonal complement of every root in  $E_8(-1)$  is isometric to  $E_7(-1)$ .*

*Proof.* In  $\tilde{E}_8(-1)$  the root  $\beta$  corresponds to  $-\alpha_0$  so that  $\beta \cdot \alpha_i = 0$  for  $i = 1, \dots, 6$ , and, clearly, the part of the graph of  $E_8$  obtained by omitting  $\alpha_7$  is the graph of  $E_7$ . By Observation 4.1.2 this then holds for all roots in  $E_8(-1)$ .  $\square$

**4.1.B Characterization of the semi-definite Dynkin diagrams.** We let  $\Gamma$  be a connected graph on  $n + 1$  vertices  $\{e_1, \dots, e_{n+1}\}$  with  $e_i \cdot e_i = -2$  and  $e_i \cdot e_j = 0$

if the vertices are  $e_i$  and  $e_j$  are not connected and  $= 1$  if they are connected. If  $x = \sum x_i e_i$  we then have

$$\begin{aligned} x \cdot x &= \sum_j x_j^2 (e_j \cdot e_j) + 2 \sum_{i < j} x_i x_j (e_i \cdot e_j) \leq - \sum_j 2 \cdot x_j^2 + 2 \sum_{i < j} |x_i x_j| (e_i \cdot e_j) \\ &= \left( \sum_j |x_j| e_j \right) \cdot \left( \sum_j |x_j| e_j \right). \end{aligned} \quad (4.3)$$

**Proposition 4.1.4.** *Let  $\Gamma$  be as above.*

1. *If  $b_\Gamma$  is negative semi-definite, there are two possibilities, namely  $b_\Gamma$  is negative definite or  $b_\Gamma$  is negative semi-definite and  $b_\Gamma \otimes \mathbb{Q}$  has a one-dimensional null-space spanned by a vector all of whose coordinates are positive.*
2. *The form  $b_\Gamma$  is negative definite if and only if it is one of the Dynkin diagrams  $A_n(-1)$ ,  $D_n(-1)$ ,  $E_6(-1)$ ,  $E_7(-1)$ ,  $E_8(-1)$ . In the negative semi-definite case we have in addition the extended Dynkin diagrams (with the exception of  $\widetilde{A}(-1)$  where two edges meet in two vertices).*

*Proof.* 1. We let  $N$  be the null-space of  $b_\Gamma \otimes \mathbb{Q}$ . Let  $x$  be isotropic. For any  $y \in \mathbb{Q}^{n+1}$  and  $a \in \mathbb{Q}$  we have  $(ax + y) \cdot (ax + y) \leq 0$  so that  $2ax \cdot y + y \cdot y \leq 0$ . Then  $x \cdot y = 0$  and so  $x \in N$ .

Suppose that  $x = \sum x_i e_i \in N$  then by (4.3) and the preceding remark, writing  $b_{ij} = e_i \cdot e_j$ , we have

$$0 = x \cdot x \leq \left( \sum |x_j| e_j \right) \cdot \left( \sum |x_j| e_j \right) \leq 0.$$

Hence  $\sum |x_j| e_j$  is isotropic and belongs to  $N$ . But then  $\sum_j b_{ij} |x_j| = (\sum |x_j| e_j) \cdot e_i = 0$ . Let  $J$  be the set of indices  $j$  with  $x_j \neq 0$ . Since  $b_{ij} = 0$  or  $1$  if  $i \neq j$  one has

$$b_{ij} |x_j| = \begin{cases} 0 & \text{if } j \notin J \\ \geq 0 & \text{if } i \notin J, j \in J. \end{cases}$$

But since  $\sum_j b_{ij} |x_j| = 0$  we find  $b_{ij} = 0$  if  $i \notin J$  and  $j \in J$ . This means that the graph is not connected, unless  $J = \emptyset$  or  $J = \{1, \dots, n+1\}$ . In other words: either  $N = 0$  or all coordinates of  $x \in N$  are non-zero and then  $\dim N = 1$  and since  $N$  contains a vector with positive coordinates, it is spanned by such a vector.

2. We first want to find out when  $b = b_\Gamma \leq 0$ . To do this, we compare  $b_\Gamma$  and  $b' = b_{\Gamma'}$ , where  $\Gamma'$  is a proper connected subgraph of  $\Gamma$ . Our previous study of  $N$  implies

$$b \leq 0 \implies b' < 0.$$

We use this first of all to consider graphs  $\Gamma$  with more than one triple point. These contain a subgraph of type  $\widetilde{D}_n(-1)$  whose associated form is not strictly definite and so the only possibility here are the graphs  $\widetilde{D}_n(-1)$ . If the graph  $\Gamma$  has exactly one triple point it must be a graph of type  $\widetilde{T}_{p,q,r}$  and we have seen that the associated forms are strictly negative definite if  $1/p + 1/q + 1/r > 1$  and semi-negative definite if  $1/p + 1/q + 1/r = 1$ . It follows that here only the graphs  $\widetilde{D}_n(-1)$ ,  $\widetilde{E}_6(-1)$ ,  $\widetilde{E}_7(-1)$ ,  $\widetilde{E}_8(-1)$  are possible. The remaining graphs can only be of type  $\widetilde{A}_n(-1)$  or  $A_n(-1)$ .  $\square$

**4.1.C Root lattices contained in the Lorentz lattice.** The *Lorentz lattice* of signature  $(1, n)$  is the lattice

$$\mathbb{Z}^{1,n} := \langle 1 \rangle \oplus \underbrace{\langle -1 \rangle \oplus \cdots \oplus \langle -1 \rangle}_{n \text{ summands}}. \quad (4.4)$$

We claim that the sublattice

$$E_n(-1) = (-3, 1, \dots, 1)^\perp \subset \mathbb{Z}^{1,n}, \quad n \geq 3, \quad (4.5)$$

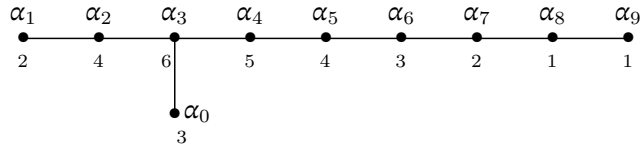
is a root lattice. Indeed, if  $\{e_0, \dots, e_n\}$  is the standard basis for  $\mathbb{R}^{n+1}$ , the roots

$$\begin{aligned} \alpha_0 &= (1, -1, -1, -1, 0, \dots, 0), \\ \alpha_j &= e_j - e_{j+1}, \quad j = 1, \dots, n-1, \end{aligned}$$

give a basis for the orthogonal complement of  $(-3, 1, \dots, 1) \subset \mathbb{Z}^{1,n}$ . To see this, first observe that they are linearly independent and all belong to  $E_n(-1)$ . Next, since for  $(x_0, x_1, x_2, x_3, \dots, x_n) \in E_n(-1)$  we have

$$\begin{aligned} (x_0, x_1, x_2, x_3, \dots, x_n) &= x_0 \alpha_0 + (x_0 + x_1) \alpha_1 + \\ &\quad + (2x_0 + x_1 + x_2) \alpha_2 + (3x_0 + x_1 + x_2 + x_3) \alpha_3 \\ &\quad + \cdots + \underbrace{(3x_0 + x_1 + \cdots + x_{n-1})}_{-x_n} \alpha_{n-1}, \end{aligned}$$

the subspace  $E_n(-1) = (-3, 1, \dots, 1)^\perp$  is generated by these roots. For  $n \geq 4$  it coincides with the lattice  $\tilde{T}_{2,3,n-3}$  as we can see from the graph that the basis defines, while  $E_3(-1) \simeq A_2(-1) \oplus A_1(-1)$ . Also, note that  $E_4(-1) = A_4(-1)$ ,  $E_5 = D_5(-1)$ , while  $E_6(-1)$ ,  $E_7(-1)$  and  $E_8(-1)$  are the usual Dynkin diagrams. The lattice  $E_9(-1)$  with rank 1 null-space coincides with  $\tilde{E}_8(-1)$ . For  $n \geq 10$  all lattices have signature  $(1, n)$  and there is the following result.



The lattice  $E_{10}(-1)$

**Lemma 4.1.5.** *The hyperbolic unimodular lattice  $\tilde{T}_{2,3,7} = E_{10}(-1)$  is isometric to the Enriques lattice  $U \oplus E_8(-1)$ . More generally, for  $n \geq 8$  one has*

$$E_{n+3}(-1) \simeq E_8(-1) \oplus U \oplus A_{n-7}(-1).$$

*Proof.* First consider the lattice  $E_{10}(-1)$ . A summand  $E_8(-1)$  is found back as the left end side of the diagram; it is generated by the roots  $\alpha_0, \dots, \alpha_7$ . Since the radical of  $\tilde{E}_8(-1) = E_9(-1)$  is generated by  $f = 3\alpha_0 + 2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 5\alpha_4 + 4\alpha_5 + 3\alpha_6 + 2\alpha_7 + \alpha_8$

we find that  $f$  and  $g = f + \alpha_9$  generate a hyperbolic plane orthogonal to the left hand  $E_8(-1)$  and hence  $E_{10}(-1) \simeq E_8(-1) \oplus U$ .

For  $n = 8$  the root  $\beta = \alpha_{10} - f$  and for  $n \geq 9$  the extra roots  $\{\alpha_{11}, \dots, \alpha_{n+2}\}$  together with the root  $\beta$  generate the lattice  $A_{n-7}(-1)$ . Indeed,  $\beta$  is easily seen to be a root, and perpendicular to  $\alpha_0, \dots, \alpha_9$ , that is  $E_8(-1) \oplus U$ . Now  $\beta$  connects to the right-hand  $A_{n-8}$ -chain to give a lattice of type  $A_{n-7}(-1)$ .  $\square$

Next, we prove a result on the root lattice  $E_8$  which gives an alternative treatment of Example 1.7.5.2.

**Lemma 4.1.6.** *The roots of  $E_8(-1)$  are the 240 vectors  $\pm\alpha_{ij}, \pm\alpha_{ijk}, \pm\beta_{ij}, \pm\gamma_i$ ,  $1 \leq i < j < k \leq 8$ , where*

$$\begin{aligned}\alpha_{ij} &= e_i - e_j, \\ \alpha_{ijk} &= e_0 - e_i - e_j - e_k, \\ \beta_{ij} &= 2e_0 - (e_1 + \dots + e_8) + e_i + e_j, \\ \gamma_i &= 3e_0 - (e_1 + \dots + e_8) - e_i.\end{aligned}$$

All the roots of  $E_8(-1)$  are in the same orbit under the Weyl group of  $E_8(-1)$ .

Moreover, the 8 roots  $\alpha_{ij}, \beta_{ij}$ ,  $ij \in \{12, 34, 56, 78\}$  are mutually orthogonal and hence span a sublattice isometric to  $\mathbb{Q}^8 A_1(-1)$ .

*Proof.* A root is a vector  $x = (x_0, x_1, \dots, x_8) \in \mathbb{R}^9$  with  $x \cdot x = -2$  orthogonal to  $(3, -1, -1, \dots, -1)$ . Hence  $x_0^2 = \sum x_i^2 - 2$  and  $3x_0 = \sum_{i=1}^8 x_i$ . Using

$$\left(\sum_{i=1}^N x_i\right)^2 + \sum_{1 \leq i, j \leq N} (x_i - x_j)^2 = N \sum_{i=1}^N x_i^2,$$

comparison gives

$$9x_0^2 = \left(\sum_{i=1}^8 x_i\right)^2 \leq 8 \sum_{i=1}^8 x_i^2 = 8(x_0^2 + 2).$$

We see that  $|x_0| \leq 4$ . Equality only occurs if all coordinates  $x_i$ ,  $i \geq 1$ , are equal which is readily seen to give a contradiction. So one may assume  $x_0 = 0, 1, 2, 3$ . From this the possible roots are quickly found.

The reflection  $\sigma_{\alpha_{ij}}$ ,  $1 \leq i < j \leq 8$ , permutes the  $i$ -th and  $j$ -th coordinates and so all permutations of indices can be realized. Hence we only have to see that a root of any of the four types is conjugate to one of a different type. This follows from

$$\sigma_{\alpha_{134}}(\alpha_{234}) = \alpha_{12}, \quad \sigma_{\alpha_{123}}(\beta_{78}) = \alpha_{456}, \quad \sigma_{\alpha_{123}}(\gamma_3) = \beta_{12}.$$

The last assertion follows upon inspection.  $\square$

**4.1.D Discriminant forms of the definite Dynkin diagrams.** For a summary see Table 4.1.1. We treat these one by one as follows.

**The root lattice  $A_n(-1)$ .** We claim that  $b_{A_n(-1)}^\# = \langle \frac{-n}{n+1} \rangle$  (and hence  $q_{A_n(-1)}^\# = [\frac{-n}{2(n+1)}]$ ). To show this, we describe the dual lattice of  $A_n(-1)$ :

**Lemma 4.1.7.** *The dual lattice of  $A_n(-1)$  can be identified with the  $\mathbb{Q}$ -valued lattice  $A'_n := (\mathbb{Z}^n, Q_n)$  where*

$$Q_n := \begin{pmatrix} -1+s & s & \cdots & s \\ s & -1+s & s & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ s & \cdots & -1+s & s \\ s & \cdots & s & -1+s \end{pmatrix} \quad s = \frac{1}{n+1}.$$

The discriminant group is cyclic of order  $n+1$  and generated by any basis vector  $e_i$ ,  $i = 1, \dots, n$ , of  $\mathbb{Z}^n$ . In particular,  $b_{A_n(-1)}^\#(e_1, e_1) = \frac{-n}{n+1}$ .

*Proof.* Let  $\{e_1, \dots, e_n\}$  be the standard basis of  $\mathbb{Z}^n$ . Set

$$e_{n+1} = -(e_1 + \cdots + e_n).$$

To simplify the notation we shall write  $x \cdot y$  for vectors  $x, y \in A'_n$  instead of  $Q_n(x, y)$ . Observing that

$$\begin{aligned} e_{n+1} \cdot e_j &= s, \quad j \neq n+1, \\ e_{n+1} \cdot e_{n+1} &= -1+s, \end{aligned}$$

one sees that  $e_{n+1}$  behaves with respect to  $Q_n$  just like a basis vector. Using this, we observe that the lattice  $A_n(-1)$  can be identified with the sublattice of  $A'_n$  spanned by the roots  $\alpha_1 = e_1 - e_2, \alpha_2 = e_2 - e_3, \dots, \alpha_n = e_n - e_{n+1}$  since  $\alpha_j \cdot \alpha_{j+1} = (e_j - e_{j+1}) \cdot (e_{j+1} - e_{j+2}) = 1$  and since all other products  $\alpha_j \cdot \alpha_k$ ,  $|j-k| \geq 2$ , vanish.

Now we can show that the dual of this sublattice is  $A'_n$ . First note that since

$$\alpha_i \cdot e_j = (e_i - e_{i+1}) \cdot e_j = -\delta_{i,j} + s + \delta_{i+1,j} - s \in \mathbb{Z},$$

the lattice  $A'_n$  is contained in the dual of  $A_n(-1)$ . Next note that  $e_1$  can be expressed as a linear combination of the  $\alpha_i$  as follows

$$e_1 = \frac{1}{n+1}(n\alpha_1 + (n-1)\alpha_2 + \cdots + \alpha_n),$$

and that there exist similar expressions for  $e_2, \dots, e_n$ . Hence  $A'_n/A_n(-1)$  is generated by the class of any of the vectors  $e_k$ . Consequently,  $[A'_n : A_n(-1)] \geq n+1$ . But by (1.8) we also know that  $[A_n^*(-1) : A_n(-1)] = |\text{disc}(A_n(-1))| = n+1$  so indeed  $A'_n = A_n^*(-1)$ . Finally,

$$e_1 \cdot e_1 = -1 + \frac{1}{n+1} = \frac{-n}{n+1},$$

thereby completing the proof.  $\square$

lattice $L$	$\text{disc}(L)$	discrim. group $L^*/L$	discrim. quadratic form $q_L^\#$
$A_n(-1)$	$(-1)^n(n+1)$	$\mathbb{Z}/(n+1)\mathbb{Z}$	$[\frac{-n}{2(n+1)}]$
$D_{8k}(-1)$	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$u_1$
$D_{8k+1}(-1)$	-4	$\mathbb{Z}/4\mathbb{Z}$	$[\frac{-1}{8}]$
$D_{8k+2}(-1)$	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$[\frac{-1}{4}] \oplus [\frac{-1}{4}]$
$D_{8k+3}(-1)$	-4	$\mathbb{Z}/4\mathbb{Z}$	$[\frac{-3}{8}]$
$D_{8k+4}(-1)$	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$v_1$
$D_{8k+5}(-1)$	-4	$\mathbb{Z}/4\mathbb{Z}$	$[\frac{3}{8}]$
$D_{8k+6}(-1)$	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$[\frac{1}{4}] \oplus [\frac{1}{4}]$
$D_{8k+7}(-1)$	-4	$\mathbb{Z}/4\mathbb{Z}$	$[\frac{1}{8}]$
$E_6(-1)$	3	$\mathbb{Z}/3\mathbb{Z}$	$[\frac{-4}{6}]$
$E_7(-1)$	-2	$\mathbb{Z}/2\mathbb{Z}$	$[\frac{-3}{4}]$
$E_8(-1), E_{10}(-1)$	1	0	0
$E_n(-1), n \geq 11$	$(-1)^n(n-9)$	$\mathbb{Z}/(n-9)\mathbb{Z}$	$[\frac{10-n}{2(n-9)}]$

Table 4.1.1: Discriminant and discriminant quadratic forms for basic root lattices

**The root lattice  $D_n(-1)$ .** We use the description of the lattice  $D_n(-1)$  given in Lemma 4.1.1 as a sublattice of  $\mathbb{Z}^n(-1)$  of integral vectors whose coordinate sums are even. It follows that the dual lattice is

$$D_n^*(-1) = \mathbb{Z}^n + \frac{1}{2}\mathbb{Z}(1, \dots, 1).$$

Let  $\{e_1, \dots, e_n\}$  be the standard basis of  $\mathbb{Z}^n$ . The quotient  $D_n^*(-1)/D_n(-1)$  consists of the classes mod  $D_n(-1)$  of the vectors 0 and

$$e = \frac{1}{2}(e_1 + \dots + e_n), \quad 2e, \quad 3e \quad (n \text{ odd})$$

$$f = e_1, \quad g = \frac{1}{2}(e_1 + \dots + e_n), \quad h = \frac{1}{2}(-e_1 + e_2 + \dots + e_n) \quad (n \text{ even}).$$

We shall denote the classes of the above elements by putting a bar above the vectors. The resulting group is cyclic of order 4 precisely if  $n$  is odd, and isomorphic to the Klein 4-group  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  in the even case. We write a dot for the standard euclidean product on  $\mathbb{Z}^n$ .

**$n$  is odd:** a generator of the group is given by  $\bar{e}$  and  $q^\#(\bar{e}) \equiv -\frac{1}{8}n \pmod{\mathbb{Z}}$ , that is, the discriminant bilinear and quadratic form is isometric to  $\langle -\frac{n}{4} \rangle$ . The isometry class of the discriminant quadratic form  $q_{D_n(-1)}^\#$  depends on the value of  $n \pmod{8}$  and so there are 4 isometry types.

**$n$  is even:** the two generators are  $\bar{f}$  and  $\bar{g}$  with  $q^\#(\bar{f}) \equiv \frac{1}{2} \pmod{\mathbb{Z}}$ ,  $q^\#(\bar{g}) \equiv \frac{n}{8} \pmod{\mathbb{Z}}$ . So, if  $n \equiv 0 \pmod{8}$  the discriminant form takes the values  $\frac{1}{2}, 0$  modulo integers on the generators which means that we have  $u_1$ . If  $n \equiv 4 \pmod{8}$  we get  $\frac{1}{2}, \frac{1}{2}$  modulo integers which gives  $v_1$ . In the two other cases the form splits: for  $n \equiv \pm 2 \pmod{8}$  the four values are  $0, \frac{1}{2}, \mp\frac{1}{4}, \mp\frac{1}{4}$  modulo integers and we get  $\langle \frac{\mp 1}{2} \rangle \oplus \langle \frac{\mp 1}{2} \rangle$ . The results are summarized in Table 4.1.1.

**The root lattice  $E_n(-1)$ .** We use the representation as a sublattice of the Lorentz lattice  $\mathbb{Z}^{1,n}$  (cf. (4.4)). A small calculation shows that for  $n \neq 9$

$$y = \frac{1}{n-9}(-3, 1, 1, \dots, 1, -n+10) \in E_n(-1) \otimes \mathbb{Q}$$

generates the discriminant group, a cyclic group isomorphic to  $\mathbb{Z}/|n-9|\mathbb{Z}$ . We get

$$q(y) = \frac{1}{2}y \cdot y = \frac{1}{2} \cdot \frac{n-10}{9-n} \pmod{\mathbb{Z}}.$$

It follows that the discriminant quadratic form of  $E_n(-1)$  is  $\langle \frac{10-n}{n-9} \rangle$ . In particular,  $E_8(-1)$  and  $E_{10}(-1)$  are unimodular, as we already saw in Section 4.1.

## 4.2 Other Root Lattices

In this section we consider positive semi-definite lattices spanned by  $k$ -roots where  $k$  is not fixed.

To agree with the existing literature, in the present section the lattice will be positive definite. Of course a negative semi-definite lattice  $L$  transforms in a positive semi-definite one by replacing it by  $L(-1)$ . Classically, in the positive definite case, one also assumes that  $Q_{ij} \leq 0$  for  $i \neq j$ . To relate the two conventions, we use a weighted graph  $\Gamma$  with  $n$  vertices  $v_1, \dots, v_n$  representing the lattice  $L(-1)$ . We put negative integral weights  $-Q_{jj}$  on the vertices,  $j = 1, \dots, n$ , and we draw an edge between  $v_i$  and  $v_j$  if  $Q_{ij} \neq 0$  and give it weight  $Q_{ij}$  in case  $Q_{ij} \neq 1$ . This weight is an integer but a priori it might be negative. Conversely, such a weighted graph  $\Gamma$  yields an integral lattice  $L_\Gamma$ , but not necessarily a root lattice.

To obtain a criterion for  $L_\Gamma$  to be a root lattice, let us first consider the abstract situation of a plane spanned by two roots  $\alpha, \beta \in L$  to which the form restricts positive definitively. Since the reflection

$$\sigma_\alpha(x) = x - \frac{2x \cdot \alpha}{\alpha \cdot \alpha} \alpha$$

preserves the lattice  $L$ , for any root  $\beta$ , the integrality condition

$$\frac{2\beta \cdot \alpha}{\alpha \cdot \alpha} \in \mathbb{Z} \tag{4.6}$$

holds, and likewise if we interchange  $\alpha$  and  $\beta$ . The product of these numbers is related to the angle  $\theta_{\alpha,\beta}$  between the roots  $\alpha$  and  $\beta$ :

$$4 \frac{(\alpha \cdot \beta)^2}{(\alpha \cdot \alpha)(\beta \cdot \beta)} = 4 \cos^2(\theta_{\alpha,\beta}) = s_{\alpha\beta} \in \mathbb{Z}. \tag{4.7}$$

This inequality has far-reaching consequences:

**Lemma 4.2.1.** *Let  $\alpha, \beta$  be independent roots such that the form is positive definite on the plane spanned by these roots. Assume also that  $\alpha \cdot \alpha \leq \beta \cdot \beta$  and that the angle between the two roots is obtuse. Then we have*

$$\theta_{\alpha, \beta} = \pi - \frac{\pi}{m_{\alpha, \beta}}, m_{\alpha, \beta} \geq 2$$

and only the following possibilities occur:

$m_{\alpha\beta}$	$s_{\alpha\beta} = 4 \cos^2(\theta_{\alpha,\beta})$	$\alpha \cdot \beta / \alpha \cdot \alpha$	$\beta \cdot \beta / \alpha \cdot \alpha$
2	0	0	1
3	1	-1/2	1
4	2	-1	2
6	3	-3/2	3

*Proof.* Condition (4.7) implies that  $4 \cos^2(\theta_{\alpha, \beta}) \in \{0, 1, 2, 3, 4\}$ . We abbreviate  $\lambda = \beta \cdot \beta / \alpha \cdot \alpha$  and let  $s = s_{\alpha\beta} \in \{0, 1, 2, 3, 4\}$ . The product of the two integers  $2 \frac{\alpha \cdot \beta}{\alpha \cdot \alpha}$ ,  $2 \frac{\alpha \cdot \beta}{\beta \cdot \beta}$  belongs to  $\{1, 2, 3, 4\}$ . Analyzing the possibilities leads to the entries in the table.  $\square$

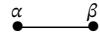
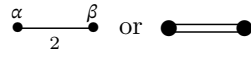

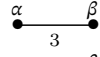

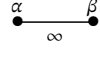

	if $\alpha \cdot \alpha = \beta \cdot \beta, \theta_{\alpha\beta} = \frac{2}{3}\pi$
 or 	if $2\alpha \cdot \alpha = \beta \cdot \beta, \theta_{\alpha\beta} = \frac{3}{4}\pi$
 or 	if $3\alpha \cdot \alpha = \beta \cdot \beta, \theta_{\alpha\beta} = \frac{5}{6}\pi$
 or 	if $\alpha \cdot \alpha = \beta \cdot \beta, \theta_{\alpha\beta} = \pi$ or $\alpha \cdot \alpha = 4\beta \cdot \beta, \theta_{\alpha\beta} = \pi$ .

Table 4.2.1: Edges in Dynkin diagrams

*Remark 4.2.2.* 1. The conditions of Lemma 4.2.1 are equivalent to the rotation  $\tau_{\alpha\beta} = \sigma_\alpha \circ \sigma_\beta$  having finite order. To see this, one first observes that

$$\text{Tr}(\tau_{\alpha\beta}) = -2 + 4 \frac{(\alpha \cdot \beta)^2}{(\alpha \cdot \alpha)(\beta \cdot \beta)}$$

and so  $\text{Tr}(\tau_{\alpha\beta}) < 2$  is equivalent to  $(\alpha \cdot \alpha)(\beta \cdot \beta) > (\alpha \cdot \beta)^2$  which is a necessary and sufficient condition for  $P$  to be a definite sublattice. On the other hand, if  $\tau_{\alpha\beta} \neq \text{id}$  has finite order, the two complex conjugate eigenvalues are roots of unity, say  $\exp(2\pi ic)$  and  $\exp(-2\pi ic)$ ,  $c \in \mathbb{Q} - \mathbb{Z}$ , with sum  $2 \cos(2\pi c) < 2$ . So  $P$  is definite and we are in the situation of the lemma.

In the more general situation where we assume that  $b|_L$  takes real values, a group generated by reflections  $\sigma_\alpha$  is called a **Coxeter group** if each rotation  $\tau_{\alpha\beta} = \sigma_\alpha \circ \sigma_\beta$  has finite order  $2s_{\alpha\beta} = m_{\alpha\beta}$ , and the corresponding graph is called a Coxeter graph.



2. Allowing  $m_{\alpha\beta} = \infty$  gives  $s_{\alpha\beta} = 4$  (angle  $\pi$ ) and  $\beta \cdot \beta = \alpha \cdot \alpha$  or  $\beta \cdot \beta = 4\alpha \cdot \alpha$ . This is the last graph in Table 4.2.1. It occurs indeed for hyperbolic type lattices. See Example 17.2.10.3.

Suppose now that  $L$  is a root lattice with a basis of roots  $R = \{v_1, \dots, v_n\}$ . Besides the graph we just described, which represents the Gram matrix with respect to  $R$ , there is another graph, the *Dynkin diagram*. It is the graph consisting of  $n$  vertices  $v_i$ ,  $i = 1, \dots, n$ , and with  $r_{i,j} = (v_i \cdot v_i)/(v_j \cdot v_j)$  edges between  $v_i$  and  $v_j$  (note that if  $v_i \cdot v_i \geq v_j \cdot v_j$ , Lemma 4.2.1 implies that the number  $r_{ij}$  is an integer). If the angle between roots is 0 or  $\pi$  one puts a thick edge between the roots. Alternatively, one assigns the number  $s_{\alpha\beta}$  to the edge in case  $s_{\alpha\beta} > 1$ . See Table 4.2.1.

Note that only the proportion between the squared lengths is determined. This allows for adjusting to minimal integral lengths as illustrated for the following classical examples of lattices with roots of varying length. Note that since in these examples  $\theta_{\alpha\beta} \neq \infty$ , the scaling makes the numbers  $s_{\alpha\beta}$  and  $-\alpha \cdot \beta$  equal. Hence the alternative way of giving the Dynkin diagram (the left-hand side of Table 4.2.1) gives the graph for the corresponding negative definite root lattice.

**Examples 4.2.3.** 1. **The lattice  $G_2$ .** This is the lattice  $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2$  with symmetric form given by the Gram matrix

$$\begin{pmatrix} 2 & -3 \\ -3 & 6 \end{pmatrix}.$$

This is a positive definite form and the two reflections  $\sigma_{e_i}$ ,  $i = 1, 2$ , which turn out to generate the full isometry group also denoted  $G_2$ . Observe that  $e_1$  is the 2-root associated to  $\sigma_{e_1}$  and  $e_2$  is the 6-root associated to  $\sigma_{e_2}$ . The two make an angle of  $5\pi/6$  radians and  $G_2$  is the symmetry group of a regular 6-gon with its barycenter in the origin. The group is one of the classical finite reflection groups, cf. [47, Table IV]. Here is the graph of  $G_2(-1)$  and its Dynkin diagram:

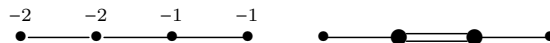


Graph  $G_2(-1)$  and Dynkin diagram  $G_2$

2. **The lattice  $F_4$ .** This is the lattice  $\mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_4$  with symmetric form given by the Gram matrix

$$\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

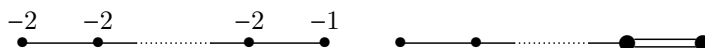
It is positive definite and has  $k$ -roots for  $k = 1, 2$ . Its isometry group turns out to be generated by the reflections in roots  $e_1, \dots, e_4$ , the four basis vectors.



Graph  $F_4(-1)$  and Dynkin diagram  $F_4$

The group is the classical reflection group of order 1152 which is the symmetry group of the so-called 24-cell in  $\mathbb{R}^4$ . See for example [47, Table I (ii) and Table IV].

- 3. Two other important classes are the two closely related odd lattices  $B_n$  and  $C_n$ . To the first there corresponds a negative definite lattice  $B_n(-1)$  described by the following graph. The numbers above the vertices  $x$  indicate whether  $2q(x) = -2$  or  $-1$ . All edges indicate intersection 1 between corresponding roots.



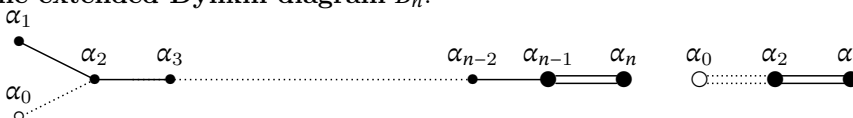
The graph  $B_n(-1)$  and Dynkin diagram  $B_n$

This is in accordance with the convention for the root system<sup>1</sup>  $B_n$  which has a basis of roots  $\{\alpha_1, \dots, \alpha_{n-1}, \alpha_n\}$  such that the length of the first  $n - 1$  roots is the same, but  $\alpha_n$  has shorter length with ratio  $\sqrt{2}$  between the two. If we scale lengths so that  $b(\alpha_1, \alpha_1) = 2$ , then indeed  $b(\alpha_n, \alpha_n) = 1$ . This gives the above Dynkin diagram for  $B_n$ . There is a variant, denoted  $C_n$ , where we interchange the role of the  $(-1)$ -roots and the  $(-2)$ -roots. The graph is then different but the Dynkin diagram is the same, although one sometimes draws an arrow from the smaller to the larger root to distinguish the two.

The Weyl group is by definition generated by reflections in all roots and in all three examples this group turns out to be the full orthogonal group. See [26, Planches II, VIII, IX].

Besides the  $A$ - $D$ - $E$  series, the preceding examples in fact are the only other irreducible definite root lattices and they all have a semi-definite extension whose graphs are as follows.

1. The extended Dynkin diagram  $\widetilde{B}_n$ .



The left diagram is for  $n \geq 3$ , the right one for  $n = 2$ . For  $\widetilde{B}_n$  all roots except  $\alpha_n$  are  $(-2)$ -roots and  $\alpha_n$  is a  $(-1)$ -root. The null-space of  $\widetilde{B}_n$  is spanned by  $\alpha_0 + \alpha_1 + 2 \sum_{i=2}^n \alpha_i$ .

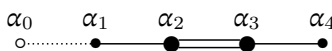
2. The extended Dynkin diagram  $\widetilde{C}_n, n \geq 2$ .



For  $\widetilde{C}_n$  all roots except  $\alpha_0$  and  $\alpha_n$  are  $(-1)$ -roots and  $\alpha_0, \alpha_n$  are  $(-1)$ -roots. Its null-space is spanned by  $\alpha_0 + \alpha_n + 2 \sum_{i=1}^n \alpha_{i-1}$ .

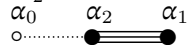
<sup>1</sup>For the background on root systems, see e.g. [26, 103].

3. The extended Dynkin diagram  $\tilde{F}_4$ .



For  $\tilde{F}_4$  the roots  $\alpha_0, \alpha_1$  and  $\alpha_2$  are  $(-1)$ -roots while  $\alpha_3$  and  $\alpha_4$  are  $(-2)$ -roots. Its null-space is spanned by  $\alpha_0 + 2(\alpha_1 + \alpha_4) + 3\alpha_2 + 4\alpha_3$ .

4. The extended Dynkin diagram  $\tilde{G}_2$ .



For  $\tilde{G}_2$  the root  $\alpha_1$  is a  $(-2)$ -root, the other two are  $(-6)$ -roots. Its null-space is spanned by  $\alpha_0 + 3\alpha_1 + 2\alpha_2$ .

**Proposition 4.2.4.** *Let  $L$  be a positive semi-definite irreducible root lattice of rank  $n$  with Dynkin diagram  $\Gamma$ . There are two possibilities:*

1.  $b_\Gamma$  is positive definite and then  $\Gamma = A_n, B_n, C_n, D_n$  or  $E_6, E_7, E_8, F_2, G_4$ ;
2.  $b_\Gamma$  is positive semi-definite and  $b_\Gamma \otimes \mathbb{Q}$  has a one-dimensional null-space spanned by a vector all of whose coordinates are positive. In that case  $\Gamma$  is the corresponding extended Dynkin diagram.

The proofs are similar to that of Proposition 4.1.4. See for example [26, Ch. VI, §4.2–4.3].

### 4.3 Lattices Obtained From the Euclidean Algorithm

**4.3.A Weighted graphs and continued fractions.** Up to now we have related graphs and root lattices with labels  $-1$  or  $-2$  on the vertices. We shall now use non-zero integer labels on the vertex to denote arbitrary self-intersections. Two vertices  $v, w$  are connected if and only if  $v \cdot w = 1$ . We mostly use the simplest kind of such weighted graphs, namely the connected graphs  $\Gamma_{\mathbf{a}}$  consisting of one branch as in the following figure where the weights  $a_j$  are assembled in the weight vector  $\mathbf{a} = (a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$ :



Figure 4.3.1: The graph  $\Gamma_{\mathbf{a}}$

As before, this gives a rank  $n + 1$  lattice determined by the symmetric integral matrix

$$B_{\Gamma_{\mathbf{a}}} = \begin{pmatrix} a_0 & 1 & 0 & \cdots & \cdots & 0 \\ 1 & a_1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & a_2 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \cdots & \ddots & \vdots \\ 0 & \cdots & & 1 & a_{n-1} & 1 \\ 0 & \cdots & \cdots & 0 & 1 & a_n \end{pmatrix} \in \mathbb{Z}^{(n+1) \times (n+1)}.$$

Using continued fractions, a unique rational number can be assigned to such a matrix and conversely. The purpose of the section is to explain this.

First of all, the weights  $\{a_j\}$  determine a continued fraction which in standard notation<sup>2</sup> reads

$$[a_0, a_1, \dots, a_n] = a_0 - \frac{1}{a_1 - \frac{1}{a_2 - \frac{1}{\ddots - \frac{1}{a_{n-1} - \frac{1}{a_n}}}}}$$

For example,  $2/1 = 2$ ,  $2 - \frac{1}{2} = 3/2$ ,  $2 - \frac{1}{2 - \frac{1}{2}} = 4/3$  leading to

$$\frac{n+1}{n} = [2, \underbrace{\dots, 2}]_{n \text{ times}}. \quad (4.8)$$

The converse is more involved. A non-zero rational number  $t/s$  with  $\gcd(s, t) = 1$ ,  $0 < s < |t|$ , can be written as a continued fraction using (a slightly different version of) the *euclidean algorithm*. It starts with the pair  $(s, t)$  and after a first euclidean division of  $t$  by  $s$  we obtain a remainder  $< s$ , subsequent euclidean divisions are performed with smaller and smaller positive remainders until the remainder is zero and the process stops:

$$\left\{ \begin{array}{ll} d_0 = t, & d_1 = s, \\ d_0 = a_0 d_1 - d_2, & 0 < d_2 < d_1, \\ d_1 = a_1 d_2 - d_3, & 0 < d_3 < d_2, \\ \vdots & \vdots \\ d_{n-1} = a_{n-1} d_n - d_{n+1}, & \\ d_n = a_n d_{n+1} & d_{n+1} = \gcd(s, t) = 1. \end{array} \right. \quad (4.9)$$

This gives a continued fraction expansion  $t/s = [a_0, \dots, a_n]$  since, starting with  $d_0/d_1 = a_0 - d_2/d_1$ , one successively finds

$$d_{k-1}/d_k = a_{k-1} - \frac{1}{d_k/d_{k+1}}.$$

For example, for the pair  $(3, 4)$  the algorithm gives

$$\begin{aligned} 4 &= 2 \cdot 3 - 2, \text{ hence } a_0 = d_2 = 2, \\ 3 &= 2 \cdot 2 - 1, \text{ hence } a_1 = 2, d_3 = 1, \\ 2 &= 2 \cdot 1, \text{ hence } a_2 = 2 \end{aligned}$$

<sup>2</sup>Another standard convention uses plus signs instead.

and so  $4/3 = [2, 2, 2]$ .

Consequently, as asserted, given a fraction  $t/s$  with  $\gcd(s, t) = 1$ ,  $0 < s < |t|$ , the euclidean algorithm (4.9) produces a unique vector of integers  $\mathbf{a} = (a_0, \dots, a_n)$  and hence a weighted graph  $\Gamma_{\mathbf{a}}$  of the type we are considering.

We also need a version of the euclidean algorithm that produces a weight vector  $\mathbf{a}$  with even coordinates since this leads to even forms  $b_{\Gamma_{\mathbf{a}}}$ . To ensure this, a slight modification of the above algorithm can be used: one chooses  $d_i$  and  $a_i$  successively in such a way that  $a_i d_{i+1}$  is the even multiple of  $d_{i+1}$  closest to  $d_i$ . Such a multiple may be negative and so the last line of the algorithm has to be changed into  $d_n = \pm a_n$ . Consequently,  $d_n$  should be even which is only possible if  $s$  and  $t$  are not both odd. Indeed, otherwise the proposed procedure forces all  $d_i$  to be odd.

Let us now give the details. Since  $(s, t) = 1$ , the integers  $s$  and  $t$  being not both odd, must have different parity. This yields the following version of the algorithm (with all  $a_i \neq 0$ ).

$$\left\{ \begin{array}{lll} d_0 = t, & d_1 = s & 0 < s < |t| \\ d_0 = a_0 d_1 - d_2, & a_0 \text{ even,} & 0 < |d_2| < |d_1|, \\ d_1 = a_1 d_2 - d_3, & a_1 \text{ even,} & 0 < |d_3| < |d_2|, \\ d_2 = a_2 d_3 - d_4, & a_2 \text{ even,} & 0 < |d_4| < |d_3|, \\ \vdots & \vdots & \\ d_{n-1} = a_{n-1} d_n - d_{n+1}, & a_{n-1} \text{ even,} & d_{n+1} = \pm \gcd(s, t) = \pm 1, \\ d_n = d_{n+1} a_n & a_n \text{ even.} & \end{array} \right. \quad (4.10)$$

Note that in this algorithm the parity of the remainders alternate between even and odd. Now  $d_{n+1}$  is odd, so if  $t = d_0$  is odd, then  $n$  is odd; if  $t$  is even, then  $n$  is even. As before this procedure leads to a continued fraction for  $t/s$ .

*Remark 4.3.1.* Observe that the above procedure with  $t$  odd and  $s$  even leads to odd  $n$  and so this gives graphs  $\Gamma_{\mathbf{a}}$  with an even number of vertices. In case  $t$  is even and  $s$  odd, one gets graphs with an odd number of vertices. In both situations, the resulting even integers  $a_i$  are unique and so the resulting even lattices are unique.

For later use we rephrase the two euclidean algorithms using matrices.

**Proposition 4.3.2.** *Let  $s, t$  be two co-prime integers with  $1 < s < |t|$ . Setting  $d_0 = t, d_1 = s$ , the (first) euclidean algorithm inductively gives integers  $d_k$ ,  $k = 2, \dots, n+1$ , and matrices*

$$A_k := \begin{pmatrix} a_k & -1 \\ 1 & 0 \end{pmatrix}, \quad k = 0, \dots, n, \quad \text{with } A_k \begin{pmatrix} d_{k+1} \\ d_{k+2} \end{pmatrix} = \begin{pmatrix} d_k \\ d_{k+1} \end{pmatrix} \text{ for } k < n.$$

The integers  $a_k$  are such that  $d_k = a_k d_{k+1} - d_{k+2}$  with  $0 < d_{k+2} < d_{k+1}$  and  $d_{n+1} = 1$ .

Using the second algorithm one produces even  $a_k$  starting with  $s$  and  $t$  that are not both odd and choosing  $a_k$  such that  $a_k d_{k+1}$  is the even multiple of  $d_{k+1}$  closest to  $d_k$ . In this case  $0 < |d_{k+1}| < |d_k|$  and  $d_{n+1} = \pm 1$ .

For practical purposes it is better to use instead the inverses  $A_k^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & a_k \end{pmatrix}$ , since then starting from  $(t, s)$  we get the required numbers  $a_0, \dots, a_n$  directly.

**Example 4.3.3.** Take  $(s, t) = (2, 5)$ . For the first algorithm one finds  $A_0^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}$  and then  $A_0^{-1} \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$  and thus  $A_1^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$ . So  $a_0 = 3, a_1 = 2$  and so  $5/2 = [3, 2]$ .

To get even  $a_k$ , one uses instead  $A_0^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$  with  $A_0^{-1} \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}$  giving  $d_2 = -1$  and  $a_0 = 2, a_1 = -2$  and so  $5/2 = [2, -2]$ .

The matrices  $A_k$  are also useful to perform a reverse euclidean algorithm. In order to proceed, we collect some properties of the products of these matrices.

**Lemma 4.3.4.** *Multiplying successive  $A_k$  gives the identity*

$$A_k \cdots A_n = \pm \begin{pmatrix} d_k & -d_{n-k+1}^* \\ d_{k+1} & -d_{n-k}^* \end{pmatrix}, \quad d_{n-k+1}^* = a_k d_{n-k}^* - d_{n-k-1}^*, \quad (4.11)$$

with  $d_0^* = 0$  and non-zero  $d_1^* = d_{n+1}, d_2^*, \dots, d_{n+1}^*$  and where the sign is the sign of  $d_{n+1} = \pm 1$  (this can only be  $-1$  for the second algorithm). Setting  $c_k := d_k/d_{k+1}$  and similarly  $c_k^* := d_k^*/d_{k-1}^*$ , one has the equalities

$$a_k = c_k + \frac{1}{c_{k+1}} = c_{n-k+1}^* + \frac{1}{c_{n-k}^*}.$$

For the second algorithm one also has the inequalities  $0 < |d_1^*| < \dots < |d_n^*| < |d_{n+1}^*|$ .

*Proof.* The equality (4.11) follows inductively. The inductive step of the euclidean division (4.9) and the stated recursion formula for  $d_k^*$  directly give the two expressions for  $a_k$ .

To show that  $d_1^*, \dots, d_{n+1}^*$  are non-zero, we consider the right-hand columns of the matrix in (4.11) for  $k < n$ . If  $d_{n-k+1}^* = 0$  or  $d_{n-k}^* = 0$  in such a column, then its determinant, which equals  $\det A_k \cdots \det A_n = 1$ , would be divisible by  $d_k$  or  $d_{k+1}$ . This can not happen since  $|d_k| > |d_{k+1}| > 1$  for  $k < n$ .

The inequalities follow by induction on  $k$ . For  $k = n - 1$  relation (4.11) implies  $c_2^* = d_2^*/d_1^* = a_{n-1}$ . So  $|d_2^*/d_1^*| = |c_2^*| = |a_{n-1}|$  is an integer  $\geq 2$ , which starts the induction. Now  $|c_{k+1}^*| = |a_{n-k} - 1/c_k^*|$  and since the  $|a_k|$  are at least 2 and by induction we may assume that  $|c_k^*| > 1$ , it follows that also  $|c_{k+1}^*| > 1$ .  $\square$

As a consequence of this result, for the second algorithm the integers  $d_k^*$  follow the euclidean algorithm for the pair  $(d_n^*, d_{n+1}^*)$ , but in reverse order. Moreover, if the  $a_k$  are even, the  $d_k^*$  alternate between odd and even since  $d_2^* = a_{n-1}$  and  $d_1^* = \pm 1$ . Finally, remark that the algorithm ends with  $a_{n-1}$  since  $d_1^* = \pm 1$ . As an example,

consider  $\frac{27}{4} = [6, -2, -2, -2]$ . Then  $A_0 A_1 A_2 A_3 = - \begin{pmatrix} 27 & 20 \\ 4 & 3 \end{pmatrix}$  and  $\frac{20}{3} = [6, -2, -2]$ .

Summarizing the preceding discussion, we have shown:

**Corollary 4.3.5.** *Assume we have performed the second algorithm for  $(s, t)$ , where  $1 < s < |t|$ , and where  $t, s$  are not both odd, yielding a continued fraction  $t/s = [a_0, \dots, a_n]$  with  $a_i$  even. Suppose  $d_{n+1} = \pm 1$  and write*

$$A_0 \cdots A_n = d_{n+1} \begin{pmatrix} t & -s^* \\ s & -t^* \end{pmatrix}, \quad ss^* - tt^* = 1. \quad (4.12)$$

Then (4.11) gives the (second variant of) the euclidean algorithm for  $(t^*, s^*)$  in reverse order and yields the continued fraction expansion  $s^*/t^* = [a_0, \dots, a_{n-1}]$ .

**4.3.B On the bilinear form associated to the graph  $\Gamma_{\mathbf{a}}$ .** We start with  $(s, t)$  as before (i.e.,  $1 < s < |t|$ ,  $\gcd(s, t) = 1$ ),  $s$  and  $t$  not both odd in the case of the second algorithm. We introduce the following vectors based on the euclidean algorithm

$$\begin{aligned} \mathbf{a} &= (a_0, \dots, a_n) \in \mathbb{Z}^{n+1}, \\ \mathbf{c} &= (c_0, \dots, c_n) \in \mathbb{Q}^{n+1}, \quad c_k = [a_k, \dots, a_n] \\ \mathbf{d} &= (d_0, \dots, d_n) \in \mathbb{Z}^{n+1}. \end{aligned}$$

Recall that

$$B_{\Gamma_{\mathbf{a}}} = \begin{pmatrix} a_0 & 1 & 0 & \cdots & \cdots & 0 \\ 1 & a_1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & a_2 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 1 & a_{n-1} & 1 \\ 0 & \cdots & \cdots & 0 & 1 & a_n \end{pmatrix} \in \mathbb{Z}^{(n+1) \times (n+1)}.$$

We have:

**Lemma 4.3.6.** *Let  $B_{n+1-k}$  be the matrix obtained from  $B_{n+1} = B_{\Gamma_{\mathbf{a}}}$  by deleting the first  $k$  rows and columns. Then*

1. *the coordinates of  $\mathbf{c}$  are  $c_k = d_k/d_{k+1}$ ,  $k = 0, \dots, n$ ; and  $a_k = c_k + \frac{1}{c_{k+1}}$ ,  $k = 0, \dots, n-1$ . Moreover, if the  $a_k$  are even,  $a_k$  and  $c_k$  have the same sign;*
2. *the coordinates of  $\mathbf{d}$  are  $d_k = \pm \det B_{n+1-k}$ ,  $k = 0, \dots, n$ , and the sign is the sign of  $d_{n+1}$ . In particular,  $\text{disc}(b_{\Gamma_{\mathbf{a}}}) = \pm d_0$ ;*
3. *over  $\mathbb{Q}$  the form given by  $B_{n+1-m}$  is isometric to the diagonal form  $\text{diag}(c_m, \dots, c_n)$ ,  $m = 0, \dots, n$ .*

*Proof.* We follow either the euclidean algorithm (4.9) (in that case  $d_{n+1} = 1$ ) or (4.10) (then both signs are possible, i.e.,  $d_{n+1} = \pm 1$ ).

1. The steps  $d_\ell = a_\ell d_{\ell+1} - d_{\ell+2}$  of the euclidean algorithm can be rewritten as  $\tilde{c}_\ell = a_\ell - \frac{1}{c_{\ell+1}}$ , where we provisionally write  $\tilde{c}_\ell = d_\ell/d_{\ell+1}$ . Now  $c_\ell = [a_\ell, \dots, a_n] = a_\ell - \frac{1}{[a_{\ell+1}, \dots, a_n]} = a_\ell - \frac{1}{c_{\ell+1}}$ . Combining the two recursions with  $c_n = a_n = d_n/d_{n+1} = \tilde{c}_n$  we conclude  $c_k = \tilde{c}_k = d_k/d_{k+1}$  for  $k = 0, \dots, n$ . Since  $c_k = a_k - 1/c_{k+1}$ ,  $|\frac{1}{c_{k+1}}| < 1$  and  $|a_k| \geq 2$  in case  $a_k \neq 0$  is even,  $a_k$  and  $c_k$  have the same sign.

2. We prove this by reverse induction starting with  $d_n = d_{n+1}a_n = \pm a_n$ . For the induction step we expand the determinant of  $B_{n+1-k}$  along its first column. This gives  $\det B_{n+1-k} = a_k \det B_{n-k} - \det B_{n-k-1} = \pm(a_k d_{k+1} - d_{k+2}) = \pm d_k$  completing the

induction.

3. Set  $y_m = x_m$  and  $y_\ell = x_\ell + \frac{1}{c_\ell} x_{\ell-1}$ ,  $\ell = m+1, \dots, n$ . Then one has

$$\begin{aligned}
\sum_{k=m}^n c_k y_k^2 &= c_m x_m^2 + \sum_{k>m} c_k \left( x_k + \frac{1}{c_k} x_{k-1} \right)^2 \\
&= a_m x_m^2 - \frac{1}{c_{m+1}} x_m^2 + \sum_{k>m} \left( 2x_k x_{k-1} + c_k x_k^2 + \frac{1}{c_k} x_{k-1}^2 \right) \\
&= a_m x_m^2 - \frac{1}{c_{m+1}} x_m^2 + \sum_{k>m} \left( 2x_k x_{k-1} + a_k x_k^2 - \frac{1}{c_{k+1}} x_k^2 + \frac{1}{c_k} x_{k-1}^2 \right) \\
&= \sum_{k=m}^n a_k x_k^2 + 2 \sum_{k=m}^{n-1} x_k x_{k+1}. \quad \square
\end{aligned}$$

The signature of  $B_{\Gamma_{\mathbf{a}}}$  is the same as that of the diagonal form  $\text{diag}(c_0, \dots, c_n)$  and so the last assertion of item 1 of Lemma 4.3.6 implies

**Corollary 4.3.7.** *Given two co-prime integers  $s, t$  with  $1 < s < |t|$ ,  $s$  and  $t$  not both odd. The euclidean algorithm (4.10) yields a unique continued fraction expansion  $t/s = [a_0, \dots, a_n]$  with  $a_j$  even. The associated graph  $\Gamma_{\mathbf{a}}$ ,  $\mathbf{a} = (a_0, \dots, a_n)$ , defines an even bilinear form  $b_{\Gamma_{\mathbf{a}}}$ . Let  $n_{\pm}$  be the number of positive, respectively negative  $a_i$ . Then the signature of  $b_{\Gamma_{\mathbf{a}}}$  equals  $(n_+, n_-)$ .*

**Example 4.3.8.** Let us revisit  $\Gamma = A_m(-1)$ . We have seen (cf. Eqn. (4.1)) that  $\text{disc}(\Gamma) = (-1)^m(m+1)$  and by Eqn. (4.8) we know that  $-(m+1)/m = [-2, \dots, -2]$  ( $m$ -fold repeated). Using this for  $m = 1, \dots, n+1$ , this shows

$$\begin{aligned}
\mathbf{a} &= (-2, -2, \dots, -2) \in \mathbb{Z}^{n+1} \\
\mathbf{c} &= \left( -\frac{n+2}{n+1}, -\frac{n+1}{n}, \dots, -2 \right) \in \mathbb{Q}^{n+1} \\
\mathbf{d} &= ((-1)^{n+1}(n+2), (-1)^n(n+1), \dots, -2) \in \mathbb{Z}^{n+1}.
\end{aligned}$$

One checks that these vectors all satisfy the relations of Lemma 4.3.6.

### 4.3.C Construction of even integral forms with discriminant form $\langle s/t \rangle$ .

We assume, that  $s$  and  $t$  are co-prime integers with  $0 < s < |t|$  and that  $s$  and  $t$  are not both odd, so we now allow for  $s = 1$ . In that case the even bilinear form  $\langle t \rangle$  has discriminant bilinear form  $\langle 1/t \rangle$ . So we may assume  $s > 1$ .

**Proposition 4.3.9.** *Let  $(s, t)$  be two co-prime integers satisfying  $1 < s < |t|$ ,*



which are not both odd and such that  $t/s = [a_0, \dots, a_n]$  with  $a_j$  even. Let

$$Q^{-1} = \begin{pmatrix} s/t & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 1 & a_0 & 1 & 0 & & \cdots & 0 \\ 0 & 1 & a_1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 1 & 0 \\ 0 & \cdots & & \ddots & 1 & a_{n-2} & 1 \\ 0 & \cdots & & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}.$$

Then  $Q$  is the Gram matrix of an even integral bilinear form with  $\text{disc}(Q) = \pm t$ , and with discriminant bilinear form  $(\mathbb{Z}/t\mathbb{Z}, \langle s/t \rangle)$ .

*Proof.* We first prove that  $Q$  is integral. Recall that  $Q = (Q^{-1})^{-1}$  can be calculated from  $\det(Q) \cdot Q^*$ , where  $Q^*$  is the adjugate matrix of  $Q^{-1}$ . To calculate  $\det(Q^{-1})$ , we expand along the first column. If we remove the first column and row from  $Q^{-1}$ , the resulting determinant equals  $\pm s^*$  by Lemma 4.3.6 applied to  $s^*/t^*$ . Upon removing the first two columns and rows, the resulting determinant is  $\pm t^*$  (with the same sign as for the first determinant). Hence,  $\det(Q^{-1}) = \pm(s/t \cdot s^* - t^*) = \pm 1/t$ , where the last equality is derived from  $ss^* - tt^* = 1$ . So  $\det(Q) = \pm t$  which ensures that  $Q$  is indeed integral.

We next show that the diagonal elements of  $Q$  are even by considering  $tQ^*$  and in particular the cofactors of the diagonal elements of  $Q^{-1}$ . Some observations before we do so. First, by induction it follows that a square  $m$  by  $m$  integral matrix with even diagonal entries and 1's in positions  $i, j$  with  $|i - j| = 1$  (and zero entries elsewhere) has even determinant if and only if  $m$  is odd. Secondly,  $t$  is odd if and only if  $s$  is even if and only if  $n$  is odd. We provisionally write  $B[i, j]$ , where  $0 \leq i \leq j \leq n - 1$ , for the matrix obtained from  $Q^{-1}$  by deleting the first  $i + 1$  rows and columns and the last  $n - j$  rows and columns (so that a square  $j - i + 1$  matrix with  $a_i, \dots, a_j$  along the diagonal remains).

Now we turn to the various cofactors. By the first observation, the cofactor of the element  $s/t$  in  $Q^*$  is even if  $n$  is odd; if  $n$  is even,  $t$  is even. So  $tQ^*$  has an even entry in position  $(1, 1)$ . The cofactor of  $a_0$  in position  $(2, 2)$  in  $Q^*$  multiplied by  $t$  is the product of  $s$  and  $\det B[1, n - 1]$  which is even if  $n$  is even; if  $n$  is odd, then  $s$  is even. So  $tQ^*$  has an even entry in position  $2, 2$ . The cases of the cofactors of  $a_j$ ,  $j = 1, \dots, n - 1$ , in position  $(i + 2, i + 2)$  are all similar to the case  $j = n - 1$ . The cofactor of  $a_{n-1}$  multiplied by  $t$  equals (expand along the first row and column)  $s \det B[0, n - 2] - t \det B[1, n - 2]$ . If  $n$  is odd, then  $\det B[1, n - 2]$  and  $s$  are even; if  $n$  is even, then  $t$  and  $\det B[0, n - 2]$  are even.

Finally, we have to affirm that  $Q$  represents a form with discriminant bilinear form  $\langle s/t \rangle$ . So, let  $b$  be the integral bilinear form on  $\mathbb{Z}^n$  whose Gram matrix is  $Q$ . Lemma 1.6.3 tells us that  $Q^{-1}$  is the Gram matrix of the form  $b_{\mathbb{Q}}$  with respect to the dual basis of  $(\mathbb{Z}^n, b)$  given by the columns of the matrix  $Q^{-1}$ . So  $Q^{-1}$  represents the discriminant form of  $Q$  and since all entries of  $Q^{-1}$  are integral except the top left entry  $s/t$ , this yields the discriminant form  $\langle s/t \rangle$ , as desired.  $\square$

*Remark 4.3.10.* Since the lattice  $(\mathbb{Z}^n, b)$  is even, the form  $b$  is the polar form of a quadratic form  $q$ . This  $q$  induces the quadratic torsion form  $[(t/2)/s]$  if  $t$  is even, and  $[t/(2s)]$  if  $t$  is odd.

**Example 4.3.11.** We continue with the algorithm of Example 4.3.3 for  $5/2 = [2, -2]$ . Here  $A_0A_1 = -\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$  and so  $s^* = -2, t^* = -1$ . Since  $a_0 = 2$  and  $a_1 = -2$  we find  $Q^{-1} = \begin{pmatrix} \frac{2}{5} & 1 \\ 1 & 2 \end{pmatrix}$  and  $Q = -\begin{pmatrix} 10 & -5 \\ -5 & 2 \end{pmatrix}$ , an even matrix with discriminant  $-5$  and signature  $(1, 1)$ . By construction the corresponding even lattice has the right discriminant form  $\langle 2 \cdot 5^{-1} \rangle$ .

## 4.4 Lens Spaces

**4.4.A Topological background.** Given a pair  $(t, s)$  of coprime positive integers, a lens space  $L(t, s)$  can be constructed as follows. Let  $\zeta$  be a primitive  $t$ -th root of unity. The unit three-sphere can be realized as a submanifold of  $\mathbb{C}^2$ :

$$S^3 = \{(z, w) \in \mathbb{C}^2 \mid z\bar{z} + w\bar{w} = 1\}.$$

The group of  $t$ -th roots of unity  $\mu_t \subset \mathbb{C}^\times$  acts coordinate-wise as  $\zeta \cdot (z, w) = (\zeta \cdot z, \zeta^s \cdot w)$ , where  $\zeta = \exp(2\pi i/t)$ . This action is without fixed points and hence the quotient

$$L(t, s) = S^3/\mu_t$$

is an oriented differentiable 3-manifold for which  $H_1(L(t, s), \mathbb{Z}) = \mathbb{Z}/t\mathbb{Z}$ .

The classification of lens spaces has a long history. The homotopy classification was first completed by J. H. C. Whitehead:

**Theorem 4.4.1** ([250]). *Two lens spaces  $L(t, s)$  and  $L(t, s')$  have the same oriented homotopy type<sup>3</sup> if and only if  $ss'$  is a quadratic residue modulo  $t$ .*

The finer topological classification reads as follows:

**Theorem 4.4.2.**  *$L(t, s)$  and  $L(t', s')$  are oriented homeomorphic (diffeomorphic) if and only if  $t = t'$  and either  $s \equiv s' \pmod{t}$ , or  $s \equiv (s')^{-1} \pmod{t}$ .*

For the history of this result with references to proofs we refer the reader to the historical notes at the end of this chapter. We only mention that the proof uses the so-called Reidemeister torsion which turns out to be a complete topological invariant. In this section, instead we shall consider a more easily computable oriented homeomorphism invariant, the index modulo 16. Moreover, its calculation fits well within the theme of this book since it uses the euclidean algorithm for  $(t, s)$  and hence is directly related to the quadratic form associated to a graph.

<sup>3</sup>Two varieties  $M$  and  $M'$  are homotopy equivalent or have the same *homotopy type* if there are two continuous maps  $f : M \rightarrow M'$  and  $g : M' \rightarrow M$  such that  $f \circ g$  and  $g \circ f$  are homotopic to the respective identity maps. If  $M, M'$  are oriented and  $f$  (or  $g$ ) preserve the orientations, one speaks of oriented homotopy equivalence.

**4.4.B The linking pairing and the index mod 16.** In this subsection we consider three-manifolds  $X$  which bound a 4-dimensional oriented manifold  $Y$ , that is  $\partial Y = X$ . The cup product pairing in the middle cohomology gives

$$H^2(Y, \partial Y; \mathbb{Z}) \times H^2(Y, \partial Y; \mathbb{Z}) \rightarrow H^4(Y, \partial Y; \mathbb{Z}) \simeq \mathbb{Z}$$

and via Lefschetz duality [86, Theorem 28.18], [94, Theorem 3.43] this translates into a symmetric bilinear form, the intersection form

$$S_Y : H_2(Y, \mathbb{Z})/(\text{torsion}) \times H_2(Y, \mathbb{Z})/(\text{torsion}) \rightarrow \mathbb{Z}$$

as in the case of compact manifolds  $Y$  with  $\partial Y = \emptyset$ , (see Eqn. (2.1)). But unlike for manifolds without boundary, the intersection form need not be unimodular, that is, it can have non-trivial discriminant form. It is this aspect that we can take advantage of in case  $X = \partial Y$  is a  $\mathbb{Q}$ -homology sphere.

Let us briefly explain this notion. A  $\mathbb{Q}$ -homology  $d$ -sphere is a (differentiable) manifold  $X$  which has the same Betti numbers as the sphere  $S^d$ . In other words,  $H_j(X, \mathbb{Q}) = 0$  for  $j \neq 0, d$  and  $H_0(X, \mathbb{Q}) \simeq H_d(X, \mathbb{Q}) \simeq \mathbb{Q}$ . Observe that this allows for torsion in the homology. Any free action of a finite group on  $S^3$  gives a  $\mathbb{Q}$ -homology three sphere; lens spaces are such examples.

A seemingly weaker notion is that of an  $\mathbb{F}_2$ -homology sphere: the definition is the same, except that instead of Betti numbers we use the numbers  $\dim_{\mathbb{F}_2} H_j(X, \mathbb{F}_2)$ . It turns out (cf. [99, Lemma 7.3]) that if  $X$  is an  $\mathbb{F}_2$ -homology sphere where  $H_j(X, \mathbb{Z})$  has at most odd torsion in the range  $j = 1, \dots, \dim X - 1$ , then it is also a  $\mathbb{Q}$ -homology sphere. In particular, if  $t$  is odd, a lens space  $L(t, s)$  is an  $\mathbb{F}_2$ -homology sphere. The merit of  $\mathbb{F}_2$ -homology three-spheres is that these are always the boundary of a closed manifold  $Y$  with nice properties:

**Lemma 4.4.3** ([99, §7]). *If  $X$  is an  $\mathbb{F}_2$ -homology three-sphere, there exists a four-manifold  $Y$  with boundary  $X$  such that*

1.  $H_1(Y, \mathbb{Z})$  has no 2-torsion;
2.  $S_Y$  is an even form.

For lens spaces we shall give a direct construction of a simply connected four-manifold  $Y$  with boundary any given lens space  $L(t, s)$  and with  $S_Y$  even (see Proposition 4.4.5). From now on we assume that we are in this situation. We use Lefschetz duality for homology [86, 28.18], [94, Theorem 3.43] to relate the cohomology of  $Y$  and its boundary  $X$ . It states that the orientation induces an isomorphism

$$H_2(Y, \partial Y; \mathbb{Z}) = H_2(Y, X; \mathbb{Z}) \xrightarrow{\simeq} H^2(Y, \mathbb{Z}).$$

By the universal coefficient theorem [94, p. 190], if  $H_1(Y, \mathbb{Z})$  has no torsion, there is also an isomorphism

$$H^2(Y, \mathbb{Z}) \simeq \text{Hom}(H_2(Y, \mathbb{Z}), \mathbb{Z}).$$

Consequently, in our situation, the exact sequence for the pair  $(X, Y)$  gives us a commutative diagram

$$\begin{array}{ccccccc}
 H_2(Y, \mathbb{Z}) & \xrightarrow{\alpha} & H_2(Y, X; \mathbb{Z}) & \xrightarrow{\delta} & H_1(X, \mathbb{Z}) & \longrightarrow & 0 \\
 & \searrow \phi & \parallel \wr & & \nearrow & & \\
 & & H^2(Y, \mathbb{Z}) & & & & \\
 & & \parallel \wr & & & & \\
 & & H_2(Y, \mathbb{Z})^* = \text{Hom}(H_2(Y, \mathbb{Z}), \mathbb{Z}) & & & & 
 \end{array}$$

Tracing through the isomorphisms, one can show that  $\phi$  is the correlation morphism for the intersection product so that  $H_1(X, \mathbb{Z})$  gets identified with the cokernel of the correlation map, the discriminant group of  $S_Y$ . The discriminant bilinear form  $b_{S_Y}^\#$  on this torsion group therefore yields an induced pairing

$$L : H_1(X, \mathbb{Z}) \times H_1(X, \mathbb{Z}) \rightarrow \mathbb{Q}/\mathbb{Z}.$$

This turns out to be the *linking pairing* which is defined as follows. Take two classes  $c = [\gamma]$  and  $c' = [\gamma']$  in  $H_1(X) = \mathbb{Z}/t\mathbb{Z}$  where  $\gamma, \gamma'$  are representative oriented cycles. Then  $tc = 0$  so there is an oriented 2-chain  $\Sigma$  which bounds  $t\gamma$ . Assume that  $\gamma'$  is chosen general enough to meet  $\Sigma$  transversely. The intersection number  $\Sigma \cdot \gamma'$  leads to the rational number  $t^{-1}(\Sigma \cdot \gamma')$  which modulo integers turns out to depend only on the two torsion classes  $c, c'$ . See [203, §77]. It is called the *linking number*

$$t^{-1}(\Sigma \cdot \gamma') = \text{lnk}(c, c') \in \mathbb{Q}/\mathbb{Z}.$$

That the linking numbers indeed give the discriminant pairing  $L$  on  $H_2(X, \mathbb{Z})^*/H_2(X, \mathbb{Z})$  can be seen as follows (up to choices of representatives). By the definition of  $\delta$ , a class  $c'$  lying in the image of  $\delta$  is the class of the boundary  $\partial\Gamma'$  of a relative 2-cycle  $\Gamma'$  in  $Y$ . So we have

$$t \text{lnk}(c, c') = \Sigma \cdot \Gamma' \quad \text{in } Y.$$

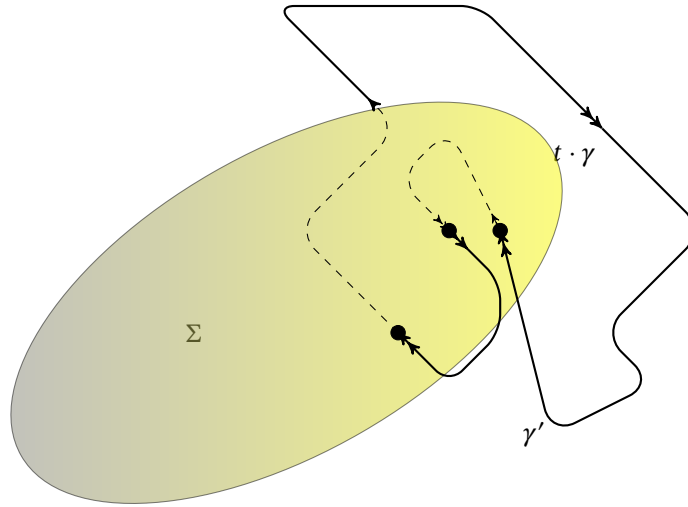
Similarly,  $c = \delta([\Gamma])$ , where  $\Gamma$  is a 2-chain in  $Y$  with boundary the 1-cycle  $\gamma$ . Hence  $\Sigma - t\Gamma$  is a 2-cycle in  $Y$  and so intersecting this with the relative cycle  $\Gamma'$  gives

$$(\Sigma - t\Gamma) \cdot \Gamma' \equiv t \text{lnk}(c, c') \pmod{t\mathbb{Z}},$$

since  $\Gamma \cdot \Gamma'$  is an integer. On the other hand, because  $\delta([\Sigma]) = 0$ , there is some  $\sigma \in H_2(Y, \mathbb{Z})$  with  $\alpha(\sigma) = [\Sigma]$ . The discriminant bilinear form  $b_{S_Y}^\#$  is given by the intersection pairing on  $H_2(Y, \mathbb{Z}) \otimes \mathbb{Q}$ , and in our identification the classes  $c, c' \in H_1(X, \mathbb{Z})$  correspond to  $t^{-1}\sigma \in H_2(Y, \mathbb{Q})$ , respectively  $[\Gamma'] \in H_2(Y, X; \mathbb{Z})$ . We deduce that

$$b_{S_Y}^\#(t^{-1}\sigma, \Gamma') = t^{-1}(\Sigma - t\Gamma) \cdot \Gamma' = \text{lnk}(c, c') \in \mathbb{Q}/\mathbb{Z}.$$

What happens if we choose another four-manifold  $Y'$  with  $\partial Y' = X$ ? We glue  $Y$  and  $-Y'$  along the common boundary, the variety  $Y'$  taken with opposite orientation, along the common boundary. Recall we have assumed that  $Y$  and  $Y'$  are



Linking number  $\text{lnk}(\gamma, \gamma')$  of  $\gamma$  and  $\gamma'$  (here  $\text{lnk}(\gamma, \gamma') = \pm 1/t$ ).

simply connected. Then the resulting compact oriented four-manifold  $Y \cup_X Y'$  is simply connected (by van Kampen's theorem [94, §1.2]) and the intersection form of  $Y \cup_X Y'$  is the orthogonal direct sum  $S_Y \oplus S_{Y'}(-1)$ . It follows for the indices that  $\tau(Y) - \tau(Y') = \tau(Y \cup_X Y')$ .

Up to now we did not suppose that  $S_Y$  and  $S_{Y'}$  are even forms, but if this is the case as for lens spaces  $L(t, s)$  with  $t$  odd, we can apply Rohlin's theorem 2.5.7 and infer that the right-hand side  $\tau(Y \cup_X Y')$  is divisible by 16. It follows that the index mod 16 is well defined:

**Definition 4.4.4.** The index mod 16 of  $X$  is defined as the index mod 16 of the intersection form of any bounding fourfold  $Y$  as in Lemma 4.4.3:

$$\tau_{16}(X) := \tau(S_Y) \bmod 16.$$

Its opposite,  $\mu(X) := -\tau_{16}(X)$  is also called the  *$\mu$ -invariant*.

**4.4.C Lens spaces via graphs.** In this section we shall show that a lens space is directly related to a graph constructed from the two integers  $s$  and  $t$  similar to the construction of Corollary 4.3.7. Since the associated form is the intersection form of the four-manifold  $Y(s, t)$  bounding the lens space  $L(s, t)$ , we can read off the index modulo 16.

Start with the tautological line bundle  $L$  on the complex projective line  $\mathbb{P}^1 \simeq S^2$ . Endow  $\mathbb{P}^1$  with homogeneous coordinates  $z_0, z_1$ . By definition, the fiber of  $L$  over the point  $(z_0 : z_1)$  is the line in  $\mathbb{C}^2$  spanned by the vector  $(z_0, z_1)$ . In algebraic geometry language, this line bundle is the dual of the ample line bundle  $\mathcal{O}_{\mathbb{P}^1}(1)$ . The unit circles in the fibers of this bundle trace out an  $S^1$  bundle over  $S^2$ . The total space  $X(-1)$  of the resulting bundle is the three sphere  $S^3$  as one easily sees.

The resulting fibration  $S^3 \rightarrow S^2$  is the Hopf fibration (cf. [94, Example 4.45]). Similarly, if  $X(-m)$  is the total space of the circle bundle associated to  $\mathcal{O}_{\mathbb{P}^1}(-m)$ , one has the identification  $L(m, 1) = X(-m)$ .

There is another way to describe  $L(m, 1)$  by glueing together  $S^1 \times D^+$  and  $S^1 \times D^-$  over the equator  $E$  where  $D^\pm$  is the slightly enlarged upper (lower) hemisphere. The glueing  $S^1 \times E \xrightarrow{\gamma} S^1 \times E$  is given by the matrix  $\begin{pmatrix} -1 & 0 \\ m & 1 \end{pmatrix}$  where we identify the circle with  $\{\exp\{(2\pi it)\} \in \mathbb{C} \mid t \in \mathbb{R}\}$ . In other words, we glue via

$$(\exp(2\pi ix), \exp(2\pi iy)) \xrightarrow{\gamma} (\exp(2\pi i(-x + my)), \exp(2\pi iy)).$$

It is well known (see e.g. [203, §62, Satz II]) that the lens space  $L(t, s)$  is obtained in a similar fashion by glueing via  $\begin{pmatrix} -s & t^* \\ t & s^* \end{pmatrix}$  where  $s \cdot s^* - t \cdot t^* = 1$ .

Any lens space is obtained by means of a procedure which is called **plumbing disc bundles along a tree** which we now explain. The starting point are the lens spaces  $X(a) = L(-a, 1)$  which correspond to a graph with one vertex weighted by  $a$ . A graph with two vertices with weights  $(a_1, a_2)$  leads to plumbing of  $X_1 = X(a_1)$  and  $X_2 = X(a_2)$  given by the following procedure. Let  $Y_i$  be the disc bundle corresponding to  $X_i$ ,  $i = 1, 2$ . Pick a small disc  $D_{\text{base}}^i$  in the base sphere  $S^2$  of  $Y_i$  so that the disc bundle over it is homeomorphic to a product  $D_{\text{base}}^i \times D_{\text{fiber}}^i$ . Now glue  $D_{\text{base}}^1 \times D_{\text{fiber}}^1$  to  $D_{\text{base}}^2 \times D_{\text{fiber}}^2$  by flipping the two discs. The plumbing procedure is available in all dimensions.

For instance in Figure 4.4.2 we show how 1-disc bundles over  $S^1$  are glued together to give a chain of connected ribbons.

In the present situation, the resulting disc-bundle is described by the glueing matrix

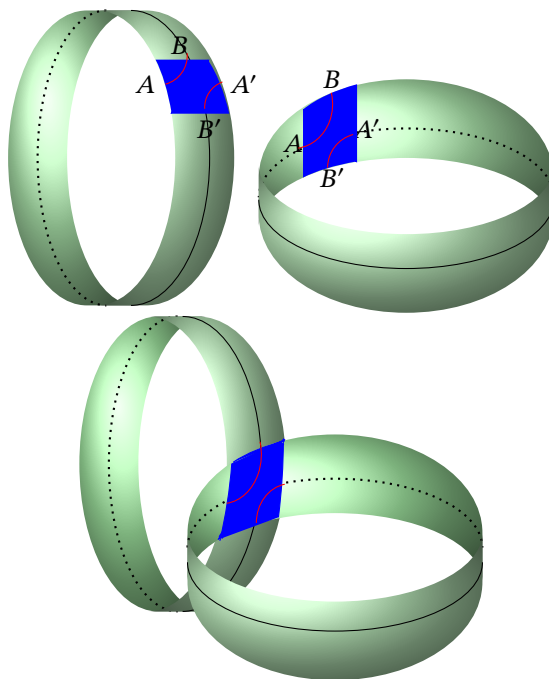
$$\begin{pmatrix} -1 & 0 \\ -a_2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ -a_1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -a_2 & 1 \end{pmatrix} \begin{pmatrix} -a_1 & 1 \\ -1 & 0 \end{pmatrix}.$$

The boundary is a circle bundle over a one-point union of two copies of  $S^2$ . Doing this repeatedly with lens spaces  $L(a_i, 1)$  for  $i = 0, \dots, n$  gives a disc bundle  $Y(a_0, \dots, a_n)$  over a surface which is the iterated wedge

$$E^{(n+1)} = \underbrace{S^2 \vee \dots \vee S^2}_{n+1 \text{ copies}}$$

of one-point unions of two-spheres. A result of Thom guarantees that the glueing does not depend on choices. See the references in [99]. The boundary  $X(a_0, \dots, a_n) = \partial Y(a_0, \dots, a_n)$  is a circle bundle over this surface. One can show that this bundle is also a circle bundle over  $S^2$  by proving that a small deformation of the "singular" zero-section, considered as the embedded base manifold  $E^{(n+1)}$ , "smoothes" to a manifold homeomorphic to  $S^2$ . We have illustrated this for the ribbon case of Figure 4.4.2. Here the product of the 1-discs is a blue square with sides  $A, B, A', B'$  which is glued to the second blue square by glueing the sides as exhibited. The common point of the two middle circles forms a double point of their union. The part of this singular curve within the square deforms into two

Figure 4.4.2: Plumbing in dimension 1



disjoint arcs. These glue to the remainder of the two circles to give a simple closed curve. This shows also that we get a 1-disc bundle over  $S^1$ .

In the present situation of lens spaces  $L(m_0, 1), \dots, L(m_n, 1)$  the resulting glueing matrix becomes

$$\begin{pmatrix} -s & * \\ t & * \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -m_n & 1 \end{pmatrix} \cdot \begin{pmatrix} -m_{n-1} & 1 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -m_0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (4.13)$$

This shows that  $X(m_0, \dots, m_n)$  is homeomorphic to the lens space  $L(t, s)$ . If we multiply the preceding equation on the left with  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  and transpose the result, we find that for certain integers  $s^*, t^*$  with  $ss^* - tt^* = 1$  we have

$$\begin{pmatrix} t & -s \\ s^* & -t^* \end{pmatrix} = \begin{pmatrix} -m_0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -m_1 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -m_n & -1 \\ 1 & 0 \end{pmatrix}. \quad (4.14)$$

From relation (4.12) we see that equation (4.14) is related to the euclidean algorithm for the pair  $(t, s^*)$ . It yields the graph  $\Gamma_{\mathbf{a}}$ ,  $\mathbf{a} = (a_0, \dots, a_n) = (-m_0, \dots, -m_n)$ . If we reverse the order of the plumbing in equation (4.13) we must reverse the order of the  $m_j$  and the modified equation (4.14) is associated to the euclidean algorithm for  $(t, -s)$ . Of course this procedure neither changes the non-oriented

graph  $\Gamma_{\mathbf{a}}$  nor the oriented homeomorphism type of  $L(t, s)$  and we say that  $L(t, s)$  is obtained by **plumbing circle bundles over  $S^2$  along the graph  $\Gamma_{\mathbf{a}}$** . The lens space  $L(t, s)$  is the boundary of a disc bundle, say  $Y(s, t)$ . It is simply connected because, by construction, the base of the fibration, a connected string of  $n+1$  two spheres – a simply connected topological space – is a deformation retract of  $Y(s, t)$ . The 2-homology of  $Y(s, t)$  is a free group with generators  $\gamma_i$  the zero-sections of the disc bundle over each copy  $S^2$  in the string of spheres. Two consecutive generators meet in a point and one can show that  $\gamma_i \cdot \gamma_i = -m_i$ .

The usual euclidean algorithm does not always give a bounding fourfold  $Y(s, t)$  with an even intersection form. However, this will be the case if  $t$  and  $s$  are not both odd and we use the modified euclidean algorithm (4.10). Summarizing:

**Proposition 4.4.5.** *The lens space  $L(t, s)$  is homeomorphic to the threefold obtained by plumbing  $S^1$ -bundles over  $S^2$  along the graph  $\Gamma_{(-m_0, \dots, -m_n)}$  where*

$$-t/s = [-m_n, \dots, -m_0].$$

*The lens space  $L(t, s)$  bounds an oriented simply connected 4-dimensional manifold  $Y(t, s)$  which is a disc bundle over a string of  $n+1$  one-point connected two-spheres. Its homology classes give a basis of  $H_2(Y(t, s), \mathbb{Z})$ . The Gram matrix of the intersection pairing with respect to this basis is the matrix  $B_{\Gamma}$ ,  $\Gamma = \Gamma_{(-m_0, \dots, -m_n)}$ . If  $s$  and  $t$  have different parity, one may assume that the  $m_i$  are even and then the index mod 16 of the lens space  $L(t, s)$  equals  $\tau(B_{\Gamma}) \bmod 16$ .*

To deal with the case where  $s$  and  $t$  are both odd, we first introduce the orientation reversing diffeomorphism  $c : (z_1, z_2) \mapsto (z_1, \bar{z}_2)$  of  $\mathbb{C}^2$ . Note that

$$\begin{aligned} c \circ \zeta \cdot (z_1, z_2) &= c(\zeta z_1, \zeta^s z_2) \\ &= (\zeta z_1, \zeta^{-s} \bar{z}_2) \\ &= \zeta^{-s} \circ c(z_1, z_2). \end{aligned}$$

This shows that the lens spaces  $L(t, s)$  and  $-L(t, t-s)$  are oriented homeomorphic. So, if  $s$  and  $t$  are both odd,  $t-s$  is even and we may instead consider  $-L(t, t-s)$ .

We now give some examples where we use the euclidean algorithm (4.10) to calculate the index mod 16. If  $s$  and  $t$  are both odd, we instead apply it to  $t$  and  $t-s$ .

**Example 4.4.6** (Non-diffeomorphic lens spaces of the same homotopy type). Let us consider  $L(7, s)$ . As we just explained,  $L(7, s) = -L(7, 7-s)$  and so we need only consider even  $s$ . It is easy to see (cf. also (4.8)) that the relevant continued fractions are given by

$$\begin{aligned} \frac{7}{2} &= 4 - \frac{1}{2} = [4, 2] \\ \frac{7}{4} &= 2 - \frac{1}{4} = [2, 4] \\ \frac{7}{6} &= \underbrace{[2, \dots, 2]}_{6 \text{ times}}. \end{aligned}$$



By the above remarks, observing the change of sign in Proposition 4.4.5, this gives

$$\begin{aligned}\tau_{16}(L(7, 5)) &= -\tau_{16}(L(7, 2)) = -2 \pmod{16} \\ \tau_{16}(L(7, 3)) &= -\tau_{16}(L(7, 4)) = -2 \pmod{16}, \\ \tau_{16}(L(7, 1)) &= -\tau_{16}(L(7, 6)) = -6 \pmod{16}.\end{aligned}$$

By Theorem 4.4.2 we have  $L(7, 2) \sim_{\text{homeo}} L(7, 4)$  (since  $4 \cdot 2 \equiv 1 \pmod{7}$ ) and hence also  $L(7, 5) \sim_{\text{homeo}} L(7, 3)$ . We see that in this case the signature mod 16 gives a complete topological classification. However, by the homotopy classification Theorem 4.4.1, the lens spaces  $L(7, 1), L(7, 2)$  and  $L(7, 4)$  have the same oriented homotopy type which differs from the collective homotopy type of  $L(7, 3), L(7, 6)$  and  $L(7, 5)$ . The upshot is that there are two oriented homotopy types but three oriented homeomorphism types.

*Remark.* The linking pairing on  $L(s, t)$  gives the torsion quadratic form  $\langle \frac{s}{t} \rangle$ . In fact the isometry class of the torsion form classifies lens spaces up to homotopy. In this example the two non-isometric torsion quadratic forms are  $\langle \frac{1}{7} \rangle$  and for example  $\langle \frac{6}{7} \rangle$ , since 1 is a quadratic residue modulo 7, but 6 is not. The example exhibits forms with different  $\mu$ -invariants but isometric linking forms such as the ones for  $L(7, 1)$  and  $L(7, 2)$ .

**Outlook.** As we saw, the  $\mu$ -invariant of a lens space is computed from the intersection form of a fourfold having the lens space as its boundary. In Section 12.1 we define the index mod 8 for any torsion quadratic form. In the preceding example we see that the linking pairings on  $L(7, 1)$  and  $L(7, 2)$  have the same index mod 8 since  $6 \equiv -2 \pmod{8}$ . The reason that the construction in loc. cit. gives a mod 8 invariant is because even unimodular forms have index divisible by 8. However, because of Rohlin's theorem, two even forms associated to the same lens space differ by even unimodular forms which have index modulo 16. This geometric reason explains why the  $\mu$ -invariant is a finer invariant.

## 4.5 Surface Singularities, Surface Fibrations and Mordell–Weil Lattices

**4.5.A Some special singularities.** In the previous section we considered the action of the cyclic group of  $t$ -th roots of unity  $\mu_t \simeq \mathbb{Z}/t\mathbb{Z}$  on the complex plane with coordinates  $(z, w)$  given by

$$\rho_{t,s}(\zeta)(z, w) = (\zeta \cdot z, \zeta^s \cdot w). \quad (4.15)$$

We restricted the action to the unit three sphere  $S^3$  in  $\mathbb{C}^2$  and investigated properties of the resulting lens space  $L(t, s)$ . The action is without fixed points on  $S^3$ .

In this section we consider the action on  $\mathbb{C}^2$  where it has a unique fixed point, the origin. Hence

$$W_{t,s} := \mathbb{C}^2 / \rho_{t,s}(\mu_t)$$

has a singularity at the origin. It is called the **Hirzebruch–Jung singularity**  $A_{t,s}$ .

The disk bundle  $Y(t,s)$  considered in Proposition 4.4.5 constructed using the non-modified euclidean algorithm (4.9) has a natural complex structure, as shown in [15, Ch. III.5]. Moreover, away from the zero section this structure is compatible with the complex structure on  $[\mathbb{C}^2 - \{0\}] / \rho_{t,s}(\mu_t)$ . The zero section of the disc bundle is a string of complex projective lines  $E^{(n+1)} := E_1 \cup \dots \cup E_{n+1}$  whose intersection behaviour is given by the graph  $\Gamma_{(-m_0, \dots, -m_n)}$  where  $-t/s = [-m_n, \dots, -m_0]$ . Hence  $E_j \cdot E_j = -m_j$ , and consecutively numbered  $E_j$  meet transversely in a point and there are no other intersections between the curves  $E_j$ . The graph  $\Gamma_{(-m_0, \dots, -m_n)}$  is called the **dual graph of the configuration** consisting of the  $E_j$ . Glueing  $Y(t,s)$  and  $\mathbb{C}^2 - \{0\}$  along  $Y(t,s) - E^{(n+1)}$  results in a complex surface  $\widetilde{W}_{t,s}$  together with a holomorphic map  $\pi : \widetilde{W}_{t,s} \rightarrow W_{t,s}$  which is biholomorphic outside  $E^{(n+1)}$  and contracts  $E^{(n+1)}$  to the singularity at 0. The subvariety  $E^{(n+1)}$  is called the **exceptional divisor**. A holomorphic map such as  $\pi$  from a smooth surface to a surface with an isolated singularity  $p$  and which is biholomorphic outside  $\pi^{-1}p$  is a **resolution of the singularity  $p$** . The simplest example is the singularity  $A_{2,1}$ , an ordinary double point with local equation  $uv = w^2$ . The exceptional subvariety consists of a single  $\mathbb{P}^1$  with self-intersection  $-2$ . More generally, we may consider  $A_{n+1,n}$  with local equation  $uv = w^{n+1}$ . This is also a double point, usually denoted  $A_n$ . By Eqn. (4.8) one has  $\frac{n+1}{n} = [2, 2, \dots, 2]$  ( $n$  times), and so the exceptional set consists of a string of  $n$  curves with self-intersection  $-2$ . In other words, its dual graph is  $A_n(-1)$ .

**4.5.B On isolated surface singularities.** Any isolated singularity can be desingularised in several ways but there is a canonical way to do this such that the exceptional divisor does not contain  $(-1)$ -curves. See e.g. [15, §III.6]. Moreover, the intersection matrix for the components of the exceptional divisor is always negative definite as we shall now demonstrate. We first recall that the group of divisors on an algebraic surface  $X$  modulo homological equivalence by definition is the **Néron–Severi group**  $\text{NS}(X)$  of  $X$ . It has finite rank  $\rho(X)$ , the **Picard number** of  $X$ . We can now show our claim:

**Proposition 4.5.1** (Mumford [163]). *The intersection matrix for the components of the exceptional divisor of an isolated singularity is negative definite.*

*Proof.* Suppose  $p$  is an isolated singular point in a complex projective variety  $\bar{X} \subset \mathbb{P}^n$  of dimension 2 and let

$$\pi : X \rightarrow \bar{X}$$

be a resolution of singularities. Pick a hyperplane  $H$  in  $\mathbb{P}^n$  not passing through  $p$  and let  $D = \pi^{-1}(H \cap \bar{X})$ . Two hyperplanes intersect in a codimension 2 linear space which generically meets the surface  $\bar{X}$  in a finite (positive) number of points, the

degree of  $\bar{X}$ . Hence we have  $D \cdot D = H \cdot H > 0$ . Any component of the exceptional divisor  $E$  is orthogonal to  $D$ . The algebraic index theorem (cf. Theorem B.2.6) states that the intersection pairing on  $\text{NS}(X)$  is non-degenerate and has signature  $(1, \rho - 1)$ . So it is negative definite on the orthogonal complement of  $D$ .  $\square$

We shall now discuss some singularities which play a major role in this book. The quotient singularities  $A_n$  we discussed in the previous paragraph are special cases of the so-called **du Val singularities**. For the remaining du Val singularities

Table 4.5.1: List of du Val singularities

Name	equation	dual graph
$A_n$	$uv + t^{n+1} = 0$	$A_n(-1)$
$D_n$	$u^2 + tv^2 + t^{n-1} = 0$	$D_n(-1)$
$E_6$	$u^2 + v^3 + t^4 = 0 = 0$	$E_6(-1)$
$E_7$	$u^2 + v^3 + vt^3 = 0$	$E_7(-1)$
$E_8$	$u^2 + v^3 + t^5 = 0$	$E_8(-1)$

the dual graph is one of the graphs of type  $D$  or  $E$  which we have encountered in Section 4.1. These are not cyclic quotient singularities since their dual graphs have vertices where 3 or more edges come together. However, as we recall below in Proposition 4.5.2, these are still **quotient singularities**, i.e. singularities obtained by taking quotients by finite groups, but in this case these groups are not cyclic. A list of local equations for these singularities is given in [15, Ch. III.7]. The reader also finds an explicit procedure to resolve such a singularity and this process shows that indeed the dual graph for the exceptional divisor is exactly the corresponding graph we just listed.

The du Val singularities are precisely the so-called **rational surface singularities** which have several equivalent characterizations collected in A. Durfee's survey paper [57]:

**Proposition 4.5.2.** *Let  $x \in \bar{X}$  be an isolated surface singularity and let  $X$  be the minimal resolution of singularities of  $\bar{X}$ . The singularity  $x$  is rational if one of the following equivalent conditions is true:*

1.  $K_X$  is trivial in the neighborhood of the exceptional locus;
2.  $x$  is a Du Val singularity;
3.  $x$  is an isolated quotient singularity, that is, there is a neighborhood of  $x$  in  $\bar{X}$  which is biholomorphic to  $U/G$  where  $U$  is a neighborhood of the origin in  $\mathbb{C}^2$  and  $G$  is a finite subgroup of  $\text{SU}(2)$ .

**4.5.C Surface fibrations give semi-definite lattices.** By definition a *surface fibration* is a holomorphic map  $f : X \rightarrow C$  from a surface  $X$  to a smooth curve  $C$  with connected curves as fibers. Let  $F$  be the generic (smooth) fiber. Since two such fibers are clearly homologous as cycles and since different fibers don't meet, we have  $F \cdot F = 0$ . Let  $\sum m_i D_i$  be a reducible fiber with irreducible components  $D_i$  and with dual graph  $\Gamma$ .

**Lemma 4.5.3** (Zariski's Lemma). *Denote the span of the classes of the  $D_j$  by  $\langle \Gamma \rangle \subset \text{NS}(X)$ . Then the intersection form restricted to  $\langle \Gamma \rangle$  is negative semi-definite. Its null-space is one-dimensional and spanned by the class  $[F]$  of a generic fiber.*

*Proof.* The intersection form on  $\langle \Gamma \rangle$  is negative semi-definite since it is the orthogonal complement of the isotropic vector  $[F]$  in a lattice of signature  $(1, \rho(X) - 1)$ . Since  $\Gamma$  is connected, Lemma 4.1.4 then implies that the null-space of  $\langle \Gamma \rangle$  is one-dimensional and spanned by  $[F]$ .  $\square$

*Remark.* It is possible that  $f$  admits multiple fibers with multiplicity  $> 1$  (this cannot occur if the fibration has a section). For a multiple fiber there are local coordinates  $(u, v)$  in  $X$  such that the fibration is given by  $f(u, v) = v^k$ . In that case the fiber  $F_0$  over  $v = 0$  has multiplicity  $k$  and thus  $[F_0] = k \cdot [F]$ .

Next, we investigate a special case, that of a fibration in genus 1 curves, also called an *elliptic fibration*. A surface equipped with an elliptic fibration is called an *elliptic surface*. We assume in addition that there is a section, and that  $f$  is *relatively minimal*, that is,  $X$  does not contain  $(-1)$ -curves as component of a fiber of  $f$ . The canonical divisor of  $X$  is an integral multiple of the class of a fiber, as expressed by the *canonical bundle formula*

$$[K_X] = r \cdot [F], \quad r = 2g(C) - 2 + \frac{1}{12}e(X). \tag{4.16}$$

This formula follows from [15, Ch. V, Thm. (12.1), Prop. (12.2)], stating that  $K_X = f^*L$  where  $L$  is a line bundle on the curve  $C$  of degree  $2g(C) - 2 + \chi(\mathcal{O}_X)$ , where  $\chi(\mathcal{O}_X) = \frac{1}{12}(c_1^2(X) + c_2(X))$ . But since  $c_1^2(X) = K_X \cdot K_X = f^*L \cdot f^*L = 0$ , the relation (4.16) follows. Using the canonical bundle formula one arrives at a description of the possible singular fibers:

**Corollary 4.5.4.** *Suppose that  $f : X \rightarrow C$  is a fibration in elliptic curves with a section. Then the dual graph of a reducible singular fiber is an extended Dynkin diagram of type  $\tilde{A}$ - $\tilde{D}$ - $\tilde{E}$ .<sup>4</sup>*

*Proof.* Suppose that  $F$  is a reducible singular fiber. An irreducible component  $C_i$  of  $F$  is necessarily a smooth  $\mathbb{P}^1$  and two components  $C_i, C_j$  can only meet in at most one point. To see this, by (4.16), one has  $K_X \cdot C_i = rF \cdot C_i = 0$  in this case. Hence, by the adjunction formula (B.7),

$$-2 \leq 2p_a(C_i) - 2 = C_i \cdot C_i.$$

---

<sup>4</sup>If  $f$  has no sections there are multiple fibers. For this case see Remark 4.5.5.

On the other hand, Zariski's lemma implies that  $C_i \cdot C_i < 0$ . Since by the above formula it is even, we must have  $C_i \cdot C_i = -2$  and it follows that  $p_a(C_i) = 0$ . Hence, by (B.7) the curve  $C_i$  is a smooth rational curve. Zariski's Lemma applied to  $C_i + C_j$  then implies that

$$0 \geq (C_i + C_j) \cdot (C_i + C_j) = -4 + 2C_i \cdot C_j$$

and so  $C_i \cdot C_j \in \{0, 1, 2\}$ . In the last case  $C_i + C_j$  spans the kernel and so  $\Gamma = \widetilde{A_1(-1)}$ . In the other cases we apply Proposition 4.1.4 to see that  $\Gamma$  is one of the extended Dynkin diagrams of type  $\widetilde{A}$ - $\widetilde{D}$ - $\widetilde{E}$ .  $\square$

*Remark 4.5.5.* In Table 4.5.2 below we give Kodaira's list of singular fibers (cf. [15, Ch. V.7]). The multiple fibers are either multiple non-singular elliptic curves or multiple  $A_n$ -fibers. The irreducible singular fibers are either nodal ( $\widetilde{A}_0$ ) or cuspidal (type *II*). There are two  $\widetilde{A}_1$ -fibers: the two components meet in two points transversally or are tangent in one point. There are also two type  $\widetilde{A}_2$ -fibers: the three components either meet transversally and form a cycle or they meet transversally in one point. The different types have specific Kodaira symbols. We collect these as well as the values of the Euler numbers of the singular fibers in a table. Here  $T$  is an irreducible Dynkin diagram and  $\widetilde{T}$  the corresponding extended Dynkin diagram.

Kodaira symbol	extended Dynkin diagram $\widetilde{T}$	disc( $T$ )	Euler number
$I_b, b \geq 1$	$\widetilde{A}_{b-1}$	$b$	$b$
<i>II</i>	cuspidal	-	2
<i>III</i>	$\widetilde{A}_1$ (tangential)	2	3
<i>IV</i>	$\widetilde{A}_2$ (concurrent)	3	4
$I_b^*, b \geq 0$	$\widetilde{D}_{4+b}$	4	$b + 6$
<i>II</i> *	$\widetilde{E}_8$	1	10
<i>III</i> *	$\widetilde{E}_7$	2	9
<i>IV</i> *	$\widetilde{E}_6$	3	8

Table 4.5.2: Singular non-multiple fibers of an elliptic fibration.

We list a few further properties of elliptic fibrations that we shall make use of:

**Proposition 4.5.6.** *Let  $f : X \rightarrow C$  be a (relatively minimal) elliptic fibration with a section  $s$  and singular fibers over  $\Sigma \subset C$ . Then*

1.  $e(X) = \sum_{c \in \Sigma} e(F_c) \geq 0$  and  $> 0$  as soon as there is at least one singular fiber.
2.  $[s] \cdot [s] = -\frac{1}{12}e(X)$ .
3.  $\tau(X) = -\frac{2}{3}e(X)$ .

*Proof.* 1. The first equality follows from the additive nature of the Euler number and the fact that a smooth elliptic curve has zero Euler number. Since  $f$  has a section, there are no multiple singular fibers. Table 4.5.2 shows that the singular fibers all have positive Euler number.

2. The adjunction formula (B.7), item 1 and the fact that  $s$  is isomorphic to the base curve  $C$  show that

$$\begin{aligned} 2g(C) - 2 &= [s] \cdot [s] + [s] \cdot K_X \\ &= [s] \cdot [s] + 2g(C) - 2 + \frac{1}{12}e(X) \end{aligned}$$

and hence  $[s] \cdot [s] = -\frac{1}{12}e(X)$ .

3. Since  $c_1^2 = 0$  and  $c_2(X) = e(X)$ , this follows from the Index Theorem B.2.1.  $\square$

**4.5.D Picard lattices of elliptic surfaces.** We investigate the Picard lattice of an elliptic surface  $X$ . Let  $\pi : X \rightarrow C$  be a relatively minimal elliptic fibration with a section. The Picard lattice  $\text{NS}(X)$  contains some obvious divisor classes: the class  $s$  of the (zero) section, the class  $f$  of a smooth fiber  $\pi^{-1}c, c \in C$ , and the components of the reducible fibers. These span the so-called *trivial lattice*  $\text{NS}(S)_{\text{triv}}$ . A basis for this lattice is given by  $s, f$  together with the components of the reducible fibers not meeting the zero section. So  $\text{NS}(S)_{\text{triv}}$  is isometric to  $U \oplus R$ , where  $R$  is a direct sum of irreducible negative definite root-lattices.

There might be many more sections. It is known that these form a finitely generated abelian group, the Mordell–Weil group  $\text{MWL}(X)$  which is the subject of the next subsection. In particular, we shall see that the Picard number of  $X$  is given by

$$\text{rank}(\text{NS}(X)) = \text{rank}(\text{NS}(S)_{\text{triv}}) + \text{rank}(\text{MWL}(X)).$$

Torsion sections meet the singular fibers also in torsion points of a group structure on the fiber which can be described as follows. Delete the singularities of the singular fiber (the multiple components, the crossings and self-crossings of the components). The resulting smooth curve  $F$  has a natural group structure with identity component  $F_0$ , torsion  $F/F_0 = T(F)$  as collected in the following table.

Type of $F$	$F_0$	$T(F)$
$I_b, b \geq 1$	$\mathbb{C}^*$	$\mathbb{Z}/b\mathbb{Z}$
$II$	$\mathbb{C}$	$0$
$III$	$\mathbb{C}$	$\mathbb{Z}/2\mathbb{Z}$
$IV$	$\mathbb{C}$	$\mathbb{Z}/3\mathbb{Z}$
$I_b^*, b > 0$ odd	$\mathbb{C}$	$\mathbb{Z}/2\mathbb{Z}$
$I_b^*, b > 0$ even	$\mathbb{C}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$II^*$	$\mathbb{C}$	$0$
$III^*$	$\mathbb{C}$	$\mathbb{Z}/2\mathbb{Z}$
$IV^*$	$\mathbb{C}$	$\mathbb{Z}/3\mathbb{Z}$

In case the Mordell–Weil group is a torsion group, the fact that  $\text{NS}(X)/\text{NS}(X)_{\text{triv}} = \text{MWL}(X)$  implies that

$$\text{disc}(\text{NS}(X)_{\text{triv}}) = \text{disc}(\text{NS}(X)) \cdot [\text{NS}(X) : \text{NS}(X)_{\text{triv}}]^2. \tag{4.17}$$

So in this situation square-freeness of the trivial lattice prevents torsion. Even if the Mordell–Weil group has positive rank it follows from [202, Prop. 6.31]) that in case  $\text{disc}(\text{NS}(X)_{\text{triv}})$  is square free, there is no torsion in the Mordell–Weil group. Since the discriminant of the trivial lattice can be found immediately from Table 4.5.2, this gives restrictions on the size of the torsion group. For instance there is no torsion if there are no reducible fibers, only one reducible fiber of type  $II^*$  or of type  $I_m$ ,  $m$  square free, or two reducible fibers, one of type  $IV$  and one of type  $III$ .

We finish this subsection with an example showing how lattice theory is used to find the Picard lattice of a given elliptic K3 surface.

**Example 4.5.7.** Let  $\pi : X \rightarrow \mathbb{P}^1$  be an elliptic fibration with  $s$  the class of a section, and  $f$  the class of a smooth fiber. Suppose that  $\pi$  has the following singular fibers: 7 type  $I_1$ -fibres, 7 type  $I_2$ -fibres and one type  $III$ -fiber. From Table 4.5.2 one sees that  $e(X) = 7 \times 1 + 7 \times 2 + 3 = 24$  so that the canonical bundle formula (4.16) tells us that  $K_X$  is trivial. It then follows from the Classification Theorem B.5.4 that  $X$  is a K3 surface. The lattice  $\text{NS}(X)_{\text{triv}}$  is isometric to  $U \oplus \bigoplus^8 A_1(-1)$  and so has discriminant  $-2^8$ .

From now on we suppose that the Mordell–Weil group is torsion. It then embeds in the direct sum of the torsion groups of the reducible fibers. In view of the above table this means that  $\text{MWL}(X) \subset \bigoplus^8 \mathbb{Z}/2\mathbb{Z}$ . In particular, a section representing a torsion element in the Mordell–Weil group is 2-torsion. Suppose that there exists a non-zero 2-torsion section  $s'$ . Because of the assumption on the Mordell–Weil group  $s'$  is a  $\mathbb{Q}$ -linear combination of  $s, f$  and  $\alpha_1, \dots, \alpha_8$ , the standard root basis of  $\bigoplus^8 A_1(-1)$  represented by nodal classes that do not intersect the section  $s$ . So  $s \cdot \alpha_i = 0$ ,  $i = 1, \dots, 8$ . Also  $s \cdot s' = 0$ ,  $s \cdot f = s' \cdot f = 1$  and  $s \cdot s = s' \cdot s' = -2$ . Since every section meets exactly one of the 2 components of the 8 reducible fibers, this shows that in this case  $s' = 2f + s - \frac{1}{2} \sum_{i=1}^8 \alpha_i$ . In particular, there cannot be another 2-torsion section since it must be numerically equivalent to  $s'$ , but since  $s' \cdot s' = -2$  it must coincide with  $s'$ . So this implies that a non-trivial torsion group is the cyclic group  $\mathbb{Z}/2\mathbb{Z}$ .

If this is the case,  $L = \text{NS}(X)$  has basis  $s, f, \alpha_1, \dots, \alpha_7, \beta := -\frac{1}{2} \sum_{i=1}^8 \alpha_i$ . The discriminant of the lattice equals  $-2^6$ . Using results of later chapters one can show that  $M = U(2) \oplus \bigoplus^2 D_4(-1)$  and  $L$  are in the same genus. In view of Theorem 1.13.2 they are then isometric as well.

Surfaces with a Picard lattice isometric to  $M$  do exist. We shall outline how to show that the minimal smooth model of a general surface of degree 14 in weighted projective space <sup>5</sup>  $\mathbb{P}(2, 2, 3, 7)$  with coordinates  $x, y, z, w$  indeed has such a Picard lattice. Note that hypersurfaces in weighted projective space in general have singularities. In the present situation a general enough surface has the following singularities:

- a singular point at  $(0 : 0 : 1 : 0) \in \mathbb{P}(2, 2, 3, 7)$  which can be resolved by an  $A_2$ -configuration;

<sup>5</sup> [107] is a general reference for properties of surfaces in weighted projective space.

- 7 ordinary double points where the line  $\{z = w = 0\} \subset \mathbb{P}(2, 2, 3, 7)$  meets the surface.

Such a surface is in fact number 22 in Reid’s list of K3 surfaces reproduced in [107, §13.1]. The minimal resolution of singularities has 7 nodal curves and one  $A_2$ -configuration and so the Picard rank is at least  $9 + 1 = 10$ . By [21, Lemma 3.1] this is the Picard number of a general such surface. In fact, one can take the minimal resolution  $X$  of the hypersurface whose equation in weighted homogeneous coordinates is given by  $w^2 - (x^7 + y^7 + yz^4 + x^2y^2z^2) = 0$ . The latter has an elliptic pencil given by  $(x : y : w : z) \mapsto (x : y)$ , i.e., it is cut out by the pencil of planes through the line  $x = y = 0$  containing the singular point  $(0 : 0 : 1 : 1)$ . On  $X$  this point is resolved by an  $A_2$ -configuration and one of the nodal curves is a section for the pencil. Now pass to the double cover inside  $\mathbb{P}(1, 2, 3, 7)$  which in weighted homogeneous coordinates  $\xi, y, z, w$  is given by

$$w^2 - (\xi^{14} + y^7 + yz^4 + \xi^4y^2z^2) = 0.$$

The elliptic pencil on  $X$  comes from the pencil  $(\xi : y : w : z) \mapsto (\xi^2 : y)$  which admits the involution  $\xi \mapsto -\xi$ . One can show (see [181, Prop.3.3.1]) that the minimal resolution  $Y$  of the double cover is a properly elliptic surface with  $e(Y) = 24$  and using this, that the set of reduced singular fibers consists of 7 fibers of type  $I_2$  (at the double roots of  $(4t^7 - t^3 + 4)^2 = 0$ ), one of type  $III$  (at  $t = 0$ ) and 7 fibers of type  $I_1$  (at the roots of  $1 + t^7 = 0$ ). Moreover, the fiber at  $t = \infty$  is a double fiber whose reduction is a smooth elliptic curve. The involution preserves the elliptic fibration fiberwise and induces a translation  $j$  of order 2 in each smooth fiber. By [181, Prop.3.1.1]) the unique singular point  $(0 : 0 : 1 : 0)$  of the cover is resolved by a rational curve of self-intersection  $-3$  which on  $Y$  becomes a bi-section of the fibration. It intersects every elliptic curve in two points which are interchanged under  $j$ . Its quotient under  $j$  is a section of the elliptic fibration on  $X$ . Moreover, the quotients under  $j$  of the 7 type  $I_2$  fibers become of type  $I_1$  in  $X$ , while the quotients of the 7 type  $A_1$  singularities become  $I_2$ -fibers on  $X$ . The fiber at  $t = 0$  remains of type  $III$ . The fiber structure of  $X$  is the same as for a general quasi-smooth surface of degree 14 in  $\mathbb{P}(2, 2, 3, 7)$ . So the trivial Picard lattice is isometric to  $U \oplus \bigoplus^8 A_1(-1)$  as claimed. On  $Y$  one has a further bi-section given by  $t \mapsto (1, t, 0, \pm\sqrt{1+t^7})$ . After taking the quotient by  $j$  this becomes a second section for the pencil on  $X$  which is disjoint from the one coming from the singular point. By the preceding arguments this is a non-trivial 2-torsion section and the Picard lattice of the K3 surface  $X$  is isometric to  $M = U(2) \oplus \bigoplus^2 D_4(-1)$ . This turns out to be the case for all sufficiently general members of the family to which  $X$  belongs.<sup>6</sup> This confirms [20, §3.32] in the thesis of Belcastro.

**4.5.E Mordell–Weil lattices.** In this section we describe Elkies–Shioda’s construction [69, 210] of the Mordell–Weil lattice following the monograph [202] by

<sup>6</sup>Using [181, Prop.2.2.1(a)] each member of the family is projectively equivalent to a surface whose equation has the form  $yz^4 + G_4(\xi^2, y)z^2 + G_7(\xi^2, y) = 0$  where  $G_j$  is an ordinary homogeneous polynomial of degree  $j = 4, 7$  (so that the bisection is given by  $t \mapsto (1, t, 0, \pm\sqrt{G_7(1, t)})$ ).



M. Schütt and T. Shioda. We only give a minimal introduction to this fascinating subject and present some instructive examples.

If  $K$  is the function field of the base curve  $C$  of an elliptic fibration  $\pi : X \rightarrow C$  with a section, one can view  $X$  as an elliptic curve  $E$  over  $K$ . The section gives a  $K$ -rational point, say  $o_K$ . If we view  $X$  in this way we shall write  $E_K$ . The point  $o_K$  serves as the origin of an additive group on  $E_K$ , the **Mordell–Weil group** of  $E_K$ , written  $\text{MWL}(E_K)$ . In geometric language  $\text{MWL}(E_K)$  is the group of sections for the fibration  $f$ . In the previous subsection we wrote  $\text{MWL}(\cdot)X$  to stress the surface. In particular, there is a natural map  $\text{MWL}(E_K) \rightarrow \text{NS}(X)$  sending a section  $s$  to its class  $[s]$  in  $\text{NS}(X)$ . However, this map is in general not injective and of course never surjective since it misses the class of a fiber. Surprisingly, by [210] one does obtain an isomorphism of groups

$$\begin{aligned} \psi : \text{MWL}(E_K) &\xrightarrow{\sim} \text{NS}(X)/\text{NS}(X)_{\text{triv}} \\ s &\mapsto [s] \bmod \text{NS}(S)_{\text{triv}}. \end{aligned}$$

The next step is to put a lattice structure on the Mordell–Weil group. To do this, one shows ([202, Lemma 6.16]):

**Lemma 4.5.8.** *The homomorphism  $\psi$  lifts to a group homomorphism*

$$\phi : \text{MWL}(E_K) \longrightarrow \text{NS}(X)_{\mathbb{Q}},$$

which is uniquely defined by the properties that

- $[s] = \phi(s) \bmod \text{NS}(X)_{\text{triv}}$ ;
- $\phi(s) \in \text{NS}(X)_{\text{triv}}^{\perp}$ .

One has  $\ker \phi = \text{MWL}(E_K)_{\text{torsion}}$  and the induced injection

$$\text{MWL}(f) := \text{MWL}(E_K)/\text{MWL}(E_K)_{\text{torsion}} \hookrightarrow \text{NS}(X)_{\text{triv}, \mathbb{Q}}^{\perp}$$

induces an isomorphism over  $\mathbb{Q}$ .

We now pass to the intersection pairing. We have seen that it restricts to a non-degenerate bilinear pairing on  $\text{NS}(X)$  of signature  $(1, \rho - 1)$ . Since the image of  $\phi$  is orthogonal to the trivial lattice, it contains the classes of a fiber and a section which together generate a sublattice isometric to the hyperbolic plane  $U$  with signature  $(1, -1)$ . It follows that the induced pairing on the orthogonal complement of the trivial lattice is negative definite. Consequently, the pairing

$$\begin{aligned} \text{MWL}(f) \times \text{MWL}(f) &\xrightarrow{\langle \cdot, \cdot \rangle} \mathbb{Q} \\ (s, s') &\longmapsto \langle s, s' \rangle = -\phi(s) \cdot \phi(s') \end{aligned}$$

is positive definite. It is called the **height pairing**. Although it is in general not integer valued, the pair  $(\text{MWL}(f), \langle \cdot, \cdot \rangle)$  thus obtained is usually called the **Mordell–Weil lattice**. Its rank is called the **Mordell–Weil rank** of the elliptic surface.

**Examples 4.5.9. 1. The Hesse pencil.** See [202, Example 3.13, 6.36]. This is the pencil of plane cubics given by

$$x^3 + y^3 + z^3 + txyz = 0.$$

The curve is singular exactly for  $t = 3, 3\rho, 3\rho^2$ , where  $\rho$  is a primitive cube root of unity. Also for  $t = \infty$  one has a singular fiber. Each singular fiber is a union of three distinct lines, and so is of type  $\tilde{A}_2$ .

The base points of the pencil are the nine points  $(1, -1, 0)$ ,  $(1, -\rho, 0)$ ,  $(1, -\rho^2, 0)$  and their cyclic permutations. These are the 9 inflection points for each of the smooth members of the pencil and so the addition law of the elliptic curve shows that they correspond to 3-torsion.

Replacing  $t$  with  $t_1/t_0$  gives a surface  $X \subset \mathbb{P}^1 \times \mathbb{P}^2$  which is smooth as one easily verifies. The projection of  $\mathbb{P}^1 \times \mathbb{P}^2$  onto the first factor induces an elliptic fibration  $\pi : X \rightarrow \mathbb{P}^1$ . Since  $\infty$  corresponds to  $(1, 0) \in \mathbb{P}^1$  the fiber at infinity corresponds to the curve  $xyz = 0$ , a union of three lines. The base points of the pencil become 9 sections, e.g.  $(1, -1, 0)$  becomes  $t \mapsto t \times (1, -1, 0)$ . We may take the latter as the zero section. The 9 sections give a full 3-torsion group of the Mordell–Weil group.

Adding the Euler numbers of the singular fibers, Proposition 4.5.6.1 gives  $e(X) = 4 \cdot 3 = 12$ , in accordance with the rationality of  $X$ . Indeed,  $X$  is the projective plane blown up at the 9 base points of the pencil and so  $e(X) = 3 + 9 = 12$ . The Néron–Severi lattice is the full intersection lattice  $H^2(X, \mathbb{Z})$  and hence is unimodular. Indeed, it is easy to see that  $\text{NS}(X) \simeq \langle 1 \rangle \oplus \bigoplus^9 \langle -1 \rangle$  with basis given by the class of a line and the classes of the 9 disjoint exceptional curves coming from blowing up the base points of the pencil. The trivial lattice has rank  $2 + 4 \cdot 2 = 10$  since it is isometric to  $U \oplus \bigoplus^4 A_2(-1)$  and so the Mordell–Weil group is torsion, more precisely  $\text{MWL}(\pi) \simeq \bigoplus^2 \mathbb{Z}/3\mathbb{Z}$ . This shows that the class map  $\text{MWL}(\pi) \rightarrow \text{NS}(X)$  need not be injective, since as in the present example,  $\text{NS}(X)$  can be torsion free while  $\text{MWL}(\pi)$  contains torsion. For this example the Mordell–Weil lattice is the trivial lattice 0.

**2.** We consider in detail the *hexagonal lattice* which is the leading example in the book [202]. See in particular [202, Example 5.9, 6.26, 6.41]. One starts with an elliptic pencil in the plane given in inhomogeneous coordinates  $x, y$  by

$$y^2 + ty = (x - a_1)(x - a_2)(x - a_3), a_i \in \mathbb{C},$$

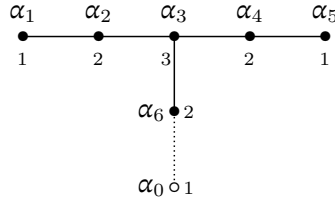
where the  $a_i$  are pairwise distinct. Making this homogeneous by setting  $x = z_1/z_0, y = z_2/z_0$  and  $t = t_1/t_0$ , one obtains

$$t_0 z_0 z_2^2 + t_1 z_0^2 z_2 = t_0 (z_1 - a_1 z_0)(z_1 - a_2 z_0)(z_1 - a_3 z_0),$$

a surface in  $\mathbb{P}^2 \times \mathbb{P}^1$  which has a single singularity at  $\infty \times (0, 0, 1)$ , where  $\infty = (0, 1) \in \mathbb{P}^1$ . A local calculation shows it to be a double point of type  $A_5$ . Let  $X$  be its minimal desingularisation. The projection of  $\mathbb{P}^1 \times \mathbb{P}^2$  onto the first factor induces an elliptic fibration

$$f : X \rightarrow \mathbb{P}^1$$

which has 4 singular fibers of type  $I_1^*$  (irreducible with one node) and a single reducible fiber over  $\infty$  which is of type  $\widetilde{E}_6$  (matching the  $A_5$ -singularity). We reproduce the corresponding Dynkin diagram with multiplicities which now correspond to multiplicities of the fiber components.

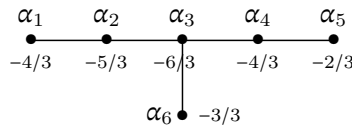


The zero section is given by  $t \mapsto (1, t) \times (0, 1, 0)$ . We consider three more sections  $P_i$  given by  $t \mapsto (1, t) \times (1, a_i, 0)$ ,  $i = 1, 2, 3$ . The addition law on the cubic curve shows that  $P_1 + P_2 + P_3 = 0$ . All sections meet the  $\widetilde{E}_6$ -fiber at  $\infty$  in components with multiplicity 1, i.e., the components corresponding to either one of the three extremal edges. We assume that the zero section meets the  $\alpha_0$ -component. We claim that the four sections  $0, P_1, P_2, P_3$  are mutually disjoint and meet the same fiber component of the  $\widetilde{E}_6$ -fiber, which we may assume to correspond to  $\alpha_1$ . This is easy to see away from the fiber at  $\infty$  and requires a careful local computation at the point  $\infty \times (0, 0, 1)$ .

Let us compute the Mordell–Weil rank. Adding the Euler numbers of the singular fibers gives  $4 + 8 = 12$  in accordance with the rationality of  $X$ . Indeed,  $p_g(X) = 0 = q(X)$  and so  $b_2(X) = 10$ . The Néron–Severi lattice is the full intersection lattice  $H^2(X, \mathbb{Z})$  and hence is unimodular. It is odd, since by Lemma 4.5.6, sub 2, three sections  $P_i$  as well as the zero section all have self-intersection  $-\frac{1}{12}e(X) = -1$ . As in the case of the Hesse pencil, we find that  $\text{NS}(X)$  is isometric to  $\langle 1 \rangle \oplus \oplus^9 \langle -1 \rangle$ , but this time we use Lemma 4.5.6, sub 3 to see that the index equals  $-\frac{2}{3}e(X) = -8$ . The trivial lattice is isometric to  $U \oplus \oplus^6 E_6(-1)$  and so the Mordell–Weil rank is 2. One can show that there is no torsion (cf. [202, Example 6.32]) and that  $P_1, P_2$  give a basis for  $\text{MWL}(f)$ . Then an easy calculation using Lemma 4.5.8 shows:

$$\phi(P_i) = [P_i] - [0] - F - R, \quad R = \sum_{j=1}^6 m_j \alpha_j,$$

where the  $m_i$  are given in the diagram below, just underneath the roots. Indeed the equations  $0 = \phi(P_i) \cdot [0] = \phi(P_i) \cdot F = \phi(P_i) \cdot \alpha_j$ ,  $j = 1, \dots, 6$ , together with  $\phi(P_i) \equiv [P_i] \pmod{\text{NS}(S)_{\text{triv}}}$  give the (unique) solution we just described.



Finally, let us compute the height pairing. We give a direct computation, although there is a general recipe for which we refer to [202, Theorem 6.24].

Observe first that  $R \cdot R = R \cdot P_i = -\frac{4}{3}$  and  $([0] + F + R)^2 = ([0] + F + R) \cdot P_i = -\frac{1}{3}$  and hence

$$\begin{aligned} -\langle P_i, P_j \rangle &= \phi(P_i) \cdot \phi(P_j) = [P_i] \cdot [P_j] - 2([0] + F + R) \cdot [P_i] + ([0] + F + R)^2 \\ &= [P_i] \cdot [P_j] + \frac{2}{3} - \frac{1}{3} \\ &= -\delta_{ij} + \frac{1}{3}. \end{aligned}$$

Taking  $P_1, P_2$  for the generators of  $\text{MWL}(f)$ , we conclude that the Gram matrix for the height pairing is  $\begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$ . This is the inverse of the Gram matrix for  $A_2$  with respect to the basic roots  $\alpha_1, \alpha_2$  of  $A_2$  (cf. Section 4.1.A), and so  $\text{MWL}(f) \simeq A_2^*$ . This lattice is the hexagonal lattice in the euclidean plane as pictured as [202, Fig. 1.3].

**3. Large Mordell–Weil rank.** In [202] many examples are given. Let us describe just one example due to Shioda [202, Theorem 13.26]. Consider the complex surface

$$X_m : y^2 = x^3 + t^m + 1, \quad m \in \mathbb{N}.$$

The map  $(x, y, t) \mapsto t$  gives it the structure of an elliptic fibration. When  $m = 6d$  all singular fibers are irreducible of type *II* at the zeroes of  $t^m + 1$ . By Table 4.5.2 this implies that  $e(X_m) = 2m = 12d$  and thus  $b_2(X_m) = 2m - 2$ . The Hodge decomposition shows that the rank of the Néron–Severi group is potentially as large as  $10d - 4$  which implies that the Mordell–Weil rank of  $X_m$  can be at most  $10d - 6$ . It turns out that, however, it is much smaller: it has rank at most 68 with equality if and only if  $m$  is divisible by 360.

**Historical and Bibliographical Notes.** The classical reference for the Dynkin diagrams of types A–D–E–F–G and their extended cousins is the Bourbaki volume [26]. The role of the Lorentz lattice has been pointed out in Chapter 8 of I. Dolgachev’s book [52]. Both references inspired our presentation in Sections 4.1 and 4.2.

The idea to use the euclidean algorithm to construct lattices with given torsion quadratic groups is due to C. T. C. Wall [245]. The use of the algorithm as a tool to calculate invariants for certain types of lattices stems from the book [99]. These two references form the source and the main inspiration for Sections 4.3 and 4.4.

Lens spaces constitute a classical subject and date back to the 1908 article by H. Tietze [225, §20]. At that time they were considered in the combinatorial category, that is, as polyhedra. In the famous 1934 book [203] by H. Seifert and W. Threlfall the homeomorphism problem for lens spaces is stated as still open (loc. cit. page 210), but already in the 1935 article [191] K. Reidemeister established the classification in the combinatorial category. He used a complete combinatorial invariant which since then is called the Reidemeister torsion. The homeomorphism classification had to wait until 1952 when E. Moise in [157] proved the three dimensional ”Hauptvermutung”. For a proof not using this result, see [30]. For further background on this history and also for a detailed ”modern” explanation of the concept of Reidemeister torsion, see the introductory course notes [147] by G. Massuyeau. We finally remark that in contrast to what happens in higher dimension, a topological threefold admits an essentially unique

differentiable structure (see [224, §3.10]) and so threefolds that are homeomorphic are also diffeomorphic. There is an obvious variant of this statement which holds for oriented threefolds. In particular, the Reidemeister torsion is an oriented diffeomorphism invariant. Our treatment of the lens spaces closely follows the book [99, §7–8] by F. Hirzebruch, W. Neumann, and S. Koh.

The A-D-E singularities or du Val singularities date from 1934, see P. du Val's original articles [229, 230, 231]. The cyclic quotient singularities or Hirzebruch–Jung singularities are named after F. Hirzebruch and H. Jung. The latter described the singularities in his 1908 article [114]. The method of resolving such a singularity using continued fractions is due to F. Hirzebruch [97].

The general properties of surface fibrations as presented here is based on the monograph [15]. As indicated in loc. cit., the results in the special case of elliptic fibrations go back to K. Kodaira [124, 125]. The canonical lattice structure on the Mordell–Weil group of an elliptic fibration has been proposed in 1990 by N. Elkies and T. Shioda [69, 210]. We have followed the treatment in the monograph [202] by M. Schütt and T. Shioda.

## Forms Related to Coding Theory and Number Theory

### Introduction

A linear code is a subspace of a finite dimensional vector space over a finite field  $\mathbb{F}_p$ ,  $p$  prime. In this chapter we restrict ourselves to the case  $r = 1$ . There is a canonical way to associate a lattice to a so-called isotropic code. These lattices turn out to be  $p$ -elementary as shown in Lemma 5.1.2.3. This procedure also has a direct relation to overlattices as expressed by Corollary 5.1.3. It turns out that several classical codes yield remarkable lattices, especially the extended binary Golay code and the Reed–Muller codes. The first code is, as we show in Section 5.1, related to the Leech lattice and the second to configurations of ordinary double points on complex surfaces (cf. Section 5.2). Kummer surfaces have a specific configuration of such double points which leads to the Kummer lattice. Codes are also essential to determine the maximal number of double points for quintic hypersurfaces, a further topic of Section 5.2.

Using prime ideals in number fields and codes in vector spaces over  $\mathbb{F}_p$ , the residue field of the prime ideal gives alternative constructions of lattices. In particular, as we shall see at the end of Section 5.3, the cyclotomic fields lead us to the Niemeier lattices that also occur in the context of K3 surfaces (cf. Section 20.2).

The final Section 5.4 reviews some known constructions of  $\mathbb{Q}$ -valued and  $\mathbb{Z}$ -valued symmetric forms of rank three (“ternary forms”) that are directly related to quaternion algebras. These play a role when we construct supersingular K3 surfaces in Section 19.5.

### 5.1 Codes and Lattices

For background on codes we refer to [140, 64].

**5.1.A Lattices obtained from codes.** A *linear code* is a linear subspace of  $\mathbb{F}_q^n$  where  $q = p^s$ , a power of a prime number  $p$ . If  $p = 2$  the code is called a *binary code*. A vector  $x$  of a code  $C$  is also called a *word*. It has *weight*

$$w(x) = \text{number of non-zero coordinates of } x, \quad x = (x_1, \dots, x_n) \in C \subset \mathbb{F}_q^n.$$

The dot-product  $x \cdot y = \sum x_j y_j \in \mathbb{F}_q$  of two vectors  $x = (x_1, \dots, x_n)$  and  $y = (y_1, \dots, y_n)$  in  $\mathbb{F}_q^n$  defines a non-degenerate symmetric bilinear form and a code is

called *isotropic* if  $C$  is an isotropic subspace of  $\mathbb{F}_q^n$  with respect to the dot-product, i.e., if  $C \subset C^\perp$ , and *self-dual* if  $C = C^\perp$ .

*Remark 5.1.1.* In Chapter 8 we answer the obvious question: how to place the dot-product on vector spaces over  $\mathbb{F}_2$  in the isometry classification? It turns out that Corollary 8.3.4 implies that in odd characteristic  $b$  is isometric to the dot-product if and only if  $\text{disc}(b) = 1$ . As a consequence of Proposition 8.2.1 if  $p = 2$  the odd form  $b$  is isometric to the dot-product if and only if  $\text{disc}(b) = 1$  and  $b$  is totally anisotropic, i.e., there are no isotropic vectors.

From now on we assume  $s = 1$ , that is, we consider codes  $C \subset \mathbb{F}_p^n$ . Then, using the reduction modulo  $p$  map

$$\rho : \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n, \quad (x_1, \dots, x_n) \mapsto (x_1 \bmod p, \dots, x_n \bmod p),$$

a code  $C$  lifts to a submodule  $\rho^{-1}C$  of  $\mathbb{Z}^n$  which contains the submodule  $p \cdot \mathbb{Z}^n = \rho^{-1}(0)$  and hence is of finite index in  $\mathbb{Z}^n$ . It inherits the structure of a lattice from  $\mathbb{Z}^n$  equipped with its dot-product. However, it turns out to be more convenient to use a different lattice structure, namely  $\mathbb{Z}^n$  equipped with the standard euclidean form scaled by  $p^{-1}$  which we denote

$$\mathbb{Z}^n(p^{-1}) = \mathfrak{O}^n\langle p^{-1} \rangle. \quad (5.1)$$

Hence we have

$$\Gamma_C = \rho^{-1}C \subset \mathbb{Z}^n(p^{-1}),$$

a not necessarily integral lattice of rank  $n$ . It is also positive definite.

We view the submodule  $p\mathbb{Z}^n$  as a sublattice of  $\Gamma_C$ .

**Lemma 5.1.2.** *1. The sublattice  $p\mathbb{Z}^n$  of  $\Gamma_C$  is isometric to  $\mathfrak{O}^n\langle p \rangle$ . In particular, if  $p = 2$ , the root lattice  $\mathfrak{O}^n A_1$  is contained in  $\Gamma_C$ .*

*2.  $\Gamma_C$  is an integral lattice if and only if  $C$  is isotropic.*

*3.  $\Gamma_C^* \subset \mathbb{Z}^n(p^{-1})$ . Moreover, if  $C$  is isotropic, the integral lattice  $\Gamma_C$  is a  $p$ -elementary lattice, that is, we recall (cf. Subsection 1.7.B)*

$$p \cdot \Gamma_C^* \subset \Gamma_C.$$

*Proof.* 1. As we have observed  $\Gamma_C$  contains the submodule  $p\mathbb{Z}^n = \rho^{-1}(0)$ . If  $\{e_1, \dots, e_n\}$  is the standard basis of  $\mathbb{Z}^n$ , we have  $p^{-1} \cdot (pe_i \cdot pe_j) = p\delta_{ij}$  and so  $p\mathbb{Z}^n$  equipped with  $p^{-1}$  times the standard product is isometric to  $\mathbb{Z}^n(p) = \mathfrak{O}^n\langle p \rangle$ .

2. Let  $x = (x_1, \dots, x_n)$ ,  $y = (y_1, \dots, y_n) \in \Gamma_C$  and denote their images in  $C$  by  $\bar{x}, \bar{y}$ . We have

$$p^{-1}(x \cdot y) = \frac{1}{p} \sum x_i y_i \in \mathbb{Z} \iff \sum x_i y_i \in p\mathbb{Z} \iff \bar{x} \cdot \bar{y} = 0 \text{ in } \mathbb{F}_p.$$

3. Since  $\Gamma_C$  contains  $p\mathbb{Z}^n$ , its dual  $\Gamma_C^*$  is contained in the dual of  $p\mathbb{Z}^n$  which is  $\mathbb{Z}^n(p^{-1})$ , and so  $p\Gamma_C^* \subset p\mathbb{Z}^n \subset \Gamma_C$ .  $\square$

**Corollary 5.1.3.** *Isotropic codes in  $\mathbb{F}_p^n$  are in a natural way in one-to-one correspondence with (integral) overlattices of  $\mathfrak{O}^n\langle p \rangle$  contained in  $\mathbb{Z}^n(p^{-1})$ .*

*Proof.* By Proposition 1.7.4, it suffices to establish a (natural) bijective correspondence between isotropic codes in  $\mathbb{F}_p^n$  and isotropic subgroups of  $(\mathfrak{O}^n\langle p \rangle)^*/\mathfrak{O}^n\langle p \rangle$ . Let  $\Gamma := \mathbb{Z}^n(p^{-1})$ . Now identify  $\mathfrak{O}^n\langle p \rangle$  with  $p\Gamma$  as in Lemma 5.1.2-1. Since  $(p\Gamma)^* = \Gamma$  (an easy verification), we see that  $(\mathfrak{O}^n\langle p \rangle)^*/\mathfrak{O}^n\langle p \rangle$  and  $\Gamma/p\Gamma$  are isometric. We continue with  $\Gamma/p\Gamma$ .

The identity map  $\Gamma = \mathbb{Z}^n(p^{-1}) \rightarrow \mathbb{Z}^n$  is an isometry up to a factor  $p$ . Hence the induced map  $\Gamma/p\Gamma \rightarrow \mathbb{F}_p^n$  identifies the  $p^{-1}\mathbb{Z}/\mathbb{Z}$ -valued discriminant bilinear form on  $\Gamma/p\Gamma$  with the  $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ -valued bilinear form on  $\mathbb{F}_p^n$  through multiplication by  $p$ . Consequently, isotropic codes in  $\mathbb{F}_p^n$  correspond to isotropic subgroups in  $\Gamma/p\Gamma$ .  $\square$

**Proposition 5.1.4.** *Let  $C \subset \mathbb{F}_p^n$  be an isotropic code and  $\Gamma_C \subset \mathbb{Z}^n(p^{-1})$  the corresponding integral lattice. Then  $\Gamma_C$  has the following properties:*

1.  $\text{disc}(\Gamma_C) = p^{n-2m}$ ,  $m = \dim C$ .
2. The lattice  $\Gamma_C$  is unimodular if and only if  $C$  is self-dual.
3.  $\Gamma_C^* = \rho^{-1}C^\perp$ .
4. If  $p = 2$ , the lattice  $\Gamma_C$  is even if and only if all of the weights of  $C$  are divisible by 4.

*Proof.* Observe that some of the lattices we consider are  $\mathbb{Q}$ -valued and so we must interpret the discriminant appropriately as in Remark 1.2.1.

1. The index of  $\Gamma_C$  in  $\mathbb{Z}^n(p^{-1})$  equals the index  $[\mathbb{F}_p^n : C] = p^{n-m}$  and hence by Lemma 1.2.2 we find

$$\text{disc}(\Gamma_C) = [\mathbb{Z}^n(p^{-1}) : \Gamma_C]^2 \cdot \text{disc}(\mathbb{Z}^n(p^{-1})) = p^{n-2m}.$$

2. This follows from 1, using  $\dim C^\perp = n - \dim C$  and  $\dim C \leq \dim C^\perp$ .

3. To show that  $\Gamma_C^* \supset \rho^{-1}C^\perp = \Gamma_{C^\perp}$ , let  $y \in \Gamma_{C^\perp}$ . Now let  $x \in \Gamma_C$  be arbitrary. Then  $\rho(x) \cdot \rho(y) = 0$  in  $\mathbb{F}_p^n$  and so  $p^{-1}(x \cdot y) \in \mathbb{Z}$ . This implies that  $y \in \Gamma_C^*$  and hence  $\Gamma_{C^\perp} \subset \Gamma_C^*$ . We show equality by comparing their indices in  $\mathbb{Z}^n(p^{-1})$ . A similar computation as in the proof of 1 shows that  $\text{disc}(\Gamma_{C^\perp}) = p^{2m-n} = \text{disc}(\Gamma_C)^{-1}$ . Using Lemma 1.6.3 we find that  $\text{disc}(\Gamma_C^*) = \text{disc}(\Gamma_{C^\perp})$ . But then  $\Gamma_C^*$  has the same index in  $\mathbb{Z}^n(p^{-1})$  as  $\Gamma_{C^\perp}$ .

4. For  $x = (x_1, \dots, x_n) \in \Gamma_C$ , write  $x_i = 2y_i + z_i$ ,  $i = 1, \dots, n$ , with  $z_i = 0$  or 1. For the prime  $p = 2$ , the weight of the corresponding words in  $C$  is  $\sum_i z_i$ . Then one has

$$\frac{1}{2}x \cdot x \equiv \frac{1}{2} \sum_i z_i^2 \equiv 0 \pmod{2\mathbb{Z}} \iff \sum_i z_i \equiv 0 \pmod{4} \iff w(\rho(x)) \equiv 0 \pmod{4}.$$

We conclude that  $\Gamma_C$  is even precisely if all weights of the code words are divisible by 4.  $\square$



In view of the assertion 4 we introduce an appropriate terminology for codes giving even lattices: we say that a binary code is **doubly even** if all its code words have weights divisible by 4.

We next investigate the discriminant groups and forms.

**Proposition 5.1.5.** *Let  $C \subset \mathbb{F}_p^n$  be an isotropic code of dimension  $m$ . The discriminant group of the lattice  $\Gamma_C$  is isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^{n-2m}$ . If  $p = 2$  and  $C$  is doubly even, the discriminant quadratic form takes values in  $\frac{1}{4}\mathbb{Z}$ . If, moreover, all words in  $C^\perp$  have even weights, the values are taken in  $\frac{1}{2}\mathbb{Z}$ . In that case  $\Gamma_C$  is a 2-elementary lattice of type II.*

*Proof.* The first assertion follows since  $\Gamma_C$  is  $p$ -elementary and the order of the discriminant group equals  $\text{disc}(\Gamma_C) = p^{n-2m}$ . For  $p = 2$ , the code  $C$  being doubly even ensures that the form on  $\Gamma_C$  is even and hence the polar form of a quadratic form, say  $q$ . In other words, if  $x \in \Gamma_C$ , then  $q(x) = \frac{1}{2} \cdot \frac{1}{2}(x \cdot x) \in \mathbb{Z}$ . Now use that  $\Gamma_C^* \subset \frac{1}{2}\Gamma_C$  to conclude that the discriminant quadratic form takes values in  $\frac{1}{4}\mathbb{Z}$ .

If, moreover, the image of  $x$  in  $C$  has even weight,  $x \cdot x$  is even and then  $q(x) \in \frac{1}{2}\mathbb{Z}$ .  $\square$

**5.1.B Lattices constructed from binary codes.** We discuss a few codes over  $\mathbb{F}_2$  related to geometry.

**The Hamming code  $H \subset \mathbb{F}_2^7$ .** This is the linear code of dimension 4 defined in so-called standard form as

$$H = \ker A, \quad A = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

It is not isotropic, but the extended version  $\tilde{H} \subset \mathbb{F}_2^8$  given (in standard form) as

$$\tilde{H} = \ker \tilde{A}, \quad \tilde{A} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

can be shown to be self-dual and doubly even. Hence  $\Gamma_{\tilde{H}}$  is a unimodular positive definite even lattice of rank 8. This lattice must be isometric to  $E_8$  since, as we have mentioned in Section 1.12, Kneser [119] has shown that there is only one isometry class.

**Root lattices from codes.** It can be shown [64, §1.4] that the only irreducible root lattices that arise from codes are  $A_1, E_7, E_8$  and  $D_{2n}$  for  $n \geq 2$ . The proof uses that all lattices  $\Gamma_C$  from binary codes  $C \subset \mathbb{F}_2^n$  contain the root lattice  $A_1^{\oplus n}$ , as claimed in Lemma 5.1.2.

**The Golay code and the Leech lattice.** The *extended binary Golay code*  $C_{\text{Gol}} \subset \mathbb{F}_2^{24}$  is a code of dimension 12. It is constructed as follows. The icosahedron considered as a graph with all weights equal to 1 defines, as we have seen in Chapter 4, a quadratic form on  $\mathbb{Z}^{12}$ . It is given by the matrix  $A = (A_{ij})$  with  $A_{ij} = 1$  if the vertices  $i$  and  $j$  are an edge of the icosahedron and  $A_{ij} = 0$  otherwise. Let  $J_{12}$  be the square matrix of size 12 with all ones and put

$$B = (I_{12} \quad J_{12} - A).$$

The (extended) Golay code is spanned by the rows of the matrix  $B$ . In [64, §2.8] the following properties are shown:

- $C_{\text{Gol}}$  has dimension 12 (which is clear since  $\text{rank}(B) = 12$ );
- $C_{\text{Gol}}$  is doubly even and self-dual.

Rephrasing Lemma 5.1.2 in this situation, the lattice  $\Gamma = \Gamma_{C_{\text{Gol}}}$  is the unimodular sublattice of  $\mathbb{Z}^{24}(\frac{1}{2})$  such that  $C_{\text{Gol}} = \Gamma/R \subset R^*/R \simeq \mathbb{F}_2^{24}$ , where  $R = \rho^{-1}(0) = A_1^{\otimes 24}$  turns out to be the root lattice of  $\Gamma$ .

We mention the appearance of one of the sporadic groups in this context. The symmetric group  $\mathfrak{S}_{24}$  acts on  $\mathbb{F}_2^{24}$  by permuting the coordinates. The *Mathieu group* is the stabilizer of the Golay code:

$$M_{24} = \{\sigma \in \mathfrak{S}_{24} \mid \sigma(C_{\text{Gol}}) = C_{\text{Gol}}\}.$$

The *Leech lattice*  $\Gamma_{24}$  is an even neighbour lattice of the even lattice  $\Gamma = \Gamma_{C_{\text{Gol}}}$ . Since the latter is unimodular and positive definite, the same holds for the Leech lattice (use Lemma 1.7.1). We describe how it can be constructed as an index two overlattice of

$$\Gamma_0 = \{x = (x_1, \dots, x_{24}) \in \Gamma \mid \sum x_i \equiv 0 \pmod{16}\}.$$

Note that the sum of the coordinates of each row of  $B$  equals  $8 = 1 + (12 - 5)$  and so the sum of the coordinates of each vector in the lattice  $\Gamma$  is divisible by 8. It follows that  $\Gamma$  is the disjoint union of  $\Gamma_0$  and

$$\Gamma_1 = \{x = (x_1, \dots, x_{24}) \in \Gamma \mid \sum x_i \equiv 8 \pmod{16}\}.$$

This set contains  $e = (1, \dots, 1)$  since taking the sum of the rows of  $B$  shows that  $\rho(e)$  belongs to the Golay code. One easily verifies that

$$\Gamma_{24} := \Gamma_0 \cup \left[ \frac{1}{2}e + \Gamma_1 \right], \quad e = (1, \dots, 1),$$

is an even integral lattice. For instance, the evenness follows since for all  $x \in \Gamma_1$  one has

$$\begin{aligned} \frac{1}{2} \left( \frac{1}{2}e + x \right) \cdot \left( \frac{1}{2}e + x \right) &= \frac{1}{2} (6 + e \cdot x + x \cdot x) \\ &\equiv 1 + 1 + 0 \pmod{2}. \end{aligned}$$

So the lattice  $\Gamma_{24}$  is an even index two overlattice of  $\Gamma_0$  and this is the searched for Leech lattice. From this description one can deduce that the Leech lattice contains no roots. The latter is the unique Niemeier lattice<sup>1</sup> without roots. For proofs see [64, §2.8] and [44, Ch. 16].

**Reed-Muller codes.** The definition of this class of codes runs as follows. Let  $I$  be a finite set of size  $N$ . Then the functions  $I \rightarrow \mathbb{F}_2$  form the  $\mathbb{F}_2$ -vector space  $\mathbb{F}_2^I$ . Suppose that  $I$  itself consists of the points of an  $\mathbb{F}_2$ -vector space  $W$  of dimension  $m$  so that  $N = 2^m$ . We order these points as follows. Let  $\{e_0, \dots, e_{m-1}\}$  be a basis for  $W$  and identify a point  $x = \sum_{j=0}^{m-1} x_j e_j$  with the binary expansion  $n_x = \sum_{j=0}^{m-1} x_j 2^j$  of an integer between 0 and  $2^m - 1$ . The natural order gives an ordering of the points of  $W$ . An  $\mathbb{F}_2$ -valued function  $f$  on  $W$  determines a vector  $(f_0, \dots, f_{N-1}) \in \mathbb{F}_2^N$  as follows. First note that a point  $x \in W$  determines the unique integer  $j = n_x \in [0, \dots, N - 1]$  and then we set  $f_j = f(x)$ . This way, the polynomial functions of degree  $k$  on  $W$  together with the zero function define a subspace of  $\mathbb{F}_2^N$  and this is also the case for polynomial functions of degree  $\leq k$ . For  $0 \leq k < m$ , the latter define the  $k$ -th order **Reed-Muller code**  $S^{\leq k}(W) \subset \mathbb{F}_2^N$ ,  $N = 2^m$ . For an extensive treatment of these codes we refer to [140, Sect. 4.5].

**Example 5.1.6.** Take  $m = 4$  and  $k = 1$ . Then  $N = 2^4 = 16$  and  $S^{\leq 1}(\mathbb{F}_2^4) \subset \mathbb{F}_2^{16}$  is generated by the 4 code words given as the rows of the following  $4 \times 16$  matrix together with the vector with all coordinates equal to 1 arising from the constant function 1. The columns correspond to the binary expansions of the numbers  $0, \dots, 15$  and the rows correspond to the coordinate functions  $x_0, x_1, x_2, x_3$ :

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

**Proposition 5.1.7.** *Let  $W$  be an  $\mathbb{F}_2$ -vector space of dimension  $m$ . The Reed-Muller codes  $S^{\leq k}(W) \subset \mathbb{F}_2^W \simeq \mathbb{F}_2^N$ ,  $N = 2^m = |W|$ , have the following properties.*

1.  $S^{\leq k}(W)$  has even weights.
2. Suppose  $0 \leq k \leq m - 1$ . With respect to the standard dot-product on  $\mathbb{F}_2^N$ , the code orthogonal to  $S^{\leq k}(W)$  is  $S^{\leq m-k-1}(W)$ .
3. The code  $S^{\leq k}(W)$  is isotropic if  $2k \leq m - 1$  and self-dual if and only if equality holds.

*Proof.* First some preliminary remarks. Note that a linear function  $f$  and its square  $f^2$  define the same polynomial function on  $W$  since we are in characteristic 2. This implies for instance that the space  $S^{\leq k}(W)$  of polynomial functions of degree  $\leq k$

<sup>1</sup>Recall that a Niemeier lattice is a positive definite unimodular rank 24 lattice.

on  $W$  has dimension  $e_k = 1 + m + \binom{m}{2} + \cdots + \binom{m}{k}$  from which we deduce a relation between the dimensions of certain "opposite" Reed–Muller codes:

$$\dim S^{\leq k}(W) + \dim S^{\leq m-k-1}(W) = e_k + e_{m-k-1} = (1+1)^m = 2^m. \quad (5.2)$$

The above remark also implies that, starting with two monomials  $x_{i_1} \cdots x_{i_r}$  (all indices distinct) and  $x_{j_1} \cdots x_{j_s}$  (all indices distinct), the product  $x_{i_1} \cdots x_{i_r} x_{j_1} \cdots x_{j_s}$ , viewed as function, coincides with the function corresponding to a square-free monomial of degree at most  $r + s$ .

To show 1 we first remark that  $S^{\leq k}(W)$  is spanned by the words corresponding to the monomials  $x_{i_1} \cdots x_{i_\ell}$  with  $\ell \leq k$  and all indices distinct. Viewed as functions, these are the characteristic functions of the positive dimensional affine subspaces given by the equations  $x_{i_1} = \cdots = x_{i_\ell} = 1$ . Since these contain an even number of elements,  $x_{i_1} \cdots x_{i_\ell}$  assumes the value 1 an even number of times. Hence the resulting code words have even weights. Consequently, sums of such words also have even weights.

In view of (5.2), to establish 2, it suffices to show the inclusion  $S^{\leq m-k-1}(W) \subset S^{\leq k}(W)^\perp$ . It also suffices to verify this for words generating the two codes. To do so, we take two words corresponding to monomials  $x_{i_1} \cdots x_{i_r}$  with  $r \leq k$  and  $x_{j_1} \cdots x_{j_s}$  with  $s \leq m - k - 1$  as above. Viewed as functions, the product of the monomials produces the same function as a monomial of degree at most  $m - 1$ , and so its corresponding word has even weight. This word is obtained from the two words we started with by coordinate-wise multiplication. Hence, the  $\mathbb{F}_2$ -dot-product of the two words is 0.

Finally, to show 3, note that if  $k \leq m - k - 1$  we have an inclusion

$$S^{\leq k}(W) \subset S^{\leq m-k-1}(W) = S^{\leq k}(W)^\perp$$

with equality if and only if  $k = m - k - 1$ . □

We specifically consider the two codes

$$D_{m+1} := S^{\leq 1}(W), \quad (5.3)$$

$$C_m := S^1 W. \quad (5.4)$$

The former is a code of dimension  $m + 1$  given by the affine linear functions on  $W$  and is generated by the linear functions on  $W$ , forming the code  $C_m$ , together with the constant function 1. This last word has weight  $2^m$  while the non-zero weights of  $C_m$  are all  $2^{m-1}$  since the characteristic function of a hyperplane interpreted as a code word has this weight. So the non-zero weights of  $D_m$  itself (lowering the index by one) are  $2^{m-2}$  and  $2^{m-1}$ . In particular, if  $m \geq 4$  the codes are doubly even and then the corresponding lattices  $\Gamma_{C_m} \subset \mathbb{Z}^N(\frac{1}{2})$ ,  $N = 2^m - 1$ , and  $\Gamma_{D_m} \subset \mathbb{Z}^M(\frac{1}{2})$ ,  $M = 2^{m-1}$ , are even. As a consequence the discriminant groups and forms of the corresponding lattices have the following properties (using Proposition 5.1.4):

**Corollary 5.1.8.** *Assume  $m \geq 4$ . The lattices  $\Gamma_{C_m}$  and  $\Gamma_{D_m}$  have discriminant group  $\oplus^{2^m-2m-1} \mathbb{Z}/2\mathbb{Z}$ , respectively  $\oplus^{2^{m-1}-2m} \mathbb{Z}/2\mathbb{Z}$ . The discriminant quadratic form*

in both cases is  $\frac{1}{2}\mathbb{Z}$ -valued, that is,  $\Gamma_{C_m}$  and  $\Gamma_{D_m}$  are 2-elementary lattices of type II.<sup>2</sup>

The two codes  $C_m$  and  $D_m$  can be characterized as follows:

**Lemma 5.1.9** ([17, §4]). 1. Let  $C \subset \mathbb{F}_2^n$  be a code of dimension  $m$  and with non-zero weights  $> \frac{1}{2}n$ . Then  $n \geq 2^m - 1$  and, if equality holds,  $C \simeq C_m$ .

2. Let  $C \subset \mathbb{F}_2^n$  be a code of dimension  $m$  and with non-zero weights  $\geq \frac{1}{2}n$ . Then  $n \geq 2^{m-1}$  and equality holds if and only if  $C \simeq D_m$ , in which case it only has non-zero weights  $\frac{1}{2}n = 2^{m-2}$  and  $n = 2^{m-1}$ .

## 5.2 Application to Nodes, K3 Surfaces and Nodal Quintics

**5.2.A Even sets of nodes.** Let  $Y$  be a (connected compact and smooth) complex surface which is the minimal resolution of a singular surface  $Y'$  having a finite set of ordinary double points (and no other singularities). The example to have in mind is the (singular) Kummer surface (see Appendix B.3). As in that example, each double point is resolved by a *nodal curve*, by definition a smooth rational curve with self-intersection  $-2$ . Conversely, such a curve can be contracted to give a surface with an ordinary double point. A special role is played by subsets  $\{E_j\}_{j \in J}$  of disjoint nodal curves for which  $B_J = \sum_{j \in J} E_j \in 2\text{NS}(Y)$ . Such a set is called an *even set of nodal curves*.<sup>3</sup> Its role is highlighted by the following geometric construction. Evenness implies that there is a double covering<sup>4</sup> of  $Y$ , exactly ramified over  $B_J$ . The resulting surface  $X_J$  is not minimal since the curves  $E_j$ ,  $j \in J$ , lift to exceptional curves which can be blown down to points  $p_j$ , yielding a smooth surface, say  $X'_J$ . The situation can be summarized in the following commutative diagram

$$\begin{array}{ccc} (X_J, q^{-1}B_J) & \longrightarrow & (X'_J, \bigcup_{j \in J} p_j) \\ q \downarrow & & q' \downarrow \\ (Y, B_J) & \longrightarrow & (Y', \bigcup_{j \in J} q'(p_j)) \end{array} \quad (5.5)$$

Since  $X_J - q^{-1}B_J = X'_J - \bigcup_{j \in J} p_j$  and  $q^{-1}B_J = B_J$  as sets, the Euler numbers of  $Y$  and  $X'_J$  are related in a simple fashion:

$$e(X'_J) - |J| = 2[e(Y) - e(B_J)] = 2e(Y) - 4 \cdot |J| \implies e(X'_J) = 2e(Y) - 3 \cdot |J|. \quad (5.6)$$

The relation with codes stems from the following considerations. Let  $\mathcal{C} = \{E_1, \dots, E_n\}$  be a set of disjoint nodal curves on  $Y$ . So, if  $N = \mathbb{Z}E_1 \oplus \dots \oplus \mathbb{Z}E_n$  is

<sup>2</sup>See Definition 1.7.2 and Proposition 5.1.5.

<sup>3</sup>This is accepted terminology first introduced by F. Catanese in [37]; it does not mean that the set consists of an even number of curves.

<sup>4</sup>For background on ramified double covers, see e.g. [15, Ch. V.22].

the abstract lattice with basis the nodal classes, recalling the notation (5.1), we find for the dual

$$N^* = \frac{1}{2}N \simeq \mathbb{Z}^n(-\frac{1}{2}).$$

The quotient map  $N^* \rightarrow N^*/N = \frac{1}{2}N/N \simeq \mathbb{F}_2^n$  is just the modulo 2 map  $\rho : \mathbb{Z}^n \rightarrow \mathbb{F}_2^n$  used to construct lattices from codes. In what follows we assume for simplicity that  $H^2(Y, \mathbb{Z})$  has no torsion so that it becomes an integral lattice under the intersection pairing; then the Néron–Severi group  $\text{NS}(Y)$  is known to be a primitive sublattice. We do the reverse and start with the lattice:

$$N_{\mathcal{E}} := \text{primitive closure of } N \text{ in } \text{NS}(Y).$$

Since we have inclusions  $N \subset N_{\mathcal{E}} \subset N_{\mathcal{E}}^* \subset N^* \simeq \mathbb{Z}^n(-\frac{1}{2})$ , we see that, setting

$$C_{\mathcal{E}} = N_{\mathcal{E}}/N \subset N^*/N \simeq \mathbb{F}_2^n, \quad (5.7)$$

the lattice  $N_{\mathcal{E}}$  is precisely the inverse image of the code  $C_{\mathcal{E}}$  under the reduction mod 2 map. In other words, we have

$$N_{\mathcal{E}} = \Gamma_{C_{\mathcal{E}}}(-1). \quad (5.8)$$

Using that  $N_{\mathcal{E}}$  is primitive in the lattice  $\text{NS}(Y)$  and identifying  $\frac{1}{2}N/N$  with  $N/2N$ , we arrive at an equivalent description of the code  $C_{\mathcal{E}}$ , namely

$$C_{\mathcal{E}} \simeq \ker \left( \mathbb{F}_2^n = \oplus_j \mathbb{F}_2 E_j \simeq N/2N \xrightarrow{\varphi} N/2N_{\mathcal{E}} \subset N_{\mathcal{E}}/2N_{\mathcal{E}} \subset \text{NS}(Y)/2\text{NS}(Y) \right). \quad (5.9)$$

Here primitivity is used to establish the rightmost inclusion. This description shows the relation between properties of the code and geometry:

**Proposition 5.2.1.** *Suppose  $Y$  is a complex surface such that  $H^2(Y, \mathbb{Z})$  has no torsion and let  $\mathcal{E}$  be a set of disjoint nodal curves on  $Y$ . Non-zero code words in  $C_{\mathcal{E}}$  correspond to even subsets of nodal curves, and conversely. More precisely, with  $e_1, \dots, e_n$  the standard basis of  $\mathbb{F}_2^n$ , the sum  $\sum_{i \in J} e_i$ , where  $J \subset \{1, \dots, n\}$ , belongs to the code  $C_{\mathcal{E}}$  if and only if  $\sum_{i \in J} E_i$  is even in  $\text{NS}(Y)$ . The weight of a word in  $C_{\mathcal{E}}$  is the cardinality of the corresponding set.*

Description (5.9) gives a bound for  $\dim C_{\mathcal{E}}$ : since  $\text{NS}(Y)$  is primitive in  $H^2(Y, \mathbb{Z})$ , the quotient  $\text{NS}(Y)/2\text{NS}(Y)$  injects into  $H^2(Y, \mathbb{Z})/2H^2(Y, \mathbb{Z}) = H^2(Y, \mathbb{F}_2)$ , a symplectic inner product space in which the image of  $\varphi$  is isotropic, and so has dimension  $\leq \frac{1}{2}b_2(Y)$ . It follows that

$$\dim C_{\mathcal{E}} \geq n - \frac{1}{2}b_2(Y). \quad (5.10)$$

**5.2.B Even sets of nodes and K3 surfaces.** There are severe restrictions on even sets of disjoint nodal curves on a complex K3 surface:

**Lemma 5.2.2.** *Let  $Y$  be a complex K3 surface containing an even set of  $k > 0$  disjoint nodal curves. Then  $k = 8$  or  $16$ . If  $k = 8$  the associated double cover is a K3 surface and if  $k = 16$  it is a complex torus.*

*Proof.* Consider the minimal surface  $X'_J$  constructed above from an even set of nodal curves with  $|J| = k$ . Since  $e(Y) = 24$  we find from (5.6) that  $e(X'_J) = 48 - 3k$ . On the other hand, we claim that  $K_{X'_J}$  is trivial so that  $p_g(X'_J) = 1$  and  $c_1^2(X'_J) = 0$ . Indeed, the canonical bundle is trivialized on  $Y$  by a non-zero holomorphic 2-form, say  $\omega$ , which lifts to a 2-form, non-zero outside the branch locus and which descends to a holomorphic two-form  $\omega'$  on  $X'_J$  nowhere zero except maybe in the points  $p_j$ . But  $\omega'$  can only vanish along a divisor and so  $\omega'$  trivializes  $K_{X'_J}$ .

The classification theorem B.5.4 then gives two possibilities:  $X'_J$  is either a torus or a K3-surface. Since  $e(X'_J) = 48 - 3k$ , either  $e(X'_J) = 0$  and then  $k = 16$ , or  $e(X'_J) = 24$  and then  $k = 8$ .  $\square$

Proposition 5.2.1 then implies:

**Corollary 5.2.3.** *For a set of disjoint nodal curves on a complex K3 surface the weights of the associated code are 0, 8 or 16.*

Let us investigate the codes associated to a set  $\mathcal{E}$  of 16 or 8 disjoint nodal curves on a complex K3 surface and the geometry behind them.

**Case 1.**  $\#\mathcal{E} = 16$ . We will show that  $\mathcal{E}$  is always even and leads to a Kummer surface.

First, assuming that  $\mathcal{E}$  is an even set, we have seen that the corresponding  $X'_J$  is a torus, say  $X'_J = A$ . Recall (cf. Appendix B.5) that  $\text{Km}(A)$  is the minimal resolution of the quotient  $A/\langle\iota\rangle$  of a complex 2-torus  $A$  by its canonical involution  $\iota$ . The 16 fixed points of the involution give 16 nodes on  $A/\langle\iota\rangle$  which resolve into a set  $\mathcal{E}_A$  of 16 disjoint nodal curves on  $\text{Km}(A)$ . The **Kummer lattice of  $\text{Km}(A)$**  is then defined as

$\Lambda_{\text{Kum}} = N_{\mathcal{E}_A}$ , the primitive closure of the lattice spanned by the 16 nodal classes.

We next show that in this situation  $\mathcal{E}$  must be an even set of nodal curves as a consequence of the following lemma:

**Lemma 5.2.4.** *For any set  $\mathcal{E}$  of 16 nodal curves on a complex K3 surface, the associated code  $C_{\mathcal{E}}$  is isomorphic to  $D_5$ , the Reed–Muller code (5.3).*

*Proof.* We invoke Lemma 5.1.9, using first of all the estimate (5.10) for the code  $C_{\mathcal{E}} \subset \mathbb{F}_2^{16}$  which states  $m = \dim C_{\mathcal{E}} \geq 16 - \frac{1}{2} \cdot 22 = 5$ . Secondly, we apply Corollary 5.2.3, stating that its non-zero weights are  $\geq 8$ . Thus the lemma implies  $16 \geq 2^{m-1} \geq 2^4$ , and since we then must have equality,  $C_{\mathcal{E}} = D_5$ .  $\square$

This shows that the Kummer lattice of any Kummer surface is isometric to the same abstract lattice, which motivates the following nomenclature.

**Definition 5.2.5.** The lattice  $\Lambda_{\text{Kum}} = \Gamma_{D_5}(-1)$  is the **abstract Kummer lattice**.

Let us collect its properties, using Corollary 5.1.8:

**Lemma 5.2.6.** *The abstract Kummer lattice is an even lattice of rank 16 and discriminant  $2^6$ . It is a 2-elementary lattice of type II with discriminant group isomorphic to  $\oplus^6 \mathbb{Z}/2\mathbb{Z}$ .*

Since 16 disjoint nodal curves on a K3 surface have the same intersection pattern as in the abstract Kummer lattice we deduce:

**Proposition 5.2.7.** *Let  $Y$  be a complex K3 surface containing a set  $\mathcal{E}$  of 16 disjoint nodal curves. Then  $\mathcal{E}$  is an even set,  $Y$  is a Kummer surface with  $\mathcal{E}$  the canonical set of 16 nodal curves. The primitive closure  $N_{\mathcal{E}}$  of its span is isometric to the abstract Kummer lattice  $\Lambda_{\text{Kum}}$ .*

*Proof.* Since the code  $D_5$  contains the word  $(1, \dots, 1)$ , the sum of all the nodal curves is even and, as we just saw in the proof of Lemma 5.2.2, the resulting double cover gives a torus  $A$  with an involution having 16 fixed points. It thus is the standard involution and  $Y = \text{Km}(A)$ . The set  $\mathcal{E}$  is then the canonical set of nodal curves. By (5.8) the Kummer lattice  $\Lambda_{\mathcal{E}}$  is isometric to the (abstract) Kummer lattice  $\Lambda_{\text{Kum}}$ .  $\square$

**Corollary 5.2.8.** *Every Kummer surface admits a doubly covering K3 surface blown up in 8 points.*

*Proof.* The code  $D_5$  contains words of length 8 and the corresponding double cover gives a K3 surface with 8 exceptional curves.  $\square$

**Case 2.**  $\#\mathcal{E} = 8$ . This is only of interest if  $\mathcal{E}$  is an even set in which case  $X' = X'_j$  is a K3 surface. We characterize the code and the involution in this situation.

Let us start by considering the diagram (5.5) for this situation:

$$\begin{array}{ccc}
 X & \longrightarrow & X' & \begin{array}{c} \curvearrowright \\ \curvearrowleft \end{array} \\
 \downarrow & & \downarrow & \\
 Y & \longrightarrow & Y' & 
 \end{array} \tag{5.11}$$

where  $j$  is the covering involution. The latter is an example of a **Nikulin involution**, by definition an involution of a K3 surface which preserves the holomorphic 2-form on the K3 surface. Such involutions always have 8 isolated fixed points as we shall show later (cf. Lemma 20.5.2).

We next turn to the associated code  $C_{\mathcal{E}}$  in  $\mathbb{F}_2^8$ . We have  $C_{\mathcal{E}} = \mathbb{F}_2 \cdot (1, 1, 1, 1, 1, 1, 1, 1)$  since by Lemma 5.2.2 the only even subset of  $\mathcal{E}$  is  $\mathcal{E}$  itself. It follows that the primitive closure  $N_{\mathcal{E}}$  in  $H^2(Y, \mathbb{Z})$  of the span of the 8 nodal classes is the lattice  $\Gamma_{C_{\mathcal{E}}}(-1)$ . Diagram (5.11) motivates the following definition.

**Definition 5.2.9.** The **Nikulin lattice** is the rank 8 even negative definite lattice

$$\Lambda_{\text{Nik}} = \Gamma_{\mathcal{E}}(-1) \subset \frac{1}{2}\mathbb{Z}^8(-2)$$

spanned by the standard basis vectors  $e_j$  of  $\mathbb{Z}^8(-2)$  together with  $\frac{1}{2} \sum_{j=1}^8 e_j$ .

We have:

**Proposition 5.2.10.** *Let  $Y$  be a K3 surface with an even set  $\mathcal{E}$  of 8 nodal curves. Then the lattice  $\Gamma_{C_{\mathcal{E}}}(-1)$  is the Nikulin lattice, a 2-elementary type II quadratic lattice with discriminant group  $\oplus^6 \mathbb{Z}/2\mathbb{Z}$ .*



*Proof.* We already showed all but the last assertion. Note that  $C_{\mathcal{E}}^{\perp}$  is the hyperplane  $\sum x_i = 0$  in  $\mathbb{F}_2^8$  with non-zero even weights 2, 4, 6 and 8. Since the code  $C_{\mathcal{E}}$  is obviously doubly even, the statement follows from Proposition 5.1.5.  $\square$

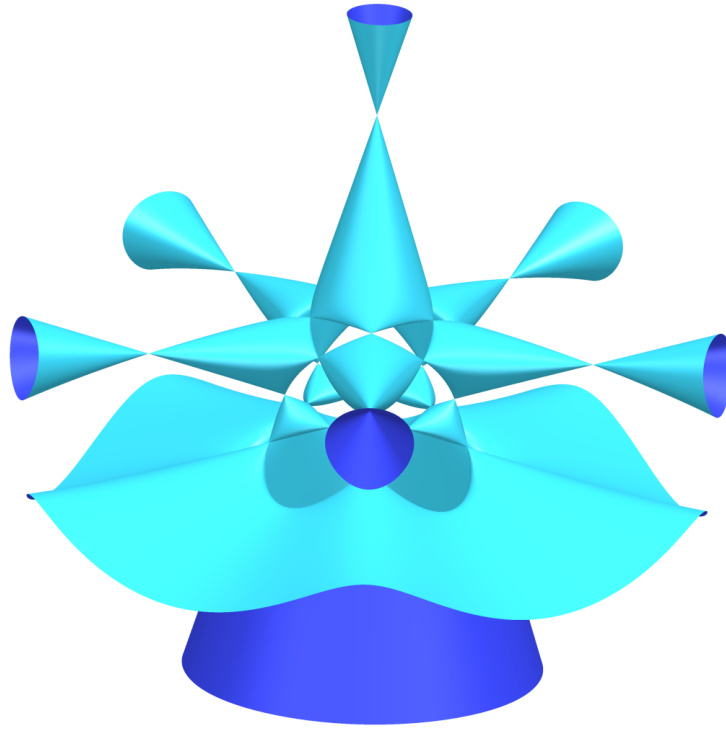


Figure 5.2.1: Togliatti's surface with 31 double points

**5.2.C Codes and double points on quintics.** Another application of the above strategy yields an upper bound for the number of double points on degree 5 surfaces in projective 3-space as we now explain. Let  $X$  be the minimal resolution of a surface  $\widehat{X}$  which has at most double points. The Betti numbers of a degree  $d$  smooth surface in  $\mathbb{P}^3$  are well known. See e.g. Appendix B.3. Degree  $d$  surfaces form a family which has members with ordinary double points. It is well known (see [29]) that their minimal resolutions have the same topological type as that of the smooth members. In our case  $d = 5$  and hence  $b_2(X) = 5^3 - 4 \cdot 5^2 + 6 \cdot 5 - 2 = 53$ , and so the lattice  $H_X$  has rank 53. Let  $C_{\mathcal{E}} \subset \mathbb{F}_2^{53} \simeq H_X \otimes \mathbb{F}_2$  be the code defined by the nodal curves coming from the double points. The crucial geometric input is as follows.

**Lemma 5.2.11** ([17]). *The code  $C_{\mathcal{E}} \subset \mathbb{F}_2^n$ ,  $n = \#\mathcal{E}$ , has non-zero weights 16 and 20.*

The proof, which we don't reproduce here, is subtler than the corresponding assertion for Kummer surfaces.

To continue, note that it is well known (loc. cit.) that  $\widehat{X}$  can have up to 31 nodes as we shall prove in a moment. This bound is sharp as shown by E. Togliatti [227]. See Figure 5.2.1.<sup>5</sup> Lemma 5.2.11 together with the characterization of Lemma 5.1.9 for the code  $C_5$  given in (5.4), indeed yields the estimate, and even more:

**Corollary 5.2.12.** *If  $\#\mathcal{E} = 31$ , we have  $C_{\mathcal{E}} = C_5$ , and so in this case  $\text{NS}(X)$  contains the lattice  $\Gamma_{C_5}(-1)$ . The surface  $\widehat{X}$  has  $\leq 31$  double points.*

*Proof.* Let  $n$  be the number of double points. Suppose first that  $n = 31 = 2^5 - 1$ . Then  $n/2 = 15\frac{1}{2}$  and so Lemmas 5.2.11, 5.1.9 and formula (5.10) imply that  $C_{\mathcal{E}} \simeq C_5$ .

To show that  $n \leq 31$ , assume that, on the contrary,  $n \geq 32$ . Selecting a set  $\mathcal{E}$  of 32 nodes we shall arrive at a contradiction. Since  $\frac{1}{2}b_2(Y) = 26\frac{1}{2}$ , (5.10) implies that  $m = \dim C_{\mathcal{E}} \geq 6$  so that the conditions of Lemma 5.1.9.2 are satisfied. On the other hand, since  $C_{\mathcal{E}}$  has weights  $\geq 16$ , the conclusion of the lemma gives us the inequality  $n = 32 \geq 2^{m-1} \geq 2^5$ , and so we have equality and  $C_{\mathcal{E}} \simeq D_5$ , a code whose weights are 16 and 32 contradicting Lemma 5.2.11.  $\square$

## 5.3 Lattices, Number Fields and Codes

**5.3.A Some basic algebraic number theory.** For details on number fields we refer to [111]. A *number field*  $K$  is an algebraic extension field of  $\mathbb{Q}$  of finite degree

$$d = d_K = [K : \mathbb{Q}].$$

The field  $K$  is a  $\mathbb{Q}$ -vector space of dimension  $d$  and multiplication with  $x \in K$  defines a  $\mathbb{Q}$ -linear map  $m_x : K \rightarrow K$  in this vector space. Its trace is the *trace*  $\text{Tr}_{K/\mathbb{Q}}(x)$  of  $x$  and its determinant is the *norm*  $N_{K/\mathbb{Q}}(x)$  of  $x$ . Using the  $d = [K : \mathbb{Q}]$  different embeddings

$$\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_d : K \hookrightarrow \mathbb{C},$$

the trace and norm can then also be given as  $\sum_{j=1}^d \sigma_j(x)$ , respectively  $\prod_{j=1}^d \sigma_j(x)$ . Using the trace, one gets the *trace form*

$$(x, y) \mapsto x \cdot y = \text{Tr}_{K/\mathbb{Q}}(xy). \quad (5.12)$$

which is a symmetric bilinear form on  $K$  with values in  $\mathbb{Q}$ . To determine the discriminant, suppose that  $\{\omega_1, \dots, \omega_d\}$  is a basis for the  $\mathbb{Q}$ -vector space  $K$ . Then one can show (cf. [111, §3.3])

$$\text{disc}(\text{Tr}_{K/\mathbb{Q}}) = \det(\text{Tr}_{K/\mathbb{Q}} a_{ij}) \neq 0, \quad a_{ij} = \omega_i \cdot \omega_j,$$

from which we deduce:

<sup>5</sup>This picture is constructed with the SURFER software. See <https://imaginary.org/program/surfer>.

**Lemma 5.3.1.** *The trace form is non-degenerate and so  $(K, \text{Tr}_{K/\mathbb{Q}})$  is a  $\mathbb{Q}$ -inner product space.*

**Example 5.3.2** (Quadratic number fields). Any quadratic extension of  $\mathbb{Q}$  can be written as  $K = \mathbb{Q}(\sqrt{d})$  where  $d \in \mathbb{Z}$  is square free. If  $x = x_1 + x_2 \cdot \sqrt{d}$  and  $y = y_1 + y_2 \cdot \sqrt{d}$ , we have  $\text{Tr}_{K/\mathbb{Q}}(xy) = 2(x_1y_1 + dx_2y_2)$ . The discriminant of the trace form is (up to squares)  $d \in \mathbb{D}(\mathbb{Q})$ . Note also that the index of the trace form is 2 if  $d > 0$  and 0 if  $d < 0$ . The relation with the norm is as follows.  $N(x) = x_1^2 - dx_2^2$  whose polarization equals  $\text{Tr}_{K/\mathbb{Q}}(xy')$  where  $y' = y_1 - y_2 \cdot \sqrt{d}$  is the *conjugate* of  $y$ . So the trace form is *not* the polarization of the quadratic form defined by the norm. The norm form plays a role later on. See § 6.3.B, example 5 and 8.3.1.

As in the preceding example, the signature of the trace form is determined by the nature of the embeddings  $\sigma_j : K \hookrightarrow \mathbb{C}$ ,  $j = 1, \dots, d$ . These can be divided into two sets: a set of, say,  $r$  real embeddings and a set of, say,  $s$  pairs of complex conjugate embeddings  $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$ . The trace form has signature  $(r + s, s)$  (see e.g. [222]). For  $s > 0$  the hermitian trace always gives a positive definite form:

**Lemma 5.3.3.** *Fix a non-real embedding  $K \hookrightarrow \mathbb{C}$  and let  $x \mapsto \bar{x}$  be the ensuing complex conjugation. The hermitian trace*

$$(x, y) \mapsto x \cdot y := \text{Tr}_{K/\mathbb{Q}}(x\bar{y})$$

*is a positive definite  $\mathbb{Q}$ -inner product on  $K$ . It is independent of the chosen non-real embedding.*

*Proof.* Let  $\alpha \in K$  be a primitive element so that  $K = \mathbb{Q}(\alpha)$ . Suppose the roots of the minimal polynomial of  $\alpha$  are  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d$ , then  $\sigma_j(\alpha) = \alpha_j$  and  $\bar{\sigma}_j(\alpha) = \bar{\alpha}_j$ . Any  $x \in K$  can be written as a polynomial in  $\alpha$  with rational coefficients, say  $x = p(\alpha)$ . Hence  $\sigma_j(x) = p(\alpha_j)$  and  $\sigma_j(\bar{x}) = p(\bar{\alpha}_j) = \overline{p(\alpha_j)} = \overline{\sigma_j(x)}$ . Hence  $\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) = \sum_j \sigma_j(x)\overline{\sigma_j(x)} \geq 0$  with equality if and only if  $x = 0$ . Clearly, a different choice of embedding just permutes the  $\sigma_j(x)$  and so the sum does not depend on the chosen embedding  $K \hookrightarrow \mathbb{C}$ .  $\square$

Let us next consider what this gives when we restrict these forms to the ring of integers of  $K$ . Let us recall the definition.

**Definition 5.3.4.** The *ring of integers of  $K$*  is defined as

$$\mathfrak{D}_K = \{x \in K \mid p_x(X) \in \mathbb{Z}[X]\}, \text{ where } p_x(X) \text{ is the monic minimal polynomial of } x.$$

This is a free  $\mathbb{Z}$ -module of rank  $d = d_K$  on which the trace is integer valued and hence the pairing  $(x, y) \mapsto \text{Tr}_{K/\mathbb{Q}}(xy)$ ,  $x, y \in \mathfrak{D}_K$ , is integer valued. In other words,  $(\mathfrak{D}_K, \text{Tr}_{K/\mathbb{Q}})$  is an integral  $\mathbb{Z}$ -lattice and so its discriminant, *discriminant of  $\mathfrak{D}_K$*  – denoted  $\mathfrak{d}_K$  – is an integer.

**Example 5.3.5.** For the quadratic extension  $K = \mathbb{Q}(\sqrt{d})$  we find

$$\mathfrak{D}_K = \begin{cases} \mathbb{Z} \oplus \sqrt{d}\mathbb{Z} & \text{if } d \equiv 2, 3 \pmod{4} \\ \mathbb{Z} \oplus \frac{1}{2}(1 + \sqrt{d})\mathbb{Z} & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

For  $d \equiv 2, 3 \pmod{4}$ , the trace form is even and its Gram matrix with respect to the given basis is the diagonal form  $\text{diag}(2, 2d)$ . In contrast, if  $d \equiv 1 \pmod{4}$ , the trace form is odd since the Gram matrix in this case is  $\begin{pmatrix} 2 & 1 \\ 1 & \frac{1}{2}(d+1) \end{pmatrix}$ . In both cases  $\mathfrak{d}_K = d$ .

**5.3.B More lattices from codes.** To make the link with codes, we consider the quotient of  $\mathfrak{D}_K$  by a prime ideal  $\mathfrak{p}$ . This is a finite field, say  $\mathbb{F}_q$ ,  $q = p^f$ , with  $p$  prime, and where  $f$  is called the *inertia index* of  $\mathfrak{p}$ . To simplify matters we assume

1.  $f = 1$ , and so  $q = p$ ;
2.  $p$  and  $d_K$  are relatively prime;
3.  $\text{Tr}_{K/\mathbb{Q}}(\mathfrak{p}) \subset (p)$  (this is in general not the case).

Under these assumptions, composing  $\text{Tr}_{K/\mathbb{Q}}$  with the reduction  $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$  is a non-trivial group homomorphism (since it sends 1 to the class of  $d_K$  in  $\mathbb{Z}/p\mathbb{Z}$ ). Its kernel contains  $\mathfrak{p}$  and since  $\mathfrak{D}_K/\mathfrak{p}$  and  $\mathbb{Z}/p\mathbb{Z}$  both have  $p$  elements, this gives a bijection  $\mathfrak{D}_K/\mathfrak{p} \xrightarrow{\sim} \mathbb{F}_p$ . Therefore coordinate-wise reduction mod  $\mathfrak{p}$  induces a map

$$\rho_p : \mathfrak{D}_K^n \longrightarrow \mathbb{F}_p^n. \quad (5.13)$$

As in the case  $K = \mathbb{Q}$ , the inverse image  $\rho_p^{-1}C$  of a code  $C \subset \mathbb{F}_p^n$  gives a sublattice of finite index, but this time an  $\mathfrak{D}_K$ -sublattice.

The standard dot-product on  $\mathfrak{D}_K^n$  has values in  $\mathfrak{D}_K$ . To pass to integral lattices we first observe  $\mathfrak{D}_K$  is a free  $\mathbb{Z}$ -module of rank  $d_K$  and that  $(x, y) \mapsto \text{Tr}_{K/\mathbb{Q}}(xy)$  provides it with an integral symmetric bilinear form. Secondly, since we assumed  $\text{Tr}_{K/\mathbb{Q}}(\mathfrak{p}) \subset (p)$ , the trace restricted to  $\rho_p^{-1}C$  takes values in  $(p)$ . This motivates to scale the trace form by  $p^{-1}$ , as before. This yields

$$\Gamma_C = \rho_p^{-1}C \subset \mathfrak{D}_K^n(p^{-1})$$

with the form

$$(x, y) \mapsto \frac{1}{p} \text{Tr}_{K/\mathbb{Q}}(x \cdot y), \quad x, y \in \mathfrak{D}_K^n.$$

**Lemma 5.3.6.** 1.  $\Gamma_C$  is an integral lattice if and only if  $C \subset \mathbb{F}_p^n$  is isotropic with respect to the standard dot product.

2. The discriminant of the lattice  $\Gamma_C$  is given by

$$\text{disc}(\Gamma_C) = p^{2n-2m} \cdot \left( \mathfrak{d}_K/p^{d_K} \right)^n = \mathfrak{d}_K^n \cdot p^{n(2-d_K)-2m}, \quad m = \dim C. \quad (5.14)$$

*Proof.* 1. From the remarks preceding the statement of the lemma the dot product of  $x, y \in \mathfrak{D}_K^n$  lands in the ideal  $\mathfrak{p}$  if and only if  $p^{-1} \cdot \text{Tr}_{K/\mathbb{Q}}(x \cdot y) \in \mathbb{Z}$ . Since  $x \cdot y \in \mathfrak{p}$  if and only if  $(x \bmod \mathfrak{p}) \cdot (y \bmod \mathfrak{p}) = 0$  in  $\mathfrak{D}/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$  if and only if  $\rho_p(x) \cdot \rho_p(y) = 0$ . The latter is the case if and only if  $C$  is an isotropic subspace of  $\mathbb{F}_p^n$ .

2. If  $\dim C = m$ , then  $\Gamma_C$  is a submodule of index  $p^{n-m}$  of  $\mathfrak{D}_K^n(p^{-1}) \simeq \mathbb{Z}^{nd_K}(p^{-1})$ . Then by Lemma 1.2.2  $\text{disc}(\Gamma_C) = \text{disc}(\mathfrak{D}_K(p^{-1}))^n \cdot (p^{n-m})^2 = (\mathfrak{d}_K^n/p^{d_K})^n \cdot (p^{n-m})^2$ .  $\square$

To obtain positive definite forms we switch to the hermitian trace form, which, by Lemma 5.3.3, is positive definite. However, it need not be integral. To ensure this we make the assumption (see § 5.3.C for an example)

$$u - \bar{u} \in \mathfrak{p} \text{ for all } u \in \mathfrak{D}_K, \quad (5.15)$$

where the complex conjugate is with respect to a fixed non-real embedding  $K \hookrightarrow \mathbb{C}$ . Under this assumption  $x \cdot \bar{y} \equiv x \cdot y \pmod{\mathfrak{p}}$  and so belongs to  $\mathfrak{p}$  if  $x, y \in \Gamma_C$ . This implies that  $C$  then is an isotropic code, and the positive definite hermitian trace form

$$(x, y) \mapsto x \bullet y := p^{-1} \text{Tr}_{K/\mathbb{Q}}(x \cdot \bar{y}), \quad x, y \in \Gamma_C, \quad (5.16)$$

is indeed an integral form on  $\Gamma_C$ . As to the formula (5.14), we need to see what changes if we use the hermitian trace when computing the discriminant of  $\mathfrak{D}_K$ . Since conjugation on the  $\mathbb{Q}$ -vector space  $K$  is a linear map with determinant  $(-1)^s$ , we see that only the sign may change. Since the form is positive definite we thus find for the new form (5.16)

$$\text{disc}(\Gamma_C) = p^{2n-2m} \cdot \left( |\mathfrak{d}_K|/p^{d_K} \right)^n = |\mathfrak{d}_K|^n \cdot p^{n(2-d_K)-2m}, \quad \text{where } m = \dim C. \quad (5.17)$$

**5.3.C Codes from cyclotomic fields.** Let  $K$  be the cyclotomic field  $\mathbb{Q}(\zeta)$ ,  $\zeta = e^{2\pi i/p}$ , where  $p$  is an odd prime. We recall some facts (cf. for example [111, §9.2]).

- The degree of the field extension  $K/\mathbb{Q}$  is  $p - 1$ .
- For a primitive  $p$ -th root of unity  $z$  we have  $\text{Tr}_{K/\mathbb{Q}}(z) = z + z^2 + \cdots + z^{p-1} = -1$ .
- $\mathfrak{D}_K = \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{p-2}$  and  $\mathfrak{d}_K = (-1)^{\frac{p-1}{2}} p^{p-2}$ .
- The ideal  $\mathfrak{p} \subset \mathfrak{D}_K$  generated by  $1 - \zeta$  is prime and its inertia index is 1.

Assumption (5.15) is satisfied in this case with respect to the given embedding. To see this, note that if  $z$  is any  $p$ -th root of unity, we have  $\bar{z} - z = z^{p-1} - z = z(z^{p-2} - 1) = z(z - 1)(z^{p-3} + z^{p-4} + \cdots + 1)$  which belongs to  $\mathfrak{p}$  since  $z - 1 = \zeta^k - 1$  is divisible by  $\zeta - 1$ , the generator of  $\mathfrak{p}$ .

Let us now investigate the lattices  $\Gamma_C$ .

**Example 5.3.7.** Take  $n = 1$ . The code  $0 \subset \mathbb{F}_p$  gives a lattice of rank  $p - 1$  and discriminant  $p$ . It is isometric to the root lattice  $A_{p-1}$ . To see this, we use the  $\mathbb{Z}$ -basis for  $\mathfrak{p} = \rho_p^{-1}0$  given by  $\{b_1 = 1 - \zeta, b_2 = \zeta(1 - \zeta), \dots, b_{p-1} = \zeta^{p-2}(1 - \zeta)\}$  and

we calculate the products  $b_i \cdot b_j$  with respect to the form (5.16) as follows. We first compute the traces of the expressions  $z^k(1-z)(1-\bar{z}) = 2z^k - z^{k+1} - z^{k-1}$ . We have

$$\mathrm{Tr}_{K/\mathbb{Q}}(2z^k - z^{k+1} - z^{k-1}) = \begin{cases} 2(p-1) + 2 = 2p & \text{if } k \equiv 0 \pmod{p}, \\ -2 + 1 - (p-1) = -p & \text{if } k \equiv \pm 1 \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$

It follows that the scaled dot product of  $z^a(1-z)$  and  $z^b(1-z)$  equals  $p^{-1} \cdot \mathrm{Tr}_{K/\mathbb{Q}} z^{a-b}(1-z)(1-\bar{z}) = 2$ , respectively  $-1$  if  $a = b$ ,  $|a - b| = 1$ , respectively, and  $0$  otherwise. Hence the Gram matrix with respect to the  $b_i$  is that of  $A_{p-1}$ . We deduce that therefore all isotropic codes  $C \subset \mathbb{F}_p^n$  give integral lattices that contain  $A_{p-1}^{\otimes n}$ .

**Lemma 5.3.8.** *Let  $K = \mathbb{Q}(\zeta)$ ,  $\mathfrak{D}_K$  and  $\rho_p : \mathfrak{D}_K^n \rightarrow \mathbb{F}_p^n$  be as above. An  $m$ -dimensional isotropic code  $C \subset \mathbb{F}_p^n$  gives a positive definite even lattice  $\Gamma_C = \rho_p^{-1}C$  of rank  $n(p-1)$  and discriminant  $p^{n-2m}$ . It is unimodular if and only if  $n = 2m$ , that is, if  $C$  is self-dual.*

*It contains  $A_{p-1}^{\otimes n}$  and if the minimal weight of  $C$  is  $> p$ , then  $A_{p-1}^{\otimes n}$  is the root sublattice of  $\Gamma_C$ .*

*Proof.* We have seen that  $d_K = p-1$  and that  $|\mathfrak{d}_K| = p^{p-2}$ . Then (5.17) gives the discriminant  $p^{n-2m}$  from which also the statement about unimodularity follows. The lattice  $\Gamma_C$  is even since the maximally totally real subfield  $k$  of  $K$  is generated by  $\zeta + \bar{\zeta}$  and thus is of index 2 in  $K$  so that for all  $x \in \mathfrak{D}_K$  the real number  $x\bar{x}$  belongs to  $k \cap \mathfrak{D}_K$  and  $\mathrm{Tr}_{K/\mathbb{Q}}(x\bar{x}) = 2 \mathrm{Tr}_{k/\mathbb{Q}}(x\bar{x})$  is even.

Example 5.3.7 shows that  $\Gamma_C$  contains  $A_{p-1}^{\otimes n}$  and that  $A_{p-1}^{\otimes n}$  maps to zero in  $C$ . For a root  $x \in \Gamma_C$  one has

$$2 = x \bullet x = (1/p) \sum_j \mathrm{Tr}_{K/\mathbb{Q}}(x_j \bar{x}_j) = (2/p) \sum_j \mathrm{Tr}_{k/\mathbb{Q}}(x_j \bar{x}_j), \quad x = (x_1, \dots, x_n).$$

Hence,  $\mathrm{Tr}_{k/\mathbb{Q}}(x_j \bar{x}_j)$ , a non-negative integer, can be positive for at most  $p$  coordinates  $x_j$ . So, if the minimal weight of  $C$  is  $> p$ , such a root cannot map to a non-zero code word. In this case  $A_{p-1}^{\otimes n}$  is the root sublattice of  $\Gamma_C$ .  $\square$

**Examples 5.3.9.** 1. Take  $p = 3$  and  $C = \mathbb{F}_3 \cdot (1, 1, 1) \subset \mathbb{F}_3^3$ . Then  $\Gamma_C$  has rank  $3 \cdot (3-1) = 6$ , discriminant  $3^{3-2} = 3$ , and turns out to be the root lattice  $E_6$ .

This can be seen by direct calculation. A more theoretical argument is given in [64, §5.2].

2. Take  $p = 5$  and  $C$  the line in the plane over  $\mathbb{F}_5$  spanned by  $(1, 2)$ . Then  $C$  is self-dual and so the positive definite lattice it gives is unimodular, even and of rank  $2 \cdot 4 = 8$ . By classification again it must be  $E_8$ .

3. **Niemeier lattices.** Recall (cf. Section 1.12) that by definition these are the positive definite unimodular even lattices of rank 24. In the present setting these occur if  $\mathrm{rank}(\Gamma_C) = n(p-1) = 24$  and  $C$  is self-dual. In other words, if  $(p, n) = (3, 12), (5, 6), (7, 4), (13, 2)$ . We follow the exposition of [64, Section 5.2] where further details can be found. Here is the list:

- $p = 3$ . Here one uses the so-called extended ternary Golay code, a self-dual code in  $\mathbb{F}_3^{12}$  of dimension 6 whose definition can be found on p. 137 of [64]. It has minimum weight 6. By Lemma 5.3.8 the corresponding lattice contains  $A_2^{\otimes 12}$  and no other roots. There is another self-dual ternary code in  $\mathbb{F}_3^{12}$  such that the corresponding Niemeier lattice contains  $E_6^{\otimes 4}$ .
- $p = 5$ . The code in  $\mathbb{F}_5^6$  spanned by the rows of

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 2 & -2 \\ 2 & -2 & 0 & 0 & 1 & 1 \\ 1 & 1 & 2 & -2 & 0 & 0 \end{pmatrix}$$

gives a Niemeier lattice containing  $A_4^{\otimes 6}$ . Without considering weights of words, we can conclude by Theorem 1.12.1 that this must be its root sublattice.

- $p = 7$ . The code in  $\mathbb{F}_7^4$  spanned by the rows of

$$\begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 3 & -2 & 1 \end{pmatrix}$$

gives a Niemeier lattice containing  $A_6^{\otimes 4}$  which again by Theorem 1.12.1 is its root sublattice.

- $p = 13$ . The Niemeier lattice corresponding to the code generated by  $(1, 5) \subset \mathbb{F}_{13}^2$  has  $A_{12}^{\otimes 2}$  as its root sublattice.

## 5.4 Lattices and Quaternions

**5.4.A Quaternion algebras over fields.** The classical algebra of quaternions  $\mathbb{H}$  is the associative  $\mathbb{R}$ -algebra with unit 1, generators  $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ , in which the product is determined by  $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ ,  $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ . It has an anti-involution given by

$$x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k} \mapsto x^* = x_0 - x_1\mathbf{i} - x_2\mathbf{j} - x_3\mathbf{k}. \quad (5.18)$$

The anti-involutive property means that  $x \mapsto x^*$  is an anti-isomorphism, i.e.  $(xy)^* = y^*x^*$  and that it is an involution, that is  $(x^*)^* = x$ .

The algebra  $\mathbb{H}$  was invented by Hamilton who called its elements *quaternions*. This construction has a variant over any field of characteristic different from 2:

**Definition 5.4.1.** A *quaternion algebra over  $k$*  is a  $k$ -algebra  $D$  with the following properties:

- $D$  is central, i.e., its center is  $k$ ;
- $D = K + K\mathbf{j}$ , a skew field of dimension 2 over a quadratic extension algebra  $K = k[\mathbf{i}]$  of  $k$ , where  $\mathbf{i}^2 \in k^\times$ ;

- for all  $z = x + \mathbf{i}y \in K$ , one has  $\mathbf{j}z = z^* \mathbf{j}$ , where  $z^* = x - \mathbf{i}y$ .

From this it follows that in particular,  $\mathbf{i}\mathbf{j} = -\mathbf{j}\mathbf{i}$ . Moreover, if  $\mathbf{i}^2 := a \in k^\times$ ,  $\mathbf{j}^2 := b \in k^\times$ , setting  $\mathbf{k} = \mathbf{i}\mathbf{j}$ , then  $\mathbf{k}^2 = -ab$ . We denote such a quaternion algebra by

$$D = \left( \frac{a, b}{k} \right).$$

Two quaternion algebras  $D, D'$  over the same field  $k$  built from the quadratic extension algebras  $K/k, K'/k$ , respectively, are said to be isomorphic if a  $k$ -algebra isomorphism  $f : D \rightarrow D'$  exists with  $f(K) = K'$ . For instance, we may take  $K = K'$  but choose a different generator for the extension  $D/K$ , or we may exchange  $\mathbf{i}$  and  $\mathbf{j}$  so that  $K' = k(\mathbf{j})$  and  $D' = K'(\mathbf{i})$ . This leads to the isomorphisms

$$\left( \frac{a, b}{k} \right) \simeq \left( \frac{b, a}{k} \right), \quad (\mathbf{i}, \mathbf{j}) \mapsto (\mathbf{j}, \mathbf{i}), \quad (5.19)$$

$$\left( \frac{at^2, b}{k} \right) \simeq \left( \frac{a, b}{k} \right), \quad (\mathbf{i}, \mathbf{j}) \mapsto (t^{-1}\mathbf{i}, \mathbf{j}), \quad t \in k^\times. \quad (5.20)$$

Note that the algebra  $M_2(k)$  of  $2 \times 2$  matrices is a quaternion algebra, the so-called *split quaternion algebra*, as shown by the assignment

$$\left( \frac{1, b}{k} \right) \simeq M_2(k), \quad \mathbf{i} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{j} \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}. \quad (5.21)$$

Over a perfect field every element is a square. In view of (5.20) and (5.21) this implies that over such fields a quaternion algebra is split. This happens in particular if we pass to an algebraic closure  $\bar{k}$  of  $k$ :

$$\left( \frac{a, b}{\bar{k}} \right) \simeq M_2(\bar{k}).$$

As in the case of the Hamilton quaternions, the involution  $z \mapsto z^*$  on  $K$  extends uniquely to an anti-involution on  $\left( \frac{a, b}{k} \right)$  and is given by (5.18). Using this anti-involution, one defines

$$N(x) = x \cdot x^* \in k \quad (\text{norm of } x) \quad (5.22)$$

$$T(x) = x + x^* \in k \quad (\text{reduced trace of } x). \quad (5.23)$$

Explicitly, if  $x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ , then  $N(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$  and  $T(x) = 2x_0$ . The norm  $N(x)$  is a quadratic form over  $k$  whose polar form is

$$T(xy^*) = N(x + y) - N(x) - N(y).$$

Note that  $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$  form an orthogonal basis. The discriminant of the polar form is a non-zero square  $a^2b^2$  and hence  $\text{disc}(N) = 1 \in D(k)$ .



**Example 5.4.2.** Consider  $\left(\frac{1,1}{k}\right)$ . An explicit isomorphism  $\left(\frac{1,1}{k}\right) \simeq M_2(k)$  is given by

$$x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k} = (x_0 + x_1\mathbf{i}) + (x_2 + x_3\mathbf{i}) \cdot \mathbf{j} \mapsto \begin{pmatrix} x_0 + x_1 & x_2 + x_3 \\ x_2 - x_3 & x_0 - x_1 \end{pmatrix}.$$

Then the anti-involution is given by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

The reduced trace is the usual trace and the norm is the determinant.

The quaternions  $\mathbb{H}$  form a division algebra or skew field: every element  $x \neq 0$  has an inverse. Indeed,  $N(x) \neq 0$  if and only if  $x \neq 0$  and hence  $x^{-1} = x^*/N(x)$ . In general, for a quaternion algebra  $\left(\frac{a,b}{k}\right)$  this might or might not be the case depending on  $a$  and  $b$ . For instance  $M_2(k)$  is not a division algebra: the matrices with zero determinant are not invertible.

Using the multiplicativity of the norm

$$N(x \cdot y) = N(x) \cdot N(y),$$

one sees that if  $x^{-1}$  exists, then  $N(x)N(x^{-1}) = 1$  and conversely, if  $N(x) \neq 0$ , then  $x^{-1} = x^*/N(x)$ . A quaternion algebra is not a division algebra if and only if  $N$  admits isotropic vectors. Such algebras turn out to be always isomorphic to matrix algebras. In fact, we have:

**Proposition 5.4.3.** *A quaternion algebra is split, i.e. isomorphic to  $M_2(k)$ , if and only if the norm admits an isotropic vector.*

One half of this statement follows from what we just said, but the proof of the implication "non-split  $\implies$  skew field" is non-trivial. For a proof we refer to [234, Ch. I, §2].

**5.4.B Ternary forms and quaternion algebras.** Let  $D = \left(\frac{a,b}{k}\right)$  be a quaternion algebra. Clearly  $k \cdot 1 \subset D$  is the fixed point set of the involution  $*$  and the trace is non-degenerate on it. We next show that we get in fact an orthogonal decomposition

$$D = k \cdot 1 \oplus D^0, \quad D^0 = \{x \in D \mid x = -x^*\} = \{x \in D \mid T(x) = 0\}.$$

It suffices to check that the traceless quaternions are orthogonal to the constants. This is based on writing  $2x = (x+x^*) + (x-x^*)$ , where we use that the characteristic  $\neq 2$ . To see this, let  $\lambda \in k$  and  $y \in D^0$ . Then

$$\begin{aligned} T(\lambda y^*) &= N(\lambda \cdot 1 + y) - N(\lambda \cdot 1) - N(y) \\ &= \lambda^2 + \lambda(y + y^*) + yy^* - \lambda^2 - yy^* \\ &= \lambda(y + y^*) = 0. \end{aligned}$$

If  $D = \left(\frac{a,b}{k}\right)$ , the norm form on  $D^0$  is given by

$$(x_1, x_2, x_3) \mapsto -ax_1^2 - bx_2^2 + abx_3^2, \quad (5.24)$$

a *ternary  $k$ -valued form*.

**Proposition 5.4.4.** *Let  $D, D'$  be quaternion algebras. The following statements are equivalent:*

1. *The quaternion algebras  $D$  and  $D'$  are isomorphic;*
2. *The associated norm forms on the  $k$ -vector spaces  $D$  and  $D'$  are isometric;*
3. *The associated norm forms on the  $k$ -vector spaces  $D^0$  and  $(D')^0$  are isometric.*

The quaternion algebra  $M_2(k)$  corresponds to the up to isometry unique isotropic ternary form  $-x_1^2 - x_2^2 + x_3^2$ .

*Proof.* 1 implies 2 since an isomorphism of quaternion algebras preserves the norm forms.

2 implies 3 because of Witt's cancelation theorem 7.2.7 which we prove in a later chapter.

Proof that 3 implies 1: First of all,  $D^0$  has an orthogonal basis, say  $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$ , and since an isometry  $f : D^0 \rightarrow (D')^0$  preserves orthogonality, the images  $f(\mathbf{i}) = \mathbf{i}'$ ,  $f(\mathbf{j}) = \mathbf{j}'$  and  $f(\mathbf{k}) = \mathbf{k}'$  are orthogonal. Let  $N$  be the quadratic form on  $D^0$  and  $N'$  the one on  $(D')^0$ . Write  $N(\mathbf{i}) = -a, N(\mathbf{j}) = -b, N(\mathbf{k}) = ab$ ,  $a, b \in k^\times$ . We use the accented symbols for  $(D')^0$ . Since  $f$  is an isometry,

$$\begin{aligned} 0 &= \mathbf{i} \cdot -\mathbf{j} + (\mathbf{j} \cdot -\mathbf{i}) = T(\mathbf{i} \cdot -\mathbf{j}) = T'(\mathbf{i}' \cdot -\mathbf{j}') \\ &= [N'(\mathbf{i}' + \mathbf{j}') - N'(\mathbf{i}') - N'(\mathbf{j}')] \\ &= (\mathbf{i}' + \mathbf{j}')^2 - (\mathbf{i}')^2 - (\mathbf{j}')^2 \\ &= \mathbf{i}'\mathbf{j}' + \mathbf{j}'\mathbf{i}'. \end{aligned}$$

So  $\mathbf{i}'\mathbf{j}' = -\mathbf{j}'\mathbf{i}'$ . By assumption,  $D' = k \cdot 1 \oplus (D')^0$  as  $k$ -vector spaces and the argument so far shows that  $D' = \left(\frac{a',b'}{k}\right)$ . Hence, setting  $f(1) = 1$ , the isometry  $f$  extends as a quaternion algebra isomorphism between  $D$  and  $D'$ .

Finally we prove the last assertion. By Proposition 5.4.3, up to isometry the algebra  $M_2(k)$  is the unique quaternion algebra for which isotropic vectors for the norm exist. Under the isomorphism (5.21) the algebra  $M_2(k)$  corresponds to  $\left(\frac{1,b}{k}\right)$  and the corresponding ternary form is  $\text{diag}(-1, -b, b)$  with isotropic vector  $(0, 1, 1)$ . This form is indeed isometric to  $\text{diag}(-1, -1, 1)$  since the basis change matrix  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2}(b+1) & \frac{1}{2}(b-1) \\ 0 & \frac{1}{2}(b-1) & \frac{1}{2}(b+1) \end{pmatrix}$  transforms  $\text{diag}(-1, -1, 1)$  into  $\text{diag}(-1, -b, b)$ .  $\square$

**Corollary 5.4.5.** *The map which sends  $D$  to the quadratic form on  $D^0$  induced by the norm defines a bijection between the set of isomorphism classes of quaternion  $k$ -algebras and the equivalence classes of  $k$ -valued ternary forms with discriminant 1.*

*Proof.* First recall (cf. Proposition 1.1.4) that a quadratic form over  $k$  is diagonalizable and such a form is non-degenerate if and only if its discriminant is non-zero. Also recall that discriminants are well defined up to squares in  $k^\times$ . Hence a ternary form with discriminant 1 can be taken to be  $\text{diag}(-a, -b, c)$  with  $abc$  a square in  $k^\times$ , say  $a^2b^2$ . This gives a form of the shape (5.24), that is, a ternary form associated to a quaternion algebra. In other words, norm forms on  $D^0$  are isometric to ternary forms with discriminant 1 and conversely. The statement is then a direct consequence of Proposition 5.4.4.  $\square$

As a consequence we may write  $D(q)$  for the quaternion algebra  $D$  associated to a given ternary form  $q$  with discriminant 1.

**5.4.C Quaternion algebras over the field  $\mathbb{Q}$ .** As explained in Chapter 3, the classification of quadratic forms over  $\mathbb{Q}$  is determined by the discriminant, the Hasse invariants at finite places and the index. The local behaviour of a quaternion algebra is governed by places over which it is non-split. This is captured in the following definition.

**Definition 5.4.6.** A  $\mathbb{Q}$ -quaternion algebra  $D$  is *non-split or ramified at the place*  $v \in \mathcal{P}$  if its localization  $D_v$  at  $v$  is a skew field.

The goal is to classify quaternion algebras  $D(q)$  over  $\mathbb{Q}$  given by quadratic forms  $q = \text{diag}(-a, -b, ab)$ . Since  $\text{disc}(q) = 1$  (modulo squares), the index can be 3 or  $-1$  depending on the signs of  $a$  and  $b$ . Only the second possibility can give rise to isotropic vectors. Then  $D(q) \otimes \mathbb{R} \simeq M_2(\mathbb{R})$ . Otherwise, if  $a, b < 0$ , we get the quaternions. The classification is as follows.

**Proposition 5.4.7.** *A quaternion algebra over  $\mathbb{Q}$  is ramified at an even number of places. Given an even number of places, there is a quaternion algebra ramified at exactly those places. In particular there is a unique isomorphism class of quaternion algebras split everywhere except at a given prime and at  $\infty$ .*

*Proof.* Suppose that the algebra is  $D(q)$  with  $q = -ax_1^2 - bx_2^2 + abx_3^2$ . One verifies that  $\epsilon_p(q) = (a, b)_p$ . By definition of the Hilbert symbol,  $(a, b)_p = 1$  is equivalent to  $q$  having an isotropic vector which is equivalent to  $\left(\frac{a, b}{\mathbb{Q}_p}\right) \simeq M_2(\mathbb{Q}_p)$ . So  $(a, b)_p = -1$  precisely means that the corresponding quaternion algebra is ramified. A representing local form with this property is  $\text{diag}(-u, -p, up)$  where  $u$  is a non-square modulo  $p$ . We already saw that at the place  $\infty$  we have ramification if and only if  $a, b < 0$ . By Remark 3.3.6, the only restriction for the existence of a quadratic form over  $\mathbb{Q}$  is the Hilbert product formula,  $\prod_{v \in \mathcal{P}} (a, b)_v = 1$ . This implies that a quaternion algebra is ramified at an even number of places and, conversely, that there exists a quaternion algebra ramified at a given even set of places.  $\square$

Finiteness of the ramification locus leads to the concept of *discriminant*  $\text{disc}(D)$  of  $D$  as the product of all finite places at which  $D$  is ramified.

**5.4.D Ternary integral quadratic forms.** To construct lattices in quaternion algebras  $D = D(q)$  over  $\mathbb{Q}$ , one uses *orders*, i.e., subrings of  $D$  that are integral  $\mathbb{Z}$ -modules of rank 4. These exist: simply take  $\mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{k}$ . By definition, the discriminant of an order  $L \subset D$  is the discriminant of  $q|_L$ . Every order of  $D$  is contained in a maximal order. These need not be unique, but we have:

**Proposition 5.4.8.** *The maximal orders of  $D = D(q)$  are the orders with discriminant  $d^2$  where  $d = \text{disc}(D)$ , the discriminant of  $D$ . Any maximal order in  $D$  gives a positive definite rank 4 quadratic lattice with discriminant  $d^2$ . Such maximal orders exist.*

For a proof see e.g. Cor. 2.5 in the lecture notes [38] where the reader also finds a short introduction to maximal orders.

**Example 5.4.9.** Consider the (unique) quaternion algebra  $D$  ramified at the prime  $p$  and the place at  $\infty$ . This is a positive definite form with  $\text{disc}(D) = p$ . We claim that for  $p \equiv 3 \pmod{4}$  this quaternion algebra is  $D = \left(\frac{-1, -p}{\mathbb{Q}}\right)$ . In that case the ternary quadratic form is  $q = x^2 + py^2 + pz^2$ , which is positive definite and hence ramified at infinity. The form has discriminant  $p^2$  and so is unimodular when localized at primes  $p' \neq p$ . Unimodular forms in  $\mathbb{Q}_{p'}$  have isotropic vectors (see e.g. Example A.4.2) and so  $D = D(q)$  is not ramified at the prime  $p'$ . Since  $D(q)$  must be ramified at an even number of finite places, it must be ramified at  $p$ . This shows our claim. A maximal order in  $D$  gives a positive definite lattice of rank 4 with discriminant  $p^2$ . Since  $N(1 + \mathbf{j}) = 1 + p \equiv 0 \pmod{4}$ , a maximal order is for instance given by

$$\mathbb{Z} + \mathbf{i}\mathbb{Z} + \frac{1}{2}(1 + \mathbf{j})\mathbb{Z} + \frac{1}{2}(\mathbf{i} + \mathbf{k})\mathbb{Z}.$$

The trace form splits into two binary forms each given by the matrix

$$\begin{pmatrix} 2 & 1 \\ 1 & \frac{1}{2}(p+1) \end{pmatrix}$$

which indeed represents an even form with discriminant  $p$ . For  $p \equiv 1 \pmod{4}$  it is a little more involved to describe maximal orders in  $D$ . See for instance [38, Example 1.9], from which it follows that the corresponding integral ternary forms are isometric to  $ax^2 + py^2 + apz^2$  for a suitable integer  $a$  prime to  $p$  (the integer depends on  $p \pmod{8}$ ).

**Historical and Bibliographical Notes.** Mathematical coding theory arguably began with the invention of the Golay code [85]. A year later, at Bell Labs, R. Hamming found the famous code named after him (cf. [91]). A few years later the Reed–Muller codes [190, 162] were constructed which are named after their inventors I. Reed and D. Muller. For the relation with lattices and the construction of codes from lattices in number fields we have followed the book [64] by W. Ebeling. In Chapter 2 of [64] also theta functions as introduced in § 1.12.B play a central role.

Classically, Kummer surfaces were the quartic surfaces in  $\mathbb{P}^3$  with 16 nodes. Their configuration has been very much studied. See e.g. the exposition [102] by R. Hudson

which has a foreword by W. Barth explaining its topics in modern language. That a K3 surface with 16 disjoint curves is an (abstract) Kummer surface was first observed by V. Nikulin in [168]. His proof is based on affine geometry over the field  $F_2$  as is the proof of Prop. VIII.6.1 in the monograph [15] where, however, the superfluous assumption of the evenness of the 16 double points was made (and used). The first proof which systematically uses coding theory is due to A. Kalker in his thesis [115] where several other geometric applications can be found. V. Nikulin [168] showed that a K3 surface cannot acquire more than 16 double points. The proof uses lattice theory. For a proof using coding theory, see [185]. The application of coding theory to estimate numbers of double points on quintic surfaces in  $\mathbb{P}^3$  is due to A. Beauville [17]. For double points on sextics and their related codes see J. Wahl's note [243] as well as [108] by D. Jaffe and D. Ruberman. For characteristic  $p$ -phenomena involving codes and double points for  $p > 0$ , see I. Shimada's articles [207, 208]. The term "Nikulin involution" probably has been coined for the first time by D. Morrison [158] where he cites Section 5 of Nikulin's article [169].

Quaternions were invented by W. R. Hamilton as can be seen from his letter [90]. The relation with ternary forms dates back to the articles by C. Latimer [136, Thm.3], G. Pall [180, Thm.4 and 5] and H. Brandt [28]. It is quite classical that isomorphism classes of quaternion algebras correspond bijectively to isometry classes of ternary forms and, if the field is  $\mathbb{Q}$ , that this correspondence is governed by the Hilbert symbols. For this and the relation with integral ternary forms, one may consult for instance Section 57 in T. O'Meara's book [177].

For more information and background on quaternions see the classical book [234] by M.-F. Vigneras, or the voluminous opus [241] by J. Voight.

## Symmetric and Quadratic Forms Revisited

In this chapter  $R$  is a commutative ring with 1, and  $F$  is an  $R$ -module.  $Q(R)$  is the fraction field of an integral domain  $R$ .

### Introduction

In Chapter 1 it became already clear that in order to study integral lattices, one has to widen one's perspective to include the  $p$ -adic situation and torsion forms. This motivates the study of finitely generated  $R$ -modules, free or not, over any commutative ring  $R$  (with 1) and equipped with symmetric forms that take values in any  $R$ -module  $F$ . In this chapter we investigate which of the constructions of Chapter 1 remain valid in this more general setting.

More specifically, in Section 6.1 we give the basic definitions, discuss orthogonality, non-degeneracy and isometry. Several examples are exhibited in § 6.1.B, and in § 6.1.D we present a list of the non-degenerate symmetric and quadratic torsion forms on the cyclic groups. We shall see in Section 6.2 that the notion of correlation morphism makes sense in this general context and hence also the notion of unimodularity.

We then turn to finite rank free  $R$ -modules and show that unimodular submodules split off orthogonally (Proposition 6.3.10). This important splitting principle plays a major role in classification theory as illustrated later on in Chapters 9 and 10 where we establish local normal forms for symmetric and quadratic torsion groups and  $p$ -adic lattices.

If we also assume that  $R$  is an integral domain, an  $R$ -valued form on a finite rank free  $R$ -module  $L$  induces a  $Q(R)$ -valued form on the torsion  $R$ -module  $L^*/L$  which is the discriminant form in this more general setting as we shall see in Section 6.4. The final Section 6.5 is devoted to isometry groups.

### 6.1 Bilinear Forms on $R$ -Modules

**6.1.A Basic definitions.** For any  $R$ -module  $V$  we consider the associated dual  $R$ -modules

$$V^* := \text{Hom}_R(V, R), \quad V_F^* = \text{Hom}_R(V, F). \quad (6.1)$$

**Definition 6.1.1.** An  $F$ -valued form  $b$  on an  $R$  module  $V$  is a bilinear form  $b : V \times V \rightarrow F$ . In other words,  $b$  has the following properties:

$$\begin{aligned} b(rx + sy, z) &= rb(x, z) + sb(y, z), \quad r, s \in R, x, y, z \in V \text{ (left-linearity),} \\ b(x, ry + sz) &= rb(x, y) + sb(x, z), \quad r, s \in R, x, y, z \in V \text{ (right-linearity).} \end{aligned}$$

An  $F$ -valued form  $b$  is called symmetric, if  $b(x, y) = b(y, x)$  for  $x, y \in V$ , skew-symmetric, if  $b(x, y) = -b(y, x)$  for  $x, y \in V$ , and alternating or symplectic, if  $b(x, x) = 0$  for all  $x \in V$ .

In this book we mainly restrict ourselves to the symmetric forms.<sup>1</sup> An  $F$ -valued **symmetric  $R$ -module** consists of a pair  $(V, b)$  of an  $R$ -module  $V$  and an  $F$ -valued symmetric form  $b$ . If  $F = R$  we speak of a **symmetric  $R$ -module**.

As we have seen in the special context of Chapter 1, symmetric forms and quadratic forms are intimately related. This remains so in this wider setting.

**Definition 6.1.2.** An  $F$ -valued **quadratic  $R$ -module** consists of an  $R$ -module  $V$  equipped with an  $R$ -quadratic function  $q : V \rightarrow F$ , i.e.,  $q(rx) = r^2q(x)$  for all  $r \in R$  and  $x \in V$ , and such that the form  $b_q(x, y) = q(x + y) - q(x) - q(y)$  is a symmetric  $F$ -valued bilinear form on  $V$ , the **polar form** of  $q$ .

If  $F = R$  we speak of a **quadratic  $R$ -module**.

It follows from the above definitions that  $b_q(x, x) = q(2x) - 2q(x) = 2q(x) \in 2F$ . In contrast to the integral situation, 2 can be a unit in  $R$  and then the bilinear form  $b = 2^{-1}b_q$  gives back  $q$ . If this is not the case, we distinguish two cases, just as in the integral situation:

**Definition 6.1.3.** Suppose  $2 \neq 0$  is not a unit in  $R$ . Then an  $F$ -valued symmetric form  $b$  on  $V$  is called **even** if  $b(x, x) \in 2F$  for all  $x \in V$ . A form which is not even is called **odd**.

By what we have just said, a quadratic form gives rise to an even form. The converse, every even form comes from a quadratic form, is true provided 2 is not a zero-divisor, that is, if multiplication by 2 on  $F$  is injective.

The preceding notions of symmetric and quadratic forms cover several important special cases:

1.  $F = R$  an integral domain. In particular we have:
  - $F = R = k$  a field and  $V$  a finite dimensional  $k$ -vector space. This covers the familiar objects from linear algebra as reviewed in § 1.1.
  - An  **$R$ -lattice** is a free  $R$ -module of finite rank equipped with a symmetric  $R$ -valued form.

For  $R = F = \mathbb{Z}$  we recover integral lattices. Also the notion of parity (odd or even) is as before.

For  $R = F = \mathbb{Z}_p$  we recover the notion of a  $p$ -adic lattice. Note that only for  $p = 2$  it makes sense to speak of even forms.

<sup>1</sup>For symplectic forms see Appendix A.5

2.  $R$  an integral domain and  $F = Q(R)$ , its field of fractions. A **symmetric (respectively quadratic) torsion form over  $R$**  is a  $Q(R)/R$ -valued symmetric bilinear (respectively quadratic) form on a finitely generated torsion  $R$ -module. Observe that multiplication by  $r \neq 0$  in  $Q(R)/R$  annihilates  $1/r$  and so is never injective. But worse: all forms are even in the previous sense since a fraction  $p/q \in Q(R)$  can be rewritten as  $p/q = 2 \cdot p/2q$  and so the terminology does not make sense in this situation.

Special cases of torsion forms arise when  $R = \mathbb{Z}$ . These are forms on finite abelian groups with values in  $\mathbb{Q}/\mathbb{Z}$  and in this case we simply speak of **symmetric, respectively quadratic torsion forms**.

One of our goals is to classify symmetric and quadratic forms up to suitable equivalence. We already encountered the notion of isometry in Section 1.5. This can be extended to the present setting and provides the equivalence relation we employ:

**Definition 6.1.4.** Let  $(V_j, b_j)$ ,  $j = 1, 2$ , be two symmetric  $F$ -valued  $R$ -bilinear modules. A homomorphism of  $R$ -modules  $\varphi : V_1 \rightarrow V_2$  such that  $b_2(\varphi(x), \varphi(y)) = b_1(x, y)$  for all  $x, y \in V_1$  is called a **morphism of  $F$ -valued symmetric  $R$ -modules**. If such a morphism is injective, it is called an **isometric embedding** and if it is bijective it is called an **isometry**.

Two symmetric  $F$ -valued  $R$ -bilinear modules  $(V_1, b_1)$  and  $(V_2, b_2)$  are called **isometric**, written  $V_1 \simeq V_2$  or  $b_1 \simeq b_2$ , if there exists an isometry  $V_1 \rightarrow V_2$ . The forms  $b_1$  and  $b_2$  are then said to be **equivalent over  $R$** . For quadratic  $F$ -valued  $R$ -modules the definitions are similar.

If  $V_1 = V_2$  and  $b_1 = b_2$  we speak of self-isometries. These form a group, the **orthogonal group**  $O(V_1, b_1)$  of  $(V_1, b_1)$ .

We shall give a more detailed discussion of isometries in Sections 6.5 and 7.1.

**6.1.B Examples. 1. Rank one forms.** A choice of  $r \in R$  defines the symmetric form  $\langle r \rangle$  on the rank one  $R$ -module  $R \cdot e$  by setting  $e \cdot e = r$ . This is in accordance with the notation we previously used for lattices and vector spaces. Isomorphisms of  $R \cdot e$  are given by multiplying with a unit  $u$  of  $R$ . It transforms  $\langle r \rangle$  into  $\langle u^2 r \rangle$ . So  $\langle r \rangle_R \simeq \langle s \rangle_R$  if and only if  $r = u^2 s$  for a unit  $u \in R^\times$  and isometry classes of non-degenerate (see § 6.1.C below) rank one symmetric  $R$ -modules are in one-to-one correspondence with the set of equivalence classes  $r \cdot (R^\times)^2$ ,  $r \in R - \{0\}$ .

The quadratic form  $[r']$ ,  $r' \in R$ , given by  $x \mapsto r'x^2$  has the symmetric form  $\langle 2r' \rangle$  as its polar form. Isometry classes of non-degenerate rank one quadratic  $R$ -modules are in one-to-one correspondence with  $(2R - \{0\}) \cdot (R^\times)^2$ .

**2.  $p$ -Adic forms.** We apply the preceding classification principle to rank one  $p$ -adic forms. Recall that for odd primes  $p$  the group  $D(\mathbb{Z}_p)$  is cyclic, generated by a non-square modulo  $p$ . The group  $D(\mathbb{Z}_2)$  plays a role in the dyadic situation. This group can be viewed as a subset of the multiplicative group  $(\mathbb{Z}/2^3\mathbb{Z})^\times$ . We represent the elements by the integers  $\pm 1, \pm 3$ . Applying the preceding classification principle in this setting, one obtains:



Lattice	isometry classes of symmetric $\mathbb{Z}_p$ -modules	of quadratic $\mathbb{Z}_p$ -modules
$\langle u \cdot p^k \rangle_{\mathbb{Z}_p}$ , $p$ an odd prime	$u$ square mod $p$ $k \geq 0$	$u$ even square mod $p$ $k \geq 0$
	$u$ non-square mod $p$ $k \geq 0$	$u$ even non-square mod $p$ $k \geq 0$
$\langle u \cdot 2^k \rangle_{\mathbb{Z}_2}$	$u \in \{\pm 1, \pm 3\}$ $k \geq 0$	$u \in \{\pm 1, \pm 3\}$ $k \geq 1$

**3. Scaling a form.** In the same way as for integral lattices, if  $b$  is an  $F$ -valued symmetric form over  $R$  and  $r \in R$ , we let  $b(r)$  be the form defined by  $(x, y) \mapsto r \cdot b(x, y)$ . It is called the form  $b$  *scaled by  $r$* .

We frequently write  $V(r)$  or  $b(r)$  instead of  $(V, b(r))$ . In particular, for  $k = -1$  we obtain the form  $b(-1)$ , the *opposite* of  $b$ .

**6.1.C Orthogonality and non-degeneracy.** Our first task is to extend the *notion of orthogonality* from Section 1.3 to the present setting. Let  $(V, b)$  be a symmetric  $R$ -module. We say that  $X \subset V$  is orthogonal to  $Y \subset V$  if  $b(x, y) = 0$  for all  $x \in X$  and  $y \in Y$ . For a submodule  $W$  of  $V$ , the set of elements in  $V$  *orthogonal* to  $W$  is again a submodule of  $V$  which we write  $W^\perp$ . Similar definitions hold for quadratic modules using the corresponding polar forms.

**Definition 6.1.5. 1.** A submodule  $W \subset V$  is called *isotropic* if  $b(x, y) = 0$  for all  $x, y \in W$ . In other words  $W \subset W^\perp$ . It is called *totally isotropic* if  $W = W^\perp$ . A generator of a rank one isotropic submodule is called an *isotropic vector*. In other words  $x \neq 0$  is isotropic if  $b(x, x) = 0$ . A submodule  $W$  without isotropic vectors is called *totally anisotropic*. In other words,  $W$  is totally anisotropic if the quadratic equation  $b(x, x) = 0$  has only the trivial solution in  $W$ . In the quadratic module setting, one uses the polar form to define these notions.

**2.** The *radical* or *null-space* of a symmetric (quadratic)  $R$ -module  $(V, b)$  (respectively  $(V, q)$ ) is given by

$$\begin{aligned} \text{rad}(b) &= V^\perp = \{x \in V \mid b(x, y) = 0 \text{ for all } y \in V\} \\ \text{rad}(q) &= \{x \in \text{rad}(b_q) \mid q(x) = 0\}, \text{ respectively.} \end{aligned}$$

**3.** The form  $b$  on  $V$  is *non-degenerate* if  $V^\perp = 0$ , i.e. if  $b(x, V) = 0$  implies  $x = 0$ . A quadratic form  $q$  is *non-degenerate* if  $\text{rad}(b_q) = 0$ .

**4.** If  $V$  is a direct sum  $V = W_1 \oplus \cdots \oplus W_m$  of  $R$ -submodules such that the  $W_j$  are mutually orthogonal, we say that  $V$  is the (internal) *orthogonal direct sum* of the  $W_j$ , written as  $V = W_1 \oplus \cdots \oplus W_m$ .

If  $(V_1, b_1), \dots, (V_m, b_m)$  are  $F$ -valued symmetric  $R$ -modules their (external) orthogonal sum is  $V_1 \oplus \cdots \oplus V_m = (V_1 \oplus \cdots \oplus V_m, b_1 \oplus \cdots \oplus b_m)$ .

We point out that the radical of a quadratic form might be different from the radical of its polar form:

**Lemma 6.1.6.** *Let  $(V, q)$  be a quadratic  $R$ -module with polar form  $b_q$ . Then*

1.  $\text{rad}(q)$  is a submodule of  $V$ .
2.  $\text{rad}(q) \subset \text{rad}(b_q)$  with equality if 2 is invertible in  $R$ .

*Proof.* 1. By definition  $q(x+y) = b_q(x, y) + q(x) + q(y)$  and hence, if  $x, y \in \text{rad}(q)$ , so is  $x+y$ .

2. The inclusion  $\text{rad}(q) \subset \text{rad}(b_q)$  follows from the definitions. If 2  $\in R$  is invertible,  $q(x) = 2^{-1}b_q(x, x)$ , which implies that, conversely,  $\text{rad}(b_q) \subset \text{rad}(q)$ .  $\square$

The condition that 2 be a unit is really necessary: consider the quadratic form  $q = x^2 + y^2$  on  $V = \mathbb{F}_2^{\oplus 2}$ . The associated bilinear form is the zero form and so  $\text{rad}(b_q) = V$  while  $\text{rad}(q) = \mathbb{F}_2(1, 1)$ .

*Remark 6.1.7.* Suppose that  $R$  is an integral domain. If  $(V, b)$  is non-degenerate and has values in  $R$ , then  $V$  is free of torsion. Indeed, if  $x \in V$  would be torsion, say  $mx = 0$ , then  $mb(x, V) = 0$  and since  $R$  has no torsion,  $x$  belongs to  $V^\perp = \{0\}$ .

On the other hand, if  $(V, b)$  is a finitely generated non-degenerate  $Q(R)/R$ -valued symmetric bilinear  $R$ -module, then all elements of  $V$  are torsion. Indeed,  $b(x, y) \in Q(R)/R$  implies that there is some  $r = r(x, y) \in R - \{0\}$  such that  $rb(x, y) = 0$ . If  $\{y_1, \dots, y_m\}$  is a set of generators of  $V$ , the non-zero product  $r(x) = r(x, y_1) \cdots r(x, y_m)$  is such that  $r(x)b(x, y) = 0$  for all  $y \in V$ . Hence  $r(x)x \in V^\perp = \{0\}$  and so  $x$  is torsion.

**6.1.D Non-degenerate cyclic torsion forms.** The finite cyclic group  $C_m$  of order  $m$  can be identified with  $\mathbb{Z}/m\mathbb{Z}$ . This unambiguously shows the  $\mathbb{Z}$ -module structure.

**Proposition 6.1.8.** 1. *Any non-degenerate  $\mathbb{Q}/\mathbb{Z}$ -valued cyclic symmetric torsion form on  $C_m$  is given by  $(x, y) \mapsto a \cdot m^{-1} \cdot xy \in \mathbb{Q}/\mathbb{Z}$  for some integer  $a$  with  $(a, m) = 1$ . In other words, it is isometric to  $\langle a \cdot m^{-1} \rangle$ .*

2. *Isometry classes of non-degenerate bilinear cyclic torsion forms on  $C_m$  are classified by  $D(\mathbb{Z}/m\mathbb{Z})$ .*

3. *Any quadratic torsion form on  $C_m$  is of the form  $[\frac{1}{2}am^{-1}]$ , i.e.,  $x \mapsto a(2m)^{-1}x^2$ , with  $am$  even. Its polar form is  $\langle am^{-1} \rangle$ . The quadratic form is non-degenerate if and only if  $(a, m) = 1$ .*

4. *The non-degenerate quadratic forms on  $C_m$  are classified by elements in  $D(\mathbb{Z}/2m\mathbb{Z})$ .*

*Proof.* 1. Any non-zero form on  $C_m$  is of the shape  $(x, y) \mapsto \frac{a}{\ell} \cdot xy$  with  $(a, \ell) = 1$  and  $\ell|m$ . Writing  $m = \mu\ell$ , we see that the form takes the value 0 on the pair  $(1, \ell)$  and so, unless  $\mu = 1$ , the form is degenerate.

2. Since two integers differing by a multiple of  $m$  give the same form on  $C_m$ , the form is specified by giving a residue class modulo  $m$ . Two non-zero residue classes  $a, a' \pmod m$  give isometric forms if and only if  $a' \equiv au^2$  with  $u$  invertible in  $\mathbb{Z}/m\mathbb{Z}$ .

3. For  $q(x) = \frac{a}{b}x^2$  with  $(a, b) = 1$  to be well defined on  $\mathbb{Z}/m\mathbb{Z}$ , first substitute

$x = m$  to conclude  $b \mid m^2$ , and then substitute  $x = 1$  and  $x = m$  to conclude that  $b \mid 2m$ . So the quadratic form can be written in the form  $q(x) = \frac{r}{2m}x^2$  for some integer  $r$ . Substituting  $x = m$  again, we find that  $rm$  should be even. The last part follows from the first item of the proposition.

4. If  $m$  is even, the previous part shows that  $[\frac{1}{2}am^{-1}]$  gives a well-defined non-degenerate quadratic torsion form precisely for those integers  $a$  with  $(a, m) = 1$ . As  $m$  is even, these are also the integers relatively prime with  $2m$ . Two such integers differing by a multiple of  $2m$  determine the same form. Note that automorphisms of  $C_m$  are induced by multiplication with integers  $u$  with  $(u, 2m) = 1$ . Using these, two such torsion forms determined by the integers  $a$  and  $a'$  are easily seen to be isometric if and only if there exists an integer  $u$  with  $(u, 2m) = 1$  such that  $2m \mid a' - au^2$ . So the two forms are equivalent if and only if their classes in  $D(\mathbb{Z}/2m\mathbb{Z})$  are equal.

For  $m$  odd, the integer  $a$  with  $(a, m) = 1$  in  $[\frac{1}{2}am^{-1}]$  is even, since  $am$  is even. In a similar way as in the case  $m$  even we see that such forms are classified by elements of  $D(\mathbb{Z}/m\mathbb{Z})$ , but since  $m$  is odd,  $D(\mathbb{Z}/m\mathbb{Z}) \simeq D(\mathbb{Z}/2m\mathbb{Z})$ , as one easily sees. In practice, we may assign to the form  $[\frac{1}{2}am^{-1}]$  with  $a$  even and  $0 < a < 2m$ , the class of  $a + m$  or  $a - m$  in  $D(\mathbb{Z}/2m\mathbb{Z})$ .  $\square$

Observe also that in case  $m$  is even  $(a + m)m^{-1} \cdot xy \equiv am^{-1} \cdot xy \pmod{\mathbb{Z}}$  and so the two torsion quadratic forms  $[\frac{1}{2}a \cdot m^{-1}]$  and  $[\frac{1}{2}(a + m) \cdot m^{-1}]$  on  $C_m$  have the same polar form  $\langle a \cdot m^{-1} \rangle$  but they may or may not be isometric:

**Examples 6.1.9. 1.**  $C_9$ . Units in this group are  $\{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$  and these form a cyclic group generated by  $\bar{2}$ . The non-zero squares are  $\bar{1}, \bar{4}, \bar{7}$  and  $\bar{2}, \bar{8}, \bar{5}$  are the non-squares. Therefore, there are two non-degenerate non-isometric symmetric forms:  $\langle \frac{1}{9} \rangle$  and  $\langle \frac{2}{9} \rangle$ . Next we turn to quadratic forms. The group  $D(\mathbb{Z}/18\mathbb{Z})$  is the cyclic group generated by  $\bar{5}$ , the class of 5 mod 18. The squares are  $\{\bar{1}, \bar{7}, \bar{13}\}$  and the non-squares  $\{\bar{5}, \bar{11}, \bar{17}\}$ . We find the two non-isometric quadratic forms  $[\frac{1}{9}]$  and  $[\frac{2}{9}]$ .

**2.**  $C_6$ . Consider the set  $\{1, 5\}$  of numbers coprime to 6, one a square and one a non-square. So there are two symmetric forms  $\langle \frac{1}{6} \rangle$  and  $\langle \frac{5}{6} \rangle$ . For the quadratic forms we consider the set  $\{1, 5, 7, 11\}$  of numbers coprime to 12. Since  $5^2 = 7^2 = 11^2 = 1$  and  $5 \cdot 7 = 11$  the group  $(\mathbb{Z}/12\mathbb{Z})^\times$  modulo squares is isomorphic to the product of two cyclic groups of order 2 and hence there are four non-degenerate non-isometric quadratic forms  $[\frac{a}{12}]$ ,  $a \in \{1, 5, 7, 11\}$ , while the polar forms for  $a = 1, 7$  as well as for  $a = 5, 11$  are the same and give the two non-isometric symmetric torsion forms on  $C_6$ .

We now pass to non-degenerate torsion forms on the groups  $C_m$ ,  $m = p^k$  a prime power. These have been enumerated in Example 1.9.5. Here we discuss the isometry problem. We have just seen that the symmetric forms on  $C_{p^k}$  are classified by  $D(\mathbb{Z}/p^k\mathbb{Z})$  and the quadratic forms by  $D(\mathbb{Z}/2p^k\mathbb{Z})$ . Recall (Lemma A.1.5) that for odd primes  $p$  the group  $D(\mathbb{Z}/2p^k\mathbb{Z}) \simeq D(\mathbb{Z}_{p^k}) \simeq D(\mathbb{Z}_p)$  is cyclic, generated by a non-square modulo  $p$ . The groups  $D(\mathbb{Z}/2^k\mathbb{Z})$  which enter the classification for  $p = 2$  can be viewed as subgroups of the multiplicative group  $(\mathbb{Z}/2^3\mathbb{Z})^\times$ : for  $k = 1$

Group	isometry classes of symmetric torsion forms	isometry classes of quadratic torsion forms
$C_{p^k}$ $p$ odd	$\langle p^{-k} \rangle, \langle u \cdot p^{-k} \rangle$ $u$ a non-square unit	$[\frac{1}{2}u \cdot p^{-k}]$ , $u$ an even square unit
		$[\frac{1}{2}u \cdot p^{-k}]$ , $u$ an even non-square unit
$C_2$	$\langle 2^{-1} \rangle$	$[2^{-2}]$ , $[3 \cdot 2^{-2}]$
$C_4$	$\langle 2^{-2} \rangle$ $\langle 3 \cdot 2^{-2} \rangle$	$[2^{-3}]$ , $[-3 \cdot 2^{-3}]$ $[3 \cdot 2^{-3}]$ , $[-1 \cdot 2^{-3}]$
$C_{2^k}$ , $k \geq 3$	$\langle u \cdot 2^{-k} \rangle$ , $u \equiv \pm 1, \pm 3 \pmod 8$	$[u \cdot 2^{-k-1}]$ , $u \equiv \pm 1, \pm 3 \pmod 8$

Table 6.1.1: Cyclic torsion forms of prime power order

the group consists of the class of 1, for  $k = 2$  one has the cyclic group  $\{\bar{1}, \bar{3}\}$ , and for  $k \geq 2$  one has the full multiplicative group of  $\mathbb{Z}/2^k\mathbb{Z}$ . Since  $D(\mathbb{Z}/2^k\mathbb{Z})$  and  $D(\mathbb{Z}/2^{k+1}\mathbb{Z})$  differ for  $k = 1, 2$ , some non-isometric quadratic forms have isometric polar forms as indicated in Table 6.1.1 by putting them in the same row.

## 6.2 The Correlation Morphism

An  $F$ -valued symmetric  $R$ -module  $(V, b)$  comes with a canonically associated morphism, the *correlation morphism* or *adjoint map*

$$V \xrightarrow{b_V} V_F^*, \quad x \mapsto b_V(x) = b(x, -). \quad (6.2)$$

The kernel of the adjoint map equals  $V^\perp$  and so, by definition,  $b$  is non-degenerate if and only if  $b_V$  is injective. If, moreover,  $b_V$  is an isomorphism, we say that  $(V, b)$  is *unimodular*. For a quadratic  $R$ -module  $(V, q)$  the correlation map  $b_V : V \rightarrow V_F^*$  is the one associated to the polar form of  $q$  and if it is injective, respectively bijective we speak of a non-degenerate, respectively unimodular quadratic  $R$ -module.<sup>2</sup>

*Remark. 1.* Observe also that unimodularity imposes a rather severe restriction on the possible  $R$ -modules  $F$  in which  $b$  takes values.

**2.** Starting from an  $F$ -valued symmetric  $R$ -module  $(V, b)$ , there is a canonical way to transport the structure to rings  $S$  that are  $R$ -algebras. Take for example  $R = \mathbb{Z}$  and  $S = \mathbb{R}$ . The correlation morphism for  $(V, b)_S = (V \otimes_R S, b \otimes 1)$  is the composition

$$V \otimes_R S \xrightarrow{b_V \otimes \text{id}} V_F^* \otimes S = \text{Hom}_R(V, F) \otimes_R S \xrightarrow{\alpha} \text{Hom}_S(V_S, F_S),$$

where the rightmost map is the natural map. In many cases, if  $b_V$  is an isomorphism, then so is  $b_{V_S} = \alpha \circ (b_V \otimes \text{id})$ , e.g. if  $F = R$  and  $V$  is a finitely generated free  $R$ -module. In particular, if  $V$  is a finitely generated free  $R$ -module and  $(V, b)$  is unimodular, then so is  $(V, b)_S$ .

<sup>2</sup>Several authors use a different terminology and speak of *regular symmetric or quadratic forms* instead of unimodular ones.

To investigate  $R$ -submodules  $W \subset V$ , we use a variant of the correlation morphism

$$\beta_W : V \rightarrow W_F^*, \quad x \mapsto b(x, -)|_W. \quad (6.3)$$

Note that the correlation morphism  $b_W : W \rightarrow W_F^*$  is just the restriction of  $\beta_W$  to  $W$  itself. It has the following properties.

**Lemma 6.2.1.** *Let  $V$  be an  $F$ -valued symmetric  $R$ -module of finite rank and  $W \subset V$  a submodule. Then*

1.  $\beta_W$  is injective on  $W$  if and only if  $b$  restricts to a non-degenerate form on  $W$ .
2. If  $\beta_W|_W$  is an isomorphism, that is,  $(W, b|_W)$  is a unimodular submodule, then  $V = W \oplus W^\perp$ . In other words, **unimodular submodules split off**.

*Proof.* 1. The kernel of  $\beta_W$  is precisely  $W^\perp$  and so  $b_W$ , its restriction to  $W$ , is injective if and only if  $W \cap W^\perp = \{0\}$ , which means that  $b$  restricts non-degenerately to  $W$ .

2. Since  $\beta_W|_W$  is surjective, for  $y \in V$ , the element  $\beta_W(y) \in W_F^*$  equals  $b_W(z)$  for some  $z \in W$ . But then  $b(y - z, x) = 0$  for all  $x \in W$  by the definition of  $\beta_W$ . This means that  $y - z \in W^\perp$  and, writing  $y = z + (y - z)$ , gives the required decomposition. Uniqueness follows from the injectivity of  $\beta_W|_W$   $\square$

### 6.3 Forms on Free $R$ -Modules

In this section  $L$  is a free  $R$ -module of finite rank.

**6.3.A General structure.** Recall that a free finite rank  $R$ -module equipped with a symmetric  $R$ -valued form is called an  $R$ -lattice. The special case  $R = \mathbb{Z}$  has been extensively considered in Section 1.2. Several results from that section, suitably modified, hold also over general rings. For instance, the choice of an ordered basis  $E = \{e_1, \dots, e_n\}$  for  $L \simeq R^n$  leads to the ***Gram matrix***

$$B_E = (b(e_i, e_j)) \in R^{n \times n}.$$

As we saw in Section 1.2, a change of basis multiplies the determinant of  $B_E$  by the square of a unit and hence we have the following invariant.

**Definition 6.3.1.** The ***discriminant***  $\text{disc}(b)$  of  $b$  is the value of  $\det(B_E)$  up to squares of units.

As an immediate consequence of the definitions we have:

**Proposition 6.3.2.** *Let  $(L, b)$  be an  $R$ -lattice. Then:*

1.  $b$  is non-degenerate if  $\text{disc}(b)$  is not a zero-divisor. It is unimodular if  $\text{disc}(b) \in D(R) = R^\times / (R^\times)^2$ .
2. For  $R = k$  a field,  $b$  is non-degenerate if and only if  $b$  is unimodular.

Note that rings  $R$  in which 2 is not invertible play a special role in relation to quadratic forms. For instance rank one lattices  $R \cdot x$  are never unimodular since  $b_q(x, x) = 2q(x)$  is not a unit. This is true for all odd rank quadratic  $R$ -lattices  $(L, q)$ . We see this as follows. Let, as before,  $\mathbf{E} = \{e_1, \dots, e_n\}$  be an ordered basis of  $L$  and write  $q(x) = \sum_{i \leq j} a_{ij} x_i x_j$ ,  $x = \sum x_i e_i$ . Using the upper triangular matrix  $Q = (a_{ij})$ , the Gram matrix of  $b_q$  in this basis is  $B := Q^\top + Q$ . Develop  $\det B$  as sum of  $n!$  terms of products of the entries of  $B$ . If such a term is invariant under reflection in the diagonal of  $B$ , it is a product containing at least one diagonal element, since  $n$  is odd. If such a term is not invariant under the reflection, it occurs twice. It follows that  $\det B = 2P$ , where  $P$  is a polynomial in the  $a_{ij}$  with integer coefficients and so  $\det B$  is never invertible. Instead,

$$\text{sdisc}(q) := P(a_{ij}) = P(q(e_1), b_q(e_1, e_2), \dots, b_q(e_{n-1}, e_n), q(e_n))$$

is well defined up to squares of units in  $R$  and might be invertible as we shall see. This leads to the following notion.

**Definition 6.3.3.** For a quadratic  $R$ -module  $(V, q)$  of odd rank over a ring  $R$  the *semi-discriminant* is the invariant  $\text{sdisc}(q) \in R/(R^\times)^2$ . The module  $(V, q)$  (or the form  $q$ ) is called *semi-unimodular* if the semi-discriminant is invertible, that is  $\text{sdisc}(q) \in D(R)$ . If 2 is invertible, then  $q$  is semi-unimodular if and only if it is unimodular.

**Examples 6.3.4.** Here we assume that  $2 \in R$  is not invertible.

1.  $n = 1$ . Here the bilinear form is never unimodular, but since  $\text{sdisc}(q) = a_{11} = q(e_1, e_1)$ , the form is semi-unimodular if and only if  $a_{11}$  is a unit.
2.  $n = 3$ . Expanding the determinant we find  $\text{sdisc}(q) = 4a_{11}a_{22}a_{23} + a_{12}a_{23}a_{13} - a_{13}^2a_{12} - a_{23}^2a_{11} - a_{12}^2a_{23}$ . In particular, if  $B$  is diagonal  $\text{sdisc}(q)$  is not invertible. This is evidently true for all odd  $n \geq 3$ , and so diagonal forms of odd rank  $\geq 3$  are not semi-unimodular.

*Remark 6.3.5.* An  $R$ -valued symmetric  $R$ -module  $(L, b)$  such that  $b$  is unimodular is also called an *inner product space* over  $R$ . Similarly, one speaks of a *quadratic inner product space* over  $R$ . In Chapter 1 we used this terminology for a field  $R$ , but in the literature it is often used when working over integral domains.

As before, we can speak of primitive sublattices. Observe however that for free modules over general commutative rings  $R$  the characterizations of Definition 1.2.4 valid for  $R = \mathbb{Z}$  do not all make sense, since  $R$  and hence  $L$  can have non-trivial zero-divisors. However, they remain valid for rings without zero-divisors. The following definition makes sense in general.

**Definition 6.3.6.** A sublattice  $S$  of  $L$  is called **primitive** if it is a direct summand of  $L$ . Equivalently: any basis of  $S$  can be extended to a basis of  $L$ . A vector  $x \in L$  is called primitive if  $Rx$  is a primitive sublattice of  $L$ .

Primitivity plays a crucial role in the next result.

**Lemma 6.3.7.** *Let  $(L, b)$  be a unimodular  $R$ -lattice.*

1. *For any basis  $\{e_1, \dots, e_n\}$  of  $L$  there exists a (unique) **b-dual basis**  $\{e_1^\#, \dots, e_n^\#\}$  for  $L$ , that is, a basis for which  $b(e_i, e_j^\#) = \delta_{ij}$ .*
2. *If  $S$  is a primitive submodule of  $L$  and  $\{e_1, \dots, e_n\}$  a basis of  $L$  such that the first  $m$  vectors  $\{e_1, \dots, e_m\}$  form a basis of  $S$ , then  $\{e_{m+1}^\#, \dots, e_n^\#\}$  is a basis of  $S^\perp$ . In particular,  $(S^\perp)^\perp = S$ .*
3. *Let  $Rx \subset L$  be primitive. Then there exists a vector  $y \in L$  for which  $b(x, y) = 1$ .*

*Proof.* 1. Write  $x \in L$  as  $x = \sum_{i=1}^n x_i e_i$ . Since the correlation morphism is an isomorphism, the coordinate function  $x \mapsto x_j$  can be written as  $x \mapsto b(x, e_j^\#)$  for some vector  $e_j^\# \in L$ , and hence  $b(e_i, e_j^\#) = \delta_{ij}$ . Now write  $e_j^\# = \sum_k a_{jk} e_k$  and  $b(e_k, e_\ell) = b_{k\ell}$ . Then  $\delta_{j\ell} = b(e_j^\#, e_\ell) = \sum_k a_{jk} b_{k\ell}$  which implies that the matrix  $(a_{jk})$  is the inverse of the matrix  $(b_{k\ell})$ . Since  $e_j = \sum b_{j\ell} e_\ell^\#$ , the set  $\{e_1^\#, \dots, e_n^\#\}$  is a basis.

2. This is evidently the case.

3. Just augment  $x = e_1$  to a basis  $\{e_1, \dots, e_n\}$  for  $L$  and take for  $y$  the vector  $e_1^\#$ .  $\square$

We use the last property of Lemma 6.3.7 to show a remarkable characterization of the hyperbolic plane  $U_R$ , that is, the rank two lattice with basis  $\{e, f\}$  and with  $e \cdot e = f \cdot f = 0$  and  $e \cdot f = 1$ .

**Lemma 6.3.8.** *Let  $R$  be a ring in which 2 is invertible. The hyperbolic plane  $U_R$  over  $R$  represents all elements of  $R$ . A unimodular quadratic  $R$ -module  $(L, q)$  represents 0 if and only if  $L$  splits off a hyperbolic plane.*

*Proof.* For any  $a \in R$  we have  $e + \frac{1}{2}af \cdot e + \frac{1}{2}af = a$ . Here we use that 2 is invertible.

To show the second assertion, observe that if  $x \in L$  is primitive, by Lemma 6.3.7 there exists a vector  $y \in L$  with  $b_q(x, y) = 1$ . Then, if moreover  $x$  is isotropic,  $z = y - q(y)x$  is isotropic and  $b_q(x, z) = 1$  so that  $\{x, z\}$  spans a hyperbolic plane. By Lemma 6.2.1 we may split off  $U_R$ . Conversely, if  $U_R$  is an  $R$ -submodule of  $L$  (necessarily an orthogonal direct summand), it represents 0 and so  $L$  represents 0.  $\square$

### 6.3.B Examples.

1. Proposition 6.3.2 implies that for symmetric  $\mathbb{Z}$ -lattices the notions of non-degeneracy and unimodularity agree with those from Section 1.2.

2. A rank 1 integral or dyadic quadratic lattice is never unimodular since the corresponding bilinear form is even and so has even discriminant.
3. A canonical incarnation of the hyperbolic plane  $U_R$  is the module  $R \oplus R^*$  equipped with the symmetric form given by  $((x, f), (y, g)) \mapsto f(y) + g(x)$ .
4. Consider the lattices  $V_k$  from Examples 1.9.5. The dyadic lattice  $V_0$  is unimodular since it has discriminant 3 which is a unit in  $\mathbb{Z}_2$ . However, for  $k \geq 1$  the lattice  $V_k$  is non-degenerate but not unimodular.
5. **Binary forms.** Let  $R$  be an integral domain,  $k = Q(R)$  its quotient field and  $S = R[\xi]$  a degree 2 separable extension of  $R$  with minimal polynomial  $X^2 + uX + v$ ,  $u, v \in R$ , for  $\xi$ , i.e.  $\xi$  is integral over  $R$ . The quotient field of  $S$  is the field  $K = k(\xi)$ . Now  $\xi' = -u - \xi$  is the conjugate of  $\xi$  and the norm map  $N_{K/k} : K \rightarrow k$  given by  $N_{K/k}(x + y\xi) = (x + y\xi)(x + y\xi')$  induces a quadratic form  $N_{S/R}$  on  $R \oplus R$ , the **norm form**. Explicitly, in the basis  $\{1, \xi\}$  of  $S/R$  we have

$$N_{S/R}(x + y\xi) = x^2 - uxy + vy^2 \in R.$$

The associated bilinear form is the **trace form**

$$\text{Tr}_{S/R}([x + y\xi] \cdot [x' + y'\xi']) = 2xx' - u[yx' + xy'] + 2yy'v$$

with Gram matrix  $\begin{pmatrix} 2 & -u \\ -u & 2v \end{pmatrix}$ . Its determinant  $4v - u^2$  is a non-square since the extension  $K/k$  is a separable degree 2 extension and, hence, the trace form is non-degenerate. Note that all *unital* binary quadratic forms over  $R$  with non-square discriminant are isometric to a norm form for some quadratic extension  $S = R[\xi]$  with quotient field  $K$ . Indeed,  $q(x, y) = x^2 + bxy + cy^2$  is isometric to  $N_{K/k}(x + y\xi)$  with  $\xi^2 - b\xi + c = 0$ . More generally, a form  $ax^2 + bxy + cy^2$  with non-square discriminant is isometric to a norm form up to scale. Otherwise, if the discriminant is a non-zero square, say  $b^2 - 4ac = \delta^2$ , then  $a(x - \delta y)(x + \delta y)$  shows that the form is isometric to the hyperbolic  $R$ -plane up to scaling.

The binary forms  $V_k$  over  $\mathbb{Z}_2$  are examples of scaled norm forms; the quadratic forms are given by  $2^k(x^2 + xy + y^2)$  associated to the quadratic extension  $\mathbb{Z}_2[\xi]$  of  $\mathbb{Z}_2$  with minimal polynomial  $X^2 - X + 1$ . We show (cf. Proposition 10.2.2) that  $V_k$  and  $U_k$  are the only binary dyadic lattices.

Let us tie this in with the discussion of quadratic forms over fields  $k$ . We have seen (cf. Proposition 1.1.4) that if  $\text{char}(k) \neq 2$  a quadratic form diagonalizes and so a non-degenerate binary form has the shape  $ax^2 + cy^2$  with  $ac \neq 0$ . Such a form has an isotropic vector if and only if  $-c/a$  is a square in  $k$ . Then the form is isometric to  $U$ . If not, the polynomial  $x^2 + c/a \cdot y^2$  is irreducible and defines a quadratic extension and so, up to isometry, the form  $ax^2 + cy^2$  equals  $a \cdot N_{K/k}(x + \sqrt{-c/a} \cdot y)$ . We set this apart:

**Lemma 6.3.9.** *A quadratic binary form  $q(x, y) = ax^2 + cy^2$  over a field of characteristic different from 2 is a norm form if and only if  $-c/a$  is not a square. If  $-c/a$  is a square, then  $q$  is isometric to the hyperbolic plane.*



There is a variant of this argument which is also valid for *perfect* fields  $k$  of characteristic 2. Consider the form  $q(x, y) = ax^2 + bxy + cy^2$ . If  $a = c = 0$  then, since  $b$  is a square ( $k$  is perfect!) we have  $U(b) \simeq U$  and otherwise we may assume that  $a \neq 0$  and then we decompose the form in the algebraic closure as  $a(x - uy)(x - u'y)$ . In case  $u, u' \in k$ , changing variables we get  $ax(x - u''y)$  for some  $u'' \in k$ , and since  $u'' \neq 0$  (we assume that the form is non-degenerate), making another change of variables we see that the form is isometric to  $U(a) \simeq U$ . Otherwise  $u, u'$  are conjugate in a quadratic extension  $K/k$  and  $q$  is isometric to the norm form of the extension.

- 6. Lattices over local rings and their residue fields** Let  $(R, \mathfrak{m})$  be a local ring with residue field  $k = R/\mathfrak{m}$  and  $(L, b)$  be an  $R$ -valued symmetric  $R$ -module. The form  $b$  induces a  $k$ -valued symmetric form  $b_k$  on the  $k$  vector space  $L/\mathfrak{m}L = L \otimes_R k$  upon setting  $b_k(x \bmod \mathfrak{m}, y \bmod \mathfrak{m}) = b(x, y) \bmod \mathfrak{m}$ . Note that  $\text{disc}(b_k) = \text{disc}(b) \bmod \mathfrak{m}$ , and so  $b$  is non-degenerate if  $b_k$  is. The converse need not be true as exemplified by the forms  $\langle p^k \rangle$ ,  $k \geq 2$ , on  $\mathbb{Z}_p$ . However, since  $R^\times = R - \mathfrak{m}$ ,  $b$  is unimodular if and only if this is the case for  $b_k$ .

**6.3.C Splitting off units.** Let us now make use of the concept of discriminant to draw some conclusions from Lemma 6.2.1 in the present situation where  $b$  is assumed to be an  $R$ -valued form. Suppose that  $W \subset L$  is generated by a single element  $v$ , that is,  $W$  is free of rank 1. Note that for  $x \in R^\times$  the  $R$ -homomorphism which sends  $y$  to  $xy$  establishes isomorphisms  $R \simeq R^*$  and  $W \simeq W^*$ . Using this,  $b_L|_W : W \rightarrow W^* \simeq W$  becomes multiplication with  $b(v, v)$ . So, if  $b(v, v)$  is a unit, this morphism is an isomorphism. Then Lemma 6.2.1.2 implies the following splitting phenomenon.

**Proposition 6.3.10** (Splitting off units). *Let  $(L, b)$  be an  $R$ -valued symmetric form,  $v \in L$ , such that  $b(v, v) = u$ , a unit in  $R$ . Then  $L = Rv \oplus (Rv)^\perp \simeq \langle u \rangle \oplus (Rv)^\perp$ . Consequently, there exists an orthogonal splitting*

$$L \simeq \langle u_1 \rangle \oplus \cdots \oplus \langle u_s \rangle \oplus N,$$

where  $u_1, \dots, u_s$  are units in  $R$ , and  $b(x, x)$  is a non-unit for every  $x \in N$ .

The following consequence concerns diagonalizable forms over local rings.

**Proposition 6.3.11** (Splitting over local rings). *Let  $R$  be a local ring in which 2 is a unit and let  $(L, b)$  be a unimodular form on a free  $R$ -module of finite rank. Then  $b$  is diagonalizable.*

*Proof.* Proposition 6.3.10 states that, if the bilinear form  $b$  is not diagonalizable, there is an orthogonal summand  $N$  on which the values  $b(x, x)$ ,  $x \in N$ , are non-units. We want to show that this summand is zero. If  $R$  is local with maximal ideal  $\mathfrak{m}$ , the set of non-units is  $\mathfrak{m}$ . So  $b(x, x) \in \mathfrak{m}$  for  $x \in N$ . Since  $2b(x, y) = b(x + y, x + y) - b(x, x) - b(y, y)$ , the assumption  $2 \in R^\times$  implies then that the restriction of  $b$  to  $N$  takes values in  $\mathfrak{m}$  and so does the discriminant  $\text{disc}(b|_N)$ . But  $b$  and hence  $b|_N$  is unimodular, that is,  $\text{disc}(b|_N) \in R^\times = R - \mathfrak{m}$  if  $N \neq 0$ . It follows that  $N = 0$ .  $\square$

**6.3.D Hyperbolic modules.** Hyperbolic planes form a special case of a more general structure, that of a *hyperbolic  $R$ -module*  $U_L$  associated to any free  $R$ -module  $L$  of finite rank:

$$U_L = (L \oplus L^*, u_L), \quad u_L : (L \oplus L^*) \times (L \oplus L^*) \longrightarrow R \quad (6.4)$$

$$((x, f), (y, g)) \mapsto f(y) + g(x).$$

The *hyperbolic form*  $u_L$  equips  $L \oplus L^*$  with a natural structure of a unimodular symmetric  $R$ -lattice without assuming the presence of a bilinear form on  $L$ . To see that the symmetric form  $u_L$  is unimodular, let  $\{e_1, \dots, e_m\}$  be a basis for  $L$  and let  $\{e_1^*, \dots, e_m^*\}$  be the dual basis for  $L^*$ . Then the matrix for  $u_L$  with respect to the ordered basis  $\{e_1, \dots, e_m, e_1^*, \dots, e_m^*\}$  is the matrix

$$J := \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

and so has determinant  $\pm 1$ . The form  $u_L$  is the polar form of the quadratic form  $q_L$  given by  $q_L(x, f) = f(x)$ . Consequently,  $(U_L, q_L)$  stands for this quadratic lattice.

There is a variant of the above construction which presumes the existence of a quadratic form  $q$  on  $L$ , namely the *quadratic hyperbolic  $R$ -module*  $U_{L,q}$ , given by  $L \oplus L^*$  equipped with the quadratic form

$$(x, f) \in L \oplus L^* \mapsto u_q(x, f) = q(x) + f(x). \quad (6.5)$$

The form  $u_q$  is indeed unimodular since the Gram matrix for  $b_{u_q} = b_q + u_L$  with respect to the ordered basis  $\{e_1, \dots, e_m, e_1^*, \dots, e_m^*\}$  is the matrix

$$B = \begin{pmatrix} A & I \\ I & 0 \end{pmatrix},$$

where  $A$  is the Gram matrix of  $b_q$  with respect to  $\{e_1, \dots, e_m\}$ , and we have  $\det B = \pm 1$ . The  $R$ -module  $U_{L,q}$  splits non-orthogonally into two summands  $L$  and  $L^*$  and  $L^*$  is isotropic, but this need not be the case for  $L$ .

Note that in case 2 is a unit in  $R$ , the quadratic lattices  $(U_L, q_L)$  and  $U_{L,q}$  are isometric under the linear isomorphism  $(x, f) \mapsto (x, f - \frac{1}{2}b_q(x, -))$  since  $\frac{1}{2}b_q(x, x) = q(x)$ . In terms of standard bases, this isomorphism is given by the matrix  $C := \begin{pmatrix} I & 0 \\ -\frac{1}{2}A & I \end{pmatrix}$  and that it is an isometry follows from  $C^T B C = J$ . Hyperbolic modules give certain natural lattice embeddings (cf. Section 1.8):

**Proposition 6.3.12** (Embedding in hyperbolic modules). *Let  $L$  be a free  $R$ -module of finite rank  $m$  endowed with a non-degenerate  $R$ -valued quadratic form  $q$ .*

1. *The embedding  $j : L \rightarrow L \oplus L^*$ ,  $j(x) = (x, 0)$  induces an isometric embedding from  $(L, q)$  into  $U_{L,q}$  such that  $j(L)^\perp \simeq L(-1)$ .*
2. *If  $L$  is unimodular, then  $U_{L,q} = j(L) \oplus j(L)^\perp \simeq L \oplus L(-1)$ .*

*Proof.* 1. The embedding  $j$  is an isometric embedding since  $u_q(x, 0) = q(x)$ . We next show that the orthogonal complement is isometric to  $L(-1)$ . By definition, for  $(y, g)$  to be orthogonal to  $L \oplus 0$  is equivalent to  $g(x) + b_q(x, y) = 0$  for all  $x \in L$  and conversely, which means  $g = -b_L(y)$  and then  $y \mapsto (y, -b_L(y))$  is an isomorphism of modules from  $L$  to  $j(L)^\perp$ . For the forms we have

$$u_q(y, -b_L(y)) = q(y) - b_L(y)y = q(y) - b(y, y) = -q(y)$$

proving that  $j(L)^\perp \simeq L(-1)$ .

2. This follows since unimodular summands split off by Lemma 6.2.1.  $\square$

## 6.4 Discriminant Forms

In this section  $F = R$  is an integral domain,  $Q(R)$  its field of fractions,  $(L, b)$  is an  $R$ -lattice and  $(L, q)$  a quadratic lattice. .

Recall that the correlation morphism (6.2) for a non-degenerate symmetric  $R$ -lattice  $(L, b)$  is the injective homomorphism

$$b_L : L \rightarrow L^*, \quad x \mapsto b_L(x) \text{ (=the function sending } y \text{ to } b(x, y)).$$

In general it is not surjective and the quotient,  $\text{dg}_L := L^*/L$ , is by Remark 6.1.7 a torsion  $R$ -module, the **discriminant torsion module**. Since  $R \subset Q(R)$  we may extend scalars to  $Q(R)$  and then the correlation morphism becomes a  $Q(R)$ -isomorphism  $L_{Q(R)} \xrightarrow{\sim} L_{Q(R)}^*$ . The bilinear extension  $b_{Q(R)}$  can be transported to  $L_{Q(R)}^*$  via this isomorphism. Hence every element of  $L_{Q(R)}^*$  is of the form  $x \mapsto b_{Q(R)}(y, x)$  for some  $y \in L_{Q(R)}$ . This gives an explicit identification of  $L_{Q(R)}$  with its dual. The same proof as the one for Lemma 1.6.3 can be used to show:

**Lemma 6.4.1.** 1. Under the above identification of  $L_{Q(R)}$  with  $L_{Q(R)}^*$  we have

$$L^* = \{y \in L_{Q(R)} \mid b_{Q(R)}(y, x) \in R \text{ for all } x \in L\}.$$

2. If  $A = B_E$  is the Gram matrix of  $b$  with respect to the basis  $E = \{e_1, \dots, e_n\}$ , then  $A^{-1}$  is the Gram matrix of  $b_{Q(R)}$  with respect to the dual basis  $E^*$ . This is also the matrix expressing the basis  $E^*$  of  $L_{Q(R)}^* = L_{Q(R)}$  in the basis  $E$ .

3. There is a canonical identification  $L = (L^*)^*$  induced by  $b_{Q(R)}^* \circ b_{Q(R)}$ .

The form  $b_{Q(R)}$  induces a bilinear form on  $\text{dg}_L$ , the **discriminant bilinear form**. Explicitly, with the notation  $\bar{x} = x \bmod L \in L^*/L$ , we set

$$\begin{aligned} b_L^\# : \text{dg}_L \times \text{dg}_L &\longrightarrow Q(R)/R, \\ (\bar{x}, \bar{y}) &\longmapsto b_{Q(R)}(x, y) \bmod R. \end{aligned}$$

For a non-degenerate quadratic  $R$ -lattice  $(L, q)$  we use the associated bilinear form  $b_q$  to embed  $L^*$  in  $L_{Q(R)}$ . The *discriminant quadratic form* is the torsion quadratic form

$$\begin{aligned} q_L^\# : \mathfrak{d}g_L &\longrightarrow Q(R)/R \\ \bar{x} &\longmapsto q_{Q(R)}(x) \bmod R. \end{aligned}$$

As for integral forms, the discriminant bilinear form of a non-degenerate form is also non-degenerate. Indeed, if  $b_{Q(R)}(x, L^*) \in R$  for some  $x \in L^*$ , then  $x \in L^{**} = L$  and so  $\bar{x} = 0$ .

## 6.5 Isometry Groups

In this section we continue to assume that  $F = R$  is an integral domain,  $Q(R)$  its field of fractions,  $(L, b)$  a symmetric  $R$ -lattice and  $(L, q)$  a quadratic lattice.

Recalling the notions of Definition 6.1.4, in this situation the orthogonal group of  $(L, b)$  is given by

$$\mathcal{O}(L) = \mathcal{O}(b) := \{\varphi : L \rightarrow L \text{ an } R\text{-linear bijection} \mid b(\varphi(x), \varphi(y)) = b(x, y), \forall x, y \in L\}.$$

If  $(L, q)$  is a quadratic lattice, by  $\mathcal{O}(L)$  we shall mean  $\mathcal{O}(b_q)$ . Occasionally we shall also use

$$\mathcal{O}(q) := \{\varphi : L \rightarrow L \text{ an } R\text{-linear bijection} \mid q(\varphi(x)) = q(x), \forall x \in L\}.$$

Clearly, if  $\varphi$  preserves  $q$ , then it preserves  $b_q$ . In other words,  $\mathcal{O}(q) \subset \mathcal{O}(b_q)$ . We have seen (cf. the discussion just below Definition 6.1.2) that, in case 2 is not a zero-divisor, an even bilinear form  $b$  determines a unique quadratic form  $q$  of which it is the polar form. Since  $R$  is an integral domain, if  $2 \neq 0$ , then  $\mathcal{O}(q) = \mathcal{O}(b_q)$ . However, if  $2 = 0$ , this need not be the case.

**Example 6.5.1.** Consider a non-degenerate quadratic form  $q$  on a vector space  $V$  over a field of characteristic 2 such that  $q$  has an isotropic vector, e.g. if  $q$  is an orthogonal direct sum of hyperbolic planes. The so-called symplectic transvection  $t(x) = x + b_q(u, x)u$ ,  $u \in V$  isotropic, preserves  $b_q$  as one directly checks. However, since we are in characteristic two,  $q(t(x)) = q(x) + b_q(u, x)^2$  and so  $t \notin \mathcal{O}(q)$ . The simplest such example is the hyperbolic plane  $U_{\mathbb{F}_2}$  over  $\mathbb{F}_2$ . Then  $\mathcal{O}(U_{\mathbb{F}_2})$  consists of the six transformations  $\text{id}$ ,  $t := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ,  $s := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ ,  $s^2$ ,  $st = ts^2$  and  $st^2 = ts$ , while  $\mathcal{O}(q) = \{\text{id}, t\}$ .

There is a criterion for an  $R$ -module isomorphism  $\varphi$  of (the non-degenerate)  $L$  to be an isometry which is similar to the one we gave in Section 1.5 for integral lattices. Explicitly, if  $\mathbf{E} = \{e_1, \dots, e_n\}$  is a basis for  $L$ ,  $F$ , and  $B_{\mathbf{E}} = (b(e_i, e_j))$  the

matrix of  $\varphi$ , respectively the Gram matrix of  $b$  with respect to  $\mathbf{E}$ , then  $\varphi$  is an isometry if and only if  $F^\top B_{\mathbf{E}} F = B_{\mathbf{E}}$ . In the case of an isometry  $\det^2(F) = 1$  and so  $\det(F) = \pm 1$ . Since  $\det(\varphi) = \det(F)$  does not depend on the choice of basis we deduce that  $\det(\varphi) = \pm 1$ . If  $2 = 0$  in the ring  $R$ , all isometries have determinant 1. Otherwise, those isometries  $\varphi$  for which  $\det(\varphi) = 1$  are called *rotations* and these form a normal subgroup:

**Definition 6.5.2.** Suppose  $2 \neq 0$  in  $R$ . The *special orthogonal group* (or the *group of rotations* of  $L$ ) is the group  $\text{SO}(L) = \{g \in \text{O}(L) \mid \det(\varphi) = 1\}$ , a normal subgroup of  $\text{O}(L)$  of index at most 2. An isometry  $\varphi$  with  $\det \varphi = -1$  will be called a *reflection*.

**Example 6.5.3.** As in (1.4), a non-isotropic vector  $x$  in an  $R$ -lattice  $L$  for which

$$2b(x, L) \subset b(x, x)R, \quad (6.6)$$

determines an isometry

$$\sigma_x(y) = y - 2 \frac{b(x, y)}{b(x, x)} \cdot x$$

with  $\det(\sigma_x) = -1$ , the *hyperplane reflection defined by  $x$* . It is the identity on the hyperplane orthogonal to  $x$  and sends  $x$  to  $-x$

If we have a quadratic lattice  $(L, q)$  and an element  $x \in L$  satisfying the above condition with respect to  $b_q$ , we find that the reflection in  $x$  is given by

$$\sigma_x(y) = y - \frac{b_q(x, y)}{q(x)} x. \quad (6.7)$$

Observe that for all non-zero  $r \in R$  we have  $\sigma_x = \sigma_{rx}$  and so we may assume that  $x$  is primitive. In this situation we have a hyperplane reflection if for instance  $q(x)$  is a unit.

Primitivity of  $x$  also ensures that there is a basis  $e_1 = x, e_2, \dots, e_n$  of  $L$ . Then the matrix of  $\sigma_x$  in this basis is

$$\begin{pmatrix} -1 & * & \cdots & * \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

and so  $\det(\sigma_x) = -1$  as claimed.

*Remark 6.5.4. 1.* One can define the determinant for an isometry with values in any commutative ring  $A$ . However, if  $A$  has zero-divisors, this is a less useful concept, especially if all elements are zero-divisors since then  $1 = 0$ . This applies for example to the ring  $Q(R)/R$  and hence to  $R$ -torsion modules.

*2.* There are lattices  $(L, b)$  that do not admit reflections, i.e., for which  $\text{O}(L) = \text{SO}(L)$ . See Example 6.5.5.4 below.

An isometry  $\varphi$  of  $L$  induces an isometry  $\varphi_{Q(R)}$  of  $L_{Q(R)}$  preserving  $L^* \subset L_{Q(R)}$ . Hence there is an induced isomorphism  $\bar{\varphi}$  of the discriminant group  $L^*/L$  which preserves the discriminant form. Isomorphisms of  $L^*/L$  preserving  $b_L^\#$  form the group  $O(b_L^\#)$ . The assignment  $\varphi \mapsto \bar{\varphi}$  defines the so called **reduction homomorphisms**

$$r_L^b : O(L, b) \longrightarrow O(b_L^\#), \quad (r_L^b)' = r_L | SO(L, b). \quad (6.8)$$

If  $b = b_q$  is an even non-degenerate polar form of the quadratic form  $q$ ,  $\varphi$  also preserves the discriminant quadratic form  $q_L^\#$  on  $L^*/L$  and the reduction morphism factors as

$$r_L^b : O(L, b_q) \xrightarrow{r_L^q} O(q_L^\#) \hookrightarrow O(b_L^\#). \quad (6.9)$$

The reduction homomorphisms are in general injective nor surjective. Note that the group  $O(q_L^\#)$  might be a proper subgroup of  $O(b_L^\#)$  and if this is the case  $r_L^b$  is not surjective, but  $r_L^q$  might be surjective.

As in the case of integral lattices (cf. Lemma 1.5.4), an  $R$ -lattice  $L$  has the same isometry group as  $L(r)$ ,  $r \in R - \{0\}$ . This is a useful remark for calculating isometry groups in examples as illustrated below.

**Examples 6.5.5. 1. Rank one lattices.** The isometry group of  $\langle a \rangle$ ,  $a \in R - \{0\}$ , is the kernel  $R_{[2]}^\times$  of the squaring map on  $R^\times$ . If  $(R, \mathfrak{m})$  is a local ring with 2 a unit, this group only consists of  $\pm 1$ , as we shall see in Remark 7.2.2.

The isometry group of the discriminant bilinear form  $\langle a^{-1} \rangle$  is the kernel  $(R/aR)_{[2]}^\times$  of the squaring map on  $(R/aR)^\times$ . Indeed, in the latter case an isometry is given by an invertible element  $\xi \in a^{-1}R/R$  such that  $a^{-1}\xi^2xy - a^{-1}xy = 0$  in  $a^{-1}R/R$  for all  $x, y \in a^{-1}R$ , which is equivalent to  $\xi^2 - 1 = 0$  in  $R/aR$ . The reduction homomorphism is the quotient morphism  $R_{[2]}^\times \rightarrow (R/aR)_{[2]}^\times$ .

We turn now to the quadratic form  $[\frac{1}{2}a]$ ,  $a \in 2R$ , which, we recall, is given by  $x \mapsto \frac{1}{2}ax^2$  and has  $\langle a \rangle$  as its polar form. One has  $O([\frac{1}{2}a]) = O(\langle a \rangle) = R_{[2]}^\times$ . The isometry group of its discriminant quadratic form  $[\frac{1}{2}a^{-1}]$  is the same as for its polar form. Indeed,  $\frac{1}{2}a^{-1}\xi^2x^2 - \frac{1}{2}a^{-1}x^2 = 0$  in  $a^{-1}R/R$  for all  $x \in a^{-1}R/R$  is equivalent to  $\xi^2 - 1 = 0$  in  $2a^{-1}R/2R \simeq R/aR$ .

Consider for example  $R = \mathbb{Z}$  and  $a = 2^k$ ,  $k \geq 1$ . Then  $O(\langle 2^{-k} \rangle)$  is the identity for  $k = 1$ , the cyclic group generated by  $-id$  for  $k = 2$ , and the Klein 4-group  $C_2 \times C_2$  generated by  $-id$  and multiplication by  $-1 + 2^{k-1} \pmod{2^k}$  for all  $k \geq 3$  (since its square is 1 in  $\mathbb{Z}/2^k\mathbb{Z}$ ). Since the isometry group of rank one integral lattices consists of  $\pm id$ , we see that the reduction homomorphism (for the symmetric as well as the quadratic form) is not surjective if  $k \geq 3$ .

If instead  $R = \mathbb{Z}_2$ , the group  $R_{[2]}^\times$  is isomorphic to  $C_2 \times C_2$ , since the units up to squares are represented by  $\pm 1, \pm 3$ , each with square 1. The preceding calculation for the isometry groups of the discriminant forms for  $R = \mathbb{Z}$  is also valid for  $R = \mathbb{Z}_2$ . So in this case the reduction morphisms are surjective.

## 2. Binary forms.

(a) We first consider the **hyperbolic plane**  $U_R = Re \oplus Rf$ ,  $e \cdot e = f \cdot f = 0$ ,  $e \cdot f = 1$ .

Assume  $2 \neq 0$ . Up to units  $e$  and  $f$  are the only primitive isotropic vectors. Since these are preserved under isometries, the only isometries are the rotations  $i_a := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ ,  $a \in R^\times$ , and the reflections  $j_b := \begin{pmatrix} 0 & b^{-1} \\ b & 0 \end{pmatrix}$ ,  $b \in R^\times$ . Observe that  $j_b$  is the hyperplane reflection in  $e - bf$ . Since  $j_1 \circ j_a = i_a$ , all isometries of  $U_R$  are products of at most two hyperplane reflections. Note that these isometries are also the isometries for the corresponding quadratic form.

In case  $2 = 0$ , also the vector  $e + f$  is a primitive isotropic vector and as we saw in Example 6.5.1, this gives an isometry of the bilinear form but not of the quadratic form. Indeed, if  $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$  represents an isometry with respect to the quadratic form, then  $(a_{11}x + a_{12}y)(a_{21}x + a_{22}y) = xy$ . This implies  $a_{11}a_{21} = a_{12}a_{22} = 0$  and  $a_{11}a_{22} + a_{12}a_{21} = 1$  so that the only isometries preserving the quadratic form are just the  $j_a$  and the  $i_b$  for suitable units  $a, b$ .

For a non-zero  $s$  which is not a unit, the lattice  $U_R(s)$  is not unimodular and its discriminant torsion module  $[s^{-1}R/R]^{\oplus 2}$  inherits the hyperbolic form. Its isometry group consists of the isometries  $i_{\bar{a}}$  and  $j_{\bar{b}}$  where now  $\bar{a}, \bar{b} \in (R/sR)^\times$ . Hence the reduction homomorphism  $r_{U_R(s)}^q$  is surjective.

(b) Next, we return to the situation (see Section 6.3.B) where  $k = Q(R)$ ,  $K = Q(S)$ ,  $S = R[\xi]$ , a quadratic extension with  $\xi^2 + u\xi + v = 0$ , and associated quadratic form  $N_{K/k}(x + y\xi) = x^2 - uxy + vy^2$  on  $K$  (i.e.,  $x^2 - uxy + vy^2$  on  $\oplus^2 k$ , where  $(x, y)$  is identified with  $x + y\xi$ ).

(b1) Determining the **rotations** in case  $2 \neq 0$ . Multiplication with any  $U \in S$  with  $N_{K/k}(U) = 1$  induces a  $k$ -linear map from  $K$  to  $K$  that preserves the quadratic form since  $N_{K/k}$  is multiplicative. The matrix of multiplication by  $U = a + b\xi$ ,  $a, b \in R$ , in the basis  $\{1, \xi\}$  is given by

$$M_{a,b} = \begin{pmatrix} a & -bv \\ b & a - ub \end{pmatrix}.$$

Since  $\det(M_{a,b}) = a^2 - uab + vb^2 = N_{K/k}(U) = 1$ , this is a rotation. We claim that all rotations occur this way. Let  $\rho$  be any rotation and let  $\rho(1) = a \cdot 1 + b\xi$ . Then  $N_{K/k}(a + b\xi) = 1$  and  $\rho^{-1} \cdot M_{a,b}(1) = 1$ . A small matrix computation shows that the only rotation which fixes 1 is the identity. It follows that  $\rho = M_{a,b}$ .

(b2) On **reflections** in case  $2 \neq 0$ . The reflection in  $a - 1 + b\xi$  with  $N_{K/k}(a + b\xi) = a^2 - uab + vb^2 = 1$  has matrix

$$M'_{a,b} = \begin{pmatrix} a & -ua + vb \\ b & -a \end{pmatrix}.$$

As in the case of rotations, any orthogonal transformation with determinant  $-1$  is of this shape. Observe also that  $M'_{a,b} \circ M'_{1,0} = M_{a,b}$ , and so all isometries are products of at most two reflections.

(b3) **The case**  $2 = 0$ . We still have the preceding two types of orthogonal transformations despite both having determinant 1. The first type  $M_{a,b}$  comes from multiplication with norm 1 elements. However, a matrix for a reflection cannot come from multiplication with norm 1 vectors, since if this were the case, we would

have  $ub = 0 = ua$  and so  $u = 0$  but then the extension  $R(\xi)/R$  would not be separable. We shall see later (cf. Example 16.2.5.3) that in this case the two types of orthogonal transformations are distinguished by their Dickson invariants.

**3.** The form  $V$  over  $\mathbb{Z}_2$ , that is, the norm form for the extension  $\mathbb{Z}_2[\xi]$  with  $\xi^2 + \xi + 1 = 0$ . Hence we can apply the calculation in § 6.3.B, example 4: The rotation group of  $V$  (and so of  $V_k$ ) consists of matrices of the form  $\begin{pmatrix} a & -b \\ b & a-b \end{pmatrix}$  and those with determinant equal to  $-1$  are given by  $\begin{pmatrix} a & -a+b \\ b & -a \end{pmatrix}$ . Since  $a^2 - ab + b^2 = 1$  either  $a$  or  $b$  must be a dyadic unit. As in the previous example  $O(q_{V_k}^\#)$  is of similar shape where one replaces  $a, b$  by residue classes of integers modulo  $2^k$  with  $a^2 - ab + b^2 \equiv 1 \pmod{2^k}$ . In particular, the reduction homomorphism  $r_{V_k}^q$  is surjective.

**4.** Consider the quadratic form  $q(x, y) = ax^2 + 2xy + cy^2$  on  $\mathbb{Z}^2$  with  $a, c \in \mathbb{Z}$  and  $a \geq 2$  and  $c > a$ . The only integral solution for  $q(x, y) = a$  is  $(x, y) = (\pm 1, 0)$ . Indeed, writing

$$q(x, y) = a(x + a^{-1}y)^2 + (c - a^{-1})y^2,$$

and observing that  $c - a^{-1} > a$ , one sees that if  $|y| \geq 1$ , there is no solution, and if  $y = 0$ , then  $x = \pm 1$ . Hence, an isometry of  $q(x, y)$  must preserve the first basis vector up to sign. Then the matrix representing the isometry is of the shape  $\begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix}$  and a small calculation shows that if  $a > 2$  such an isometry can only be  $\pm \text{id}$  and  $q$  does not admit reflections. However, for  $a = 2$  there are two reflections,  $\pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ .

**Historical and Bibliographical Notes.** Our formulation of the "splitting principle" is motivated by [122, Satz (1.6)] in M. Kneser's book. The material in Sections 6.1 and 6.3 is based on M. Kneser's approach (loc. cit.) as well as on §I.3 in the book [151] by J. Milnor and D. Husemoller. Note that they use the terminology "of type I, II" for odd, respectively even forms.

The properties of torsion bilinear and quadratic forms over general rings as given in Section 6.4 follows the treatment in A. Durfee's thesis [56]. Observe that instead of the term "discriminant form" he uses "induced form".

The notion of a split inner product space goes back to M. Knebusch [116] under the name of "metabolic inner product space". The terminology "split inner product space" has been coined by J. Milnor and D. Husemoller in [151, §I.6].



## Reflections and the Witt Decomposition

### Introduction

In this chapter we investigate the existence of hyperplane reflections in  $R$ -lattices. Over a field such reflections exist, but these may or may not preserve a lattice. Over the ring  $R = \mathbb{Z}_p$  these also exist. See Section 7.1. Moreover, as shown in Section 7.2 we show that isometries are always products of hyperplane reflections provided  $R$  is a local ring in which 2 is a unit. This is crucial for the definition of the spinor norm later on in Chapter 13.

An application of a different nature is discussed in this section as well: Witt's theorems give a particular splitting of inner product spaces over local rings to which we come back in Chapter 8. This decomposition can also be used to classify  $R$ -inner product spaces "up to split inner product spaces" leading to an invariant for the ring  $R$ , the Witt ring of  $R$ . This is briefly explained in Section 7.3.

### 7.1 Reflections

In this section  $R$  is an integral domain.

Suppose for the moment that  $2 \neq 0$  so that quadratic forms can be identified with even bilinear forms. Recall that the group  $O(L)$  of isometries of an  $R$ -lattice  $(L, b)$  contains the subgroup  $SO(L)$  of rotations as a subgroup of index at most 2. Rotations  $g \in SO(L)$  are characterized by  $\det g = 1$ . Reflections are the isometries  $g$  of  $L$  with  $\det g = -1$ .

Some examples are obtained as follows. If  $S$  is a sublattice of  $L$  such that  $L = S \oplus S^\perp$ , then the map  $(s, t) \mapsto (s, -t)$  is an isometry; it is a reflection precisely if the rank of  $S^\perp$  is odd. A special case occurs if  $S = x^\perp$  with  $b(x, x)$  a unit. In this case  $L = x^\perp \oplus \langle b(x, x) \rangle$  by Proposition 6.3.10 and the isometry is the hyperplane reflection  $\sigma_x$  in the hyperplane  $x^\perp$ , which, we recall, is given by

$$\sigma_x(y) = y - \frac{2b(x, y)}{b(x, x)} \cdot x, \quad y \in L.$$

Note that the hyperplane reflection is also defined if  $2/b(x, x) \in R$  (but  $L$  need not decompose in this case: take for instance  $L = E_8$  and an  $x$  with  $b(x, x) = 2$ ).

As to the effect of hyperplane isometries on the discriminant group, we have:

**Lemma 7.1.1.** *Let  $(L, q)$  be a quadratic lattice. Suppose  $x \in L$  is primitive, non-isotropic such that  $b_q(x, L^*) \subset q(x) \cdot R$  (in particular this is the case if  $q(x)$  is a unit). Then the hyperplane reflection  $y \xrightarrow{\sigma_x} y - (b_q(x, y)/q(x)) \cdot x$ ,  $y \in L$ , induces the identity on the discriminant group.*

*Proof.* Since for all  $u \in L^*$ ,  $b_q(x, u) \cdot q(x)^{-1} \in R$ , it follows that  $\sigma_x u \equiv u \pmod{L}$ . This precisely means that  $\sigma_x$  induces the identity on  $\text{dg}_L$ .  $\square$

**Examples 7.1.2. 1.** Let  $R = \mathbb{Z}_p$  where  $p$  is any prime. Quadratic modules over this ring are the quadratic  $p$ -adic lattices. We claim that every (non-degenerate) quadratic  $p$ -adic lattice  $(L, q)$  admits reflections and so here also  $\text{SO}(L)$  is of index 2 in  $\text{O}(L)$ . We see this as follows. Since the valuation  $v_p$  is non-archimedean and since for all  $z, y \in L$ ,  $b_q(z, y) = q(z + y) - q(z) - q(y)$ , equation (A.4) implies  $v_p(b_q(z, y)) \geq \inf_{u \in L, q(u) \neq 0} v_p(q(u))$ . That the (non-zero) infimum is attained, say at  $x$ , is clear since the valuation is discrete. It follows that  $v_p(b_q(x, y)/q(x)) \geq 0$ , which translates as  $b_q(x, y) \in q(x) \cdot \mathbb{Z}_p$  and so (6.6) holds. Hence the reflection  $\sigma_x$  in  $x$  is a well-defined isometry. We set this result apart since it will be used later:

$$\inf_{z \in L, q(z) \neq 0} v_p(q(z)) = v_p(q(x)) \implies \sigma_x \text{ is a hyperplane reflection of } L. \quad (7.1)$$

**2.** In Example 6.5.5.2 we saw that the isometry group of the hyperbolic plane  $U$  over  $R$  consists of the rotations  $i_a := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ ,  $a \in R^\times$ , and the reflections

$j_b = \begin{pmatrix} 0 & b^{-1} \\ b & 0 \end{pmatrix}$ ,  $b \in R^\times$ . The condition (6.6) implies that a reflection is of the form  $\sigma_c$  with  $c = ue + vf$  for some units  $u, v$ . Then  $\sigma_c(e) = -vu^{-1} \cdot f$  and  $\sigma_c(f) = -v^{-1}u \cdot e$ , i.e.,  $\sigma_c = j_b$  with  $b = -vu^{-1}$ . It follows that products of an even number of reflections form a proper subgroup of  $\text{O}(U)$  regardless whether  $2 = 0$  in  $R$  or not.

**3.** Consider the unimodular dyadic lattice  $V_0$ , i.e.,  $\mathbb{Z}_2^{\oplus 2}$  with quadratic form  $x = (x_1, x_2) \mapsto q(x) = x_1^2 + x_1x_2 + x_2^2$ . It contains no isotropic vectors (such an isotropic vector would lead to a solution of the equation  $x^2 = -3$  in  $\mathbb{Q}_2$  which is impossible by Theorem A.2.1-2) and all reflections are of the form  $\sigma_x$ ,  $q(x) \in \mathbb{Z}_2^*$ . This concerns every primitive vector since then, as we readily see,  $q(x)$  is a unit due to the special shape of the quadratic form.

We end this sections with a few words about the case  $2 = 0$ . Here the situation is quite different. For example, if  $V = W \oplus ke$  is a quadratic space over a field of characteristic 2 such that  $q(e) = 1$ , then  $\sigma_e$  is the identity. More generally, if  $(V, q)$  is quadratic  $k$ -space and  $x$  satisfies  $q(x) \neq 0$  and  $x \in \text{rad}(b_q)$ , then  $\sigma_x$  is the identity on  $V$ . If  $q(x) \neq 0$ , then the corresponding map  $\sigma_x$  is an example of a so-called transvection w.r.t. the bilinear form  $b_q$ , see Appendix A.5.

## 7.2 The Theorems of Cartan–Dieudonné and Witt

In this section  $R$  is a local ring in which 2 is a unit.

The main goal of this section is to demonstrate the Cartan–Dieudonné theorem 7.2.4 which makes the assertion precise that reflections are ubiquitous. The proof uses the following result.

**Lemma 7.2.1.** *Let  $(V, b)$  be an inner product space over  $R$ . If  $x, y \in V$ ,  $x \neq y$ , are such that  $b(x, x) = b(y, y) \in R^\times$ , there exists an isometry  $\sigma$  sending  $x$  to  $y$  which is a product of at most two hyperplane reflections.*

*Proof.* The two vectors  $v = \frac{1}{2}(x + y)$  and  $w = \frac{1}{2}(x - y)$  are mutually orthogonal and have sum  $x$ . Consequently,

$$b(x, x) = b(v, v) + b(w, w). \quad (7.2)$$

Since  $R$  is local, the unit  $b(x, x)$  cannot be the sum of two non-units. If  $b(v, v)$  is a unit, then by Proposition 6.3.10 we have  $L = Rv \oplus Rv^\perp$  and  $\sigma_{y \circ \sigma_v}(x) = y$ . If  $b(w, w)$  is a unit, the reflection  $\sigma_w$  sends  $x$  to  $y$ .  $\square$

*Remark 7.2.2.* If  $(V, b)$  has rank 1, say  $V = Rx$ , the above proof can easily be adapted to show that the only reflection is  $-\text{id} = \sigma_x$ .

There is a more specific version of Lemma 7.2.1 in the  $p$ -adic setting which we are going to use later. Its statement involves the  $p$ -adic invariant  $m_q$  associated to the non-degenerate quadratic form  $q$  defined by

$$m_q = \inf_{z \in V} v_p(q(z)), \quad (7.3)$$

and reads as follows.

**Lemma 7.2.3.** *Let  $R = \mathbb{Z}_p$  ( $p \neq 2$ ) and let  $(V, q)$  be a non-degenerate quadratic  $\mathbb{Z}_p$ -module. If  $x, y \in V$  are such that  $q(x) = q(y)$  have  $p$ -adic valuation  $m_q$ , then there is an isometry which is the product of at most two hyperplane reflections  $\sigma_z$  and carries  $x$  to  $y$ . Moreover, we can choose  $z$  such that  $v_p(q(z)) = m_q$ .*

*Proof.* As before we let  $v = \frac{1}{2}(x + y)$ ,  $w = \frac{1}{2}(x - y)$ . Since  $b_q(x, x) = 2q(x)$  for all  $x \in V$  and since 2 is invertible, (7.2) can be rewritten as  $q(x) = q(v) + q(w)$ . Because of the non-archimedean nature of the  $p$ -adic valuation at least one of  $q(v)$  and  $q(w)$  must have  $p$ -adic valuation equal to  $m_q$ . In case  $v_p(q(v)) = m_q$ , then by (7.1)  $\sigma_v$  is a reflection belonging to  $O(V)$  and  $\sigma_{y \circ \sigma_v}$  sends  $x$  to  $y$  as before. Otherwise,  $\sigma_w \in O(V)$  and we may use  $\sigma_w$ .  $\square$

**Theorem 7.2.4** (Cartan–Dieudonné). *Every isometry of an inner product space  $(V, b)$  of rank  $n$  over a local ring  $R$  in which 2 is a unit, is a product of at most  $2n$  hyperplane reflections.*

*Proof.* If  $n = 1$  this follows from Remark 7.2.2.

Assume now that  $n > 1$  and let  $x \in V$  be a vector with  $b(x, x)$  a unit, e.g., a vector from an orthogonal basis (cf. Proposition 6.3.11). Let  $\tau \in O(V)$ . By Lemma 7.2.1 there is an isometry  $\sigma$  which is a product of at most two hyperplane reflections sending  $\tau(x)$  to  $x$ . Then  $\sigma \circ \tau(x) = x$  and  $\sigma \circ \tau$  preserves  $Rx^\perp$ . Since the restriction of  $b$  to  $Rx^\perp$  is unimodular, by induction we may write the restriction of  $\sigma \circ \tau$  to  $Rx^\perp$  as a product of at most  $2n - 2$  hyperplane reflections in  $Rx^\perp$ . Such a product  $\tau'$  can be extended to  $V$  by letting it act as the identity on  $x$ . Then  $\tau = \sigma^{-1} \circ \tau'$  is a product of at most  $2n$  isometries.  $\square$

Using Lemma 7.2.3, we observe that in the special case of  $R = \mathbb{Z}_p$ , the proof shows:

**Corollary 7.2.5.** *If  $R = \mathbb{Z}_p$ ,  $p$  odd, we can write an isometry of a quadratic inner product space  $(V, q)$  over  $R$  as a product of hyperplane reflections in vectors  $z$  for which  $v_p(z) = m_q$  (cf. Eqn. (7.3)).*

*Remark 7.2.6.* **1.** The Cartan–Dieudonné theorem<sup>1</sup> is true more generally for quadratic inner product spaces  $V$  over any local ring  $R$  – with one exception, the case where the residue field of  $R$  is  $k = \mathbb{F}_2$  and  $\text{rank}(V) = 4$ . We have placed a proof in Appendix C.1. This proof is based on [122, Sect. 4]. Over  $\mathbb{F}_2$  the quadratic form  $q = x^2 + xy + y^2 + u^2 + uv + v^2$  over  $\mathbb{F}_2$  gives an exception. Indeed, the isometry  $(x, y, u, v) \mapsto (u, v, x, y)$  is not a product of two reflections. To see this, remark that any non-isotropic vector belongs either to the  $(x, y)$ -plane or to the  $(u, v)$ -plane, and so the corresponding reflection preserves both planes. However, then the isometry  $\tau(x, y, u, v) = (u, v, x, y)$  cannot be a product of reflections. This also happens for the same quadratic form now considered over  $\mathbb{Z}_2$ . Indeed, this form is isometric to  $L = V \oplus V$  and non-isotropic vectors  $x \in L$  and the corresponding reflections  $\sigma_x$  after passing to the residue field give non-isotropic vectors with their corresponding reflections. The same is true for products of reflections. Hence these preserve the two summands  $V$  up to vectors in  $2L$ . However the isometry  $\tau$  which exchanges these two summands does not satisfy this condition and so cannot be a product of reflections.

**2.** Over a field of characteristic different from 2, a more elaborate proof shows that the upperbound  $2n$  can be replaced by  $n$ . See [8, pp. 129–130] or [177, pp. 102–103]. The number  $n = \dim V$  for the number of reflections is actually attained for  $-\text{id}$ . This follows from a general fact which is left as an exercise: every isometry  $f$  of  $V$  is the product of at most  $\text{codim}(\text{Fix}(f))$  hyperplane reflections, where  $\text{Fix}(f) = \{v \in V \mid f(v) = v\}$ . We apply this to  $f = -\text{id}$ , an isometry whose fixed point locus has dimension 0. Now since every hyperplane reflection has an  $n - 1$  dimensional fixed point space, the product of  $r$  reflections is fixed on at least the intersection of the  $r$  hyperplanes. This intersection has dimension  $\geq n - r$ . So we need at least  $n$  reflections to deal with  $-\text{id}$ .

Reflections are used to prove a central result:

<sup>1</sup>in the sense that every isometry is the product of an unspecified number of reflections.

**Theorem 7.2.7** (Witt’s cancellation theorem). *Let  $V, W_1, W_2$  be inner product spaces over  $R$ . If  $V \oplus W_1 \simeq V \oplus W_2$ , then  $W_1 \simeq W_2$ .<sup>2</sup>*

*Proof.* Since by Proposition 6.3.11 the inner product space  $V$  is an orthogonal direct sum of rank 1 inner product spaces over  $R$ , we may by induction assume that  $V = R \cdot e$ . Suppose now that  $f : R \cdot e \oplus W_1 \rightarrow R \cdot e \oplus W_2$  is an isometry. The two elements  $f(e, 0)$  and  $(e, 0)$  in  $R \cdot e \oplus W_2$  satisfy the hypothesis of Lemma 7.2.1 (since  $R \cdot e$  is a rank 1 inner product space) and so there is a product  $\sigma$  of at most two reflections of the target space sending  $f(e, 0)$  to  $(e, 0)$ . The isometry  $\sigma \circ f$  then maps  $(e, 0) \in R \cdot e \oplus W_1$  to  $(e, 0) \in R \cdot e \oplus W_2$  and hence carries the orthogonal complement, that is, the summand  $W_1$ , to the summand  $W_2$ .  $\square$

Next, we investigate extendability of isometries between subspaces  $W, W'$  of  $V$ . We say that two embeddings  $i : W \hookrightarrow V$  and  $i' : W' \hookrightarrow V$  are **equivalent** if there exists an isometry  $\varphi : V \rightarrow V$  making the following diagram commutative:

$$\begin{array}{ccc}
 W \hookrightarrow & \xrightarrow{\quad} & V \\
 \varphi|_W \downarrow \simeq & & \downarrow \simeq \\
 W' \hookrightarrow & \xrightarrow{\quad} & V.
 \end{array}
 \tag{7.4}$$

**Corollary 7.2.8** (Witt’s extension theorem). *Let  $(V, b)$  be an inner product space over  $R$  and  $W_1, W_2 \subset V$  two  $R$ -submodules such that  $b|_{W_1}, b|_{W_2}$  are unimodular. Any isometry  $W_1 \xrightarrow{\simeq} W_2$  can be extended to an isometry of  $V$ . In particular, any two primitive embeddings  $W \hookrightarrow V$ ,  $W$  unimodular, are equivalent. In other words,  $O(V)$  acts transitively on such primitive embeddings.*

*Proof.* Using Lemma 6.2.1 we see that  $V = W_j \oplus W_j^\perp$ ,  $j = 1, 2$ , since  $b$  and  $b|_{W_j}$  are unimodular. Also  $W_1 \oplus W_1^\perp = W_2 \oplus W_2^\perp \simeq W_1 \oplus W_2^\perp$  and the cancellation theorem gives an isomorphism  $s : W_1^\perp \simeq W_2^\perp$ . Hence any isometry  $t : W_1 \xrightarrow{\simeq} W_2$  can be extended as  $t \oplus s \in O(V)$ .  $\square$

*Remark 7.2.9.* **1.** Witt’s extension theorem is actually equivalent to Witt’s cancellation theorem 7.2.7. This can be seen by starting with an isometry  $f : V \oplus W_1 \rightarrow V \oplus W_2$  and applying Witt’s extension theorem to the first summand  $V$  of  $V \oplus W_2$  and the image  $f(V)$ .

**2.** Witt’s theorems are in fact true for (finite rank) quadratic inner product spaces  $V$  over any local ring  $R$  (so 2 need not be a unit) and for unimodular free submodules  $W_1, W_2$ . Actually, it suffices to assume that the correlation map  $\beta_W$  given by (6.3) is surjective. See Corollary C.1.3 in Appendix C.1 which elaborates [122, Folgerung 4.4].

**3.** Over local rings in which 2 is not a unit, there are symmetric inner product spaces that are not quadratic. Witt’s theorem is false for those. Here is a counterexample. We claim the existence of an isometry

$$\langle -1 \rangle \oplus \langle -1 \rangle \oplus \langle 1 \rangle \simeq \langle -1 \rangle \oplus U$$

<sup>2</sup>Recall that the symbol “ $\simeq$ ” stands for isometry and *not* isomorphism.

of symmetric lattices over  $\mathbb{Z}_2$ . To show this, let  $\{e_1, e_2, e_3\}$  be an orthogonal basis realizing the left-hand form. In the basis  $\mathbf{E} = \{e_1 + e_2 + e_3, e_1 + e_3, e_2 + e_3\}$  the Gram matrix reads as follows:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

This is indeed the matrix for  $\langle -1 \rangle \oplus U$ , establishing the claim. Clearly  $U$  is not isometric to  $\langle -1 \rangle \oplus \langle 1 \rangle$  since the first one is an even form while the second is odd. Observe that this also gives counterexamples over any ring in which 2 is not invertible, like the ring of integers.

**Proposition 7.2.10.** *Let  $(V, q)$  be a quadratic inner product space over  $R$ . Up to isometry  $V$  has a unique orthogonal decomposition*

$$V = \widehat{U} \oplus V', \quad \widehat{U} \simeq \underbrace{U \oplus \cdots \oplus U}_{m \text{ copies}}, \quad V' \text{ totally anisotropic}, \quad (7.5)$$

*the Witt decomposition. The subspace  $\widehat{U}$  contains a maximal totally isotropic sublattice of rank  $m$ . Moreover, all maximal isotropic sublattices of  $V$  have rank  $m$ .*

*Proof.* By Lemma 6.3.8,  $q$  represents 0 if and only if  $q$  splits off a hyperbolic plane. Continuing in this way we may write  $V = \widehat{U} \oplus V'$ ,  $\widehat{U} \simeq \oplus^m U$  and where  $q|_{V'}$  does not represent zero. Suppose  $V = \oplus^m U \oplus V'$  and  $V = \oplus^{m'} U \oplus V''$  are two such splittings, say with  $m < m'$ . Then  $\oplus^m U \oplus V' \simeq \oplus^m U \oplus (\oplus^{m'-m} U \oplus V'')$ . By Witt's theorem 7.2.7 we conclude  $V' \simeq \oplus^{m'-m} U \oplus V''$  so that  $V'$  represents zero, a contradiction. So  $m = m'$ . Likewise, a splitting  $V = \oplus^m U \oplus V''$  leads to an isometry between  $V'$  and  $V''$ . This shows uniqueness of the Witt decomposition up to isometry.

Taking the standard basis for each copy of  $U$  gives a basis  $\{e_1, f_1, \dots, e_m, f_m\}$  of  $\widehat{U}$ . Then  $\{e_1, \dots, e_m\}$  spans an isotropic sublattice  $W$  of  $\widehat{U}$ . Any isotropic  $y \in W^\perp$  is of the form  $z + t$  with  $z \in W$  and  $t \in V'$ . But then  $q(t) = 0$  which implies  $t = 0$ . Hence  $W$  is a maximal isotropic sublattice.

To show the last assertion, let  $W$  be a primitive maximal isotropic submodule of  $V$  with basis  $\{e_1, \dots, e_k\}$ . As in the proof of Lemma 6.3.8 one can then find inductively vectors  $f_1, \dots, f_k$  such that  $Re_j + Rf_j$  is an  $R$ -hyperbolic plane  $U_j$  and  $U_1 \oplus \cdots \oplus U_k$  splits off. Its orthogonal complement cannot contain isotropic vectors, otherwise  $W$  would not have been maximal. By uniqueness of the splitting (7.5), the number of copies of the hyperbolic plane in the resulting splitting must be  $m$  and so  $\text{rank}(W) = k = m$ .  $\square$

We encountered the number  $m$  already in Chapter 1 as the Witt index (cf. page 27). This makes sense for all local rings, even if 2 is not invertible:

**Definition 7.2.11.** Let  $(V, q)$  be an inner-product space over a local ring. The **Witt index**  $W_\tau(V, q)$  of  $(V, q)$  is the dimension of a maximal isotropic submodule of  $V$ .

By Proposition 7.2.10 this is well defined over local rings in which 2 is invertible. We need another argument if this is not the case using Remark 7.2.9.2 which tells us that in this situation the theorems of Witt remain valid for primitive submodules. Applying this we can show that the Witt index is well defined. Indeed, Let  $W, W' \subset V$  be two primitive isotropic submodules. If  $\dim W' \leq \dim W$ , choose  $W'' \subset W$  with  $\dim W'' = \dim W'$ . Then  $W''$  and  $W'$  are isomorphic submodules and any isomorphism  $W'' \simeq W'$  can be extended to an isometry  $f : V \xrightarrow{\simeq} V$ . It follows that  $f(W) \supset f(W'') = W'$  is a primitive isotropic submodule of  $V$  and by maximality  $f(W) = W'$ .

The Witt decomposition 7.2.10 still holds in this general framework, but instead  $\widehat{U}$  has to be replaced by a suitable split  $R$ -inner product space as defined by equation (6.5).

*Remark 7.2.12.* The Witt index is not stable under ring extension since a form which does not represent zero over  $R$  may very well do so over a larger ring. However, if  $R$  is an integral domain with quotient field  $Q(R)$ , the Witt indices over  $R$  and  $Q(R)$  are the same. This applies to integral lattices  $L$  and shows that for those the Witt index is an invariant of  $L_{\mathbb{Q}}$  and  $W_{\tau}(L_{\mathbb{Q}}) \leq W_{\tau}(L_{\mathbb{R}})$ . The equality may be strict. We have seen this already in Example 1.10.6 where we showed that  $x^2 + y^2 - 3z^2$  has no isotropic vector over  $\mathbb{Q}$  and so has Witt index 0 while over the reals it has Witt index 1. Note that the latter is directly related to the signature. Indeed, if  $L$  is non-degenerate with signature  $(s, t)$  one has  $W_{\tau}(L_{\mathbb{R}}) = \min(s, t)$ .

### 7.3 Excursion: The Witt Ring

In this section  $R$  is a commutative ring with unit 1.

Since in this book the Witt ring will not play a role, we only sketch the construction and discuss its properties without proofs. For further details we refer to [36, 151].

The construction of the Witt ring is inspired by the Witt decomposition (7.5) of a quadratic space  $V$  over local rings where 2 is a unit (cf. (7.5)). If  $V = V' \oplus \widehat{U}$  is the Witt decomposition, the idea is to declare  $V$  and  $V'$  to be equivalent. Over rings in which 2 is not a unit, instead of  $\widehat{U}$  the more general “split inner product spaces”  $U_{L,q}$  (cf. (6.5)) should be used. This leads to the following definition.

**Definition 7.3.1.** Two quadratic spaces  $V, V'$  are in the same **Witt class**  $[V] = [V']$  if there exist split inner product spaces  $U', U''$  such that

$$V \oplus U' \simeq V' \oplus U''.$$

This then indeed turns out to be an equivalence relation. The set of equivalence classes is denoted  $W(R)$ . Since the orthogonal sum of split spaces is split, we also see that this equivalence relation is compatible with orthogonal direct sums. One

can show that this gives a commutative group structure to  $W(R)$ . The resulting group is the **Witt group**.

One can also define a product structure, using tensor products. For this to make sense we put a quadratic form on the tensor product  $V \otimes V'$  of two quadratic  $R$ -spaces  $(V, q), (V', q')$  by setting

$$q \otimes q'(x \otimes x') = q(x) \cdot q'(x').$$

This tensor product turns out to be compatible with Witt equivalence and, moreover, the Witt group  $W(R)$  equipped with this product structure becomes a ring, the **Witt ring**.

- Examples 7.3.2.**
1. Since the rank of a split inner product space is even (cf. (6.5)), the parity of the rank is a well-defined ring homomorphism  $W(R) \rightarrow \mathbb{Z}/2\mathbb{Z}$ . For any algebraically closed field  $R$  of characteristic not equal to 2 this gives an isomorphism. This follows since according to Proposition 6.3.11 all forms can be diagonalized so that the Witt ring is generated by the class of a form of odd rank.
  2. The index of a split inner product space over  $\mathbb{R}$  is zero and induces an isomorphism  $W(\mathbb{R}) \xrightarrow{\sim} \mathbb{Z}$ . This is a direct consequence of Sylvester's theorem (cf. Corollary 8.1.3) and the uniqueness of the Witt splitting.
  3. The Witt groups for the basic finite fields  $\mathbb{F}_p$ ,  $p$  prime, are as follows.

$$W(\mathbb{F}_p) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{for } p = 2 \\ \mathbb{Z}/4\mathbb{Z} & p \text{ odd, } p \equiv 3 \pmod{4} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p \text{ odd, } p \equiv 1 \pmod{4}. \end{cases}$$

The Witt ring of  $\mathbb{Q}$  can be described by a split exact sequence

$$0 \rightarrow \mathbb{Z} \xrightarrow{i} W(\mathbb{Q}) \xrightarrow{\partial} \bigoplus_{p \text{ prime}} W(\mathbb{F}_p) \rightarrow 0.$$

Here  $i$  is defined by sending 1 to  $[\langle 1 \rangle]$  and  $\partial$  sends a class of a form  $\langle a \rangle$  to the class of its localizations (obviously, Witt equivalence is compatible with localization). See [151, IV.2].

**Historical and Bibliographical Notes.** The Cartan–Dieudonné theorem dates back to the 1938 book of É. Cartan on spinors (see the reprint [34]) and the 1955 monograph by J. Dieudonné reprinted as [49]. E. Witt's classic 1937 article [251] is the origin of the results that we now know as "Witt's theorems". In the same article E. Witt introduces the Witt group. For more on the Witt group we refer to [36, § 4.3, § 6.11] and [122, § 9]. Several people observed that the tensor product induces a ring structure, e.g. W. Scharlau [201], F. Lorenz [145] and M. Knebusch [116]. For calculations of the Witt ring for  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  and for finite fields one may consult [151].



---

## Inner Product Spaces Over Fields

### Introduction

An inner product space over a field  $k$  is a  $k$ -vector space equipped with a non-degenerate symmetric bilinear form. A quadratic inner product space is equipped with a non-degenerate quadratic form. Of course, only in characteristic 2 there is a difference between the two and the classification in this case is much more involved. It is based on the Arf invariant for which we present an elementary treatment. We treat the two cases in Sections 8.1 and 8.2 respectively. Over finite fields the classification can be given in greater detail. This is explained in Section 8.3.

### 8.1 Characteristic Different from Two

In characteristics different from two, we have already observed (cf. Proposition 1.1.4) that all forms are diagonalizable:

**Theorem 8.1.1** (Diagonalization;  $\text{char}(k) \neq 2$ ). *Every non-degenerate symmetric bilinear form over a field  $k$  of characteristic different from 2 is isometric to a diagonal form*

$$\langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle, \quad \text{with } a_j \in k^\times, j = 1, \dots, n.$$

*Remark 8.1.2.* **1.** For the field  $\mathbb{R}$  we may further simplify this: since every positive number is a square, we may assume that  $a_j \in \{1, -1\}$ . The number of times 1 or  $-1$  appears is unique as stated by Sylvester's theorem. Its proof is recalled below (see Corollary 8.1.3).

**2.** For an algebraically closed field such as the field  $\mathbb{C}$  we may assume that the  $a_j$  are all equal to 1, i.e., every form is equivalent to a sum of squares.

What about uniqueness of the above representations? The Witt decomposition  $V = U^{\oplus m} \oplus V'$ , where  $V'$  is totally anisotropic, has the merit of being unique. Over  $\mathbb{R}$  and  $\mathbb{C}$  the diagonal decomposition of  $V'$  is also unique. It is instructive to compare this with what we said about the Witt ring of  $\mathbb{C}$  and  $\mathbb{R}$  in Example 7.3.2. In Section 8.3 we show uniqueness over finite fields. However, in general we have no uniqueness, as explained in Chapter 3 where we investigated this for the field  $\mathbb{Q}$ .

**Corollary 8.1.3** (Sylvester's Law). *Let  $(V, b)$  be a real inner product space. There is a subspace  $V^+$  (respectively  $V^-$ ) of maximal dimension  $d^+$  (respectively  $d^-$ ) on which  $b$  is positive (negative) such that*

$$V = V^+ \oplus V^-. \quad (8.1)$$

Moreover, all such spaces  $V^\pm$  have the same dimension  $d^\pm$ .

*Proof.* By Theorem 8.1.1, there is a  $b$ -orthogonal basis  $\{e_1, \dots, e_n\}$  for  $V$  such that  $V = V^+ \oplus V^-$  with  $V^+ \simeq \bigoplus^p \langle 1 \rangle$  and  $V^- \simeq \bigoplus^{n-p} \langle -1 \rangle$ . If  $W$  is a subspace with  $b|_W > 0$ , then  $W \cap V^- = \{0\}$  and the dimension formula gives

$$\begin{aligned} \dim(W) &= \dim(W + V^-) - \dim(V^-) \\ &\leq \dim V - \dim(V^-) \\ &= \dim V^+. \end{aligned}$$

So  $V^+$  is a subspace of maximal dimension on which  $b$  is positive. Similarly for  $V^-$ . Moreover, the proof shows that if  $V = W^+ \oplus W^-$  is another such splitting, then  $\dim(W^\pm) \leq d^\pm$  and so one must have equality.  $\square$

We already saw in Sections 1.2 and 1.3, that this leads to the following invariants.

**Definition 8.1.4.** Referring to (8.1), the pair  $(\dim V^+, \dim V^-)$  is called the *signature* of the inner product space  $V$  over  $\mathbb{R}$ . The difference  $\tau(V) = \dim V^+ - \dim V^-$  is called the *index*. If  $V = V^+$ , the inner product space is called *positive definite*, if  $V = V^-$  we say that  $V$  is *negative definite*.

Summarizing, we have shown that the signature is a complete invariant for inner product spaces over  $\mathbb{R}$ . Equivalently this can be stated as follows.

**Theorem 8.1.5** (Classification of real forms). *Two real inner product spaces  $(V, b)$  and  $(V', b')$  are isometric if and only if  $\dim V = \dim V'$  and  $\tau(V) = \tau(V')$ .*

## 8.2 Characteristic Two

**8.2.A The non-degenerate case.** Since we are in characteristic 2 we need to make a distinction between the classification of quadratic and that of symmetric inner product spaces. Symmetric inner product spaces are easy to classify:

**Proposition 8.2.1.** *Let  $(V, b)$  be a symmetric inner product space over a field  $k$  of characteristic 2. Then  $V$  is isometric to an orthogonal direct sum  $V_1 \oplus V_2$ , where  $V_1$  is a diagonal form and  $V_2$  is a direct sum of hyperbolic planes.*

*Proof.* This can be seen by induction as follows. If  $b(x, x) \neq 0$  for some  $x \in V$ , by Lemma 6.2.1 we may split off  $k \cdot x$ . We continue splitting off such lines until

$b(x, x) = 0$  for all  $x$  in the orthogonal complement  $V_2$  of the split off lines. Then  $V = V_1 \oplus V_2$ . Pick a non-zero vector  $v \in V_2$ . Since  $b|_{V_2}$  is non-degenerate, there exists a  $u \in V_2$  with  $b(u, v) \neq 0$ . Replacing  $v$  with a suitable multiple, we may assume that  $b(u, v) = 1$  and then the plane spanned by  $u$  and  $v$  is a hyperbolic plane. Again by Lemma 6.2.1 we may split off this plane and apply induction.  $\square$

Next, consider the quadratic case. Hyperbolic planes and their direct sums give examples, but these do not exhaust the possibilities. To see this, let  $(V, q)$  be a quadratic inner product space and observe that first of all its polar form  $b_q$  is a symplectic form since  $b_q(x, x) = 2q(x, x) = 0$ . Secondly, by assumption  $b_q$  is non-degenerate and so by Appendix A.5,  $V$  has even dimension and there is a symplectic basis  $\mathbf{E} = \{e_1, \dots, e_{2n}\}$ , that is, a basis in which the Gram matrix is  $J_n = \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}$  giving the standard symplectic form

$$(x, y) \mapsto \sum_{j=1}^n x_j y_{n+j} + y_j x_{n+j}, \quad x = \sum_{j=1}^{2n} x_j e_j, y = \sum_{j=1}^{2n} y_j e_j.$$

The collection of quadratic forms  $q$  for which this is the polar form is as follows:

$$q = \sum_{i=1}^n x_i x_{n+i} + \sum_{j=1}^{2n} a_j x_j^2, \quad a_j \in k, \quad (8.2)$$

which in the basis  $\mathbf{E}$  is given by the upper triangular matrix  $Q = \begin{pmatrix} \mathbf{a} & I_n \\ 0_n & \mathbf{a}' \end{pmatrix}$  with  $\mathbf{a}$ ,  $\mathbf{a}'$ , the diagonal matrices with diagonal entries  $a_1, \dots, a_n$ , respectively  $a_{n+1}, \dots, a_{2n}$ .

Since the polar form is non-degenerate these quadratic forms are non-degenerate themselves. It turns out that the quantity  $\sum_{i=1}^n a_i a_{n+i} = \sum_{i=1}^n q(e_i)q(e_{i+n})$  serves to distinguish non-isometric quadratic forms. A priori this sum depends on the choice of a symplectic basis, but we shall see shortly that the ambiguity is captured by the image of the additive homomorphism  $\varphi : k \rightarrow k$  given by  $a \mapsto a + a^2$ , the **Artin–Schreier map** in characteristic two. In other words, the class

$$\text{arf}(q) \equiv \sum_{i=1}^n a_i a_{n+i} \pmod{\varphi(k)}$$

no longer depends on the particular symplectic basis. It is called the **Arf invariant** of  $q$ :

**Theorem 8.2.2.** *A non-degenerate quadratic form on  $V$  in characteristic 2 is equivalent to a form  $q = \sum_{i=1}^n x_i x_{n+i} + \sum_{j=1}^{2n} a_j x_j^2$ , for some  $a_j \in k$ .*

1. *The Arf invariant of such a form is well defined.*
2. *Isometric non-degenerate quadratic forms have the same Arf invariant.*
3. *If  $k$  is a perfect field of characteristic 2, then two non-degenerate quadratic forms of the same rank and the same Arf invariant are isometric.*

*Proof.* 1. Two symplectic bases are related by a symplectic transformation. By Proposition A.5.4 any symplectic transformation is a product of symplectic transvections. These are all of the form

$$\tau_{u,a}(x) = x + a \cdot b(x, u) \cdot u, \quad a \in k, u \in V,$$

where we write  $b$  in place of  $b_q$ . So it suffices to show that the Arf invariant of  $q$  in a given symplectic basis  $\mathbf{E} = \{e_1, \dots, e_{2n}\}$  differs from the Arf invariant in the basis  $\tau(\mathbf{E}) = \{\tau(e_1), \dots, \tau(e_{2n})\}$ ,  $\tau = \tau_{u,a}$ , by an element in  $\wp(k)$ . To show this, write

$$\hat{q}(x) := q(\tau(x))$$

and note that

$$\begin{aligned} \hat{q}(x) &= q(x + a' \cdot u), \quad a' = a \cdot b(x, u) \\ &= q(x) + a'^2 q(u) + a' \cdot b(x, u) \\ &= q(x) + \underbrace{(a^2 q(u) + a)}_c \cdot b(x, u)^2 \end{aligned} \tag{8.3}$$

and so with  $u = \sum_{j=1}^{2n} u_j e_j$ , using the expression (8.2), one finds

$$\begin{aligned} \hat{q}(x) &= \sum_{i=1}^n x_i x_{n+i} + \sum_{j=1}^{2n} a_j x_j^2 + c \sum_{i=1}^n (x_i^2 u_{i+n}^2 + x_{i+n}^2 u_i^2) \\ &= \sum_{i=1}^n x_i x_{n+i} + \sum_{i=1}^n (a_i + c u_{i+n}^2) x_i^2 + \sum_{i=1}^n (a_{i+n} + c u_i^2) x_{i+n}^2. \end{aligned}$$

Computing  $\text{arf}(\hat{q})$  with respect to  $\mathbf{E}$  is the same as computing  $\text{arf}(q)$  with respect to  $\tau(\mathbf{E})$ . So

$$\begin{aligned} \text{arf}(\hat{q}) &= \sum_{i=1}^n (a_i + c u_{n+i}^2) \cdot (a_{n+i} + c u_i^2) \\ &= \text{arf}(q) + c \left( \sum_{i=1}^n u_i^2 a_i + u_{n+i}^2 a_{n+i} \right) + c^2 \sum_{i=1}^n u_i^2 u_{n+i}^2 \\ &= \text{arf}(q) + c \underbrace{\left( \sum_{i=1}^{2n} a_i u_i^2 + \sum_{i=1}^n u_i u_{i+n} \right)}_{q(u)} + c \sum_{i=1}^n u_i u_{i+n} + \left[ c \sum_{i=1}^n u_i u_{i+n} \right]^2 \\ &= \text{arf}(q) + c q(u) + c \sum_{i=1}^n u_i u_{i+n} + \left[ c \sum_{i=1}^n u_i u_{i+n} \right]^2 \end{aligned}$$

and hence

$$\text{arf}(\hat{q}) - \text{arf}(q) \equiv c q(u) + \wp \left( c \sum_{i=1}^n u_i u_{i+n} \right), \tag{8.4}$$

so that it suffices to show that  $cq(u) \in \wp(k)$ . But now we recall that  $c = a^2q(u) + a$  and so

$$cq(u) = a^2q(u)^2 + aq(u) = \wp(aq(u))$$

and the result follows. For later use we set apart the result of the previous calculations:

$$\begin{aligned} \operatorname{arf}(\hat{q}) - \operatorname{arf}(q) &= \wp\left(c \sum_{i=1}^n u_i u_{i+n} + aq(u)\right) \\ &= \wp\left((a^2q(u) + a) \cdot \sum_{i=1}^n u_i u_{i+n} + aq(u)\right) \\ &= \wp(D(\tau)), \quad D(\tau) = a[q(u) + (aq(u) + 1) \cdot \sum_{i=1}^n u_i u_{i+n}]. \end{aligned} \tag{8.5}$$

2. If  $q'$  and  $q$  are isometric (as quadratic forms), there is some invertible map  $A$  with  $q(Ax) = q'(x)$ . For the associated polar forms  $b, b'$  we have  $b'(x, y) = b(Ax, Ay)$  and  $A^{-1}\mathbf{E}$  is a symplectic basis for  $b'$ . The Arf invariant of  $q'$  with respect to this basis is

$$\begin{aligned} \operatorname{arf}(q') &= \sum_{i=1}^n q'(A^{-1}e_i)q'(A^{-1}e_{i+n}) \\ &= \sum_{i=1}^n q(e_i)q(e_{n+i}) \\ &= \operatorname{arf}(q). \end{aligned}$$

3. Let  $q, q'$  be two non-degenerate quadratic forms of rank  $2n$  with the same Arf invariant. Since both polar forms are in standard form, we may assume that  $q$  and  $q'$  are described with respect to a single symplectic basis. So we can write the difference as  $q(x) - q'(x) = \sum_{i=1}^n c_i x_i^2 + \sum_{i=1}^n c_{i+n} x_{n+i}^2$  for some  $c_i \in k, i = 1, \dots, 2n$ . Since  $k$  is perfect, we may write  $c_i = u_{i+n}^2, c_{i+n} = u_i^2, i = 1, \dots, n$ , and so

$$\begin{aligned} q(x) - q'(x) &= \sum_{i=1}^n (u_{i+n}x_i + u_i x_{n+i})^2 \\ &= b(x, u)^2, \quad u = \sum_{i=1}^{2n} u_i e_i. \end{aligned}$$

This means that we are in the situation of (8.3) with  $c = 1$ . Since  $\operatorname{arf}(q) = \operatorname{arf}(q')$ , equation (8.4) then shows we have  $q(u) \in \wp(k)$  and so, for some  $a \in k$ ,

$$q(u) = a^2 + a = a(a + 1) = (a + 1)^2 + (a + 1).$$

Now at least one of  $a, a + 1$  is non-zero and so we may assume that  $a \neq 0$  and we put  $b = a^{-1}$ . Then  $b^2q(u) + b = a^{-2}(a^2 + a) + a^{-1} = 1$ . Using the transvection

$\tau = \tau_{u,b}$ , by the calculation (8.3) we thus have

$$\begin{aligned} q(\tau(x)) &= q(x) + (b^2q(u) + b)b(x, u)^2 \\ &= q(x) + b(x, u)^2 \\ &= q'(x) \end{aligned}$$

and so  $q'$  and  $q$  are isometric.  $\square$

If in formula (8.2) we take  $a_i = a_{n+i} = 0$  for  $i = 1, \dots, n-1$  and  $a_n = a_{2n} = c$ , the Arf invariant equals  $c^2 \equiv c \pmod{\wp(k)}$  and so we have:

**Corollary 8.2.3.** *Let  $(V, q)$  be a quadratic inner product space of rank  $2n$  over a perfect field of characteristic 2. Then coordinates may be chosen so that  $q$  is equivalent to a form with Arf invariant  $c^2 \equiv c \pmod{\wp(k)}$  given by*

$$q^{(c)}(x) := \sum_{i=1}^n x_i x_{n+i} + c(x_n^2 + x_{2n}^2) = \sum_{i=1}^{n-1} x_i x_{n+i} + x_n x_{2n} + c(x_n^2 + x_{2n}^2), \quad c \in k.$$

This form is isometric to  $\mathbb{1}^{n-1}U \oplus P^{(c)}$  where the binary form on  $P^{(c)}$  is given by  $xy + c(x^2 + y^2)$ .

**Example 8.2.4.** The cyclic group  $\mathbb{Z}/2\mathbb{Z}$  can also be viewed as the field  $\mathbb{F}_2$  and the  $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ -valued torsion forms  $u_1$  and  $v_1$  from Examples 1.9.5 give  $\mathbb{F}_2$ -valued forms  $U$  and  $V$  with Arf invariants 0, 1, respectively. So for  $k = \mathbb{F}_2$  the only two types of rank  $2n$  non-degenerate quadratic forms are  $U^{\oplus n}$  and  $U^{\oplus(n-1)} \oplus V$ . Below, in Section 8.3, we generalize this for all finite fields.

**8.2.B The general case.** The main result is as follows:

**Proposition 8.2.5.** *Let  $k$  be a field of characteristic 2.*

1. *A  $k$ -vector space  $V$  with a symmetric bilinear form  $b$  is isometric to  $\mathbb{1}_{i=1}^s \langle a_i \rangle \oplus U^{\oplus t} \oplus \text{rad}(b)$ ,  $a_i \in k^\times$ ,  $i = 1, \dots, s$ .*
2. *A  $k$ -vector space  $V$  with a quadratic form  $q$  is isometric to  $q' \oplus \text{rad}(b_q)$  where*
  - (a)  *$q'$  is a non-degenerate quadratic form equivalent to a form  $\sum_{i=1}^m x_i x_{m+i} + \sum_{j=1}^{2m} a_j x_j^2$ , for some  $a_j \in k$ .*
  - (b)  *$\text{rad}(b_q) = V_q \oplus \text{rad}(q)$ , with  $q|_{V_q}$  diagonal of rank equal to  $\dim V_q = s$ ,  $s \leq [k : k^2]$ .*

*If  $k$  is a perfect field (e.g. if  $k = \mathbb{F}_{2^r}$ , a finite field, or  $k$  is algebraically closed), then*

- (a)  *$q' \simeq U^{\oplus(m-1)} \oplus P^{(c)}$ .*
- (b)  *$s = 0$  or  $s = 1$ . Hence  $\text{rad}(b_q) = \text{rad}(q)$  or  $\text{rad}(b_q) = \langle a \rangle \oplus \text{rad}(q)$ ,  $a \in k^\times$ . In the last case, if  $\text{rad}(q) = 0$ ,  $q$  is semi-unimodular.*

*Proof.* 1. Any symmetric form is an orthogonal direct sum of a non-degenerate form and its radical. Then apply Proposition 8.2.1.

2. For a quadratic space  $(V, q)$  we have  $q' \oplus \text{rad}(b_q)$  where  $q'$  is a non-degenerate quadratic form. By Theorem 8.2.2 and Corollary 8.2.3 it suffices to show 2(b) (both items) and so we may assume that  $V = \text{rad}(b_q)$ . In other words,  $V$  is a maximally degenerate quadratic space. Then the quadratic form is necessarily diagonal with respect to any basis. Our aim is to find an explicit description of such forms. To do this we recall (Lemma 6.1.6) that  $\text{rad}(q) = \{x \in V \mid q(x) = 0\}$  is a  $k$ -linear subspace contained in the radical of  $b_q$ . Consider the tautological map

$$q : V = \text{rad}(b_q) \rightarrow k.$$

For  $x, y \in \text{rad}(b_q)$  we have  $q(x) + q(y) = q(x+y)$ . We also have  $a^2 q(x) = q(a \cdot x)$  for all scalars  $a \in k$ . So  $q(V) \subset k$  is a  $k^2$ -vector space, where  $k^2$  denotes the subfield of squares in  $k$ . Let  $e_1, \dots, e_s \in V$  be a set of vectors such that their classes  $\bar{e}_i$  modulo  $\text{rad}(q)$  form a basis for the  $k$ -vector space  $V/\text{rad}(q)$ . Because  $q(x) = 0$  if and only if  $x \in \text{rad}(q)$ , we see that

$$\sum_{i=1}^s x_i^2 q(e_i) = q\left(\sum_{i=1}^s x_i e_i\right) = 0 \in k \iff \sum_{i=1}^s x_i \bar{e}_i = 0 \iff x_i = 0, i = 1, \dots, s.$$

Hence the  $q(e_i)$  span a  $k^2$ -subspace of  $k$  of dimension  $s$ . Consequently,  $s \leq \dim_{k^2} k$ . If  $k$  is perfect,  $k^2 = k$  and then  $s \leq 1$ .  $\square$

*Remark 8.2.6.* Note that if  $\text{rad}(q) = 0$  and  $\dim V = s$  is odd, the semi-discriminant  $\text{sdisc}(q)$  (see Definition 6.3.3) is non-zero precisely if  $s = 1$ . Hence if  $k$  is perfect and  $b_q = 0$ , but  $q$  is non-degenerate, necessarily  $s = 1$  and the form is semi-unimodular.

**Example 8.2.7.** Let us specialize the above results to the case  $k = \mathbb{F}_2$ . In this case the Artin–Schreier homomorphism is trivial and so the Arf-invariant only takes the values 0 or 1. If the  $k$ -vector space  $V$  has even dimension  $2m$  and the quadratic form  $q$  is non-degenerate,  $q$  is equivalent to  $\sum_{i=1}^m x_i x_{i+m}$  and has Arf invariant 0 (and is isometric to  $\bigoplus^n U$ ) or to  $\sum_{i=1}^m x_i x_{i+m} + x_1^2 + x_2^2$  with Arf invariant 1.

If the  $k$ -vector space  $V$  has odd dimension  $2m + 1$  and  $q$  is semi-unimodular, then  $q$  is equivalent to  $\sum_{i=1}^m x_i x_{i+m} + x_{m+1}^2$ . Otherwise, assuming that  $\text{rad}(q)$  has dimension 1,  $q$  is equivalent to  $\sum_{i=1}^k x_i x_{i+m}$  or to  $\sum_{i=1}^m x_i x_{i+m} + x_1^2 + x_2^2$ .

### 8.3 Classification of Quadratic Inner Product Spaces over Finite Fields

We recall a few facts about finite fields and their extensions. First of all, the multiplicative group of any finite field  $\mathbb{F}_q$  is cyclic of order  $q - 1$ . Secondly, a finite field extension  $K/k$  gives  $K$  a  $k$ -vector space structure  $K \simeq k^m$  for some positive integer  $m$ , and so if  $k = \mathbb{F}_q$  such an extension has  $q^m$  elements and  $K = \mathbb{F}_{q^m}$ .

This field extension is Galois with cyclic Galois group of order  $m$  generated by the **Frobenius automorphism** which sends  $x \in K$  to  $x^q$ . The norm thus equals

$$N_{K/k}(x) = \prod_{k=0}^{m-1} x^{q^k} = x^{\sum_{k=0}^{m-1} q^k} = x^{(q^m-1)/(q-1)}$$

and sends  $K^\times$  onto the subgroup of  $K^\times$  of elements having order dividing  $q - 1$ , which is precisely  $k^\times$ . In particular, the norm map is surjective. For the trace we find

$$\text{Tr}_{K/k}(x) = x + x^q + x^{q^2} + \dots + x^{q^{m-1}}. \tag{8.6}$$

We now come back to norm forms treated in § 6.3.B example 5.

**Example 8.3.1** (Binary norm forms III). A finite field  $k = \mathbb{F}_q$ ,  $q = p^r$ , has a unique (separable) quadratic extension  $K = \mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$ . We shall explain how the norm  $N_{K/k}$  defines a unique isometry class of quadratic forms on the 2-dimensional  $k$ -vector space  $K$ . Any element of  $K$  is of the form  $x + y\xi$  with  $x, y \in k$  and if  $\xi' \in K$  is the conjugate root, then

$$N_{K/k}(x + y\xi) = (x + y\xi)(x + y\xi').$$

Every quadratic form  $q$  on  $k^2$  can be written as  $q(x, y) = ax^2 - bxy + cy^2$  and it is totally anisotropic precisely if it decomposes in some quadratic extension  $K = k(\xi)$  of  $k$  as  $a(x + y\xi)(x + y\xi') = a N_{K/k}(z)$  with  $z = x + y\xi$ , and where  $\xi$  and  $\xi'$  are the roots of  $ax^2 - bx + c = 0$  in  $K - k$ . We proceed with this case. Since the norm map is surjective, there exists an element  $\alpha + \beta\xi \in k(\xi)$  such that  $N(\alpha + \beta\xi) = a \in k$ . Define the  $k$ -linear isomorphism  $F : k^2 \rightarrow k(\xi)$  by  $F(x, y) = (\alpha + \beta\xi)(x + y\xi)$ . Then

$$q(x, y) = ax^2 - bxy + cy^2 = a(x + y\xi)(x + y\xi') = N [(\alpha + \beta\xi)(x + y\xi)]$$

shows that  $F$  is an isometry. So totally anisotropic binary forms are isometric to norm forms.

Note that we have also seen that in characteristic  $p \neq 2$  all forms are diagonalizable. To make the connection, recall Lemma 6.3.9 which gives a criterion for  $ax^2 + cy^2$  to be a norm form: it must be isometric to  $x^2 - \varepsilon y^2$  where  $\varepsilon$  is a non-square.

We consider the case  $p = 2$  in more detail. First a remark about the Artin-Schreier map  $\wp : k \rightarrow k$  given by  $x \mapsto x + x^2$ . This is linear over the prime field  $\mathbb{F}_2$ ,  $\ker(\wp) = \mathbb{F}_2$ , and  $c = \wp(x)$  precisely if  $x \in k$  is a root of the **Artin-Schreier polynomial**  $X^2 + X + c$ . The other solution then is  $x + 1$  so that the polynomial is separable. After a suitable change of variables, any separable degree 2 polynomial becomes Artin-Schreier up to a scalar multiple and any quadratic extension  $K/k$  can thus be given as  $K = k(\xi)$ , where  $\xi$  satisfies an equation  $P(X) = 0$  with  $P(X) = X^2 + X + c$ ,  $c \in k$ , irreducible in  $k[X]$ . We claim that  $\text{Tr}_{k/\mathbb{F}_2} c = 1$  if and only if we are in this situation, i.e. if and only if  $P(X)$  is irreducible in  $k[X]$ . Indeed, if  $X^2 + X + c$  has a root  $u$  in  $k$ , then  $c = u + u^2$  and  $\text{Tr}_{k/\mathbb{F}_2} c = \text{Tr}_{k/\mathbb{F}_2} u + \text{Tr}_{k/\mathbb{F}_2} u^2 = 0$ .



If  $P(X)$  is irreducible, it has a root  $d$  not in  $k$ . Then, using formula (8.6) for the trace, we get

$$\begin{aligned} c + c^2 + c^{2^2} + \cdots + c^{2^{r-1}} &= (d^2 + d) + (d^2 + d)^2 + \cdots + (d^2 + d)^{2^{r-1}} \\ &= (d^2 + d) + (d^{2^2} + d^2) + (d^{2^3} + d^{2^2}) + \cdots + (d^{2^r} + d^{2^{r-1}}) \\ &= d + d^{2^r} = 1, \end{aligned}$$

since if  $d^{2^r} = d$ , then  $d \in k$ . Note that if  $r$  is odd,  $\text{Tr}_{k/\mathbb{F}_2}(1) = \deg(k/\mathbb{F}_2) \bmod 2 = r \bmod 2 = 1$  and then  $X^2 + X + 1$  is an irreducible Artin–Schreier polynomial giving the quadratic extension. For  $r$  even we get  $\text{Tr}_{k/\mathbb{F}_2} 1 = 0$  and in this case it is more complicated to find  $c$  with  $\text{Tr}_{k/\mathbb{F}_2} c = 1$ . See Remark 8.3.2 below. Once  $c$  has been determined, the corresponding binary quadratic form over  $k$  is  $x^2 + xy + cy^2$  with Arf invariant  $c$  which thus is isometric to the binary form  $P^{(c)}$  (see Corollary 8.2.3).

*Remark 8.3.2.* We just explained that to classify quadratic spaces over a finite field of characteristic 2, one needs to specify an element with absolute trace equal to 1 and that for  $k = \mathbb{F}_{2^r}$  with  $r$  odd, one can take  $c = 1$ . To see what happens for  $r$  even, let us first consider the case of  $k$  iterated quadratic extensions, say  $k_0 = \mathbb{F}_2 \subset k_1 = \mathbb{F}_2(s_1) \subset \cdots \subset k_m = k_{m-1}(s_m)$ , where  $s_j$  is a root of an Artin–Schreier polynomial  $X^2 + X + c_j$ . We claim that the product  $c_1 \cdots c_m$  has absolute trace 1. To show this, note that  $\text{Tr}_{k_j/k_{j-1}}(c_j) = 1$  by the choice of  $c_j$  so that recursively

$$\begin{aligned} \text{Tr}_{k_m/k_0}(c_1 \cdots c_m) &= \text{Tr}_{k_m/k_{m-1}}(c_m) \cdot \text{Tr}_{k_{m-1}/k_0}(c_1 \cdots c_{m-1}) \\ &= \text{Tr}_{k_{m-1}/k_0}(c_1 \cdots c_{m-1}) = 1. \end{aligned}$$

For the general case  $r = 2^m s$  with  $s$  odd, we simply write  $k$  as an extension of  $\mathbb{F}_{2^m}$ . Since  $\deg(k/\mathbb{F}_{2^m}) = s$  is odd,  $\text{Tr}_{k/\mathbb{F}_2}(c) = s \text{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(c) = 1$  as well.

**Theorem 8.3.3** (Classification of quadratic inner product spaces over finite fields). *Let  $k$  be a finite field of characteristic  $p$ ,  $K$  the unique quadratic extension field of  $k$  and let  $V$  be a quadratic inner product space over  $k$ .*

- $p \neq 2$
- $\dim V$  even. Then  $V \simeq U^{\oplus m}$  or  $V \simeq U^{\oplus m} \oplus N_{K/k}$ . The form  $N_{K/k}$  is isometric to a diagonal form  $\langle 1 \rangle \oplus \langle -\varepsilon \rangle$  with  $\varepsilon$  a non-square.
  - $\dim V$  odd. Then  $V \simeq U^{\oplus m} \oplus \langle c \rangle$  and there are two isometry classes according to whether  $c \neq 0$  is a square or not. In both cases, the given decomposition is the Witt decomposition and so the Witt index takes only the values  $\frac{1}{2} \dim V$ ,  $\frac{1}{2}(\dim V - 1)$  or  $\frac{1}{2}(\dim V - 2)$ .
- $p = 2$  Then  $\dim V$  is even, and either  $V \simeq U^{\oplus m}$  with zero Arf invariant, or  $V \simeq U^{\oplus m} \oplus N_{K/k}$  with non-zero Arf invariant. More precisely, if  $K = k(\xi)$  with  $\xi^2 + \xi + c = 0$ , then  $N_{K/k}$  is isometric to the binary form  $cx^2 + xy + cy^2$  with Arf invariant  $c^2 \equiv c \pmod{\wp(k)}$ .

*Proof.* For odd characteristics this follows from the Witt decomposition (Proposition 7.2.10) and Example 8.3.1, provided we show that a totally anisotropic space  $V'$  has dimension  $\leq 2$ . This can be seen as follows. Let  $q$  be the restriction of the quadratic form to a totally anisotropic subspace  $V'$  and suppose that  $\dim V' \geq 3$ . Then by Theorem 8.1.1, we can write  $V' = W_1 \oplus W_2$  with  $\dim W_1 = 2$  and  $\dim W_2 \geq 1$ . Pick any vector  $y \in W_2$  with  $q(y) = b \neq 0$ . The binary form  $q|_{W_1}$  being totally anisotropic implies that it is a norm form. As we showed in the just mentioned Example 8.3.1, the norm map  $N_{K/k}$  is surjective, and so we can find  $z \in W_1$  such that  $q(z) = -b$ . Then  $z + y$  is an isotropic vector, contradicting the assumption  $V'$  is totally anisotropic.

For characteristic 2 the statement follows from Corollary 8.2.3 and the previous example, since a finite field of characteristic 2 is perfect.  $\square$

There is an alternative normal form which turns out to be useful for later purposes (cf., e.g., Section 9.4):

**Corollary 8.3.4.** *If  $p \neq 2$  every quadratic inner product space  $(V, q)$  over  $\mathbb{F}_p$  of rank  $m$  is isometric to  $\langle 1 \rangle^{\oplus m}$  if  $\text{disc}(q) = 1$  and to  $\langle 1 \rangle^{\oplus m-1} \oplus \langle \epsilon \rangle$  if  $\text{disc}(q) = \epsilon$ , a non-square modulo  $\mathbb{F}_p$ .*

*Proof.* By Theorem 8.1.1, quadratic forms are all diagonalizable in this situation and hence isometric to  $\langle 1 \rangle^{\oplus s} \oplus \langle \epsilon \rangle^{\oplus t}$ , where  $\epsilon$  is a non-square in  $\mathbb{F}_p$ . This can be further reduced since the plane  $\langle \epsilon \rangle \oplus \langle \epsilon \rangle$  is isometric to the plane  $\langle 1 \rangle \oplus \langle 1 \rangle$ . To see this, note that the equation  $\epsilon(x^2 + y^2) = 1$  has a solution  $(a, b)$  in the finite field  $\mathbb{F}_p$  as one sees by using the shoebox principle (cf., e.g., Example A.4.2). But then  $\epsilon[(ax' + by')^2 + (bx' - ay')^2] = (x')^2 + (y')^2$ . The result then follows.  $\square$

*Remark 8.3.5.* Recall that in characteristic 2 several non-isometric quadratic forms have isometric polar forms and so the classification of symmetric inner product spaces is simpler than that of quadratic inner product spaces: Proposition 8.2.1 implies that inner product spaces over  $\mathbb{F}_{2^r}$  are isometric to  $\langle u^{(1)} \rangle \oplus \dots \oplus \langle u^{(a)} \rangle \oplus U^{\oplus b}$ , where  $u^{(j)} \in \mathbb{F}_{2^r}^\times$ ,  $j = 1, \dots, a$ .

**Historical and Bibliographical Notes.** For J. Sylvester’s proof of the theorem named after him see [221].

The proofs in this chapter have been inspired by Chapter IV in M. Kneser’s lecture notes [122]. Our treatment of the Arf invariant closely follows the exposition [58] of R. Dye. For the original work by C. Arf, see [3].

---

## Symmetric and Quadratic Torsion Groups

### Introduction

Recall that a torsion group splits canonically as a direct sum of  $p$ -primary groups yielding the Sylow decomposition. A  $p$ -primary group decomposes (non-canonically) as a direct sum of homogeneous forms, which is called a Jordan decomposition. All of this is recalled in Appendix A.1.

Torsion forms equipped with  $\mathbb{Q}/\mathbb{Z}$ -valued forms have been introduced before, in Section 1.9. Especially the torsion forms on  $p$ -primary cyclic groups have been enumerated before. See the summary in Table 6.1.1.

The aim of this chapter is to reduce the general classification to  $p$ -primary forms and subsequently to homogeneous ones. To this end, in Section 9.1 we first consider symmetric and quadratic torsion modules over general principal ideal domains and introduce an invariant, the reduced discriminant, which plays a central role in the classification.

Returning to symmetric and quadratic torsion groups, in Section 9.2 we first prove the orthogonal nature of the Sylow decomposition. This implies that the classification can be done prime by prime. The main result for  $p$ -primary torsion forms, established in Section 9.3, is the existence of a Jordan splitting, which, as opposed to a mere Jordan decomposition, is an orthogonal direct sum decomposition into indecomposable homogeneous forms. The latter are described in Section 9.4. Although this results in a splitting of torsion symmetric and quadratic forms into simple building blocks, different splittings may lead to isometric forms.

### 9.1 Generalities on Symmetric and Quadratic Torsion Modules

In this section  $R$  is a principal ideal domain with fraction field  $Q(R)$  and  $G$  a finitely generated torsion  $R$ -module with elementary divisors  $\{d_1, \dots, d_r\}$ .

**9.1.A Gram matrices.** Since  $R$  is a principal ideal domain,  $G$  is a direct sum of cyclic  $R$ -modules, that is,  $R$ -modules of the form  $R/aR$  for some non-zero  $a \in R$ . The dual of  $G$  is the  $R$ -module  $G_{Q(R)/R}^* = \text{Hom}_R(G, Q(R)/R)$  (see formula (6.1)). We claim that cyclic  $R$ -modules are isomorphic to their duals by considering the map

from  $R/aR$  to its dual given by

$$[x] \mapsto f_{[x]}, \quad f_{[x]}([y]) = a^{-1} \cdot xy \text{ mod } R,$$

where  $x, y \in R$  and  $[x], [y]$  are their classes in  $R/aR$ . One checks that this is well defined and gives an  $R$ -morphism. The claim then follows if we show that  $f_{[x]}$  is injective and surjective. Injectivity is clear: if  $f_{[x]}(1) = a^{-1}x = 0$  in  $Q(R)/R$ , then  $x = 0$  in  $R/aR$ . Surjectivity is slightly more involved. Pick  $f \in \text{Hom}(R/aR, Q(R)/R)$  and write  $f([1]) = p/q \text{ mod } R$ . Since

$$0 = f(0) = f([a]) = af([1]) = ap/q \text{ mod } R,$$

$q$  must divide  $ap$  in  $R$ , that is,  $ap = bq$  for some  $b \in R$ . Hence in the quotient field  $Q(R)$  one has  $p/q = b/a$  so that  $f([1]) = b/a \text{ mod } R$ . This means precisely that  $f = f_{[b]}$ .

We apply these considerations to the invariant factor decomposition of  $G$ :

**Lemma 9.1.1.** *The torsion module  $G$  is isomorphic to its dual  $G_{Q(R)/R}^*$ . Let*

$$G \simeq \bigoplus_{j=1}^r R/d_j R, \quad d_1 | d_2 | \cdots | d_r$$

be the invariant factor decomposition with corresponding generators  $e_1, \dots, e_r$ . Then the isomorphism  $G \xrightarrow{\cong} G_{Q(R)/R}^*$  can be chosen such that  $e_j$  maps to the function  $u_j^* \in G_{Q(R)/R}^*$  for which  $u_j^*(e_i) = d_j^{-1} \delta_{ij} \in Q(R)/R$ .

The invariant factor decomposition for  $G$  leads to a useful concept:

**Definition 9.1.2.** An *ordered basis* of  $G$  is a system of generators  $e_1, \dots, e_r$  of  $G$  adapted to the elementary divisors  $\{d_1, \dots, d_r\}$  ordered in such a way that  $d_1 | d_2 | \cdots | d_r$  as in the above lemma.

Using an ordered basis  $\mathbf{E} = \{e_1, \dots, e_r\}$  for  $G$ , a symmetric bilinear form  $b : G \times G \rightarrow Q(R)/R$  can be described by the Gram matrix with respect to  $\mathbf{E}$  which, we recall, has entries  $b(e_i, e_j)$  in  $Q(R)/R$ . Generalizing the observation leading to (1.14) in Chapter 1, the following result is evident:

**Lemma 9.1.3.** *Let  $B' = (B_{ij})$  be a symmetric  $r \times r$  matrix with entries in the field  $Q(R)$ . Then  $B = B' \text{ mod } R$  is the Gram matrix of a symmetric torsion form on  $G$  relative to an ordered basis for  $G$  adapted to the elementary divisors  $\{d_1, \dots, d_r\}$  if and only if  $d_i B_{ij} \in R$  and  $d_j B_{ij} \in R$  for  $i, j = 1, \dots, r$ . In other words, using that  $d_1 | d_2 | \cdots | d_r$ , this is the case if and only if  $B'$  has the form*

$$B' = (B_{ij}) = \begin{pmatrix} \frac{A_{11}}{d_1} & \frac{A_{12}}{d_1} & \cdots & \frac{A_{1r}}{d_1} \\ \frac{A_{21}}{d_1} & \frac{A_{22}}{d_2} & \cdots & \frac{A_{2r}}{d_2} \\ \vdots & \ddots & \vdots & \vdots \\ \frac{A_{r1}}{d_1} & \frac{A_{r2}}{d_2} & \cdots & \frac{A_{rr}}{d_r} \end{pmatrix} \quad \text{with } A_{ij} = A_{ji} \in R. \quad (9.1)$$

**Corollary 9.1.4.** *Let  $B' = (B_{ij})$  represent a Gram matrix of a symmetric  $R$ -torsion form  $b$  on  $G$  relative to an ordered basis corresponding to the elementary divisors  $d_1, \dots, d_r$  of  $G$  as in Lemma 9.1.3. Then*

1.  $d_1 \cdots d_r \cdot \det B \in R$ ;
2. if  $b$  is non-degenerate, then  $d_1 \cdots d_r \cdot \det B$  is relatively prime to  $d_1$ .

*Proof.* 1. The entries of the matrix  $C = (d_i B_{ij})$  (obtained by multiplying the  $i$ -th row of  $B$  with  $d_i$  for all  $i = 1, \dots, r$ ) belong to  $R$  and hence  $d_1 \cdots d_r \det B = \det(d_i B_{ij}) = \det C \in R$ .

2. This can be seen as follows. Let  $p$  be an irreducible divisor of  $d_1$  so that  $p$  divides all  $d_i$ . Assume that  $p$  divides  $\det C$  as well. Then there exists an element  $x = (x_1, \dots, x_r) \in R^r$  such that  $xC = 0$  in  $(R/pR)^r$  and there exists an index  $j$  for which  $x_j$  is not divisible by  $p$ . In particular,  $d_j/p \cdot x_j \notin d_j R$  so that the element  $e = \sum_i d_i p^{-1} x_i e_i \in G$  is not the zero-element, while for all  $k = 1, \dots, r$ ,

$$b(e, e_k) = b\left(\sum_i d_i p^{-1} x_i e_i, e_k\right) = p^{-1} \sum_i x_i d_i B_{ik} = 0 \pmod{R}$$

since by assumption  $xC \in (pR)^r$ , and so  $e \in \ker b$ , contradicting the assumption that  $b$  is non-degenerate.  $\square$

**9.1.B The reduced discriminant.** We next introduce discriminant-like invariants for non-degenerate symmetric  $R$ -torsion modules. We use the same notation as above. Because  $b$  is non-degenerate,  $d_1 \cdots d_r \cdot \det B \in R$  is relatively prime to  $d_1$ , but depends on the choice of an ordered basis. Since  $d_1$  divides all  $d_j$ , the entries of  $B$  are in any case well determined up to a multiple of  $d_1$  and so we consider  $d_1 \cdots d_r \cdot \det B$  in  $D(R/d_1 R)$ . We shall now show that the result does not depend on choices. Write  $G$  as quotient of a free  $R$ -module  $L$  on the ordered basis  $\mathbf{E}$  of  $G$ . It suffices to investigate what happens under changes of basis of  $L$  that induce changes of generators of  $G$ . Such a change corresponds to an  $R$ -isomorphism  $f : G \rightarrow G$  and an  $R$ -isomorphism  $\tilde{f} : L \rightarrow L$  inducing  $f$ . For a given irreducible element  $p|d_1$  the isomorphism  $f$  sends  $pG$  isomorphically to itself and so it induces an  $R/pR$ -homomorphism  $f_p$  of the quotient  $R/pR$ -module  $G/pG$  which, by the definition of  $L$ , is an  $R/pR$ -isomorphism. This gives a commutative diagram

$$\begin{array}{ccc} L/pL & \xrightarrow{\cong} & G/pG \\ \tilde{f}_p \downarrow & & f_p \downarrow \cong \\ L/pL & \xrightarrow{\cong} & G/pG \end{array}$$

where  $\tilde{f}_p$  is induced by  $\tilde{f}$  and  $f_p$  by  $f$ . It follows that  $\tilde{f}_p$  is an isomorphism as well and so  $\det \tilde{f}$  cannot be divisible by  $p$ . In other words  $\det \tilde{f}$  is relatively prime to  $d_1$ . Let  $M$  be the matrix of  $\tilde{f}$  in the basis  $\mathbf{E}$  and let  $B'$  be the matrix of the discriminant bilinear form with respect to the new basis  $f(\mathbf{E})$ . Then

$$d_1 \cdots d_r \cdot \det B' = d_1 \cdots d_r \cdot (\det M)^2 \cdot \det B, \quad \det M \in (R/d_1 R)^\times.$$

It follows that

$$\delta(b) = d_1 \cdots d_r \cdot \det B \in D(R/d_1 R) \quad (9.2)$$

is well defined. We call it the *reduced discriminant of the torsion symmetric form  $b$* .

For a quadratic torsion form  $(G, q)$  we consider its polar form  $b_q$ . Since the diagonal elements  $B_{ii}$  in Lemma 9.1.3 are well defined modulo  $2R$ , as a consequence,

$$\delta(q) := \delta(b_q) \in D(R/[\gcd(2, d_1)d_1] \cdot R)$$

is a well-defined invariant of  $q$ , the *reduced discriminant of the torsion quadratic form  $q$* . For examples, see Table 9.1.1.

**Lemma 9.1.5.** *Let  $(G, b)$ ,  $(G', b')$  be two non-degenerate  $p$ -primary bilinear torsion forms<sup>1</sup> and let  $p^a, p^{a'}$  be the first elementary divisors of  $G$ , respectively  $G'$ . Then the reduced discriminant of  $G \oplus G'$  is the product  $\delta(b) \cdot \delta(b')$  considered in  $D(R/p^c R)$ ,  $c = \min(a, a')$ , under the homomorphism which is induced by multiplication*

$$R/p^a R \times R/p^{a'} R \longrightarrow R/p^c R.$$

*Proof.* Choose an ordered basis  $\mathbf{E}$  for  $G$  and  $\mathbf{E}'$  for  $G'$ . The Gram matrix for  $b \oplus b'$  with respect to  $\mathbf{E} \cup \mathbf{E}'$  is a block matrix, say  $C = \begin{pmatrix} B & 0 \\ 0 & B' \end{pmatrix}$  with determinant  $\det B \cdot \det B'$ . In general the chosen basis is not an ordered basis for  $G \oplus G'$ : one might have to exchange some basis elements of  $\mathbf{E}$  against some from  $\mathbf{E}'$ , but this does not change  $\det C$  since in this process any permutation of columns occurs together with a corresponding permutation of rows. This implies that  $\delta(b \oplus b') = |G \oplus G'| \cdot \det C \in D(R/p^c R)$ , where  $c$  is the first elementary divisor of  $G \oplus G'$ . Since  $c = \min(a, a')$ , one finds  $\delta(b \oplus b') = (|G| \cdot \det B) \cdot (|G'| \cdot \det B') = \delta(b)\delta(b') \in D(R/p^c R)$  as desired.  $\square$

**Example 9.1.6.** Suppose  $R = \mathbb{Z}$  and consider the case of a homogeneous  $p$ -primary discriminant group  $G$  of exponent  $k$ . The reduced discriminant uses the group  $D(\mathbb{Z}/p^k \mathbb{Z})$  of the units in  $\mathbb{Z}/p^k \mathbb{Z}$  modulo squares. The latter group is well known, see Lemma A.1.5 in Appendix A.

In the case of an odd prime  $p$  both  $\delta(b)$  and  $\delta(q)$  belong to the same group. Indeed, for all  $k$ , the group  $D(\mathbb{Z}/p^k \mathbb{Z})$  is cyclic and generated by a non-square modulo  $p$ , say  $\epsilon_p$ . More precisely, multiplication by  $p^{k-1}$  induces an isomorphism

$$D(\mathbb{Z}/p^k \mathbb{Z}) \xrightarrow{\sim} D(\mathbb{Z}/p \mathbb{Z}) \simeq D(\mathbb{F}_p) = \{1, \epsilon_p\}. \quad (9.3)$$

This implies that for all  $p$ -primary symmetric or quadratic torsion forms, the reduced discriminant is either 1 or  $\epsilon_p$ .

For  $p = 2$ , this is more involved. Observe however, that for a symmetric or quadratic form on a cyclic group of order  $2^k$ , the reduced discriminant is precisely

<sup>1</sup>See Appendix A.1 for background on torsion forms over principal ideal domains.

the unit used to classify such a form as we see from Table 6.1.1. So, only if cyclic groups of order 2 or 4 are present, the reduced discriminant for symmetric and quadratic forms may differ. The following table gives the invariants for the basic building blocks.

Table 9.1.1: Representatives of the reduced discriminant

$p$	$k$	$b^\#$	$\delta(b^\#)$	$q^\#$	$\delta(q^\#)$
odd	$k \geq 1$	$\langle u \cdot p^{-k} \rangle$	$\bar{u} \in \{1, \epsilon_p\}$	$[\frac{1}{2}u \cdot p^{-k}]$	$\bar{u} \in \{1, \epsilon_p\},$
$p = 2$		$\langle u \cdot 2^{-1} \rangle$	$u \equiv 1 \pmod 2$	$[u \cdot 2^{-2}]$	$u \equiv 1, 3 \pmod 4$
$p = 2$		$\langle u \cdot 2^{-2} \rangle$	$u \equiv 1, 3 \pmod 4$	$[u \cdot 2^{-3}]$	$u \equiv \pm 1, \pm 3 \pmod 8$
$p = 2$	$k \geq 3$	$\langle u \cdot 2^{-k} \rangle$	$u \equiv \pm 1, \pm 3 \pmod 8$	$[u \cdot 2^{-k-1}]$	same as for bil. form
$p = 2$		$u_1, v_1$	$1 \pmod 2$	$u_1, v_1$	$3 \pmod 4$
$p = 2$		$u_2, v_2$	$3 \pmod 4$	$u_2, v_2$	$-1, 3 \pmod 8,$
$p = 2$	$k \geq 3$	$u_k, v_k$	$-1, 3 \pmod 8$	$u_k, v_k$	same as for bil. form

## 9.2 The Sylow Decomposition

From now on we assume that  $G$  is a finite abelian group. We shall write the group operation additively so that we consider  $G$  as a torsion  $\mathbb{Z}$ -module.

Consider the Sylow decomposition

$$G = \bigoplus_{p \text{ prime}} G_p, \quad G_p = \{x \in G \mid p^n \cdot x = 0 \text{ for some prime power } p^n\}.$$

We claim that if  $b$  is non-degenerate,  $b|_{G_p}$  is also non-degenerate and that the Sylow decomposition is orthogonal. To show the claim, suppose that  $x \in G_p$  is such that  $b(x, G_p) = 0$ . Then  $x$  is also orthogonal to all  $G_q$  for all primes  $q$  with  $q \neq p$ . To see this, note that for a suitable power  $p^k$  of  $p$  and  $z \in G_q$  we have  $0 = b(p^k x, z) = p^k b(x, z)$ , which implies that  $b(x, p^k z) = p^k b(x, z) = 0$  and so  $p^k z$  is orthogonal to  $x$ . Since  $p$  is invertible in  $G_q$ , also  $z$  is orthogonal to  $x$ . In other words,  $b(x, G) = 0$  and so, since  $b$  is non-degenerate,  $x = 0$ , which shows that  $b|_{G_p}$  is non-degenerate.

Next, observe that for  $x, y \in G_p$  with  $p^k x = p^\ell y = 0$  we have  $0 = b(p^k x, p^\ell y) = p^{k+\ell} b(x, y) \in \mathbb{Q}/\mathbb{Z}$  and so  $b|_{G_p}$  takes values in  $\mathbb{Q}^{(p)}/\mathbb{Z}$ , where we recall that  $\mathbb{Q}^{(p)}$  consists of those rational numbers whose denominator is a  $p$ -power. Using the isomorphism  $\mathbb{Q}^{(p)}/\mathbb{Z} \simeq \mathbb{Q}_p/\mathbb{Z}_p$ , we thus get a  $p$ -primary symmetric torsion form. Summarizing, we have shown:

**Proposition 9.2.1.** 1. *There is a commutative diagram*

$$\begin{array}{ccc}
 G \times G & \xrightarrow{b} & \mathbb{Q}/\mathbb{Z} \\
 \uparrow & & \uparrow \\
 G_p \times G_p & \xrightarrow{b|_{G_p}} & \mathbb{Q}^{(p)}/\mathbb{Z} \xrightarrow{\simeq} \mathbb{Q}_p/\mathbb{Z}_p.
 \end{array}$$

*In particular,  $(G_p, b|_{G_p})$  is in a natural way a  $p$ -primary symmetric torsion group.*

2. *The Sylow decomposition is orthogonal, i.e.  $(G, b) = \oplus_p(G_p, b|_{G_p})$ .*

Similar considerations hold for quadratic torsion forms  $(G, q)$ , where the polar form  $b_q$  is used. Since  $q(x) = \frac{1}{2}b_q(x, x)$ , the values  $q(x)$  for  $x \in G_p$  belong to  $\frac{1}{2}\mathbb{Q}^{(p)}/\mathbb{Z} \simeq \frac{1}{2}\mathbb{Q}_p/\mathbb{Z}_p$  which is isomorphic to  $\mathbb{Q}_p/\mathbb{Z}_p$  if  $p$  is odd, since then 2 is a unit in  $\mathbb{Z}_p$ . For  $p = 2$  we have  $\frac{1}{2}\mathbb{Q}^{(2)}/\mathbb{Z} = \mathbb{Q}^{(2)}/\mathbb{Z}_2 \simeq \mathbb{Q}_2/\mathbb{Z}_2$ . So for quadratic forms the diagram of Proposition 9.2.1 becomes

$$\begin{array}{ccc}
 G & \xrightarrow{q} & \mathbb{Q}/\mathbb{Z} \\
 \uparrow & & \uparrow \\
 G_p & \xrightarrow{q} & \frac{1}{2}\mathbb{Q}^{(p)}/\mathbb{Z} \xrightarrow{\simeq} \mathbb{Q}_p/\mathbb{Z}_p.
 \end{array}$$

Hence also  $(G_p, q|_{G_p})$  is in a natural way a  $p$ -primary quadratic torsion group and one has an orthogonal Sylow decomposition  $(G, q) = \oplus_p(G_p, q|_{G_p})$ .

### 9.3 Jordan Splittings for $p$ -primary Torsion Groups

The Sylow decomposition reduces classification to that of the  $p$ -primary torsion groups, the subject of this section. The proofs are valid in the context of principal ideal domains but we restrict the discussion to  $R = \mathbb{Z}$  and leave it to the reader to make the necessary changes in the general case.

**9.3.A The Jordan decomposition.** Suppose that  $G$  is a  $p$ -primary torsion group, that is, a direct sum of cyclic groups of order a power of  $p$ . Grouping the cyclic submodules of order  $p^k$  together gives  $H_k$ , the **homogeneous summand of exponent  $k$** , leading to a **Jordan decomposition**  $G = \oplus_{k=1}^s H_k$ . Recall (cf. Appendix A.1) that the elementary divisors of  $G$  are the powers of  $p^k$  for which  $H_k \neq \{0\}$  and that the length of  $H_k$  is the number of elementary divisors equal to  $p^k$ . In particular, this is an invariant of the group  $G$ . However, a Jordan decomposition itself is not intrinsically associated to the torsion group (but see



Section 9.3.C for a canonically associated filtration). Also, it is in general not an orthogonal one.

We shall follow a path which after several steps yields an orthogonal Jordan decomposition. The first step concerns the behavior of the form with regards to the Jordan decomposition:

**Lemma 9.3.1.** *1. Let  $(H, b)$  be a symmetric form on a homogeneous  $p$ -primary torsion group of exponent  $k$ . Then the Gram matrix of  $b$  with respect to an ordered basis is represented by*

$$B = p^{-k}A, \quad A = (A_{ij}), \quad A_{ij} = A_{ji} \in \mathbb{Z}, \quad (9.4)$$

*and  $b$  is non-degenerate if and only if  $\det(A)$  is relatively prime to  $p$ .*

*2. Let  $(G, b)$  be a symmetric form on a  $p$ -primary group  $G$  with Jordan decomposition  $G = \bigoplus_{k=1}^s H_k$ . If  $b$  is non-degenerate, the restriction of  $b$  to each homogeneous summand  $H_k$  is non-degenerate.*

*Proof.* 1. By Lemma 9.1.3 the Gram matrix of  $b$  has the indicated shape. By Corollary 9.1.4, if  $b$  is non-degenerate, the determinant of  $A$  is prime to  $p$ . To show the converse, observe that the matrix of the correlation morphism  $b_G$  with respect to an ordered basis  $\{e_1, \dots, e_r\}$  and the "dual" basis  $\{u_1^*, \dots, u_r^*\}$  (cf. Lemma 9.1.1) is precisely  $A$ . Indeed, since  $u_j^*(e_i) = p^{-k}\delta_{ij}$ , we see that  $b_G(e_i) = \sum A_{ik}u_k^*$ . So, if  $\det(A)$  is relatively prime to  $p$ , then  $b_G$  is injective and hence  $b$  is non-degenerate. 2. To prove this we reduce the situation so that item 1 applies. Let  $B$  be the Gram matrix of  $b$  with respect to an ordered basis of  $G$  which respects the Jordan decomposition. From Lemma 9.1.3 we see that  $B$  has a corresponding block decomposition with blocks  $p^{-k}\tilde{A}_{kk}$  on the diagonal and with off-diagonal blocks  $p^{-k}\tilde{A}_{jk}$  for  $j > k$  and  $p^{-j}\tilde{A}_{jk}$  for  $j < k$ . The matrices  $\tilde{A}_{ij}$  have entries in  $\mathbb{Z}$ . Next we study  $|G|\det(B)$ . Multiplying every column of  $B$  by the corresponding elementary divisor we see that every entry in every block corresponding to the positions of  $\tilde{A}_{jk}$  ( $j < k$ ) is divisible by  $p$ . Hence we obtain a matrix which modulo  $p$  has zero blocks above the diagonal blocks and so has determinant  $\prod_k \det \tilde{A}_{kk}$  modulo  $p$ . On the other hand, this determinant equals  $|G| \cdot \det B$ . Hence, if  $b$  is non-degenerate, by Corollary 9.1.4 the product  $\prod_k \det \tilde{A}_{kk}$  must be relatively prime to  $p$  and so each of the factors  $\det \tilde{A}_{kk}$  is relatively prime to  $p$ . By 1 this implies that  $b|_{H_k}$  is non-degenerate.  $\square$

For quadratic torsion forms special phenomena can occur as illustrated in the following example.

**Example 9.3.2** (Exponent 1). The two cases  $p$  odd and  $p = 2$  have a different flavour. For odd  $p$  a non-degenerate quadratic form on a  $p$ -primary group of exponent 1 takes values in  $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ , but in  $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$  if  $p = 2$ . Hence in the first case, since  $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{F}_p$ , the torsion module  $(G, q)$  is isometric to an inner product space over  $\mathbb{F}_p$  and, as we have seen (cf. Corollary 8.3.4), there are two isometry types according to  $\text{disc}(q)$  being a square or not. In terms of  $p$ -primary lattices, either  $q \simeq \bigoplus^{\ell(G)} \langle p^{-1} \rangle$  or  $q \simeq \bigoplus^{\ell(G)-1} \langle p^{-1} \rangle \oplus \langle u \cdot p^{-1} \rangle$  where  $u$  is a non-square modulo  $p$ .

For  $p = 2$  this is no longer the case. Referring to the discussion after Definition 1.7.2, there are essentially two types, the type I forms which can be considered as quadratic  $\mathbb{F}_2$ -spaces whose isometry type is determined by the Arf invariant, and the type II forms, the non-degenerate  $\mathbb{Z}/4\mathbb{Z}$ -valued forms assuming at least one value in  $\mathbb{Z}/4\mathbb{Z} - 2\mathbb{Z}/4\mathbb{Z}$ . The latter forms can have several isometry types, as we shall see later (cf. Table 11.2.2).

**9.3.B Homogeneous symmetric torsion groups.** Here we perform the second step of our procedure which consists in relating the exponent  $k$  case to exponent 1. So we let  $(G, b)$  be a homogeneous  $p$ -primary symmetric torsion group of exponent  $k$ . Note that  $b$  takes values in  $p^{-k}\mathbb{Z}/\mathbb{Z}$  since for  $x, y \in G$  we have  $p^k b(x, y) = b(p^k x, y) = 0 \pmod{\mathbb{Z}}$ . The following procedure  $\rho$  yields a symmetric torsion group  $(\rho(G), \rho(b))$  of exponent 1:

$$\begin{aligned} \rho : G &\rightarrow G/pG, & x &\mapsto [x] = x \pmod{pG} \\ \rho(b)([x], [y]) &= & p^{k-1}b(x, y) &\in p^{-1}\mathbb{Z}/\mathbb{Z}. \end{aligned} \tag{9.5}$$

During this simplifying procedure of multiplying the form by  $p^{k-1}$  one does not lose essential information about non-degeneracy as we shall see.

The reduced discriminant  $\delta(b) \in D(\mathbb{Z}/p^k\mathbb{Z})$  is defined by means of formula (9.2). If  $p$  is odd, by (9.3), multiplication with  $p^{k-1}$  induces an isomorphism and identifies  $\delta(b)$  with  $\delta(\rho(b)) \in D(\mathbb{Z}/p\mathbb{Z})$ . This invariant can also be viewed as  $\text{disc}(\rho(b)) \in D(\mathbb{F}_p)$  provided we identify  $\mathbb{Z}/p\mathbb{Z}$  with the field  $\mathbb{F}_p$ . The form  $\rho(b)$  reflects the non-degeneracy of  $b$ :

**Lemma 9.3.3.** *If  $G$  is a homogeneous  $p$ -primary group of exponent  $k$  equipped with a symmetric  $p$ -primary torsion form  $b$ , then  $(G, b)$  is non-degenerate if and only if  $\rho(b)$  is. More precisely,  $b \simeq p^{-k} \cdot b'$  where  $b'$  is unimodular and is (under suitable identifications) isometric to  $\rho(b)$ .*

*In that case, if  $H$  splits off orthogonally, then so does  $\rho(H)$  and conversely.*

*Proof.* First of all, by (9.4), the Gram matrix of  $b$  with respect to an ordered basis  $\mathbf{E}$  of  $G$  (cf. Definition 9.1.2) is of the form  $p^{-k}A$ , where  $A$  has its entries in  $\mathbb{Z}$ , and so the Gram matrix of  $\rho(b)$  with respect to the basis  $\rho(\mathbf{E})$  for  $\rho(G)$  is  $p^{-1}A$ . Secondly, by Lemma 9.3.1,  $b$  is non-degenerate if and only if  $\gcd(\det A, p) = 1$ . The form  $\rho(b)$  is non-degenerate if and only if the same condition holds.

Suppose that  $G = H \oplus K$ , then, by the definition of  $\rho(b)$ , one has  $\rho(G) = \rho(H) \oplus \rho(K)$ . Conversely, if  $\rho(G) = \rho(H) \oplus \tilde{K}$  and if  $b|_H$  has Gram matrix  $p^{-k} \cdot B$ , then  $\rho(H)$  has Gram matrix  $p^{-1} \cdot B$ . Since  $\rho(b|_H)$  is non-degenerate,  $b|_H$  is non-degenerate and so  $H$  splits off orthogonally, say  $G = H \oplus H'$ . But then  $\rho(H') = \tilde{K}$  and so the splitting  $G = H \oplus H'$  induces the given splitting of  $\rho(G)$ .  $\square$

**9.3.C Final step for the symmetric case.** We combine the previous results to achieve our goal, an orthogonal Jordan decomposition for a not necessarily homogeneous  $p$ -primary group  $G$ .

We start with a purely group theoretic fact, the existence of a canonical filtration  $G_1 \subset G_2 \subset \cdots \subset G$  of  $G$  by subgroups  $G_m$  and associated quotient groups  $\rho_m G$ :

$$G_m = \{a \in G \mid p^m \cdot a = 0\}$$

$$\rho_m G = G_m / (G_{m-1} + pG_{m+1}).$$

To see that the second group makes sense, first of all note that  $G_{m-1} \subset G_m$ . Secondly, since for  $x \in G_{m+1}$  one has  $0 = p^{m+1}x = p^m(px)$ , we obtain the inclusion  $pG_{m+1} \subset G_m$ .

**Example 9.3.4.** Let  $T$  be the 2-primary group with generators  $e_1, e_2, e_3$  of orders 4, 4, 16, respectively. Thus  $T$  is isomorphic to  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ . Here  $T_4 = T$  and

$$T_3 = \langle e_1, e_2, 2e_3 \rangle \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z},$$

$$T_2 = \langle e_1, e_2, 4e_3 \rangle \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},$$

$$T_1 = \langle 2e_1, 2e_2, 8e_3 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

We see that indeed  $2T_4 \subset T_3$ ,  $2T_3 \subset T_2$  and  $2T_2 = T_1$ . The quotients  $T_4/T_3 \simeq \mathbb{Z}/2\mathbb{Z}$  and  $T_2/(T_1 + 2T_3) \simeq \mathbb{Z}/2\mathbb{Z}^{\oplus 2}$  "pick out" the two homogeneous summands  $\mathbb{Z}/16\mathbb{Z}$ , respectively  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ . The remaining quotients  $\rho_3(T)$  and  $\rho_1(T)$  are zero.

Let us first state some elementary properties of this construction:

**Lemma 9.3.5.** *Let  $G$  be a  $p$ -primary torsion group.*

1. *If  $G$  is a homogeneous group of exponent  $k$ , then  $\rho_k(G)$  coincides with  $\rho(G)$  as in (9.5).*
2. *Every  $\rho_k$  is additive on direct sums.*
3. *If  $G = \oplus H_m$  with  $H_m$  homogeneous of exponent  $m$ , then  $\rho_k(G) = \rho_k(H_k) = \rho(H_k)$  for every  $k$ .*

*Proof.* 1. If  $G$  is homogeneous of exponent  $k$ , then  $G_k = G_{k+1} = G$ ,  $G_{k-1} = pG$  and so  $\rho_k G = G/pG = \rho(G)$ .

2. This is clear.

3. If  $G$  is homogeneous of exponent  $s$  and  $k < s$ , then  $G_k = pG_{k+1}$  and so  $\rho_k(G) = 0$ . Therefore  $\rho_k(G) = 0$  if  $k \neq s$ . Since  $\rho_k$  is additive on direct sums, the result follows.  $\square$

This result implies that, as in the previous example,  $\rho_k$  picks out the exponent  $k$  piece of  $G$  (in any decomposition) and replaces it with an exponent 1 group of the same rank.

We next investigate the behavior of a (non-degenerate) symmetric torsion form  $b$  on  $G$ . As in the homogeneous case  $b$  induces a  $p^{-1}\mathbb{Z}/\mathbb{Z}$ -valued form on  $\rho_k G$

analogous to the one in (9.5). Explicitly, if  $[x]$  is the coset containing  $x \in G_k$  we put for  $x, y \in G_k$

$$\rho_k(b)([x], [y]) := p^{k-1}b(x, y).$$

That this is well defined in this setting follows from

$$p^{k-1}b(x, y) = \begin{cases} b(p^{k-1}x, y) = 0 & \text{if } x \in G_{k-1} \\ b(p^{k-1}(pz), y) = b(z, p^k y) = 0 & \text{if } x = pz \in pG_{k+1}. \end{cases} \quad (9.6)$$

Let us tie this in with what we have seen in Lemma 9.3.1 for Gram matrices for  $p$ -primary torsion groups. Just as in that lemma we see: only the blocks on the diagonal matter!

**Lemma 9.3.6.** *Let  $(G, b)$  be a  $p$ -primary symmetric torsion group with Jordan decomposition  $G = \oplus H_k$ .*

1. *If  $b$  is non-degenerate, then  $\rho_k(b)$  is non-degenerate for all  $k$ .*
2. *If  $\rho_k(b)$  is non-degenerate, then  $b|_{H_k}$  is non-degenerate.*

*Proof.* 1. The Gram matrix of  $b|_{H_k}$  with respect to a system  $\mathbf{E}$  of generators of  $H_k$  can be written as  $p^{-k} \cdot A_k$  with  $A_k$  a symmetric matrix with entries in  $\mathbb{Z}$ . Then the Gram matrix of  $\rho_k$  with respect to  $\rho_k(\mathbf{E})$  is  $p^{-1}A_k$ . If  $b$  is non-degenerate, Lemma 9.3.1 implies that  $\det(A_k)$  is relatively prime to  $p$ . This implies that  $A_k$ , viewed as a matrix with coefficients in the field  $\mathbb{F}_p$ , is invertible and so  $\rho_k(b)$  is non-degenerate.

2. If  $\rho_k(b)$  is non-degenerate, then  $\det(A_k)$  is relatively prime to  $p$  which, again by Lemma 9.3.1, implies that  $b|_{H_k}$  is non-degenerate.  $\square$

Combining the above results finally leads to a splitting of  $G$  into homogeneous forms:

**Proposition 9.3.7.** *A non-degenerate symmetric  $p$ -primary torsion group  $(G, b)$  admits a **Jordan splitting**, that is, an orthogonal Jordan decomposition<sup>2</sup>  $G = \bigoplus_{k=1}^s H_k$ , where, we recall, each  $H_k$  is a homogeneous  $p$ -primary torsion group of exponent  $k$  equipped with a non-degenerate symmetric form. Moreover, each of the symmetric torsion forms  $\rho_k(b)$  are non-degenerate and the reduced discriminant<sup>3</sup>  $\delta(b)$  is invertible.<sup>4</sup>*

*Proof.* The proof is by induction on the number of different exponents. For homogeneous groups the result is true. In the filtration  $G_1 \subset G_2 \subset \dots \subset G$ , assume  $G = G_s$ . Take a maximal homogeneous subgroup  $H_s \subset G$  of exponent  $s$ . By Lemma 9.3.6 the non-degeneracy of the form on  $G$  implies that  $b|_{H_s}$  is non-degenerate and hence unimodular ( $H_s$  and its dual have the same cardinality and so the injective map induced by  $b$  is bijective). Thus we can split off  $H_s$ , say  $G = H_s \oplus H_s^\perp$ .

<sup>2</sup>This is *not* a canonical decomposition.

<sup>3</sup>See the defining formula (9.2).

<sup>4</sup>Under suitable identifications  $b|_{H_k}$  is isometric to  $p^{-k}\rho_k(b)$ .

By induction we find  $H_s^\perp = \bigoplus_{k=1}^{s-1} H_k$  with  $H_k$  homogeneous of exponent  $k$  and  $b|_{H_k}$  non-degenerate for all  $k$ . Lemma 9.3.6 implies that  $\rho_k(b)$  is non-degenerate ( $k = 1, \dots, s-1$ ). By Lemma 9.1.5, the invariant  $\delta$  is multiplicative on orthogonal sums. On a homogeneous summand  $H_k$  it is a unit since  $b|_{H_k}$  is non-degenerate and so  $\delta(b)$  is a unit.  $\square$

The advantage of the above approach is two-fold: one can recursively construct a splitting into homogeneous  $p$ -primary groups starting with a maximal homogeneous subgroup  $H_s \subset G$  of exponent  $s$  and then applying induction to  $H_s^\perp$ . The second advantage is the compatibility with the canonical operators  $\rho_k$  which allows to obtain invariants:

**Definition 9.3.8.** The *basic invariants* under isometry of a non-degenerate  $p$ -primary symmetric torsion group  $(G, b)$  are:

- the number of elementary divisors of  $G$  equal to  $p^k$   
 = the length of  $H_k$  in any Jordan splitting  $G = \bigoplus H_k$  of  $G$   
 = the rank of  $\rho_k(G)$  as a  $\mathbb{Z}/p\mathbb{Z}$ -module;
- if  $p$  is odd, for each  $k$  as above,  $\text{disc}(\rho_k(b)) \in \mathbb{D}(\mathbb{F}_p)$ .

For  $p$ -primary quadratic torsion groups  $(G, q)$  the invariants are those of the associated polar form  $b_q$ .

The reader should be warned at this point that the existence of a Jordan splitting in the quadratic case does not follow directly from what we said so far, at least for  $p = 2$ . We investigate this more closely in the next subsection.

**9.3.D The quadratic case.** Assuming that  $p$  is odd, the theory for quadratic and symmetric torsion forms is similar. This is due to the fact that in this case 2 is a unit in  $\mathbb{Q}_p$ . Indeed, a  $p$  primary quadratic torsion form takes values in  $Q^{(p)}/\mathbb{Z}$  which through the embedding  $Q^{(p)} \hookrightarrow \mathbb{Q}_p$  is isomorphic to  $\mathbb{Q}_p/\mathbb{Z}_p$  as shown in Appendix A.2. Consequently we can divide by 2 in  $\mathbb{Q}_p/\mathbb{Z}_p$ . If  $(G, q)$  is a  $p$ -primary torsion form, then for all  $x \in G$  one has  $b_q(x, x) = 2q(x) \in \mathbb{Q}_p/\mathbb{Z}_p$  and so  $q(x) = 2^{-1}b_q(x, x)$  in  $\mathbb{Q}_p/\mathbb{Z}_p$ . Using this, we prove:

**Lemma 9.3.9.** *Let  $p$  be an odd prime and let  $G$  be a  $p$ -primary torsion equipped with a quadratic form  $q$ . Define  $\rho_k(q)$  on  $\rho_k(G)$  by*

$$\rho_k(q)[x] := \text{class of } p^{k-1}q(x) \text{ in } \mathbb{Q}^{(p)}/\mathbb{Z}.$$

*This form is a well-defined  $p^{-1}\mathbb{Z}/\mathbb{Z}$ -valued quadratic form on  $\rho_k(G)$ . It is non-degenerate if and only if  $q$  is.*

*Proof.* One has  $\rho_k(b_q)(x, x) = p^{-k}b_q(x, x) = 2\rho_k(q)(x) \in \mathbb{Q}_p/\mathbb{Z}_p$  and so  $\rho_k(q)$  is well defined as a  $\mathbb{Q}_p/\mathbb{Z}_p$ -valued form and hence as a  $Q^{(p)}/\mathbb{Z}$ -valued form.

We see that also  $p \cdot p^{k-1}q(x) = 0$  since  $2p \cdot p^{k-1}q(x) = p \cdot p^{k-1}b_q(x, x) = b_q(p^k x, x) = 0$ . Hence  $\rho_k(q)$  takes values in  $p^{-1}\mathbb{Z}/\mathbb{Z}$ .

Finally, by definition  $q$  is non-degenerate if and only  $b_q$  is, while  $\rho_k(q)$  is non-degenerate if and only  $\rho_k(b_q)$  is. The result then follows from Lemma 9.3.3.  $\square$

For  $p = 2$  this argument fails since the same polar form may occur for several non-isometric quadratic forms. This problem only occurs for the exponent 1 summand, e.g. the quadratic forms  $\langle 2^{-1} \rangle$  and  $\langle -2^{-1} \rangle$  have the same polar form and this holds also for  $u_1$  and  $v_1$ . To remedy this, by "halving" one constructs from a 2-primary torsion group  $G$  one that only has generators of order  $\geq 4$  and then "doubling" gives back  $G$ .

**Definition 9.3.10.** Let  $G$  be a 2-primary torsion group equipped with a symmetric form  $b$ . Its *halving*,  $(\mathbf{G}, \mathbf{b}) = (\frac{1}{2}G, \frac{1}{2}b)$ , is the pair consisting of a 2-primary torsion group  $\mathbf{G}$  of exponent  $\geq 2$  together with a symmetric form  $\mathbf{b}$  on  $\mathbf{G}$  constructed as follows: For each summand  $G_k$  of exponent  $k$  in a chosen decomposition of  $G$ , choose generators,  $e_{k1}, \dots, e_{kr}$  (with  $r$  depending on  $k$ ). Define  $\mathbf{G}_k$  by generators  $\mathbf{e}_{kj}$ ,  $j = 1, \dots, r$ , of order precisely  $2^{k+1}$  and set  $\mathbf{G} = \bigoplus \mathbf{G}_k$ . The form  $\mathbf{b} = \frac{1}{2}b$  is given by

$$\mathbf{b}(\mathbf{e}_{ki}, \mathbf{e}_{lj}) = \frac{1}{2}b(e_{ki}, e_{lj}) \in \mathbb{Q}^{(2)}/\mathbb{Z}.$$

To check that this is well defined, assume that  $2^{k+1}\mathbf{x} = 0$  for some  $\mathbf{x} \in \mathbf{G}_k$ ,  $\mathbf{x} = \sum x_j \mathbf{e}_{kj}$  and let  $x = \sum x_j e_{kj}$  be the corresponding element in  $G$ . Since

$$\begin{aligned} 2^{k+1}\mathbf{b}(\mathbf{x}, \mathbf{e}_{lj}) &= 2^k b(x, e_{lj}) \\ &= b(2^k x, e_{lj}) = 0 \in \mathbb{Q}^{(2)}/\mathbb{Z}, \end{aligned}$$

the form  $b$  is indeed well defined.

The reverse procedure, "doubling" consists of shifting the exponents down. In detail, starting with a non-degenerate symmetric 2-primary torsion group  $(\mathbf{G}, \mathbf{b})$  without summands of order 2, this goes as follows. The group  $2\mathbf{G}$  is the group  $\mathbf{G}/\mathbf{G}_1$ , where, we recall,  $\mathbf{G}_1 := \{x \in \mathbf{G} \mid 2^1 \cdot x = 0\}$ . For  $x$  the class in  $\mathbf{G}/\mathbf{G}_1$  of an element  $\mathbf{x} \in \mathbf{G}$ , set  $q(x) := \mathbf{b}(\mathbf{x}, \mathbf{x})$ . To see that this is well defined, take  $\mathbf{z} = 2\mathbf{w} \in \mathbf{G}_1$ . Then

$$\begin{aligned} \mathbf{b}(\mathbf{x} + \mathbf{z}, \mathbf{x} + \mathbf{z}) &= \mathbf{b}(\mathbf{x}, \mathbf{x}) + 2\mathbf{b}(\mathbf{x}, \mathbf{z}) + \mathbf{b}(\mathbf{z}, \mathbf{z}) \\ &= \mathbf{b}(\mathbf{x}, \mathbf{x}) + \mathbf{b}(\mathbf{x}, 2\mathbf{z}) + \mathbf{b}(2\mathbf{w}, 2\mathbf{w}) \\ &= \mathbf{b}(\mathbf{x}, \mathbf{x}) + 4\mathbf{b}(\mathbf{w}, \mathbf{w}) \in \mathbb{Q}^{(2)}/\mathbb{Z}. \end{aligned}$$

The last equality holds since  $2\mathbf{z} = 0$ , and since  $\mathbf{b}(\mathbf{w}, \mathbf{w}) \in \frac{1}{4}\mathbb{Z}/\mathbb{Z}$ .

The just defined operation sends a non-degenerate  $\mathbf{b}$  to a non-degenerate  $q$ . Indeed,

$$\begin{aligned} b_q(x, y) &= q(x + y) - q(x) - q(y) \\ &= \mathbf{b}(\mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y}) - \mathbf{b}(\mathbf{x}, \mathbf{x}) - \mathbf{b}(\mathbf{y}, \mathbf{y}) \\ &= 2\mathbf{b}(\mathbf{x}, \mathbf{y}) = \mathbf{b}(2\mathbf{x}, \mathbf{y}), \end{aligned}$$

and so if  $\mathbf{b}(2\mathbf{x}, \mathbf{y}) = 0$  for all  $\mathbf{y} \in \mathbf{G}$ , then  $2\mathbf{x} = 0$ , that is  $\mathbf{x} \in \mathbf{G}_1$  and so  $x = 0$ .

This indeed reverses the process:

**Lemma 9.3.11.** *Let  $(G, q)$  be a 2-primary quadratic torsion group. Then the halving  $(\mathbf{G}, \mathbf{b})$  of  $(G, b_q)$  gives a symmetric torsion group (without cyclic summands of order 2) such that we retrieve  $(G, q)$  via  $2(\mathbf{G}, \mathbf{b})$  as above.*

*Also  $(G, q)$  is non-degenerate if and only if  $(\mathbf{G}, \mathbf{b})$  is non-degenerate.*

*Proof.* Since by definition  $2(\mathbf{b})(x, x) = \frac{1}{2}b_q(\mathbf{x}, \mathbf{x}) = q(x)$ , we have  $2(\mathbf{G}, \mathbf{b}) = (G, q)$ .

We already showed that a non-degenerate  $\mathbf{b}$  gives a non-degenerate  $q$ . Conversely, to verify that  $\mathbf{b}$  is non-degenerate assuming  $q$  is, observe that  $\rho_k(\mathbf{b}) = \rho_{k-1}(b_q)$ ,  $k \geq 2$ . Since  $q$  is non-degenerate, so are the forms  $\rho_k(\mathbf{b})$  and hence, so is  $\mathbf{b}$ , since  $\mathbf{G}$  has no cyclic summands of order 2.  $\square$

The previous lemma allows us to extend the results obtained so far for odd primes to the prime 2. Combining everything we arrive at the final result:

**Theorem 9.3.12.** *A non-degenerate  $p$ -primary quadratic form  $(G, q)$  admits a Jordan splitting  $G = \bigoplus_{k=1}^s H_k$ . Moreover,*

1. *For each  $k = 1, \dots, s$ , the restriction  $q|_{H_k}$  is non-degenerate if and only if the quadratic torsion form  $\rho_k(q)$  is non-degenerate. Under suitable identifications  $q|_{H_k}$  is isometric to  $p^{-k}\rho_k(q)$ .*
2. *The reduced discriminant  $\delta(b_q)$  is invertible if and only if the quadratic torsion forms  $\rho_k(q)$ ,  $k = 1, \dots, s$ , are non-degenerate.*

*Proof.* For  $p$  odd this follows from Lemma 9.3.9 which implies that the splitting of  $(G, b_q)$  from Proposition 9.3.7 gives a splitting for  $(G, q)$ .

If  $p = 2$  we first obtain a homogeneous splitting for the halving  $(\mathbf{G}, \mathbf{b})$  using Proposition 9.3.7. Since doubling preserves homogeneous orthogonal direct sums,  $(G, q) = 2(\mathbf{G}, \mathbf{b})$  admits a Jordan splitting. Lemma 9.3.11 then shows that the remaining assertions hold since they hold for  $(\mathbf{G}, \mathbf{b})$ .  $\square$

## 9.4 Building Blocks For $p$ -Primary Torsion Forms

We can now show that the length 1 and 2 symmetric and quadratic torsion groups we introduced in Chapter 1 (cf. Examples 1.9.5) indeed give all building blocks in the sense that all non-degenerate torsion forms are orthogonal direct sums of these blocks.

First of all, the Jordan splitting, Proposition 9.3.7, implies that the building blocks are homogeneous and so it suffices to classify these. By Lemma 9.3.3 one may reduce to exponent one. Explicitly, a symmetric torsion form  $b$  on a homogeneous  $p$ -primary torsion group of exponent  $k$  is isometric to  $p^{-k}\rho_k(b)$ .

Secondly, in the exponent 1 case, for  $p$  odd one uses the classification of non-degenerate symmetric forms on  $\mathbb{F}_p$ -vector spaces as given in Chapter 8 together with Proposition 9.3.12 which states that a similar assertion holds for quadratic torsion forms. For  $p = 2$ , in addition, type II forms on  $\mathbb{F}_2$ -spaces play a role as noted in Example 9.3.2.

For  $p$  odd this leads to:

**Proposition 9.4.1.** *Let  $p$  be odd. A non-degenerate homogeneous  $p$ -primary symmetric torsion form  $b$  of exponent  $k$  and length  $r$  is isometric to  $\bigoplus^r \langle p^{-k} \rangle$  if  $\text{disc}(\rho_k(b)) = 1$  and to  $\bigoplus^{r-1} \langle p^{-k} \rangle \oplus \langle \epsilon p^{-k} \rangle$  if  $\text{disc}(\rho_k(b)) = \epsilon$ , a non-square modulo  $p$ . A similar assertion holds for quadratic forms.*

*Proof.* We only have to recall that for  $p$  odd, non-degenerate symmetric or quadratic forms on an  $\mathbb{F}_p$ -vector space are diagonalizable and, by Corollary 8.3.4, such forms belong to two isometry classes. Which of the two is determined by the value of  $\text{disc}(\rho_k(b))$  (or  $\text{disc}(\rho_k(b_q))$ ).  $\square$

For  $p = 2$  one uses Proposition 8.2.1: there are three building blocks of  $\mathbb{F}_2$ -inner product spaces: the form  $\langle 1 \rangle$  and the forms  $U$  and  $V$ . These are all of type I and lead to the symmetric building blocks  $\langle u \cdot 2^{-k} \rangle$ ,  $u$  a dyadic unit,  $u_k$  and  $v_k$  on 2-primary groups of exponent  $k$ . The quadratic building blocks on such groups are  $\langle u \cdot 2^{-k-1} \rangle$ ,  $u_k$  and  $v_k$ . By Lemma 9.3.11 there is no essential difference between 2-primary quadratic torsion forms and symmetric torsion forms of exponent  $\geq 2$ . As explained above on  $\mathbb{Z}/2\mathbb{Z}$  there are the type II forms  $[2^{-2}]$ ,  $[3 \cdot 2^{-2}]$ . Moreover, the symmetric torsion forms  $u_1$  and  $v_1$  are the same since  $2 = 0$  in  $\mathbb{Z}/2\mathbb{Z}$ . Hence one deduces:

**Proposition 9.4.2.**  $\bullet$  *A non-degenerate symmetric (respectively quadratic) form on a homogeneous 2-primary group of exponent  $k \geq 2$  and length  $r$  is isometric to*

$$\begin{aligned} & \bigoplus_{j=1}^a \langle u^{(j)} 2^{-k} \rangle \oplus^b u_k \oplus^c v_k \quad a + 2(b + c) = r, \quad u^{(j)} \in D(\mathbb{Z}/2^k\mathbb{Z}) \\ & \bigoplus_{j=1}^a [u^{(j)} 2^{-k-1}] \oplus^b u_k \oplus^c v_k \quad \text{respectively.} \end{aligned}$$

- $\bullet$  *A non-degenerate symmetric form on a homogeneous 2-primary group of exponent 1 and length  $r$  is isometric to*

$$\bigoplus_{j=1}^a \langle u^{(j)} 2^{-1} \rangle \oplus^b u_1, \quad a + 2b = r, \quad u^{(j)} \in D(\mathbb{Z}/2^k\mathbb{Z}).$$

- $\bullet$  *A non-degenerate quadratic form on a homogeneous 2-primary group of exponent 1 and length  $r$  is isometric to*

$$\bigoplus^a [u \cdot 2^{-2}] \oplus^b u_1 \oplus^c v_1, \quad a + 2b + 2c = r, \quad u \in 1, 3 = D(\mathbb{Z}/4\mathbb{Z}).$$

**Historical and Bibliographical Notes.** For the material of Section 9.1 we followed Sections 1–6 in Chapter II of the notes [156] by R. Miranda and D. Morrison. That the Sylow decomposition of a torsion symmetric group is compatible with the symmetric or quadratic form, as shown in Section 9.2, has been observed by various people, e.g. by A. Durfee (cf. Lemma 1.2 in [56]). According to the latter the compatibility of the Jordan decomposition with symmetric and quadratic forms is due to E. van Kampen (cf. [232]) although the terminology "Jordan splitting" seems to be due to A. Durfee himself. Our presentation of Section 9.3 is modeled on C.T.C. Wall's paper [245].



## $p$ -adic Lattices

In this chapter all  $p$ -adic lattices are assumed to be non-degenerate.

### Introduction

In this chapter we first classify  $p$ -adic lattices of rank 1 and 2. Then, in Section 10.2 we show that these generate all  $p$ -adic lattices upon taking orthogonal sums. In particular we show that a  $p$ -adic lattice is an orthogonal direct sum of lattices of the form  $L(p^k)$  with  $L$  unimodular. The latter are called homogeneous of exponent  $k$  since their discriminant form is a homogeneous  $p$ -primary torsion form of that same exponent. Such a decomposition is called a Jordan splitting. It induces a Jordan splitting of the discriminant form (in the sense of Chapter 9). We have shown in Section 9.3 that all  $p$ -primary torsion forms admit a Jordan splitting. We use this to prove in Section 10.3 that every  $p$ -primary torsion form is the discriminant form of a  $p$ -adic lattice which is unique up to isometry if  $p$  is odd. For  $p = 2$  some ambiguity remains.

In section 10.4 Hasse invariants of  $p$ -adic lattices are calculated making use of the classification obtained in the preceding sections. The results are used later in Chapter 12 to determine the signature mod 8 for quadratic torsion forms.

### 10.1 Low Rank $p$ -adic Lattices

Recall that a (non-degenerate)  $p$ -adic lattice consists of a pair  $(L, b)$  with  $L$  a free  $\mathbb{Z}_p$ -module of finite rank and  $b : L \times L \rightarrow \mathbb{Z}_p$  a non-degenerate symmetric bilinear form with values in  $\mathbb{Z}_p$ . A quadratic  $p$ -adic lattice is a pair  $(L, q)$  with  $L$  a free  $\mathbb{Z}_p$ -module of finite rank and  $q : L \rightarrow \mathbb{Z}_p$  a non-degenerate quadratic form. In Section 1.9, we gave some examples of  $p$ -adic lattices (cf. Examples 1.9.5). We discuss these here in more detail.

**Rank one  $p$ -adic lattices.** These have been classified in Section 6.1. See the table on page 146.

**Rank two  $p$ -adic lattices,  $p$  odd.** By Proposition 6.3.11, the unimodular binary forms are  $\langle u \rangle \oplus \langle v \rangle$ , where  $u, v$  are  $p$ -adic units. We shall see later (Proposition 10.2.2) that for  $p \neq 2$  all  $p$ -adic lattices are decomposable.

**Rank two dyadic lattices. 1.** For a non-negative integer  $k$  we have the lattice

$U_k = U_{\mathbb{Z}_2}(2^k)$ , where  $U_{\mathbb{Z}_2}$  is the dyadic symmetric hyperbolic lattice. Recall that with respect to the standard basis of  $\mathbb{Z}_2^2$  the Gram matrix of  $U_k$  is  $\begin{pmatrix} 0 & 2^k \\ 2^k & 0 \end{pmatrix}$ . The form on the unimodular lattice  $U = U_0$  is the polar form of  $(x_1, x_2) \mapsto x_1x_2$ . We claim that the lattice  $U_k$  is indecomposable. It suffices to prove this for  $k = 0$ . Since  $\text{disc}(U) = -1$ , which is a unit,  $U$  cannot be an even decomposable lattice since then it would have discriminant divisible by 4.

2. Consider  $\mathbb{Z}_2^{\oplus 2}$  equipped with the unimodular bilinear form given by  $V = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ .

We are mainly interested in the quadratic form  $(x_1, x_2) \mapsto x_1^2 + x_1x_2 + x_2^2$  of which it is the polar form. The symbol  $V$  stands also for the associated quadratic (or symmetric) dyadic lattice and  $V_k$  stands for  $V(2^k)$ . We have seen in Example 1.9.5, 4. that  $\text{disc}(V_k) = 3 \cdot 2^{2k}$ , and since  $3 \neq -1$  modulo squares, this implies that this lattice is not isometric to  $U_k$ . A similar argument as for  $U_k$  shows that this lattice is also indecomposable. Summarizing, we have two indecomposable rank two lattices, here given by the corresponding quadratic forms:

$$\begin{aligned} U_k : (x_1, x_2) &\mapsto 2^k x_1 x_2, & \text{disc}(U_k) &= -2^{2k} \cdot (\mathbb{Z}_2^\times)^2 \\ V_k : (x_1, x_2) &\mapsto 2^k (x_1^2 + x_1 x_2 + x_2^2), & \text{disc}(V_k) &= 3 \cdot 2^{2k} \cdot (\mathbb{Z}_2^\times)^2. \end{aligned}$$

The above two examples exhaust the possibilities for indecomposable rank two dyadic lattices:

**Lemma 10.1.1.** *The lattices  $U_k$  are the only indecomposable rank two symmetric dyadic lattices which represent zero. There are no indecomposable symmetric rank 2 dyadic lattices other than  $U_k$  and  $V_k$ .*

*Proof.* We first show that a rank two dyadic indecomposable symmetric lattice  $(V, b)$  representing 0 is isometric to some  $U_k$ .

Suppose that  $e_1$  is a primitive isotropic vector. By primitivity, we may extend  $e_1$  to a basis  $\{e_1, e_2\}$ . Since  $b(e_1, e_2) \neq 0$ , replacing  $e_1$  with  $ue_1$  for a suitable unit  $u \in \mathbb{Z}_2$ , we may assume that for some integer  $k \geq 0$  we have  $b(e_1, e_2) = 2^k$ . Let  $r := b(e_2, e_2)$ . If  $r = 0$  we are done. Otherwise, the 2-adic valuation of  $r = b(e_2, e_2)$  is at least  $k + 1$ . Indeed, if not, then  $2^k r^{-1} \in \mathbb{Z}_2$  and

$$b(e_1 - 2^k r^{-1} e_2, e_2) = 2^k - 2^k r^{-1} \cdot r = 0.$$

In other words,  $e'_1 = e_1 - 2^k r^{-1} e_2 \in V$  would be orthogonal to  $e_2$  and the new basis  $\{e'_1, e_2\}$  of the lattice would give an orthogonal direct sum decomposition, contrary to the assumption that  $V$  is indecomposable. It follows that we can replace  $e_2$  with  $e'_2 = e_2 - r/2^{k+1} \cdot e_1$  and in the basis  $\{e_1, e'_2\}$  the Gram matrix is precisely  $U_k$  as we verify without problem.

To show that  $(V, b) \simeq V_k$  in case  $V$  is indecomposable and does not represent zero is a bit more complicated. We make essential use of the dyadic topology on  $\mathbb{Z}_2^{\oplus 2}$  underlying  $V$ , which by definition is the product dyadic topology on  $V$  induced by the dyadic valuation  $v_2$  on  $\mathbb{Z}_2$ . Since the latter ring is compact (Proposition A.2.2),

also  $V$  is compact and so every sequence in  $V$  has a converging subsequence, a property which will be used below.

Since  $V$  is indecomposable, we may assume that we have a basis  $\mathbf{E} = \{e_1, e_2\}$  for  $V$  with  $b(e_1, e_2) = 2^k$  so that the Gram matrix is of the form

$$b_{\mathbf{E}} = \begin{pmatrix} a & 2^k \\ 2^k & b \end{pmatrix}.$$

If  $a = 2^\ell a'$  with a unit  $a'$  and with  $\ell \leq k$ , then  $e'_2 = 2^{k-\ell} e_1 - a' e_2$  is orthogonal to  $e_1$ , and in the basis  $\{e_1, e'_2\}$  the Gram matrix would become diagonal, contradicting our assumption on  $V$ . A similar argument applies to  $b$ . So we may assume that  $2^{k+1}$  divides both  $a$  and  $b$ , but then  $2^k$  divides all entries of the Gram matrix and hence we may reduce to the case  $k = 0$ . Moreover,  $a = 2u, b = 2v$ . In other words, we may assume that the Gram matrix with respect to  $\{e_1, e_2\}$  is

$$b_{\mathbf{E}} = \begin{pmatrix} 2u & 1 \\ 1 & 2v \end{pmatrix}, \quad u, v \in \mathbb{Z}_2.$$

We argue that both  $u$  and  $v$  have to be odd. If for instance  $v$  is even, say  $v = v'2^n$ ,  $v'$  a unit and  $n \geq 1$ , we replace  $e_2$  with  $e_3 = 2^n e_1 + (1 - 2^{n+1}u)e_2$ . Then  $\{e_1, e_3\}$  is a new basis with  $b(e_1, e_3) = 1$  and

$$\begin{aligned} b(e_3, e_3) &= b(2^n e_1 + (1 - 2^{n+1}u)e_2, 2^n e_1 + (1 - 2^{n+1}u)e_2) \\ &= 2^{2n+1}u + 2^{n+1}(1 - 2^{n+1}u) + (1 - 2^{n+1}u)^2 2^{n+1}v' \\ &= 2^{n+1}(2^n u + 1 - 2^{n+1}u + v' - 2^{n+2}v'u + 2^{2n+2}u^2 v') \\ &= 2^{n+1}(1 + v' + w), \end{aligned}$$

where  $v_2(w) \geq n \geq 1$ . Since  $1 + v'$  is even we find  $v_2(b(e_3, e_3)) \geq n + 2$ . This process of replacing the second basis vector can be continued indefinitely. Using the dyadic compactness of  $V$ , we may assume that the resulting sequence converges to an isotropic vector  $e_\infty$ . Since also  $b(e_1, e_\infty) = 1$ , the vector  $e_\infty$  is not the zero-vector, contradicting our assumption on  $b$ . Consequently,

$$b_{\mathbf{E}} = \begin{pmatrix} 2u & 1 \\ 1 & 2v \end{pmatrix}, \quad u, v \text{ odd.}$$

If  $v \neq 1$  we set

$$v = 1 + 2^m t, \quad t \text{ odd, } m \geq 1,$$

one has  $v_2(b(e_2, e_2) - 2) = m + 1$ . The next step is to replace  $e_2$  successively with  $e_3, e_4, \dots$  such that  $v_2(b(e_k, e_k) - 2)$  becomes larger and larger. To start, take  $e_3 = 2^m e_1 + (1 - 2^{m+1}u)e_2$ . Just as before,  $b(e_1, e_3) = 1$  and, by a calculation similar to the one we just did, we find

$$\begin{aligned} b(e_3, e_3) &= 2(1 + 2^m(t + 1) + z), \quad \text{with } v_2(z) \geq m + 1 \\ &= 2(1 + 2^{m+1}w), \quad w \in \mathbb{Z}_2, \end{aligned}$$

since  $t$  is odd. Therefore  $v_2(b(e_3, e_3) - 2) \geq m + 2$ . This process can be iterated so that we obtain a sequence of vectors in  $V$  converging to some vector  $\tilde{e}_\infty$  for which  $b(\tilde{e}_\infty, \tilde{e}_\infty) = 2$ . In the basis  $\{e_1, \tilde{e}_\infty\}$  the Gram matrix for  $b$  becomes  $\begin{pmatrix} 2u & 1 \\ 1 & 2 \end{pmatrix}$ . Observe that since the Gram matrix has non-zero determinant,  $\{e_1, \tilde{e}_\infty\}$  is indeed a basis.

Now going through a similar procedure with  $e_1$  we can subsequently make  $u = 1$ .  $\square$

Given a Gram matrix of a binary dyadic symmetric form, how can one determine its isometry class? Such a Gram matrix can always be written as  $2^k A$ , where  $\det A$  is a unit and so it suffices to consider unimodular binary forms. The answer is provided by:

**Lemma 10.1.2** (Recognising binary dyadic forms). *For a Gram matrix  $\begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix}$  of a unimodular dyadic symmetric form  $b$ , setting  $d = \text{disc}(b)$ , the following possibilities occur:*

1. *The form is decomposable if and only if either  $\alpha$  or  $\gamma$  is odd, i.e., a unit. More precisely,*
  - (a) *if  $\alpha$  is odd,  $b \simeq \langle \alpha \rangle \oplus \langle \alpha \cdot d \rangle$ .*
  - (b) *if  $\gamma$  is odd,  $b \simeq \langle \gamma \rangle \oplus \langle \gamma \cdot d \rangle$ .*
2. *If  $\alpha$  and  $\gamma$  are both even (hence  $b$  is even), then  $\beta$  is odd,  $b$  is indecomposable, and*
  - (a) *if  $\frac{1}{4}\alpha\gamma$  is even,  $b \simeq U$*
  - (b) *and if  $\frac{1}{4}\alpha\gamma$  is odd,  $b \simeq V$ .*

*For a unimodular binary dyadic quadratic lattice, only case 2 occurs.*

*Proof.* 1. Lemma 10.1.1 implies that an odd rank 2 form is decomposable. Let us make this precise. Suppose first that  $\alpha$  is odd. Then changing the basis  $e_1, e_2$  into  $e_1, -\beta e_1 + \alpha e_2$ , the Gram matrix changes into

$$\begin{pmatrix} 1 & 0 \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha d \end{pmatrix}.$$

Similarly, if  $\gamma$  is odd we have the second possibility. Conversely, if the form  $b$  is decomposable, for some invertible matrix  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  the matrix  $M^T B M$  is a diagonal matrix, where  $B$  is the Gram matrix. This is equivalent to  $ab \cdot \alpha + \gamma \cdot cd + (ad - bc) \cdot \beta + 2bc \cdot \beta = 0$ . So if  $\alpha$  and  $\gamma$  are even, also  $\beta$  is even which is impossible since  $\det B$  is a unit. It follows that for a decomposable form either  $\alpha$  or  $\gamma$  is odd. 2. From item 1 we know that the form must be indecomposable. Write  $\alpha = 2\alpha_1$ ,  $\gamma = 2\gamma_1$ . By Lemma 10.1.1 there are only two types of unimodular indecomposable

such lattices,  $U$  and  $V$ , and  $U$  is the only one representing 0. We infer that the lattice is isometric to  $U$  if and only if  $\alpha_1 x^2 + \beta xy + \gamma_1 y^2 = 0$  is solvable. This is the case if and only if the discriminant  $\beta^2 - 4\alpha_1\gamma_1 = \det B$  is a square in  $\mathbb{Z}_2^\times$ , i.e., if and only if  $\beta^2 - 4\alpha_1\gamma_1 \equiv 1 \pmod{8}$ . Since  $\beta$  is odd,  $\beta^2 \equiv 1 \pmod{8}$ , and so this happens if and only if  $\alpha_1\gamma_1$  is even. And then of course,  $b \cong V$  if and only if  $\alpha_1\gamma_1$  is odd.  $\square$

As an application we mention a representability result, this time valid for any prime, even or odd.

**Lemma 10.1.3.** *A  $p$ -adic unimodular quadratic form of rank two represents all  $p$ -adic units.*

*Proof.* Let us first consider the dyadic case. The form  $xy$  with Gram matrix  $U$  clearly represents all 2-adic integers. Next, consider the form  $x^2 + xy + y^2$  with Gram matrix  $V$ . The equation  $x^2 + xy + y^2 = u$  can be solved primitively modulo 8 for any  $u \in \{1, 3, 5, 7\}$ , and Hensel's Lemma A.4.3 gives solutions in  $\mathbb{Z}_2$ . This settles representability for the lattice  $V$ . In the dyadic setting there is no decomposable unimodular lattice.

Any other rank two unimodular quadratic form is isometric to  $ux^2 + vy^2$ ,  $u, v \in \mathbb{Z}_p^\times$ ,  $p$  odd, and represents all  $p$ -adic integers by Example A.4.2.  $\square$

We are going to use this representability result for classification purposes and for the study of orthogonal groups. See e.g. the proof of Theorem 14.5.5.

**Corollary 10.1.4.** *Let  $(L, q)$  be a unimodular binary quadratic  $p$ -adic lattice and  $u$  a  $p$ -adic unit. Then  $L$  admits a reflection  $\sigma_x$  in a vector  $x \in L$  with  $q(x) = u$ .*

*Proof.* Lemma 10.1.3 implies that there exists a vector  $x \in L$  with  $q(x) = u$ . Then, by Lemma 7.1.1, the reflection  $\sigma_x$  preserves  $L$ .  $\square$

## 10.2 Jordan Splitting of $p$ -adic Lattices

We show now that the examples from Section 10.1 constitute the basic blocks for building non-degenerate  $p$ -adic symmetric (and quadratic) lattices.

Let  $(L, q)$  be a quadratic lattice. The set  $q(L)$  generates a non-zero ideal in  $\mathbb{Z}_p$  which we denote  $(q(L))$ . Any  $x_0$  for which  $v_p(q(x_0))$  is minimal provides a generator  $q(x_0)$  of this ideal, since  $v_p$  is archimedean. If  $b$  is the polar form of  $q$ , this implies that the  $p$ -adic number  $2q(x_0) = b(x_0, x_0)$  generates the ideal  $2(q(L))$ . Let  $(b(L, L))$  be the ideal of  $\mathbb{Z}_p$  generated by all  $b(y, z)$ ,  $y, z \in L$ . This ideal is generated by an element  $b(x, y)$  with  $v_p(b(x, y))$  minimal. Since  $b(z, z) = 2q(z)$ ,  $z \in L$ , we have the inclusions

$$2(q(L)) \subset (b(L, L)) \subset (q(L)) \subset \mathbb{Z}_p,$$

where the first inclusion can only be strict for  $p = 2$ , that is, for dyadic lattices, and then  $(q(L)) = (b(L, L))$ . If this is the case, and  $b(x, y)$  generates the ideal

$(b(L, L))$ , then  $x$  and  $y$  must be independent. Indeed, if not, we may assume that  $x = \alpha y$  and then  $b(x, y) = \alpha b(y, y) \in 2(q(L))$ , contrary to our assumption.

**Lemma 10.2.1.** *Let  $(L, q)$  be a non-degenerate  $p$ -adic quadratic lattice. Write  $b$  for the polar form of  $q$ . Let  $(q(L))$ ,  $(b(L, L))$  and  $x_0 \in L$  be as above. Suppose that  $2(q(L)) = (b(L, L))$  (which is the case for  $p$  odd, but not necessarily for  $p = 2$ ). Then  $\mathbb{Z}_p \cdot x_0$  splits off orthogonally. Consequently, if there is no rank one sublattice of  $L$  which splits off, then  $p = 2$  and  $2(q(L)) \subsetneq (b(L, L)) \subset \mathbb{Z}_2$ .*

*Proof.* Suppose that  $2(q(L)) = (b(L, L))$ , then  $b(x_0, x_0) = 2q(x_0)$  must generate  $(b(L, L))$ . Hence for any  $z \in L$  we can find  $r = r(z) \in \mathbb{Z}_p$  such that  $b(z, x_0) = rb(x_0, x_0)$ . So, writing  $z = r \cdot x_0 + (z - r \cdot x_0)$  shows that  $\mathbb{Z}_p \cdot x_0$  splits off orthogonally.  $\square$

We can now state and prove the basic decomposition result for  $p$ -adic lattices.

**Proposition 10.2.2** (Classification (I)). *1. For  $p$  odd, any (non-degenerate) symmetric (quadratic)  $p$ -adic lattice is isometric to an orthogonal direct sum of rank one  $p$ -adic lattices of the form  $\langle u p^k \rangle$ , where  $u \in \mathbb{Z}_p^\times$  and  $k \geq 0$ .*  
*2. Dyadic symmetric, respectively quadratic lattices split into an orthogonal direct sum of rank one lattices of the form  $\langle u \cdot 2^k \rangle$ ,  $u \in \{\pm 1, \pm 3\}$ , where  $k \geq 0$ , respectively  $k \geq 1$ , together with copies of  $U_k$  and of  $V_k$ ,  $k \geq 0$ .*

*Proof.* For  $p \neq 2$  the number 2 is a unit in the ring  $\mathbb{Z}_p$ . Hence by Lemma 10.2.1 and applying induction, the form  $b$  is diagonalizable.

Let us now assume that  $p = 2$  and let  $(L, b)$  be a non-degenerate dyadic symmetric lattice. The values  $b(x, x)$ ,  $x \in L$ , generate an ideal in  $\mathbb{Z}_2$ . If this is not a proper ideal, then, since  $\mathbb{Z}_2$  is a local ring, there exists  $x_0 \in L$  with  $b(x_0, x_0)$  a unit, and  $x_0$  splits off as in the proof of Lemma 10.2.1. Continuing in this way, we successively split off rank one lattices  $\mathbb{Z}_2 x$  with  $b(x, x)$  a unit.

The remaining lattice  $L'$  is even since now  $b(x, x) \in 2\mathbb{Z}_2$  for all  $x \in L'$ . In particular  $b$  is the polar form of a quadratic form  $q$ . As long as the condition of Lemma 10.2.1 is satisfied, we may continue splitting off rank one lattices. Next, assume that no rank one lattice can be split off from our lattice  $L$ . Lemma 10.2.1 now tells us that we may henceforth assume that  $(2q(L)) \neq (b(L, L))$ , so that  $(b(L, L))$  is generated by an element  $b(x, y)$  with  $x, y$  independent vectors in  $L$ . For any  $z \in L$  we then write

$$\begin{aligned} b(z, x) &= r_1 b(x, y) \\ b(z, y) &= r_2 b(x, y). \end{aligned}$$

Since the ideals  $(2q(L))$  and  $(b(L, L))$  are different, we have  $(b(L, L)) = (q(L))$ , and we can find elements  $r, s \in \mathbb{Z}_2$  with  $2q(x) = 2rb(x, y)$  and  $2q(y) = 2sb(x, y)$ . The unit  $u := 1 - 2^2rs$  can now be used to split off the module  $M$  generated by  $x$  and  $y$  as follows. Solving

$$\begin{aligned} 0 &= b(z + \alpha x + \beta y, x) = (r_1 + \alpha 2r + \beta) b(x, y) \\ 0 &= b(z + \alpha x + \beta y, y) = (r_2 + \alpha + \beta 2s) b(x, y) \end{aligned}$$

for  $\alpha$  and  $\beta$  leads to  $\alpha = u^{-1}(2sr_1 - r_2)$  and  $\beta = u^{-1}(2rr_2 - r_1)$ , both in  $\mathbb{Z}_2$ . So

$$z = z + \alpha x + \beta y - (\alpha x + \beta y)$$

with  $z + \alpha x + \beta y \in M^\perp$  and  $\alpha x + \beta y \in M$ . Now repeat the argument with  $M^\perp$ .

We have shown in Section 10.1 that the rank two dyadic lattices  $M$  that we have split off, which are necessarily indecomposable, can only be of two types: the ones that represent zero are isometric to some  $U_k$ , those that don't, are isometric to some  $V_k$ . This finishes the proof for  $p = 2$ .  $\square$

**Example 10.2.3.** Since  $\text{disc}(U) = -1$ ,  $\text{disc}(V) = 3$ , the lattice  $E_8 \otimes \mathbb{Z}_2$ , being even with discriminant 1, is isometric to either  $\oplus^4 U$ ,  $\oplus^4 V$  or to  $\oplus^2 U \oplus \oplus^2 V$ . We shall see (Lemma 11.2.1) that these 3 dyadic lattices are isometric.

There is a remarkable consequence of the preceding result:

**Corollary 10.2.4.** *A  $p$ -adic unimodular quadratic form of rank  $\geq 2$  represents all  $p$ -adic units. For  $p \neq 2$  the lattice admits isotropic vectors if its rank is at least 3, for  $p = 2$  this is the case if the rank is at least 4.*

*Proof.* By Proposition 10.2.2  $p$ -adic lattices of rank  $\geq 2$  always split off a rank two lattice and so the first assertion follows from Lemma 10.1.3. For the existence of an isotropic vector, we use that for odd  $p$  a unimodular quadratic lattice diagonalizes, while for  $p = 2$  it is a direct sum of lattices isometric to  $U$  or  $V$ . So it suffices to consider a lattice of the form  $L = M \oplus N$  where  $\text{rank}(M) = 2$  and  $\text{rank}(N) = 1$  if  $p \neq 2$  or  $\text{rank}(N) = 2$  in the dyadic situation. In both cases, take a vector  $y \in N$  such that  $b(y, y) = c$  is a unit. By the representation result, there exists  $x \in M$  with  $b(x, x) = -c$  and then  $x + y$  is isotropic.  $\square$

*Remark 10.2.5.* The existence of isotropic vectors is used in the proof of Corollary A.3.7. This result in particular states that the occurrence of one root in an indefinite lattice of rank  $\geq 4$  implies that there are infinitely many. This, in turn, is a crucial ingredient in the proof of Theorem 17.2.11 which roughly states that for "most" lattices with Witt index  $\geq 2$  the Weyl group is as big as possible.

The splitting described in Proposition 10.2.2 gives a **Jordan splitting**, that is, an orthogonal splitting into lattices of the form  $L(p^k)$  with  $L$  unimodular. A summand such as  $L(p^k)$  is called a **homogeneous  $p$ -adic lattice of exponent  $k$** . We give a simple direct proof of the existence of such a Jordan splitting which has the additional merit that it gives invariants. The proof is very similar to what we did in Section 9.3 for torsion groups.

**Proposition 10.2.6.** *A non-degenerate symmetric  $p$ -adic lattice  $(L, b)$  has a Jordan splitting, i.e.,*

$$L = L_0 \oplus L_1(p) \oplus \cdots \oplus L_r(p^r),$$

where each  $L_j$  is unimodular. The rank of  $L_j$  as well as its discriminant,  $\text{disc}(L_j) \in D(\mathbb{Z}_p)$ , is uniquely determined by  $(L, b)$ .

*Proof.* For  $k \geq 0$  let  $L^{(k)} = \{x \in L \mid b(x, L) \subset p^k \mathbb{Z}_p\}$ . This gives a canonical decreasing filtration of  $L$  by  $\mathbb{Z}_p$ -submodules so that the quotients

$$\rho^{(k)}L = L^{(k)} / (pL^{(k-1)} + L^{(k+1)}) \quad (\text{and } L^{(0)} / L^{(1)} \text{ for } k = 0)$$

are canonically defined  $\mathbb{Z}_p$ -modules annihilated by  $p$  and so are  $\mathbb{F}_p$ -vector spaces. In particular their dimensions are invariants. The form  $b$  descends to each of these vector spaces as an  $\mathbb{F}_p$ -valued form by setting

$$\rho^{(k)}(b)([x], [y]) = \text{class of } b(x, y) \in p^k \mathbb{Z}_p / p^{k+1} \mathbb{Z}_p \simeq \mathbb{Z}_p / p \mathbb{Z}_p \simeq \mathbb{F}_p.$$

The proof that this is well defined is analogous to the computation (9.6).<sup>1</sup>

To construct the desired splitting, we may assume that  $L^{(1)} \neq L$ , otherwise take the smallest  $k$  such that  $L^{(k)} \neq L$  and divide the form by  $p^{k-1}$ .

Since  $pL \subset L^{(1)}$ , the vector space  $L/pL$  contains  $L^{(1)}/pL$ . Choose a complementary subspace  $\bar{L}_0$  so that  $L/pL = \bar{L}_0 \oplus L^{(1)}/pL$  and let  $L_0 \subset L$  be a sublattice of the same rank as  $\bar{L}_0$  and mapping surjectively onto  $\bar{L}_0$  under the projection  $L \rightarrow L/pL$ . Note that  $L = L_0 + L^{(1)}$  for since  $L_0 + L^{(1)}$  surjects onto  $L/pL$  and  $pL \subset L^{(1)}$  we get  $L \subset L_0 + L^{(1)} + pL \subset L_0 \oplus L^{(1)}$ .

The aim is to show that  $b$  restricts unimodularly to  $L_0$ . To show this, it suffices to prove that the discriminant of this restriction is a unit, which comes down to showing that  $b$  induces a non-degenerate form  $\bar{b}$  on the  $\mathbb{F}_p$ -vector space  $\bar{L}_0$ . To check this, suppose that  $x \in L_0$  with class  $\bar{x} \in L/pL$  satisfies  $\bar{b}(\bar{x}, \bar{L}_0) = 0$ . Then  $b(x, L_0) \equiv 0 \pmod{p}$ . Since  $b(x, L^{(1)}) \equiv 0 \pmod{p}$ , one then has  $b(x, L) \equiv 0 \pmod{p}$ , that is, by definition,  $x \in L^{(1)}$ . But then  $\bar{x} \in \bar{L}_0 \cap (L^{(1)}/pL) = \{0\}$ .

As a result, we have an orthogonal splitting  $L = L_0 \oplus L_0^\perp$  with  $L_0$  unimodular. The form  $b|_{L_0^\perp}$  is divisible by  $p$  since for all  $x \in L_0^\perp$  we have  $b(x, L_0^\perp) = b(x, L) = b(x, L^{(1)}) \subset p\mathbb{Z}_p$  where we use that  $L = L_0 + L^{(1)}$ . Observe that  $\rho^{(0)}L = L/L^{(1)} = L/pL / (L^{(1)}/pL) \simeq \bar{L}_0$  and that the form induced by  $b$  on the former corresponds to the form  $\rho^{(0)}(b)$ , and so the rank of  $L_0$  and the discriminant of  $b|_{L_0}$  are invariants.

Continue now with  $(L_0^\perp, p^{-1}b)$  and apply induction to obtain a Jordan splitting. Multiplying the form by  $p$  we may then assume that we have found a Jordan decomposition  $L_0^\perp = \bigoplus_{j \geq 1} L_j(p^j)$  such that  $L_j \otimes \mathbb{Z}_p / p \mathbb{Z}_p \simeq \rho^{(j)}L$  with  $b|_{L_j}$  corresponding to  $\rho^{(j)}(b)$ . This yields the desired decomposition and it also shows that ranks and discriminants of the  $L_j$  are uniquely determined by  $b$ .  $\square$

*Remark 10.2.7.* For  $p = 2$  a Jordan splitting need not be unique. We discuss this extensively in Appendix C. See in particular Lemma C.3.3 where relation (V) as well as (VI) exhibit two distinct Jordan splittings for a non-degenerate rank 3 dyadic lattice. The summands on the left and on the right side of the equivalence are indeed non-isometric since these have different discriminants. For uniqueness for odd  $p$ , see Proposition 11.1.3.

Lemma 2.1.2 tells us that even integral lattices with odd discriminant have even rank. Let us show that this is also an application of the local classification.

<sup>1</sup>The proof gives the compatibility relation  $\rho_k(b_L^\#) = \rho^{(k)}(L, b)$ .



**Corollary 10.2.8** (Suggested by M. Schütt). *An even integral lattice of odd rank has even discriminant.*

*Proof.* The discriminant is the product of the local discriminants up to units (see (1.19)). The contribution of an odd prime is always odd. We have seen that for the prime 2 the only way to get an odd rank lattice is when diagonal forms split off. But these can only come from even forms if they are of the form  $\langle \text{unit} \cdot 2^k \rangle$  with  $k \geq 1$  and then the discriminant is even.  $\square$

### 10.3 Compatibility of Jordan Splittings for Lattices and their Discriminant Forms

In this section we compare the Jordan splitting of a given  $p$ -adic lattice with the Jordan splitting of its discriminant quadratic form as given by Theorem 9.3.12.

For  $p$  odd Proposition 9.4.1 states that homogeneous symmetric and homogeneous quadratic  $p$ -primary torsion forms are diagonalizable, just as this is the case for the  $p$ -adic lattices (cf. Proposition 10.2.2). The building blocks for homogeneous 2-primary symmetric and quadratic torsion forms are given by 9.4.2 which parallels what Proposition 10.2.2 tells us for dyadic lattices. Since Jordan splittings respect orthogonal sums, to compare Jordan splittings for  $\mathbb{Z}_p$ -lattices and those of their discriminant forms, it suffices to do this for these building blocks. The correspondence is given by Table 10.3.1. In the first two lines  $p$  is an odd prime. This table integrates the results on cyclic torsion groups from the table on page 146 and from Table 6.1.1. As a consequence, the assignment

$$\left\{ \begin{array}{l} \text{isometry classes of symmetric} \\ \text{(quadratic) } p\text{-adic lattices} \end{array} \right\} \xrightarrow{\text{discriminant form}} \left\{ \begin{array}{l} \text{isometry classes of symmetric} \\ \text{(quadratic) } p\text{-torsion groups} \end{array} \right\}$$

is surjective. It is never injective since unimodular lattices have trivial discriminant form. To make these results a bit more precise we need the following auxiliary result which is an analog of Lemma 10.2.1:

**Lemma 10.3.1.** *Let  $(G, q)$  be a non-degenerate  $p$ -adic torsion quadratic group. Write  $b$  for the polar form of  $q$ . Let  $(q(G)) \subset \mathbb{Q}_p/\mathbb{Z}_p$ ,  $(b(G, G)) \subset \mathbb{Q}_p/\mathbb{Z}_p$  be the  $\mathbb{Z}_p$ -submodule generated by the values of  $q(x)$ ,  $x \in G$ , respectively  $b(x, y)$ ,  $x, y \in G$ , and let  $x_0 \in G$  such that  $q(x_0)$  generates  $(q(G))$ . Suppose that  $2(q(G)) = (b(G, G))$  (which is the case for  $p$  odd). Then the cyclic group generated by  $x_0$  splits off orthogonally.*

*Consequently, if there is no non-degenerate cyclic torsion subgroup of  $G$  which splits off, then  $p = 2$  and  $2(q(G)) \subsetneq (b(G, G)) \subset \mathbb{Q}_2/\mathbb{Z}_2$ .*

*Proof.* A finitely generated  $\mathbb{Z}_p$ -submodule of  $\mathbb{Q}_p/\mathbb{Z}_p$  is generated by a single element: a class whose representative has smallest  $p$ -adic valuation. Using this, the proof is analogous to the proof of Lemma 10.2.1.  $\square$

Table 10.3.1: Basic non-unimodular  $p$ -adic lattices and their discriminant forms

Lattice (symmetric) —— (quadratic)	disc. group	disc. bilin. form ——	—— discr. quadr. form	
$\langle u \cdot p^k \rangle, u \in \mathbb{Z}_p^\times,$ $[u/2 \cdot p^k] u \text{ even}$	$\mathbb{Z}/p^k\mathbb{Z}$	$\langle u \cdot p^{-k} \rangle$	$[\frac{1}{2}u \cdot p^{-k}]$	
$\langle 2 \rangle, \langle -3 \cdot 2 \rangle$ [1]	$\mathbb{Z}/2\mathbb{Z}$	$\langle 2^{-1} \rangle$	$[2^{-2}]$	
$\langle 3 \cdot 2 \rangle, \langle -1 \cdot 2 \rangle$ [3]		$\langle 2^{-1} \rangle$	$[3 \cdot 2^{-2}]$	
$\langle 2^2 \rangle$ [2]	$\mathbb{Z}/2^2\mathbb{Z}$	$\langle 2^{-2} \rangle$	$[2^{-3}]$	
$\langle -3 \cdot 2^2 \rangle$ [ $-3 \cdot 2$ ]		$\langle 2^{-2} \rangle$	$[-3 \cdot 2^{-3}]$	
$\langle 3 \cdot 2^2 \rangle$ [ $3 \cdot 2$ ]		$\langle 3 \cdot 2^{-2} \rangle$	$[3 \cdot 2^{-3}]$	
$\langle -1 \cdot 2^2 \rangle$ [ $-2$ ]		$\langle 3 \cdot 2^{-2} \rangle$	$[-1 \cdot 2^{-3}]$	
$\langle u \cdot 2^k \rangle, k \geq 3$ $[u \cdot 2^{k-1}], k \geq 3$		$\mathbb{Z}/2^k\mathbb{Z}$	$\langle u \cdot 2^{-k} \rangle$	$[u \cdot 2^{-k-1}]$
$U_k, k \geq 1$			$u_k$	$u_k$
$V_1$	$u_1 = v_1$		$v_1$	
$V_k, k \geq 2$	$v_k$		$v_k$	

**Proposition 10.3.2** (Compatibility of splittings). 1. Let  $L$  be a non-degenerate symmetric or quadratic  $p$ -adic lattice with Jordan splitting

$$L = L_0 \oplus L_1(p) \oplus \cdots \oplus L_n(p^n). \tag{10.1}$$

Then its discriminant form admits a Jordan splitting

$$dg_L = dg_{L_1(p)} \oplus dg_{L_2(p^2)} \oplus \cdots \oplus dg_{L_n(p^n)}. \tag{10.2}$$

2. Given a basis for the homogeneous components of the discriminant form of  $L$ , there is a corresponding basis for the homogeneous components of  $L$ . More precisely,

$p$  odd. For all  $j \geq 1$ , let  $\{g_1^{(j)}, \dots, g_s^{(j)}\}$  be an orthogonal basis for  $dg_{L_j(p^j)}$  with  $b_j^\#(g_k^{(j)}, g_k^{(j)}) = u_{k,j} p^{-j}$ ,  $u_{k,j}$  a  $p$ -adic unit. Then there is an orthogonal basis  $\{e_1^{(j)}, \dots, e_s^{(j)}\}$  for the summand  $L_j(p^j)$  of  $L$  with  $b_j(e_k^{(j)}, e_k^{(j)}) = u_{k,j} p^j$ . A similar result is true for quadratic  $p$ -adic lattices.

$p = 2$ . For all  $j \geq 1$ , let

$$dg_{L_j(2^j)} = \bigoplus_{k=1}^{a_j} \langle u_{j,k} \cdot 2^{-j} \rangle \oplus^{b_j} v_j \oplus^{c_j} u_j, \quad u_{j,k} \in D(\mathbb{Z}/2^{j+1}\mathbb{Z}),$$

be an orthogonal direct sum splitting. Then there exists a compatible orthogonal direct sum splitting

$$L_j(2^j) = \bigoplus_{k=1}^{a_j} \langle \tilde{u}_{j,k} \cdot 2^j \rangle \oplus^{b_j} V_j \oplus^{c_j} U_j, \quad \tilde{u}_{j,k} \in D(\mathbb{Z}_2).$$

Here  $\tilde{u}_{j,k} = u_{j,k} \in \{\pm 1, \pm 3\}$  if  $j \geq 2$ , while for  $j = 1$  the representative  $\tilde{u}_{1,k} \in \{\pm 1, \pm 3\}$  coincides up to multiplication by  $-3 \pmod{8}$  with the representative  $u_{1,k} \in \{1, 3\}$ . In other words, such non-isometric rank one lattices have the same discriminant form.

For  $j \geq 2$ ,  $a_j = 0$  if and only if the ideal in  $\mathbb{Z}_2$  generated by  $b_q(L_j, L_j)$  differs from the ideal generated by  $2 \cdot q_j(L_j)$  – or – equivalently, if and only if the submodule of  $\mathbb{Q}_2/\mathbb{Z}_2$  generated by  $b_q(G_j, G_j)$ ,  $G_j = \text{dg}_{L_j(2^j)}$ , differs from the submodule generated by  $2 \cdot q_j(G_j)$ .

In particular, the vanishing or not of  $a_j$  is an intrinsic property of the lattice.

*Proof.* Assertion 1 is self-evident.

Assertion 2. We shall apply induction on the number of indecomposable summands and we may thus assume

$$L = L_j(p^j), \quad j \geq 1, \quad G = \text{dg}_L,$$

with  $(G, q)$  homogeneous of exponent  $j$ . This implies that the only elementary divisor of the discriminant group is  $(p^j)$  and that  $\langle b(L, L) \rangle = (p^j)$ .

Suppose that  $p$  is odd. Then  $2(q(G)) = (p^{-j})$ , say  $q(g) = u \cdot p^{-j}$  with  $u$  a unit and  $g \in G$ . Since  $G$  is the discriminant group of  $L$ , there is an element  $y = p^{-j}x \in L^*$  which maps to  $g$  and  $2(q(L)) = (q(x))$ . As in the proof of Lemma 10.2.1 we can split off  $\mathbb{Z}_p \cdot x$  from  $L$ . Applying induction proves the case where  $p$  is odd.

For  $p = 2$  we apply the preceding argument first to the cyclic orthogonal summands  $G$ . The corresponding rank one dyadic lattice which splits off, say  $\mathbb{Z}_2 \cdot x$ ,  $x \in L$  with  $q(x) = \tilde{u} \cdot 2^{-j}$ , is uniquely determined if  $j \geq 2$ . For  $j = 1$ , the non-isometric lattices  $\langle 2 \rangle$ ,  $\langle -3 \cdot 2 \rangle$  have the same discriminant form and the unit  $\tilde{u}$  determines which of the two we have. This is also true for the two non-isometric lattices  $\langle -1 \cdot 2 \rangle$  and  $\langle 3 \cdot 2 \rangle$ . In this way we split off all such cyclic summands. The remaining indecomposable summands have rank 2. So we now assume that  $L$  has rank 2 and  $q = b_L^\#$  with polar form  $b$ . Lemma 10.3.1 implies that there are two independent elements  $g, h \in G$  such that  $b(g, h)$  generates  $\langle b(G, G) \rangle$ . Let  $x, x' \in L$  be two independent elements such that  $2^{-j}x, 2^{-j}x' \in L^*$  and which map to  $g$  and  $h$ , respectively. By the argument used for the proof of Proposition 10.2.2, the elements  $x, x'$  span an indecomposable dyadic sublattice. If  $q = u_j$ , then  $L \simeq U_j$  and if  $q = v_j$ , then  $L \simeq V_j$ .

Finally,  $a_j = 0$  means that  $G_j$  has no cyclic summands and by Lemma 10.3.1 this is equivalent to  $2(q(G_j)) \subseteq (b_q(G_j, G_j))$ .  $\square$

*Remark 10.3.3.* In Chapter 11 we return to the nature of the discriminant form map on lattices whose rank equals the length of its discriminant quadratic form. See Proposition 11.1.3 and Proposition 11.2.4.

## 10.4 Application: the Hasse Invariants of $p$ -adic Lattices

In this section we derive some results on the Hasse invariants which are going to be used in Section 12.3. The calculations are based on the classification results for  $p$ -adic lattices we just derived. Since these split into a sum of rank one and rank two lattices, we need a general rule which governs orthogonal sums.

Recall (cf. (3.1)) that the Hasse invariant for a diagonal form  $q = \sum a_j x_j^2$ ,  $a_j \in \mathbb{Q}_v$ , is given by  $\varepsilon_v(q_v) = \prod_{i < j} (a_i, a_j)_v$ , where  $(a, b)_v$  is the Hilbert symbol (cf. Appendix A.4). From the properties of the Hilbert symbol (cf. (A.10)) we find (for any prime  $p$ ):

**Lemma 10.4.1.** *Let  $f, g$  be two non-degenerate quadratic forms over  $\mathbb{Q}_p$ . Then*

$$\varepsilon_p(f \oplus g) = \varepsilon_p(f) \cdot \varepsilon_p(g) \cdot (\text{disc}(f), \text{disc}(g))_p.$$

*Proof.* Write  $f = \sum a_k x_k^2$  and  $g = \sum b_\ell y_\ell^2$ . Then

$$\begin{aligned} \varepsilon_p(f \oplus g) &= \varepsilon_p(f) \cdot \varepsilon_p(g) \cdot \prod_{k, \ell} (a_k, b_\ell)_p \\ &= \varepsilon_p(f) \cdot \varepsilon_p(g) \cdot (\text{disc}(f), \text{disc}(g))_p. \quad \square \end{aligned}$$

Before using this, we raise a subtle point for dyadic lattices. In Chapter 3 the convention is to calculate Hasse invariants for quadratic forms  $q$  whose associated bilinear form is given by half the polar form (cf. equation (3.2)). This influences the calculation of the Hasse invariant of  $b_{\mathbb{Q}_p}$  for the prime 2 (and for that prime only). Let us illustrate this for the two basic unimodular dyadic lattices  $U$  and  $V$ . The associated 2-adic quadratic forms used for the calculation are not  $xy$  and  $x^2 + xy + y^2$  but half these forms:

$$\begin{aligned} 2^{-1}xy &= 2^{-3}((x+y)^2 - (x-y)^2) \simeq_{\mathbb{Q}_2} \frac{1}{2}u^2 - \frac{1}{2}v^2 \\ 2^{-1}(x^2 + xy + y^2) &= 2^{-1}(x + \frac{1}{2}y)^2 + \frac{3}{8}y^2 \simeq_{\mathbb{Q}_2} 2u^2 + \frac{3}{2}v^2. \end{aligned}$$

Formula (A.9) implies  $\varepsilon_2(U) = 1$  while Theorem A.4.4 can be used to show that  $\varepsilon_2(V) = -1$ . One can also verify that  $\varepsilon_2(\frac{1}{2}U) = 1$  and  $\varepsilon_2(\frac{1}{2}V) = 1$ , and so for the Hasse invariant of  $V$  the choice of  $b$  matters. With this in mind, we calculate the Hasse invariants for those lattices that we need later on.

**Lemma 10.4.2.** *1. Let  $p$  be an odd prime and suppose that  $f = p^k \cdot g$  with  $g$  unimodular of rank  $r$ . Then we have*

$$\varepsilon_p(f) = (-1)^{\frac{1}{2}r(r-1)k\varepsilon(p)} \left( \frac{\text{disc}(g)^{k(r-1)}}{p} \right), \quad \varepsilon(p) = \begin{cases} 0 & \text{if } p \equiv 1 \pmod{4} \\ 1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

*2. Let  $f$  be a unimodular dyadic quadratic lattice of rank  $r_f$  and discriminant  $d_f$ , and set*

$$\mu(f) = -r_f - d_f + 1, \quad \delta_f = \frac{1}{2}(d_f - 1).$$

Then  $\mu(f)$  is divisible by 4 and

$$\varepsilon_2(f) = (-1)^{\frac{1}{4}\mu(f)} = (-1)^{\frac{1}{4}(-r_f - d_f + 1)}.$$

If  $g$  is also a unimodular form, then  $\mu(f \oplus g) = \mu(f) + \mu(g) - 4\delta_f \cdot \delta_g$ .

*Proof.* 1. For an odd prime  $p$  a unimodular form  $g$  has Hasse invariant  $\varepsilon_p(g) = 1$  as follows from Hensel's Lemma (See Example A.4.2) and the definition of the Hasse invariant and Hilbert symbols. By Theorem A.4.4, a form  $p^k \cdot g$  thus has Hasse invariant as stated (since the exponent is only relevant modulo 2, the computation comes down to counting the number of pairs in a diagonalization of  $f$ ).

2. The addition formula for  $\mu$  follows directly. Every unimodular quadratic dyadic lattice is an orthogonal sum of copies of  $U$  and  $V$ , for both of which  $\mu$  is clearly divisible by 4. Hence  $\mu$  is divisible by 4.

The formula for  $\varepsilon_2$  for  $U$  and  $V$  can be checked directly from what we said so far. Using that for all possible dyadic units  $u, u'$  we have  $(u-1)(u'-1) \equiv 4 \pmod{8}$  if and only if  $u \equiv u' \equiv -1 \pmod{4}$ , Theorem A.4.4 implies

$$(-1)^{\frac{1}{4}(d_f - 1) \cdot (d_g - 1)} = (d_f, d_g)_2,$$

which shows that the additive formula for  $\mu$  matches the multiplicative formula for the Hasse symbols from Lemma 10.4.1. Hence the expression for  $\varepsilon_2$  holds for orthogonal sums of  $U$  and  $V$ . Again, since every unimodular quadratic dyadic lattice is an orthogonal sum of lattices isometric to  $U$  or to  $V$ , the result follows.  $\square$

**Historical and Bibliographical Notes.** That  $p$ -adic lattices admit a Jordan splitting is classical. See e.g. Chapter 8 in J. Cassels' monograph [36]. The refined version stated as Proposition 10.2.6, is essentially due to A. Durfee [56, §3]. The classification of low rank  $p$ -adic lattices in Section 10.1 as well as the material in Section 10.3 follows Chapter IV of the notes [156] by R. Miranda and D. Morrison. The application to the Hasse invariants is modeled on the proof of Theorem 8.14 in [99].

---

## Normal Forms and the Genus

### Introduction

The genus of a lattice turns out to be determined by the discriminant form and the signature of the lattice. In this chapter we shall show this for even lattices. For odd ones this is subtler and makes use of the theory developed in Chapter 12 and we relegate this to Section 12.5.

The proof uses normal forms for  $p$ -adic lattices and we compare these to the normal forms for the discriminant forms as established in Chapter 9. The Jordan splitting of a symmetric  $p$ -adic lattice given there is not unique. In Sections 11.1 and 11.2 we show that using suitable isometries essentially unique normal forms are obtained. As a consequence, each quadratic or symmetric  $p$ -primary torsion form is isometric to the discriminant form of a  $p$ -adic lattice in normal form. For  $p$  odd this is without ambiguity. In Section 11.2 we show that this is almost true for  $p = 2$  but not quite. The reason is that for the prime 2 normal forms for non-homogeneous forms can give isometric lattices. This subtle problem is relegated to Appendices C.3.A–C.3.B.

In Section 11.3, having come to grips with this problem, we achieve our goal and prove that the genus of an integral quadratic lattice is indeed completely determined by its index and discriminant quadratic form.

### 11.1 Normal Form Decomposition for odd $p$

We show that every non-degenerate symmetric torsion form  $b^\#$  on a (additively written) finite abelian  $p$ -primary group  $G$  is the discriminant form of a unique non-degenerate  $p$ -adic lattice  $L_{b^\#}$  of rank  $\ell(G)$ , the length of  $G$ . Existence has been shown in the introductory discussion of Section 10.3. To show uniqueness, we establish normal forms. We define these as follows:

**Definition 11.1.1.** Let  $p$  be an odd prime.

- A homogeneous symmetric  $p$ -adic lattice of rank  $r \geq 1$  and exponent  $k$  is in **homogeneous normal form** if it is of the form  $L_{r,u}(p^k)$ , where

$$L_{r,u} = \langle u \rangle \oplus \oplus^{r-1} \langle 1 \rangle, \quad u \in \mathbb{Z}_p^\times,$$

a unimodular lattice.

- A symmetric  $p$ -adic lattice is in **normal form** if it is an orthogonal direct sum of homogeneous normal forms.

- A  $p$ -primary symmetric torsion form is in **normal form** if it is an orthogonal sum of forms  $b_{r,u}^\#(p^{-k})$ , the symmetric discriminant form of  $L_{r,u}(p^k)$ ,  $k \geq 1$ .

Proposition 9.4.1 can be restated as the existence of normal forms for homogeneous  $p$ -primary symmetric torsion groups. We shall show that arguments similar to those of Section 9.4 establish existence of normal forms for  $p$ -adic symmetric lattices. First we observe:

**Lemma 11.1.2.** 1. For fixed  $r$  there are exactly two isometry classes for  $L_{r,u}$  distinguished by  $u$  being a square or a non-square modulo  $p$ .  
2. Every non-degenerate  $p$ -adic lattice admits a normal form of the above shape.

*Proof.* It suffices to show item 1. Because of the existence of a Jordan splitting (Proposition 10.2.6), for  $p$ -adic lattices we can reduce the proof to the unimodular situation. Any unimodular lattice is of the form  $\langle 1 \rangle \oplus \cdots \oplus \langle 1 \rangle \oplus \langle \epsilon \rangle \oplus \cdots \oplus \langle \epsilon \rangle$  where  $\epsilon$  is a non-square unit. We claim that  $\langle \epsilon \rangle \oplus \langle \epsilon \rangle$  is isometric to  $\langle 1 \rangle \oplus \langle 1 \rangle$ . To see this we turn to Example A.4.2 which shows that the equation  $\epsilon(x^2 + y^2) = 1$  has a solution in  $\mathbb{Z}_p$ , say  $(x, y) = (u, v)$ . Consequently,

$$\begin{pmatrix} u & -v \\ v & u \end{pmatrix} \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix} \begin{pmatrix} u & v \\ -v & u \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which gives an explicit isometry between  $\langle 1 \rangle \oplus \langle 1 \rangle$  and  $\langle \epsilon \rangle \oplus \langle \epsilon \rangle$ . Applying this inductively proves the result in the unimodular situation and hence in general.  $\square$

To a  $p$ -primary torsion symmetric group  $(G, b^\#)$  with  $b^\#$  in normal form

$$b^\# := b_{r_1, u_1}^\#(p^{-k_1}) \oplus \cdots \oplus b_{r_s, u_s}^\#(p^{-k_s}), \quad (11.1)$$

as given in Proposition 9.4.1, we associate the  $p$ -adic lattice

$$L_{b^\#} := L_{r_1, u_1}(p^{k_1}) \oplus \cdots \oplus L_{r_s, u_s}(p^{k_s}). \quad (11.2)$$

Here  $k_1, \dots, k_s$  are positive integers and so  $\ell(G) = \sum_{j=1}^s r_j = \text{rank}(L_{b^\#})$ . So, recalling Proposition 10.2.6, stating that the discriminant as well as the ranks of the Jordan blocks are uniquely determined, we have shown:

**Proposition 11.1.3.** Let  $p$  be an odd prime and let  $(G, b^\#)$  be a non-degenerate  $p$ -primary torsion symmetric group of length  $\ell(G)$  with  $b^\#$  in normal form (11.1). Then:

1. The lattice  $L_{b^\#}$  given by (11.2) is up to isometry the unique non-degenerate  $p$ -adic lattice of rank  $\ell(G)$  and discriminant form  $b^\#$ . Its discriminant equals  $|G| \cdot \prod_{k=1}^s u_k = |G| \cdot \delta(b^\#)$ , where  $\delta(b^\#)$  is the reduced discriminant of  $b^\#$ .
2. The discriminant form map

$$\left\{ \begin{array}{l} \text{isom. classes of } p\text{-adic} \\ \text{symmetric lattices of rank } r \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{isom. classes of } p\text{-primary torsion} \\ \text{symmetric forms of length } r \end{array} \right\}$$

is injective (and hence bijective).

Note that the restriction on the length of  $G$  is necessary in order to achieve injectivity for the map in item 2. This unicity result for normal forms makes it possible to assign unambiguously a lattice  $L_{b^\#}$  to any symmetric torsion group  $b^\#$ , even if the latter is not in normal form. Using this convention, we have the following normal forms for lattices of ranks possibly larger than the length of its discriminant form:

**Proposition 11.1.4** (Normal forms for non-degenerate  $p$ -adic lattices,  $p$  odd). *Let  $p$  be an odd prime,  $(G, b^\#)$  a non-degenerate  $p$ -primary symmetric torsion form,  $r$  an integer  $\geq \ell(G)$  and  $t = r - \ell(G)$ .*

1. *Let  $\epsilon$  be a non-square modulo  $p$ . A non-degenerate  $p$ -adic lattice  $L$  of rank  $r$  and with discriminant form  $(G, b^\#)$  is isometric to one of the following two lattices:*

$$\begin{cases} L \simeq L_{b^\#} \oplus \oplus^t \langle 1 \rangle & \text{if } \text{disc}(L) = \text{disc}(L_{b^\#}) = |G| \cdot \delta(b^\#) \\ L \simeq L_{b^\#} \oplus \langle \epsilon \rangle \oplus^{t-1} \langle 1 \rangle & \text{if } \text{disc}(L) = \epsilon \cdot \text{disc}(L_{b^\#}) = |G| \cdot \epsilon \cdot \delta(b^\#). \end{cases} \quad (11.3)$$

2. *Let  $\tilde{L}$  be a non-degenerate integral lattice of rank  $r$ . Then the discriminant form of  $\tilde{L}$  determines the localization  $\tilde{L}_p$  up to isometry.*

*Proof.* 1. This follows directly from what we have said so far since the unimodular summand has two normal forms and which of the two occurs is uniquely determined by  $\text{disc}(L)$ .

2. Let  $b^\#$  be the  $p$ -primary part of the discriminant symmetric form of the  $p$ -adic lattice  $\tilde{L}_p = \tilde{L} \otimes \mathbb{Z}_p$ . Let  $L_{b^\#}$  be the  $p$ -adic lattice determined by  $b^\#$  given in equation (11.2). For  $t$  we take  $r - \text{rank}(L_{b^\#})$ . Depending on  $p$  this results in one of the two cases mentioned in 1. To determine which of the two, one proceeds as follows. Referring to (1.18), the value of  $d_p = \text{disc}(\tilde{L}_p)$  is given by viewing the integer  $\text{disc}(\tilde{L}) = |G| \cdot \text{disc}(\tilde{L}_\infty)$  as a  $p$ -adic integer. Once  $d_p$  is found, one writes  $d_p = \epsilon_p \cdot \text{disc}(L_{b^\#})$  and if  $\epsilon_p$  is a square mod  $p$  the first alternative holds and if not, the second takes place.  $\square$

**Examples 11.1.5. 1.** We take  $p = 7$ . The squares modulo 7 are 1, 2, 4 and the non-squares are 3, 5, 6. Consider the torsion form  $b^\# = \langle 3 \cdot 7^{-1} \rangle \oplus \langle 7^{-1} \rangle \oplus \langle 5 \cdot 7^{-2} \rangle$ . This is already in normal form and it is the discriminant form of  $L_{b^\#} = \langle 3 \cdot 7 \rangle \oplus \langle 7 \rangle \oplus \langle 5 \cdot 7^2 \rangle$ . Its discriminant equals  $7^4$  (up to squares of units) and so, for example, the normal form of a 7-adic lattice  $L$  of rank 8 with discriminant  $5 \cdot 7^4$  and discriminant symmetric form  $b^\#$  is  $L = \langle 3 \cdot 7 \rangle \oplus \langle 7 \rangle \oplus \langle 5 \cdot 7^2 \rangle \oplus \langle 5 \rangle \oplus \oplus^4 \langle 1 \rangle$ .

**2.** Let us consider the normal forms of the  $p$ -adic localizations of the A-D-E root lattices, where  $p$  is an odd prime. First of all we consider the unimodular root lattice  $E_8$ . Since  $\text{disc}(E_8) = 1$ , all of its localizations have discriminant 1. Hence, the normal form of  $E_8 \otimes \mathbb{Z}_p$  is the diagonal  $p$ -adic lattice  $\oplus^8 \langle 1 \rangle$ . The normal forms of the other root lattices depend on the odd prime  $p$ . To determine these, one may use Table 4.1.1.

As an example, consider  $A_5$ , which has discriminant 6 and discriminant group isomorphic to  $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . If  $p \neq 2, 3$  the form  $A_5 \otimes \mathbb{Z}_p$  is unimodular and its discriminant is a unit in  $\mathbb{Z}_p$  which may or may not be a square modulo



$p$ . For instance, 6 is a non-square modulo 7 and so  $A_5 \otimes \mathbb{Z}_7 \cong \langle 6 \rangle \oplus \oplus^4 \langle 1 \rangle$ , while  $A_5 \otimes \mathbb{Z}_5 \cong \oplus^5 \langle 1 \rangle$  since 6 is a square modulo 5. For  $p = 3$  we need the 3-adic discriminant symmetric form of  $A_5$  which is the restriction of the discriminant form of  $A_5$  to the 3-primary part by (1.20). The discriminant form of  $A_5$  is  $\langle 5/6 \rangle$ . The 3-primary part of  $\mathbb{Z}/6\mathbb{Z}$  is isomorphic to  $\mathbb{Z}/3\mathbb{Z}$  and generated by the class of 2 in  $\mathbb{Z}/6\mathbb{Z}$ , so that the 3-adic discriminant symmetric form  $b^\#$  is determined by its value on the pair (2, 2), which is  $2^2 \cdot 5/6 \equiv 1/3$  modulo  $\mathbb{Z}$ . So  $b^\# = \langle 1/3 \rangle$  and  $L_{b^\#} = \langle 3 \rangle$ . Hence  $A_5 \otimes \mathbb{Z}_3$  has normal form  $\langle 3 \rangle \oplus \langle 2 \rangle \oplus \oplus^3 \langle 1 \rangle$  since 2 is a non-square in  $\mathbb{Z}_3$ .

## 11.2 Normal Form Decomposition for $p = 2$

For  $p = 2$  it is more involved to give normal forms. By Proposition 10.3.2 it suffices to give normal forms for homogeneous lattices and homogeneous discriminant forms. We saw that a homogeneous dyadic bilinear or quadratic form of given exponent  $j$  and given length  $\ell_j$  can be written as a direct sum

$$\bigoplus_{k=1}^{a_j} \langle \tilde{u}_{j,k} \cdot 2^j \rangle \oplus^{b_j} V_j \oplus^{c_j} U_j, \quad a_j + 2(b_j + c_j) = \ell_j,$$

but a priori this decomposition is not unique. For classifying purposes, we use the isometries below to reduce the number of representations considerably. Since the isometries are also valid between the corresponding discriminant forms, we can make similar reductions on the level of discriminant forms.

**Lemma 11.2.1** (Relations between dyadic lattices and 2-primary torsion forms). *Let  $u, u', u''$  be units in  $\mathbb{Z}_2$ . Then  $v = uu' + uu'' + u'u''$  is a 2-adic unit with  $v \equiv 3 \pmod{8}$  or  $v \equiv -1 \pmod{8}$  and the following relations hold between symmetric 2-adic lattices:*

$$U_k \oplus U_k \simeq V_k \oplus V_k, \quad k \geq 0, \quad (\text{I})$$

$$\langle u \rangle \oplus \langle u' \rangle \oplus \langle u'' \rangle (2^k) \simeq \begin{cases} V_k \oplus \langle (u + u' + u'') \cdot 2^k \rangle \\ \text{in case } uu' + uu'' + u'u'' \equiv 3 \pmod{8} \\ U_k \oplus \langle (u + u' + u'') \cdot 2^k \rangle \\ \text{in case } uu' + uu'' + u'u'' \equiv -1 \pmod{8} \end{cases} \quad k \geq 0 \quad (\text{II})$$

$$\langle u \rangle \oplus \langle u' \rangle (2^k) \simeq \langle -3u \rangle \oplus \langle -3u' \rangle (2^k), \quad k \geq 0 \quad (\text{III})$$

There are similar relations (I) – (III) between the corresponding discriminant forms.

The proofs, although straightforward, have been placed in Appendix C.3.A. The relation (II) serves to reduce the number of cyclic summands to at most 2, and using (I), the number of summands  $V_k$  can be reduced to at most 1. This leads to the following definition.

**Definition 11.2.2.** • A homogeneous symmetric dyadic lattice of rank  $r$  and exponent  $k$  is in **normal form** if it is of the form  $L(2^k)$  with

$$L = \bigoplus_{i \leq a} \langle u^{(i)} \rangle \oplus \bigoplus^b V \oplus^c U, \quad a \leq 2, b \leq 1, c = \frac{1}{2}(r - a) - b \geq 0, u^{(i)} \in \mathbb{Z}_2^\times.$$

For  $k = 0$  and  $L$  an even dyadic lattice, the cyclic forms are not present, that is,  $a = 0$  in this case.

- A symmetric dyadic lattice is in **normal form** if it is the orthogonal direct sum of homogeneous normal forms.
- A 2-primary symmetric (quadratic) torsion form is in **normal form** if it is the discriminant form of a symmetric (quadratic) dyadic lattice in normal form.

The above relations immediately imply the following result:

**Proposition 11.2.3.** • Let  $(L, b)$  be a non-degenerate symmetric (quadratic) dyadic lattice. Then  $L$  is isometric to a normal form and so is its symmetric (quadratic) discriminant form.

- Every 2-primary symmetric (quadratic) torsion form is isometric to a normal form. Moreover, there is a one-to-one correspondence between normal forms for symmetric and quadratic torsion forms on the same torsion group (with the same notation, as illustrated in the table below).

It should be observed right away that two different 2-primary quadratic torsion forms can have isometric symmetric torsion forms which complicates the classification. Table 9.1.1 shows that, furthermore, the basic symmetric (quadratic) torsion form  $b^\#$  (resp.  $q^\#$ ) of length  $\leq 2$  can be the discriminant form of several lattices (of rank equal to the length of the torsion group) which in the table are denoted  $L_{b^\#}$ , (resp.  $L_{q^\#}$ ).

Table 11.2.1: Symmetric versus quadratic torsion forms ( $p = 2$ )

exponent	$b^\#$	$L_{b^\#}$	$q^\#$	$L_{q^\#}$	$u$
1	$\langle 2^{-1} \rangle$	$\langle u \cdot 2 \rangle$	$[2^{-2}]$	$\langle u \cdot 2 \rangle$	$1, -3 \pmod 8$
1	$\langle 2^{-1} \rangle$	$\langle 3u \cdot 2 \rangle$	$[3 \cdot 2^{-2}]$	$\langle 3u \cdot 2 \rangle$	$1, -3 \pmod 8$
2	$\langle 2^{-2} \rangle$	$\langle u \cdot 2^2 \rangle$	$[3u \cdot 2^{-3}]$ ,	$\langle u \cdot 2^2 \rangle$	$1, -3 \pmod 8$
2	$\langle 3 \cdot 2^{-2} \rangle$	$\langle 3u \cdot 2^2 \rangle$	$[3u \cdot 2^{-3}]$	$\langle 3u \cdot 2^2 \rangle$	$1, -3 \pmod 8$
$\geq 3$	$\langle u \cdot 2^{-k} \rangle$	$\langle u \cdot 2^k \rangle$	$[u \cdot 2^{-k-1}]$	$\langle u \cdot 2^k \rangle$	$\pm 1, \pm 3 \pmod 8$
1	$u_1$	$U_1$	$u_1$	$U_1$	
1	$v_1 = u_1$	$V_1$	$v_1$	$V_1$	
$\geq 2$	$u_k$	$U_k$	$u_k$	$U_k$	
$\geq 2$	$v_k$	$V_k$	$v_k$	$V_k$	

To explain this, recall that symmetric (quadratic) torsion forms on the cyclic group  $\mathbb{Z}/2^k\mathbb{Z}$  have been classified in Table 6.1.1. If  $k \geq 3$  non-isometric quadratic torsion groups have non-isometric polar forms and determine the same rank one lattice  $L_{b^\#}$ . A symmetric torsion group  $G$  isomorphic to  $\mathbb{Z}/2\mathbb{Z}$  or to  $\mathbb{Z}/4\mathbb{Z}$  is the discriminant form of four, respectively two rank one dyadic lattices having different

values for  $|G|^{-1} \text{disc}(L_{b^\#}) \pmod 8$ . Hence the occurrence of two or four non-isometric dyadic lattices with isometric discriminant form. In the quadratic situation this discordance happens only for  $\mathbb{Z}/2\mathbb{Z}$  and then each form is the discriminant form of two non-isometric lattices.

As for  $U_k$  and  $V_k$ , recall (cf. Table 10.3.1) that the quadratic discriminant symmetric forms  $u_1$  and  $v_1$  have the same polar form. Consequently, the two non-isometric quadratic lattices  $U_1, V_1$  have isometric symmetric discriminant forms but non-isometric quadratic discriminant forms. For  $k \geq 2$  this discrepancy does not occur.

**Quadratic Dyadic Lattices.** The previous considerations lead to Table 11.2.2 which enumerates certain lattices  $L_{q^\#}, L_{q^\#}^{(1)}, L_{q^\#}^{(2)}$  associated to homogeneous 2-primary torsion forms  $q^\#$  in standard form (here  $u \equiv \pm 1, \pm 3 \pmod 8$  if  $k \geq 2$  and  $u \equiv 1, 3 \pmod 4$  if  $k = 1$ ).

Table 11.2.2: Homogeneous dyadic quadratic normal forms of exponent  $k \geq 1$ .

Discriminant form $q^\#$	Range	$a$	$b$	$ G ^{-1} \text{disc}(L_{q^\#})$	Normal form $L_{q^\#}$
$\oplus^c u_k$	$k \geq 1$	0	0	$(-1)^c$	$L_{q^\#} = \oplus^c U_k$
$\oplus^c u_k \oplus v_k$	$k \geq 1$	0	1	$3(-1)^c$	$L_{q^\#} = \oplus^c U_k \oplus V_k$
$[u \cdot 2^{-k-1}] \oplus^c u_k$	$k \geq 2$	1	0	$u \cdot (-1)^c$	$L_{q^\#} = \langle u \cdot 2^k \rangle \oplus^c U_k$
$[u \cdot 2^{-k-1}] \oplus$ $\oplus^c u_k \oplus v_k$	$k \geq 2$	1	1	$3u \cdot (-1)^c$	$L_{q^\#} = \langle u \cdot 2^k \rangle \oplus$ $\oplus^c U_k \oplus V_k$
$[u \cdot 2^{-k-1}] \oplus [u' \cdot 2^{-k-1}]$ $\oplus^c u_k$	$k \geq 2$	2	0	$uu' \cdot (-1)^c$	$L_{q^\#} = \langle u \cdot 2^k \rangle \oplus \langle u' \cdot 2^k \rangle$ $\oplus^c U_k$
$[u \cdot 2^{-k-1}] \oplus [u' \cdot 2^{-k-1}]$ $\oplus^c u_k \oplus v_k$	$k \geq 2$	2	1	$3uu' \cdot (-1)^c$	$L_{q^\#} = \langle u \cdot 2^k \rangle \oplus \langle u' \cdot 2^k \rangle$ $\oplus^c U_k \oplus V_k$
$\langle u \cdot 2^{-1} \rangle \oplus^c u_1$	$k = 1$	1	0	$u \cdot (-1)^c$ $-3u \cdot (-1)^c$	$L_{q^\#}^{(1)} = \langle u \cdot 2 \rangle \oplus^c U_1$ $L_{q^\#}^{(2)} = \langle -3u \cdot 2 \rangle \oplus^c U_1$
$[u \cdot 2^{-2}] \oplus$ $\oplus^c u_1 \oplus v_1$	$k = 1$	1	1	$3u \cdot (-1)^c$ $-u \cdot (-1)^c$	$L_{q^\#}^{(1)} = \langle u \cdot 2 \rangle \oplus$ $\oplus^c U_1 \oplus V_1$ $L_{q^\#}^{(2)} = \langle -3u \cdot 2 \rangle \oplus$ $\oplus^c U_1 \oplus V_1$
$[u \cdot 2^{-2}] \oplus [u' \cdot 2^{-2}]$ $\oplus^c u_1$	$k = 1$	2	0	$uu' \cdot (-1)^c$ $-3uu' \cdot (-1)^c$	$L_{q^\#}^{(1)} = \langle u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle$ $\oplus^c U_1$ $L_{q^\#}^{(2)} = \langle -3u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle$ $\oplus^c U_1$
$[u \cdot 2^{-2}] \oplus [u' \cdot 2^{-2}]$ $\oplus^c u_1 \oplus v_1$	$k = 1$	2	1	$3uu' \cdot (-1)^c$ $-uu' \cdot (-1)^c$	$L_{q^\#}^{(1)} = \langle u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle$ $\oplus^c U_1 \oplus V_1$ $L_{q^\#}^{(2)} = \langle -3u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle$ $\oplus^c U_1 \oplus V_1$

From the table we derive the classification:

**Proposition 11.2.4.** *Let  $(G, q^\#)$  be a quadratic 2-primary torsion group of length  $r$  decomposed into homogeneous normal form. Then the following two types of forms occur, each with different behaviour with respect to normal forms:*

**Type 1.** *No cyclic orthogonal summands of order 2 split off from  $q^\#$ . Then there is a unique isometry class of a dyadic lattice  $L$  of rank  $r$  with discriminant form  $q^\#$  represented by the normal form  $L_{q^\#}$  with discriminant  $\delta(q^\#) \cdot |G|$ .*

**Type 2.** *Otherwise there are precisely two isometry classes  $L_{q^\#}^{(i)}$ ,  $i = 1, 2$ , of rank  $r$  lattices with discriminant form  $q^\#$  in normal form characterized by their discriminants,  $\text{disc}(L_{q^\#}^{(1)}) = \delta(q^\#) \cdot |G|$ , respectively  $\text{disc}(L_{q^\#}^{(2)}) = -3 \cdot \delta(q^\#) \cdot |G|$ .*

Moreover the discriminant form map

$$\left\{ \begin{array}{l} \text{isom. classes of dyadic} \\ \text{quadratic lattices of rank } r \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{isom. classes of 2-primary torsion} \\ \text{quadratic forms of length } r \end{array} \right\}$$

is surjective, and injective on the preimage of type 1 forms, and two-to-one onto on the preimage of type 2 forms.

*Proof.* As we explained at the start of the section, every quadratic torsion form is isometric to one in normal form. On the other hand, by Proposition 10.3.2, every quadratic torsion form is the discriminant quadratic form of a dyadic lattice with a similar Jordan splitting. So, if we start with a quadratic dyadic form  $q^\#$ , then there is an isometry bringing  $q^\#$  in normal form and a corresponding lattice  $L$  in normal form whose discriminant quadratic torsion form is isometric to  $q^\#$ .

We only have to check in which cases several non-isometric lattices in normal form have discriminant forms with the same normal form. As explained just before the statement of this proposition, if  $k \geq 2$  this does not occur. For  $k = 1$ , one sees from the tables that as soon as one or two cyclic summands of type  $\langle u \cdot 2^{-1} \rangle$  are present there are exactly two non-isometric lattices in normal form whose discriminant form is the given one. A priori, in case  $a = 2$  (see Definition 11.2.2 and Table 11.2.2), there could be more such lattices, but relation (III) (see Lemma 11.2.1), which has not been used yet, in each case reduces the possibilities to the two stated ones.

We see from Table 11.2.2 that these two lattices in normal form have distinct discriminant and so are not isometric, while their discriminant forms are isometric. Indeed, as we recalled before starting the proof, in the latter situation the units  $u, u'$  have to be considered modulo 4 instead of modulo 8.  $\square$

**Examples 11.2.5. 1.** From Table 11.2.2 we see that there are two normal forms of non-degenerate quadratic torsion forms on  $\oplus^5 \mathbb{Z}/2^3 \mathbb{Z}$ . First of all,  $\langle u \cdot 2^{-3} \rangle \oplus^2 u_3$ , the discriminant form of  $\langle u \cdot 2^3 \rangle \oplus^2 U_3$ , and, secondly,  $\langle u \cdot 2^{-3} \rangle \oplus u_3 \oplus v_3$ , the discriminant form of  $\langle u \cdot 2^3 \rangle \oplus U_3 \oplus V_3$ .

**2.** On  $\oplus^6 \mathbb{Z}/2\mathbb{Z}$  we have the following possibilities for non-degenerate quadratic torsion forms:

- $\oplus^3 u_1$ , the discriminant form of  $\oplus^3 U_1$ ;
- $\oplus^2 u_1 \oplus v_1$ , the discriminant form of  $\oplus^2 U_1 \oplus V_1$ ;
- $\langle u \cdot 2^{-1} \rangle \oplus \langle u' \cdot 2^{-1} \rangle \oplus^2 u_1$ , the discriminant form of  $\langle u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle \oplus^2 U_1$  or of  $\langle -3u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle \oplus^2 U_1$ ;
- $\langle u \cdot 2^{-1} \rangle \oplus \langle u' \cdot 2^{-1} \rangle \oplus u_1 \oplus v_1$ , the discriminant form of  $\langle u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle \oplus U_1 \oplus V_1$  or of  $\langle -3u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle \oplus U_1 \oplus V_1$ .

We next use the above classification to find normal forms for discriminant forms of several integral lattices related to root lattices.

3. The unimodular lattice  $E_8$  has discriminant 1. Likewise,  $E_8 \otimes \mathbb{Z}_2$  is unimodular with discriminant 1. Hence (see Example 10.2.3) it is isometric to  $\oplus^4 U \otimes \mathbb{Z}_2$ . To find the discriminant form for  $L = E_8(2^k)$ , arguing as in Example 1.6.8.2, we see that  $b_{L \otimes \mathbb{Z}_2}^\# = b_L^\# \simeq \oplus^4 u_k$ .

4. The lattice  $E_7$  has 2-primary discriminant quadratic form  $q^\# = \langle 3 \cdot 2^{-1} \rangle$  with  $L_{q^\#}^{(1)} = \langle 3 \cdot 2 \rangle$  and  $L_{q^\#}^{(2)} = \langle -1 \cdot 2 \rangle$ . Then  $E_7 \otimes \mathbb{Z}_2$  has normal form  $\langle -1 \cdot 2 \rangle \oplus \oplus^3 U$  since  $\text{disc}(E_7) = 2 = (-2) \cdot (-1)^3$ . Turning to  $E_7(2^k)$ , one then finds that  $q_{E_7(2^k)}^\# = \langle -2^{-k-1} \rangle \oplus \oplus^3 u_k$ .

The next task is to describe standard forms for dyadic lattices  $L$  whose ranks are not necessarily equal to the length of their discriminant group  $\text{dg}_L$ . Observe that a unimodular even  $\mathbb{Z}_2$ -lattice must have even rank as follows from the normal form decomposition. So the unimodular summands that need to be added to the forms  $L_{q^\#}$  or  $L_{q^\#}^{(1)}, L_{q^\#}^{(2)}$  can only be of rank two. This explains why  $\text{rank}(L) - \ell(G)$  is an even number in the statement of the main result, the analog of Proposition 11.1.4.

**Proposition 11.2.6** (Normal forms for quadratic dyadic lattices). *Let  $(G, q^\#)$  be a 2-primary quadratic torsion group,  $r$  an integer  $\geq \ell(G)$  and  $t = r - \ell(G)$ .*

1. *A non-degenerate even 2-adic lattice  $L$  of rank  $r$  and with discriminant quadratic form  $(G, q^\#)$  is isometric to one of the following two types of lattices:*
  - (a) *If  $q^\#$  has no cyclic orthogonal summands of order 2 in its normal form decomposition, then*

$$L \simeq \begin{cases} \oplus^{\frac{1}{2}t} U \oplus L_{q^\#} & \text{if } \text{disc}(L) = \text{disc}(L_{q^\#}) \cdot (-1)^{\frac{1}{2}t} \\ \oplus^{\frac{1}{2}t-1} U \oplus V \oplus L_{q^\#} & \text{if } \text{disc}(L) = \text{disc}(L_{q^\#}) \cdot 3 \cdot (-1)^{\frac{1}{2}t-1}. \end{cases} \quad (11.4)$$

- (b) *Otherwise, that is, if  $q^\# \simeq \langle u \cdot 2^{-1} \rangle \oplus q'$  for some unit  $u \in \mathbb{Z}_2$ , then*

$$L \simeq \oplus^{\frac{1}{2}t} U \oplus L_{q^\#}^{(i)}, \quad i = 1, 2. \quad (11.5)$$

*Which of the two cases occurs can be determined as follows: If  $\delta(q^\#) \cdot |G| \equiv (-1)^{\frac{1}{2}t} \text{disc}(L) \pmod{4}$ , then  $i = 1$  and otherwise  $i = 2$ .*

2. Let  $\tilde{L}$  be a non-degenerate even integral lattice of rank  $r$ . Then the discriminant form of  $\tilde{L}$  determines the localization  $\tilde{L}_2$  uniquely up to isometry.

*Proof.* 1. Case (a) follows from what we have said. If  $\langle u \cdot 2^{-1} \rangle$  occurs, one uses relation (I) from Lemma 11.2.1 to replace  $V$  with  $U$  should it occur. Then apply Proposition 11.2.4.

2. This is a direct consequence of the foregoing.  $\square$

**Examples 11.2.7.** We return to the non-degenerate quadratic forms  $q^\#$  on the first two torsion groups listed in Examples 11.2.5 and corresponding dyadic lattices  $L_{q^\#}$ . Here we search for dyadic lattices  $L$  of rank  $4 + \ell(G)$  where  $G$  is the stated discriminant group.

1. For the first example with  $G = \oplus^5 \mathbb{Z}/2^3 \mathbb{Z}$ ,  $\ell(G) = 5$ , there are two possible quadratic forms  $q^\#$ :

- $q^\# = \langle u \cdot 2^{-3} \rangle \oplus^2 u_3$  with  $L_{q^\#} = \langle u \cdot 2^3 \rangle \oplus^2 U_3$ . Then either  $L \simeq \langle u \cdot 2^3 \rangle \oplus^2 U_3 \oplus^2 U$  with discriminant  $u \cdot 2^{15}$  or  $L \simeq \langle u \cdot 2^3 \rangle \oplus^2 U_3 \oplus U \oplus V$  with discriminant  $-3u \cdot 2^{15}$ . So in this case  $\text{disc}(L) \neq -u, 3u$ .
- $q^\# = \langle u \cdot 2^{-3} \rangle \oplus u_3 \oplus v_3$  with  $L_{q^\#} = \langle u \cdot 2^3 \rangle \oplus U_3 \oplus V_3$ . Then either  $L \simeq \langle u \cdot 2^3 \rangle \oplus U_3 \oplus V_3 \oplus^2 U$  with discriminant  $-3u \cdot 2^{15}$  or  $L \simeq \langle u \cdot 2^3 \rangle \oplus U_3 \oplus V_3 \oplus U \oplus V$  with discriminant  $u \cdot 2^{15}$  (up to squares of units) and here also  $\text{disc}(L) \neq -u, 3u$ . So no rank 9 lattices  $L$  with  $\text{dg}_L = G$  and  $\text{disc}(L) = -u, 3u$  exist.

2. For the second example,  $G = \oplus^6 \mathbb{Z}/2\mathbb{Z}$ ,  $\ell(G) = 6$  and there are four possible  $q^\#$ . We search for rank 10 dyadic lattices  $L$  with discriminant  $-3 \cdot 2^6$ , starting with the rank 6 lattices  $L_{q^\#}$  in the first two cases and both forms  $L_{q^\#}^{(i)}$ ,  $i = 1, 2$ , in the last two cases:

- $L_{q^\#} = \oplus^3 U_1$  has discriminant  $-2^6$ . It is impossible to get the required discriminant  $-3 \cdot 2^6$  from this since  $U \oplus U$  has discriminant 1.
- $L_{q^\#} = \oplus^2 U_1 \oplus V_1$  has discriminant  $3 \cdot 2^6$  which is not possible for the same reason.
- Here  $L_{q^\#}^{(1)} = \langle u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle \oplus^2 U_1$  and one has  $\text{disc}(L_{q^\#}^{(1)}) = uu' \cdot 2^6$ . However,  $L = L_{q^\#}^{(1)} \oplus^2 U$  has discriminant  $uu' \cdot 2^6$  which is never equal to  $-3 \cdot 2^6$  since  $u, u' \in \{1, 3\}$ .  
If  $L_{q^\#}^{(2)} = \langle -3u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle \oplus^2 U_1$ , the discriminant is  $-3uu' \cdot 2^6$  and in order that  $L = L_{q^\#}^{(2)} \oplus^2 U$ , we must have  $uu' = 1$ , i.e.,  $u = u'$ .
- Here  $L_{q^\#}^{(1)} = \langle u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle \oplus U_1 \oplus V_1$  or  $L_{q^\#}^{(2)} = \langle -3u \cdot 2 \rangle \oplus \langle u' \cdot 2 \rangle \oplus U_1 \oplus V_1$  with discriminant  $-3uu' \cdot 2^6$ , respectively  $uu' \cdot 2^6$ . In the first case  $L = L_{q^\#}^{(1)} \oplus U \oplus U$  and so we must have  $uu' = 1$ , i.e.,  $u = u'$ . The second case is impossible.

### 11.3 Characterizing the Genus of a Quadratic Lattice

Recall that the genus of a non-degenerate symmetric lattice  $L$  consists of the set of isometry classes of lattices whose localisations are isometric to those of  $L$ , and

that the isometry class of  $L_\infty = L_\mathbb{R}$  is determined by its signature since  $L_\infty$  is non-degenerate. For prime numbers  $p$  the isometry class of the localization  $L_p$  is determined by its Hasse invariant, but only over the field  $\mathbb{Q}_p$  and so extra information is needed. Classically this gives a description of the genus in terms of Hasse invariants.

We show now a major consequence of what we have done in this chapter, namely a characterization of the genus for non-degenerate quadratic lattices (equivalently, non-degenerate even symmetric lattices). It uses the notion of genus invariant:

**Definition.** The *genus invariant* of a non-degenerate integral quadratic lattice  $(L, q)$  is the triple  $\mathfrak{g}(L) := (r_+, r_-, [q_L^\#])$ , where  $(r_+, r_-)$  is the signature of  $L$  and  $[q_L^\#]$  is the isometry class of the discriminant quadratic form  $q_L^\#$  of  $L$ .

**Theorem 11.3.1** (Nikulin [171, Cor. 1.9.4]). *The genus of a non-degenerate quadratic lattice  $(L, q)$  is completely determined by its genus invariant  $\mathfrak{g}(L)$ .*

*Proof.* The discriminant group  $\text{dg}_L$  of  $L$  splits into its  $p$ -primary constituents. Now formula (1.19) from Chapter 1 shows that up to sign these determine the discriminant of  $L$  while the signature yields the sign. Formula (1.18) then shows how to extract  $\text{disc}(L_p)$  for a given prime  $p$ . The rank of  $L$  is also determined from the signature and we have now all the ingredients to apply Propositions 11.1.4 and 11.2.6. As we saw, these results make it possible to determine the isometry class of  $L_p$  given a), the  $p$ -primary part of the discriminant form  $q^\#$ , and b), the local discriminant  $\text{disc}(L_p)$ .  $\square$

**Examples 11.3.2. 1.** The lattices  $\Gamma_{16}$  and  $\Gamma_8 \oplus \Gamma_8 (\simeq E_8 \oplus E_8)$ . We calculate the Hasse invariants using Lemma 10.4.2. Being unimodular, both have  $\varepsilon_p = 1$  for  $p$  odd. Since  $\text{disc}(\Gamma_8) = \text{disc}(\Gamma_{16}) = 1$  we find  $\mu(\Gamma_8 \oplus \Gamma_8) = \mu(\Gamma_{16}) = -16$  and so  $\varepsilon_2(f) = 1$  in both cases. It follows that both lattices have the same Hasse invariants. This shows that there is an isometry between the localized lattices, but the isometry is a priori only over  $\mathbb{Q}_p$ . The case  $\mathbb{Q}_\infty$  is evident. The next example shows that they are isometric over  $\mathbb{Z}_p$ , i.e. they belong to the same genus.

**2. Unimodular quadratic lattices.** These have 0 discriminant form and hence the genus is completely determined by the signature. In particular all positive definite even unimodular lattices of the same rank are in one genus.

**Historical and Bibliographical Notes.** Most of this material is due to V. Nikulin, cf. [171]. The proof of Lemma 11.2.1 is from Ch. IV of the preprint [156] by R. Miranda–D. Morrison.

---

## Integral Lattices: the Discriminant Form

### Introduction

In this chapter we consider integral lattices in relation to their discriminant forms.

We saw in Chapter 11 that every  $p$ -primary quadratic torsion group is the discriminant form of a  $p$ -adic lattice. A further natural question is: Is every quadratic torsion group the discriminant form of an integral lattice? This is indeed the case as is shown in Section 12.1. Clearly, uniqueness does not hold since the discriminant form for a unimodular lattice is zero. Conversely, a non-degenerate lattice with zero discriminant form is unimodular. However, this is the only obstruction to uniqueness as we shall show in Section 12.2. Since the index of a unimodular even lattice is divisible by 8, this result enables us to define the mod 8 index of a quadratic torsion form  $q^\#$ , denoted  $\tau_8(q)$ , as the index of any even lattice with  $q^\#$  as discriminant quadratic form.

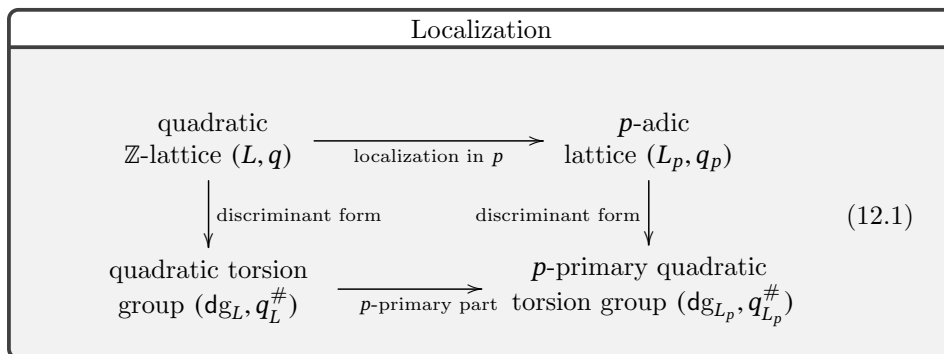
A more precise existence result can be stated provided one prescribes the signature, say  $(r_+, r_-)$ : The main result, Theorem 12.4.4 of Section 12.4, states that (modulo some technical condition), a quadratic torsion form  $q^\#$  with  $\tau_8(q^\#) \equiv r_+ - r_- \pmod{8}$  is the discriminant form of a non-degenerate even integral lattice with signature  $(r_+, r_-)$  provided of course the rank  $r_+ + r_-$  is at least as large as the length of  $q^\#$ . This result pins down the importance of the index mod 8. It turns out that knowing its values for the basic building blocks is essential. These are calculated in Section 12.3.

In Section 12.5 the techniques developed so far are applied to odd lattices. This uses the basic observation that if  $L$  is any lattice, even or odd, the lattice  $L(2)$  is certainly even. From previous results on even lattices it follows firstly that also the genus of an odd lattice is determined by its signature and discriminant bilinear form. Secondly, these lead to an existence criterion for odd lattices.

### 12.1 Existence of Quadratic Integral Lattices with Given Discriminant Form

Analogous to diagram 1.20 – which applies to symmetric lattices – there is a commutative diagram in the quadratic setting (equivalently, for even symmetric lattices):





In other words, the discriminant group of  $L_p = L \otimes \mathbb{Z}_p$  is the  $p$ -primary part  $G_p$  of the discriminant group of  $L$  and the discriminant form for  $L_p$  can be identified with the restriction to  $G_p$  of the discriminant form for  $L$ .

The main results of Chapter 11 can be summarized concisely by saying that the right-most vertical arrow is surjective. We next prove an existence result which shows that the left-most vertical arrow is a surjection:

**Theorem 12.1.1.** *Every non-degenerate quadratic torsion form is the discriminant quadratic form of a non-degenerate quadratic lattice.*

*Proof.* Let us recall that in Section 9.3 we showed that a non-degenerate quadratic torsion form splits orthogonally into homogeneous  $p$ -primary torsion groups. These decompose further, as we saw in Section 9.4, into orthogonal sums of forms on the cyclic groups  $\mathbb{Z}/p^k\mathbb{Z}$  and (if  $p = 2$ ) into the binary forms  $u_k$  or  $v_k$ . So it suffices to show that each of these is the discriminant form of some even lattice.

To start, by Proposition 4.3.9 the rank one torsion groups  $\langle a \cdot p^{-k} \rangle$  are all realized as the discriminant form of some even lattice.

Next,  $u_k$  is obtained as the discriminant quadratic form of the lattice  $\mathbb{Z}e \oplus \mathbb{Z}f$  with Gram matrix given by  $\begin{pmatrix} 0 & 2^k \\ 2^k & 0 \end{pmatrix}$ . This is clear: the dual module is given by  $\mathbb{Z}e^* \oplus \mathbb{Z}f^*$  and  $e^* = 2^{-k}e, f^* = 2^{-k}f$  with  $e^* \cdot f^* = 2^{-2k} \cdot 2^k = 2^{-k}$ .

Finally, we claim that the inverse  $\tilde{V}_k, k \geq 1$ , of the matrix

$$W_k := \begin{pmatrix} 2^{1-k} & 2^{-k} & 0 & 0 \\ 2^{-k} & 2^{1-k} & 1 & 0 \\ 0 & 1 & 2a & 1 \\ 0 & 0 & 1 & 2(-1)^{k-1} \end{pmatrix}, \quad a = \frac{1}{3}(2^k - (-1)^k), \quad (12.2)$$

is the Gram matrix of an even rank 4 lattice whose discriminant form is  $v_k$ . Note that  $a$  is a (positive) integer. To prove the claim, one first computes  $\det(W_k) = 2^{-2k}$ . Hence  $\tilde{V}_k$ , which equals  $2^{2k}$  times the adjugate matrix of  $W_k$ , is clearly integral and has even entries on the diagonal. Since  $W_k$  modulo the integers gives  $v_k$ , applying Lemma 1.6.3.2, shows that the discriminant form of  $\tilde{V}_k$  is  $v_k$ .  $\square$

*Remark 12.1.2.* The reader may wonder why one cannot find a rank 2 integral lattice in order to realize  $v_k$  of length two. To explain this, if there would have been

a rank two integral lattice with discriminant quadratic form  $v_k$ , by Theorem 12.4.4, we would have  $\text{disc}(V_k) = \pm 2^{2k}$  in  $D(\mathbb{Z}_2)$  which is not the case since  $\text{disc}(V_k) = 3 \cdot 2^{2k}$ .

## 12.2 Stable Equivalence and Discriminant Forms

Unimodular lattices have trivial discriminant lattice. This motivates the notion of stable equivalence.

**Definition 12.2.1.** Two non-degenerate symmetric lattices  $L_1$  and  $L_2$  are *stably equivalent* if there are unimodular lattices  $U_1$  and  $U_2$  such that  $L_1 \oplus U_1$  and  $L_2 \oplus U_2$  are isometric. If  $L_1$  and  $L_2$  are even and  $U_1$  and  $U_2$  can be taken even as well, then we say that  $L_1$  and  $L_2$  are *evenly stably equivalent*.

Stably equivalent lattices have isomorphic discriminant forms. The converse is also true:

**Theorem 12.2.2.** *Two non-degenerate symmetric integral lattices with isometric discriminant symmetric forms are stably equivalent. Two non-degenerate quadratic lattices with isometric discriminant quadratic forms are evenly stably equivalent.*

*Proof.*<sup>1</sup> Let  $L_1, L_2$  be two non-degenerate lattices and let  $\bar{f}$  be an isometry of their discriminant bilinear forms. Recall that we view  $L_1, L_2$  as sublattices of  $L_1^*, L_2^*$  via the correlation homomorphisms  $b_{L_1}, b_{L_2}$ . The idea is to first find a suitable lift  $f : L_1^* \rightarrow L_2^*$  of  $\bar{f}$  as a group homomorphism and as a second step to construct – using  $f$  and  $\bar{f}$  – two unimodular lattices  $U_1$  and  $U_2$  such that there is an isometry

$$L_1 \oplus U_1 \simeq L_2 \oplus U_2. \tag{12.3}$$

To construct  $f$ , choose bases for the lattices  $L_j^*$ ,  $j = 1, 2$ , such that the first  $m$  vectors, say  $e_1^{(j)}, \dots, e_m^{(j)}$ , map to generators  $\bar{e}_1^{(j)}, \dots, \bar{e}_m^{(j)}$  of  $L_j^*/L_j$  which are adapted to the elementary divisors of the respective discriminant groups (note that for  $j = 1, 2$  the  $m$  is the same by the uniqueness statement in the elementary divisor theorem A.1.2). If  $\bar{f}(\bar{e}_k^{(1)}) = \sum \bar{a}_{k\ell} \bar{e}_\ell^{(2)}$ ,  $\bar{a}_{ij} \in \mathbb{Q}/\mathbb{Z}$ , choose representatives  $a_{ij} \in \mathbb{Q}$  and set  $f(e_k^{(1)}) = \sum a_{k\ell} e_\ell^{(2)}$ . The remaining basis vectors of  $L_1^*$ , if these exist, are mapped to 0. Such a lift need not be a surjection, nor does it necessarily preserve the bilinear forms. For our choice of lift the image misses the basis vectors of  $L_2^*$  that map to zero in  $\text{dg}_{L_2}$ , but these belong to  $L_2 \subset L_2^*$ . And indeed, from the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{b_{L_1}} & L_1^* & \longrightarrow & \text{dg}_{L_1} \longrightarrow 0 \\ & & \downarrow f|_{L_1} & & \downarrow f & & \downarrow \bar{f} \simeq \\ 0 & \longrightarrow & L_2 & \xrightarrow{b_{L_2}} & L_2^* & \longrightarrow & \text{dg}_{L_2} \longrightarrow 0 \end{array}$$

<sup>1</sup>Proof is due to A. Durfee, cf. [56, Thm. 4.1].

it follows that

$$f(L_1^*) + L_2 = L_2^*. \quad (12.4)$$

The remainder of the proof is now divided into several steps. We use a dot to denote the bilinear forms on  $L_1^*$  as well as on  $L_2^*$ .

**Step 1: Constructing the unimodular lattice  $U_2$ .** We set

$$U_2 := (L_1 \oplus L_1^*, b_f), \quad b_f(x \oplus y, x' \oplus y') = x \cdot y' + y \cdot x' + (y \cdot y' - f(y) \cdot f(y')).$$

Using that  $\bar{f}$  preserves the forms on the discriminant groups we find

$$\begin{aligned} f(y) \cdot f(y') &\equiv \bar{f}(\bar{y}) \cdot \bar{f}(\bar{y}') \\ &\equiv y \cdot y' \pmod{\mathbb{Z}}, \end{aligned} \quad (12.5)$$

and so  $y \cdot y' - f(y) \cdot f(y')$  is an integer. It follows that  $U_2$  is an integral lattice. It is unimodular as we show now. First of all  $b_f(x, x') = 0$  for  $x, x' \in L_1 = L_1 \oplus 0 \subset L_1 \oplus L_1^*$ . Next, we choose a basis  $\{e_1, \dots, e_n\}$  for  $L_1$  and let  $\{e_1^*, \dots, e_n^*\}$  be the dual basis which we use for the summand  $L_1^*$ . Then  $b_f(e_i, e_j^*) = b_f(e_i^*, e_j) = \delta_{ij}$  and so the matrix of  $b_f$  becomes

$$\begin{pmatrix} 0 & \mathbf{1}_n \\ \mathbf{1}_n & * \end{pmatrix}$$

with determinant  $(-1)^n$ .

**Step 2:  $L_1^*$  embeds isometrically in  $U_2 \oplus L_2^*$  with image the graph  $\Gamma_f$  of  $f$ .**

Recall that  $U_2 = L_1 \oplus L_1^*$  and so the map  $f$  gives an embedding  $L_1^* \xrightarrow{\iota} U_2 \oplus L_2^*$ ,  $\iota(y) = (0, y, f(y))$  which preserves the symmetric form (also denoted by a dot) because

$$\begin{aligned} \iota(y) \cdot \iota(y') &= (0, y, f(y)) \cdot (0, y', f(y')) \\ &= b_f(y, y') + f(y) \cdot f(y') \\ &= y \cdot y' - f(y) \cdot f(y') + f(y) \cdot f(y') \\ &= y \cdot y', \quad y, y' \in L_1^*. \end{aligned}$$

In other words, the embedding  $\iota$  establishes an isometry between  $L_1^*$  and the graph  $\Gamma_f$  of  $f$  considered as a sublattice of  $U_2 \oplus L_2^*$ .

**Step 3: There is an orthogonal decomposition  $U_2 \oplus L_2^* = \Gamma_f \oplus \Gamma_f^\perp$  with  $\Gamma_f^\perp$  unimodular, yielding**

$$U_1 := \Gamma_f^\perp.$$

This is shown by proving the following assertions:

- (a) The form on  $U_2 \oplus L_2^*$  restricts non-degenerately to  $\Gamma_f$ ;
  - (b)  $\Gamma_f \oplus \Gamma_f^\perp = U_2 \oplus L_2^*$ .
  - (c)  $\Gamma_f^\perp$  is unimodular.
- (a) This is clear since the sublattice  $\Gamma_f \subset U_2 \oplus L_2^*$  is isometric to  $L_1^*$  which is non-degenerate.
- (b) We first prove two auxiliary assertions about  $L_1 \oplus L_1^* \oplus L_2 \subset U_2 \oplus L_2^*$ :
- Claim I:*  $L_1 \oplus L_1^* \oplus L_2 \subset L_1 + \Gamma_f^\perp$  and

*Claim II:*  $L_1 \oplus L_1^* \oplus L_2 \subset \Gamma_f + \Gamma_f^\perp$ .

To show (I), start with a vector  $\mathbf{t} = (x, y, z) \in L_1 \oplus L_1^* \oplus L_2$ . Recall that  $y \cdot u - f(y) \cdot f(u)$ ,  $u \in L_1^*$ , is an integer by (12.5). Also  $z \cdot f(u) \in \mathbb{Z}$  since  $z \in L_2$  and  $f(u) \in L_2^*$ . So the vector  $\mathbf{t}$  leads to the integral function  $\varphi_{\mathbf{t}}$  on  $L_1^*$  given by

$$\varphi_{\mathbf{t}}(u) = y \cdot u - f(y) \cdot f(u) + z \cdot f(u).$$

Since  $\varphi_{\mathbf{t}} \in \text{Hom}_{\mathbb{Z}}(L_1^*, \mathbb{Z}) = (L_1^*)^* = L_1$  we can write  $\varphi_{\mathbf{t}}(u) = -w \cdot u$  for some  $w \in L_1$ . The sign is chosen so that the vector  $(w, y, z)$  is orthogonal to the graph  $\Gamma_f$ :

$$\begin{aligned} (w, y, z) \cdot (0, u, f(u)) &= w \cdot u + (y \cdot u - f(y) \cdot f(u) + z \cdot f(u)) \\ &= w \cdot u + \varphi_{\mathbf{t}}(u) = 0. \end{aligned}$$

So  $(x, y, z) = (x-w, 0, 0) + (w, y, z) \in L_1 + \Gamma_f^\perp$ . This shows the inclusion  $L_1 \oplus L_1^* \oplus L_2 \subset L_1 + \Gamma_f^\perp$ .

We next show (II). Let  $x \in L_1$  and write  $\iota(x) = (0, x, f(x))$  so that  $x - \iota(x) = (x, -x, -f(x))$ . This vector is orthogonal to the graph of  $f$  since for all  $y \in L_1^*$  one has

$$(x, -x, -f(x)) \cdot (0, y, f(y)) = x \cdot y - x \cdot y + f(x) \cdot f(y) - f(x) \cdot f(y) = 0.$$

Since  $x = x - \iota(x) + \iota(x)$ ,  $\iota(x) \in \Gamma_f$ , it follows that  $L_1 \subset \Gamma_f + \Gamma_f^\perp$ . Claim I now implies Claim II.

*Completion of the proof of (b):* We first show the inclusion of  $U_2 \oplus L_2^* \subset \Gamma_f + \Gamma_f^\perp$ . Let  $(x, y, z) \in U_2 \oplus L_2^* = L_1 \oplus L_1^* \oplus L_2^*$ . Since  $L_2^* = f(L_1^*) + L_2$ , we can write  $z = f(u) + v$  with  $u \in L_1^*$ ,  $v \in L_2$ . Then

$$(x, y, z) = (x, y - u, v) + (0, u, f(u))$$

with  $(x, y - u, v) \in L_1 \oplus L_1^* \oplus L_2$  and  $(0, u, f(u)) \in \Gamma_f$ . By Claim II we have  $L_1 \oplus L_1^* \oplus L_2 \subset \Gamma_f + \Gamma_f^\perp$ , so that  $(x, y - u, v) + (0, u, f(u)) \in \Gamma_f + \Gamma_f^\perp$ .

Conversely,  $\Gamma_f + \Gamma_f^\perp \subset L_1 \oplus L_1^* \oplus L_2^* = U_2 \oplus L_2^*$ , and so the two sets are equal. Moreover, the sum  $\Gamma_f + \Gamma_f^\perp$  is an orthogonal direct sum because  $\Gamma_f$  is non-degenerate.

(c). To prove that  $\Gamma_f^\perp$  is unimodular, we show that  $|\text{disc}(\Gamma_f^\perp)| = 1$ . To do so we take discriminants in the equality derived in part b. First recall that by Remark 1.2.1.2 the notion of discriminant makes sense for non-integral lattices, and secondly, that by Lemma 1.6.3 one has  $|\text{disc}(L_1^*)| = 1/|\text{disc}(L_1)| = 1/|\text{dg}_{L_1}|$  and, similarly,  $\text{disc}(L_2^*) = 1/|\text{dg}_{L_2}|$ . So  $|\text{disc}(L_1^*)| = |\text{disc}(L_2^*)|$ . Next, from  $\Gamma_f \oplus \Gamma_f^\perp \cong U_2 \oplus L_2^*$  we obtain

$$|\text{disc}(\Gamma_f)| \cdot |\text{disc}(\Gamma_f^\perp)| = |\text{disc}(U_2)| \cdot |\text{disc}(L_2^*)|.$$

As  $U_2$  is unimodular,  $\Gamma_f \simeq L_1^*$  and hence  $|\text{disc}(\Gamma_f)| = |\text{disc}(L_1^*)| = |\text{disc}(L_2^*)|$ , we conclude  $|\text{disc}(\Gamma_f^\perp)| = 1$ . Consequently,  $\Gamma_f^\perp$  is unimodular.

**Step 4: Completion of the proof in the symmetric case.**

We have constructed two unimodular integral lattices,  $U_2$  and  $U_1$  with the property that  $U_2 \oplus L_2^* = \Gamma_f \oplus U_1$ . Since  $U_2$  and  $U_1$  are unimodular, and hence

self-dual, dualizing the above equality of lattices gives  $U_2 \oplus L_2 = \Gamma_f^* \oplus U_1$ . The isometry  $\iota : L_1^* \simeq \Gamma_f$  yields an isometry  $\Gamma_f^* \simeq L_1$  and so  $L_2 \oplus U_2 \simeq L_1 \oplus U_1$ , that is, we have established our goal (12.3) and so  $L_1$  and  $L_2$  are stably equivalent.

**Step 5: Quadratic lattices.**

The proof is easily adapted as follows. Let us use  $q_j$  for the quadratic forms on  $L_j$ . On  $U_2$  we have a quadratic form  $q_f(x, y) := x \cdot y + q_1(y) - q_2(f(x))$ . Its polar form is  $b_f$  and  $\iota$  preserves  $q_f$ . So the two unimodular lattices  $U_2$  and  $\Gamma_f^\perp$  are quadratic which shows the assertion for the even case.  $\square$

By Theorem 2.4.2 all even unimodular lattices  $L$  have index  $\tau(L)$  divisible by 8. This leads to the following definition.

**Definition 12.2.3.** The *index modulo 8* of a non-degenerate quadratic torsion group  $(G, q)$ , denoted  $\tau_8(q)$ , is the modulo 8 integer  $\tau(L) \bmod 8$  of any non-degenerate quadratic lattice  $L$  whose discriminant form is  $q$ .

This makes sense since by Theorem 12.1.1 we can always find a quadratic lattice for which a given quadratic torsion group is its discriminant form; any two such choices are stably equivalent by Theorem 12.2.2 and hence have the same index mod 8:

**Corollary 12.2.4.** Let  $(G, q)$  be a non-degenerate quadratic torsion group and  $L$  a non-degenerate quadratic lattice with  $q_L^\# = q$ . Then

$$\tau_8(q) \equiv \tau(L) \pmod{8}$$

is independent of the choice of  $L$ .

The index modulo 8 is additive in  $\mathbb{Z}/8\mathbb{Z}$ , that is  $\tau_8(q_1 \oplus q_2) = \tau_8(q_1) + \tau_8(q_2)$ .

**Examples 12.2.5.** Consider the examples of Section 10.1:

1. Using Table 4.1.1 we find for instance that  $\tau_8[\frac{n}{2(n+1)}] = n \bmod 8$ . This follows since the quadratic torsion group  $[\frac{n}{2(n+1)}]$  is the discriminant form of the positive definite lattice  $A_n$  of rank  $n$ .
2. We have  $\tau_8(u_k) = 0$  since  $\tau(U(k)) = 0$ .
3. Recall the notation  $\tilde{V}_k^{-1}$  for the even integral lattice (12.2) representing  $v_k$ . For  $k = 6$  we find the quadratic form  $W_6 = 2^{-5}(x_1^2 + x_1x_2 + x_2^2) + x_2x_3 + 21x_3^2 + x_3x_4 - x_4^2$  on its dual whose signature is the same as that of  $\tilde{V}_6^{-1}$ . Since  $\det(\tilde{V}_6^{-1}) > 0$  and the value of the quadratic form on the fourth basis vector is negative, the signature must be  $(2, 2)$  and so  $\tau_8(v_6) = 0$ . We give the argument for all  $k$  when proving Proposition 12.3.3.

## 12.3 Calculation of the Index Mod 8

In this section we calculate  $\tau_8$ , the index mod 8, for the quadratic torsion groups that are the basic building blocks. The simplest of these is the form  $\langle \frac{s}{t} \rangle$  with  $s$

and  $t$  co-prime, and  $0 < s < |t|$ . The main input consists of the integral lattice  $(\mathbb{Z}^{n+1}, Q)$  with discriminant  $\pm t$  up to squares and with discriminant bilinear form  $\langle \frac{s}{t} \rangle$  constructed in Proposition 4.3.9. It uses the euclidean algorithm for  $(t, s)$  which yields the inverse  $Q^{-1}$  of the Gram matrix and since the signature of  $Q$  is the same as the signature for  $Q^{-1}$ , this gives a way to calculate the index mod 8. The computations also involve the Hasse invariants.

Before we illustrate this in some numerical examples, we first recall that the euclidean algorithm for  $(t, s)$  inductively gives numbers  $a_k, d_k$  such that

$$\begin{pmatrix} d_{k+1} \\ d_{k+2} \end{pmatrix} = B_k \begin{pmatrix} d_k \\ d_{k+1} \end{pmatrix}, \quad B_k = \begin{pmatrix} 0 & 1 \\ -1 & a_k \end{pmatrix},$$

starting with  $d_0 = t, d_1 = s$  and ending if  $d_n = \pm 1$ . The  $a_k$  are determined by demanding that  $a_k d_{k+1}$  is the even multiple of  $d_{k+1}$  closest to  $d_k$ . The matrix  $Q^{-1}$  is determined from the  $a_k$ : The last  $n$  diagonal elements for  $Q^{-1}$  are  $a_0, \dots, a_{n-1}$  and the left upper diagonal entry equals  $s/t$ . The algorithm can also be given in terms of the inverses  $A_k = B_k^{-1} = \begin{pmatrix} a_k & -1 \\ 1 & 0 \end{pmatrix}$  ending with (see Corollary 4.3.5)

$$A_0 \cdots A_n = \pm \begin{pmatrix} t & -s^* \\ s & -t^* \end{pmatrix}.$$

The numbers  $s^*, t^*$ , which are not needed to determine the index mod 8 in any given example, come up in the theoretic arguments below. In the calculations that follow  $|t|$  is a prime power.

- Examples 12.3.1.** 1. We construct an even lattice with discriminant form  $\langle 4 \cdot 5^{-2} \rangle$ . Let  $s = 4, t = 5^2$ . Since  $25 = 6 \cdot 4 - (-1)$ , we get  $A_0 = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix}$  and  $A_1 = \begin{pmatrix} -4 & -1 \\ 1 & 0 \end{pmatrix}$ . Since  $a_0 = 6$  we get  $Q^{-1} = \begin{pmatrix} 4 \cdot 5^{-2} & 1 \\ 1 & 6 \end{pmatrix}$ . Hence  $Q = \begin{pmatrix} -150 & 25 \\ 25 & -4 \end{pmatrix}$ . Since  $\det Q = -25 < 0$ , the index of  $Q$  must be zero, and so the index mod 8 of  $\langle 4 \cdot 5^{-2} \rangle$  is also zero.
2. Consider now  $\langle -\frac{2}{3} \rangle$ . Here  $-3 = 2 \cdot (-2) - (-1)$  and hence  $Q^{-1} = \begin{pmatrix} -\frac{2}{3} & 1 \\ 1 & -2 \end{pmatrix}$ , with inverse  $Q = \begin{pmatrix} -6 & -3 \\ -3 & -2 \end{pmatrix}$  which is negative definite, as one easily verifies. Hence  $\tau_8(\langle -\frac{2}{3} \rangle) = -2$  (one can also use  $A_2(-1)$ ).
3. The even form with matrix  $Q$  and discriminant form  $\langle \frac{2}{5} \rangle$  we found in Example 4.3.11 shows that the signature is  $(1, 1)$  and so its index mod 8 is zero.
4. For  $\langle \frac{5}{8} \rangle$  we find  $a_0 = a_1 = 2$  and  $a_2 = -2$  so that

$$Q^{-1} = \begin{pmatrix} 5 \cdot 2^{-3} & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} \text{ and } Q = \begin{pmatrix} -24 & 16 & -8 \\ 16 & -10 & 5 \\ -8 & 5 & -2 \end{pmatrix}.$$

The signature of  $Q$  is found to be  $(2, 1)$  and hence the index mod 8 of  $\langle \frac{5}{8} \rangle$  is 1.

Let us now pass to the situation where  $t = p^k$ ,  $p$  a prime, and if  $p$  is odd,  $s$  is an even number co-prime to  $p$ , while if  $p = 2$ ,  $s$  is odd. We use the method of Lemma 4.3.6 to diagonalize this form over  $\mathbb{Q}$ . This is possible, even if this form is not integral, since the computation of  $Q^{-1}$  is based on a slight extension of the euclidean algorithm as follows. Rewrite the relation  $ss^* - tt^* = 1$  as  $1/t = (s/t) \cdot s^* - t^*$ . Recall (Corollary 4.3.5) that  $d_{n+1}^* = s^*$ ,  $d_n^* = t^*$ . Now set  $d_{n+2}^* = 1/t$ ,  $a_{-1} = s/t$  and consider

$$\begin{aligned} d_{n+2}^* &= a_{-1}d_{n+1}^* - d_n^* \\ \vdots & \\ d_k^* &= a_{n-k+1}d_{k-1}^* - d_{k-2}^* \\ \vdots & \\ d_2^* &= a_{n-1}d_1^* - d_0^*. \end{aligned}$$

To be able to imitate the procedure of Lemma 4.3.6 we let  $c_k = d_{n+1-k}^*/d_{n-k}^*$ ,  $k = -1, \dots, n-1$ . This gives the recurrence  $c_k = a_k - 1/c_{k+1}$ ,  $k = -1, \dots, n-2$ . As in the proof of Lemma 4.3.6-3 we find (with  $y_{-1} = x_{-1}$  and  $y_m = x_m + 1/c_m \cdot x_{m-1}$ ,  $m = 0, \dots, n-1$ )

$$\begin{aligned} \sum_{k=-1}^{n-1} a_k x_k^2 + \sum_{k=0}^{n-1} 2x_k x_{k-1} &= \sum_{k=-1}^{n-1} c_k y_k^2 \\ &= Q'(y_{-1}) + Q''(y_0, \dots, y_{n-1}), \end{aligned} \quad (12.6)$$

and hence  $\sum_{k=-1}^{n-1} c_k y_k^2$  of rank  $r = n+1$  as diagonal form. Now the discriminant of the first term  $Q'(y_{-1}) = c_{-1}y_{-1}^2$  equals  $c_{-1} = d_{n+2}^*/d_{n+1}^* = (1/t)/s^* = 1/(s^*t)$ . Up to squares the discriminant is then the integer  $s^*t = s^*p^k$ . Since the discriminant of  $\sum_{k=-1}^{n-1} c_k y_k^2$  is  $\pm t$  (the discriminant of  $Q$ ), the discriminant of the remaining term,  $Q''(y_0, \dots, y_{n-1})$ , is, again up to squares,  $\pm s^*$ .

To find the index mod 8, we proceed as follows. We use the splitting  $Q = Q' + Q''$  to inductively calculate the Hasse invariants  $\varepsilon_q(Q)$  at all primes  $q$ . Recall their definition (3.1) and the convention  $\varepsilon_q(Q) = 1$  if  $\text{rank}(Q) = 1$ . It turns out that only the primes  $p$  and 2 matter. The product formula (3.6) for the Hasse invariants,  $\prod_{v \in \mathcal{P}} \varepsilon_v(Q) = 1$ , then gives  $\varepsilon_\infty(Q)$  which incorporates the index. We finally recall (cf. Theorem A.4.4) that in the expressions for the Hilbert symbols the following functions on odd integers  $n$  play a role:

$$\varepsilon(n) = \begin{cases} 0 & \text{if } n \equiv 1 \pmod{4} \\ 1 & \text{if } n \equiv -1 \pmod{4} \end{cases} \quad (12.7)$$

$$\omega(n) = \begin{cases} 0 & \text{if } n \equiv \pm 1 \pmod{8} \\ 1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases} \quad (12.8)$$

**12.3.A  $p$  odd.** We write  $\text{disc}(Q) = \sigma p^k$ , where  $\sigma = \pm 1$ . For any prime  $q \neq p$ , the form  $Q$  is unimodular as a form in  $\mathbb{Z}_q$ . Applying Lemma 10.4.2 we conclude that  $\varepsilon_q(Q) = 1$  if  $q \neq 2, p$ . For the prime  $p$  we argue as follows. Write  $Q \simeq_{\mathbb{Q}} Q' + Q''$  as in (12.6). Since  $\text{disc}(Q'')$  is an integer prime to  $p$ , the form  $Q''$  is unimodular

as a form in  $\mathbb{Z}_p$  and again  $\varepsilon_p(Q'') = 1$ . Now apply Lemma 10.4.1 which shows  $\varepsilon_p(Q) = (p^k \cdot s^*, \sigma s^*)_p$ . Since in this situation  $ss^* \equiv 1 \pmod p$ , using Theorem A.4.4, we thus find

$$\begin{aligned} \varepsilon_p(Q) &= (p^k s, \sigma s)_p, \\ &= \left(\frac{s}{p}\right)^k \cdot \left(\frac{\sigma}{p}\right)^k = \begin{cases} \left(\frac{s}{p}\right)^k & \text{if } \sigma = 1 \\ \left(\frac{s}{p}\right)^k \cdot (-1)^{k\varepsilon(p)} & \text{if } \sigma = -1. \end{cases} \end{aligned} \tag{12.9}$$

Next, observe that  $Q$  is an even integral form with odd discriminant and so  $Q_2$  is a unimodular  $\mathbb{Z}_2$ -form. For those we have calculated in Lemma 10.4.2 that

$$\varepsilon_2(Q) = (-1)^{\frac{1}{4}(-\text{rank}(Q) - \text{disc}(Q) + 1)}.$$

Set  $\text{rank}(Q) = r = r_+ + r_-$  and recall that  $\tau = r_+ - r_-$  is the index of  $Q$  and that  $\varepsilon_\infty(Q) = (-1)^{\frac{1}{2}r_-(r_--1)}$  (see Remark 3.3.6.2). Then

$$\varepsilon_\infty(Q) \cdot \varepsilon_2(Q) = (-1)^{\frac{1}{4}(-r - \text{disc}(Q) + 1 + 2r_-(r_--1))}.$$

Observe that  $-r + 1 + 2r_-(r_--1) + \tau = 2r_-(r_--2) + 1$  is equal to 1 (mod 8) if  $r_-$  is even and to -1 (mod 8) otherwise, while  $\sigma$ , the sign of  $\text{disc}(Q)$ , equals  $(-1)^{r_-}$ . Hence

$$\varepsilon_\infty(Q) \cdot \varepsilon_2(Q) = \begin{cases} (-1)^{\frac{1}{4}(-\tau - p^k + 1)} & \text{if } \sigma = 1 \\ (-1)^{\frac{1}{4}(-\tau + p^k - 1)} & \text{if } \sigma = -1. \end{cases} \tag{12.10}$$

The product formula for the Hasse symbols implies that the right-hand side of (12.10) equals the right-hand side of (12.9). For  $k$  even  $p^k \equiv 1 \pmod 8$  and so we get  $\tau \equiv 0 \pmod 8$ ; for  $k$  odd we have  $p^k - 1 \equiv p - 1 \pmod 8$  and so we may take  $k = 1$ . The result does not depend on  $\sigma$  because the quotient of the values of the right-hand side of (12.9) for  $\sigma = 1$  and  $\sigma = -1$  equals  $(-1)^{\varepsilon(p)}$ , which equals  $(-1)^{\frac{1}{2}(p-1)}$ , the quotient of the two values on the right-hand side of (12.10) (remember that  $\varepsilon(p) = 0$  if  $p \equiv 1 \pmod 4$  and  $\varepsilon(p) = 1$  if  $p \equiv 3 \pmod 4$ ). So we may set  $\sigma = 1$  and a straightforward comparison gives  $\tau \equiv 1 - p \pmod 8$  if  $\left(\frac{s}{p}\right) = 1$ , and  $\tau \equiv 5 - p \pmod 8$  otherwise, as summarized in the table appearing in the next proposition.

**Proposition 12.3.2.** *The values of  $\tau_8$  for  $\langle \frac{s}{p^k} \rangle$ ,  $p$  odd, are as follows.*

$p \pmod 8$	$k$ even	$k$ odd, $\left(\frac{s}{p}\right) = 1$	$k$ odd, $\left(\frac{s}{p}\right) = -1$
1	0	0	4
-1	0	2	-2
3	0	-2	2
-3	0	4	0

As a check consider Examples 12.3.1.1 and 2. The first,  $\langle 4 \cdot 5^{-2} \rangle$ , has  $k = 2$  which is even and the table confirms that we have vanishing index mod 8. For the second,  $\langle -2 \cdot 3^{-1} \rangle$ , one has  $k = 1$  and since  $-2 \equiv 1 \pmod 3$  is a quadratic residue, we have  $\tau_8 \equiv -2 \pmod 8$  as in the table.



### 12.3.B The prime $p = 2$ .

**Proposition 12.3.3.** *The mod 8 indices of the basic building blocks for  $p = 2$  are as follows.*

- **Forms of length 1.** Here we have  $\tau_8\left(\left\langle \frac{s}{2^k} \right\rangle\right) \equiv s + 4k\omega(s) \pmod{8}$  which yields the table

$s \pmod{8}$	$k$ even	$k$ odd
1	1	1
-1	-1	-1
3	3	-1
-3	-3	1

- **The form  $u_k$ .** Here  $\tau_8(u_k) = 0$  for  $k = 1, 2, \dots$
- **The form  $v_k$ .** Depending on the parity of  $k$  we find

$$\tau_8(v_k) \equiv \begin{cases} 0 \pmod{8} & k \text{ even,} \\ 4 \pmod{8} & k \text{ odd.} \end{cases}$$

*Proof. Length 1 forms.* The cases  $k = 1, 2$  can be easily dealt with using Table 4.1.1. We next assume  $k \geq 3$ .

We calculate  $\varepsilon_2(Q)$  where  $Q^{-1}$  is now associated to the inverse euclidean algorithm for the pair  $(s, t = 2^k)$  yielding  $s^*, t^*$  with  $ss^* - tt^* = 1$ . Again, we write  $Q = Q' + Q''$  with  $\text{disc}(Q') = 2^k s^*$  and  $\text{disc}(Q'') = \sigma s^*$ , where  $\sigma$  is the sign of  $\det Q$ . So, if, as before,  $\text{rank}(Q) = r$  and  $(r_+, r_-)$  is the signature of  $Q$ , then  $r_-$  is even if and only if  $\sigma = +$ . Let us first assume that  $\sigma = -$ . Then, as before, one has

$$\begin{aligned} \varepsilon_2(Q) &= \varepsilon_2(Q') \cdot \varepsilon_2(Q'') \cdot (\text{disc}(Q'), \text{disc}(Q''))_2 \\ &= \varepsilon_2(Q'')(2^k s^*, -s^*)_2 \\ &= (-1)^{k\omega(s^*)} \varepsilon_2(Q''). \end{aligned}$$

The form  $Q''$  is unimodular in  $\mathbb{Z}_2$  and, again by Lemma 10.4.2, we find

$$\varepsilon_2(Q'') = (-1)^{\frac{1}{4}(-\text{rank}(Q'') - \text{disc}(Q'') + 1)} = (-1)^{\frac{1}{4}(-r + s^* + 2)}.$$

Now  $\varepsilon_2(Q) = \varepsilon_\infty(Q) = (-1)^{\frac{1}{2}r_-(r_- - 1)}$ , and so we find  $2r_-(r_- - 1) + r \equiv 2 + s^* + 4k\omega(s^*) \pmod{8}$ . Using  $\tau = r^+ - r^-$  this can be written  $2r_-^2 + \tau \equiv 2 + s^* + 4k\omega(s^*) \pmod{8}$ . As explained before,  $\sigma = -$  implies that  $r_-$  is odd. So the previous line gives  $\tau \equiv s^* + 4k\omega(s^*) \pmod{8}$  and the result follows since  $s^* \equiv s \pmod{8}$  for  $k \geq 3$  (use  $ss^* - tt^* = 1$ ). If  $\text{disc}(Q'') = s^*$  the calculation is similar, using that now  $r_-$  is even and  $(\text{disc}(Q'), \text{disc}(Q''))_2 = (-1)^{k\omega(s^*) + \varepsilon(s^*)^2}$ .

**The form  $u_k$ .** This is easy since the lattice  $U(2^k)$  of index 0 has  $u_k$  as its discriminant form.

**The form  $v_k$ .** The signature is the same as the signature of the matrix  $W_k$  given by (12.2). We know that  $\tilde{V}_k$ , the inverse of  $W_k$ , satisfies  $\text{disc}(\tilde{V}_k) > 0$  and so the signature can be either  $(4, 0)$ ,  $(0, 4)$  or  $(2, 2)$ . The entry of  $W_k$  at place  $(1, 1)$  is

positive and so  $(0, 4)$  is not possible. If  $k$  is even, the entry of  $W_k$  at place  $(4, 4)$  is negative and so then the signature is  $(2, 2)$ . The case of odd  $k$  remains, where we verify Sylvester's criterion stating that a matrix is positive definite if all the leading principal minors are positive. In this situation we only have to check the third principal minor which equals  $2^{1-2k}$  and so is indeed positive. Hence the index is 4 in this case.  $\square$

*Remark 12.3.4.* The previous calculations also imply that for 2-primary quadratic torsion forms  $q$  one has the equality  $\tau_8(q(\frac{1}{2})) = \tau_8(q) + 4\omega(\delta(q)) \pmod 8$ . By additivity of  $\tau_8$  and of  $\omega(\delta(q))$ , it suffices to check this for the building blocks. For rank 1 this is statement 1 of the previous proposition. Since  $\omega(\delta(u_k)) = 0$  and  $\omega(\delta(v_k)) = 1$  the claimed equality also holds for  $u_k$  and  $v_k$ .

## 12.4 Applications to the Genus: Existence of Even Lattices

By Theorem 11.3.1, the genus of a non-degenerate quadratic integral lattice is completely determined by the genus invariant, that is, the signature and the discriminant form. In this section we consider the question: which genus invariants occur? To answer it, we first quote the following well-known conditions for the existence of a rational form:

**Theorem** ([204, IV.3.3]). *Given  $d \in D(\mathbb{Q})$ , non-negative integers  $r_+, r_-$  with  $r_+ + r_- \geq 3$ , and for each  $v \in \mathcal{P}$  a number  $\varepsilon_v \in \{1, -1\}$ . There exists a rational quadratic form  $q$  of rank  $\geq 3$  with discriminant  $d$ , signature  $(r_+, r_-)$ , rank  $r = r_+ + r_-$  and Hasse invariants  $\varepsilon_v$  if and only if*

1. almost all  $\varepsilon_v$  are 1 and  $\prod_v \varepsilon_v = 1$ ;
2.  $d_\infty = (-1)^{r-}$  (in  $D(\mathbb{R})$ ) and  $\varepsilon_\infty = (-1)^s$ ,  $s = \frac{1}{2}r_-(r_- - 1)$ .

Note that the genus of a rational form  $q$  consists of the (isometry classes of) rational forms with the same local forms  $q_v$  and so the latter necessarily satisfy some conditions, for instance all local discriminants are localizations of the rational number  $d = \text{disc}(q)$ . In particular one has  $d_\infty = (-1)^{r-}$ . Likewise  $\varepsilon_\infty = (-1)^s$  and so if we impose the condition  $d = d_v$  for all  $v \in \mathcal{P}$ , the only remaining condition is the first condition.

For rank 2 forms a further condition is stated in loc. cit.: we must exclude the combination  $\text{disc}(q) = -1 \in D(\mathbb{Q}_v)$ ,  $\varepsilon_v(q) = -1$ . If we are given a genus of a rank 2 rational form this combination is automatically excluded:  $\text{disc}(q) = -1 \in D(\mathbb{Q}_v)$  is only possible for a form of signature  $(1, 1)$  and such a form is isometric to  $a(x_1^2 - x_2^2)$  which has Hasse invariant  $\varepsilon_v(q) = (1, -1)_v = 1$ . Consequently, we arrive at the following existence result (cf. also [36, Ch 6, Thm. 1.3]):

**Theorem 12.4.1.** *Let  $L$  be a  $\mathbb{Q}$ -vector space of dimension  $\geq 2$  and suppose that for every  $v \in \mathcal{P}$  a non-degenerate quadratic form  $q_v$  on  $L_v$  is given. Let  $d$  be a non-zero rational number. Suppose that*

1.  $\text{disc}(\mathbf{q}_v) = d$  for all  $v \in \mathcal{P}$  (where we consider  $d \in D(\mathbb{Q}_v)$  under the natural homomorphism  $D(\mathbb{Q}) \rightarrow D(\mathbb{Q}_v)$  induced by  $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$ );
2.  $\varepsilon_v(\mathbf{q}_v) = 1$  for almost all  $v \in \mathcal{P}$  and the product formula  $\prod_{v \in \mathcal{P}} \varepsilon_v(\mathbf{q}_v) = 1$  holds.

Then there exists a  $\mathbb{Q}$ -valued (non-degenerate) quadratic form  $\mathbf{q}$  on  $L$  such that  $\text{disc}(\mathbf{q}) = d$  (up to squares) and the localization of  $\mathbf{q}$  at  $v$  is isometric to  $\mathbf{q}_v$  for all  $v \in \mathcal{P}$ .

There is also a Hasse principle for integral lattices which roughly states that existence over  $\mathbb{Q}$  implies existence over the integers:

**Theorem 12.4.2** (Hasse principle for lattices). *Let  $n \geq 1$ ,  $d \neq 0$  be integers. Suppose that for every prime  $p$  a non-degenerate  $p$ -adic integral quadratic form  $\mathbf{q}_p$  of rank  $n$  and discriminant  $d$  is given, as well as a real valued form  $\mathbf{q}_\infty$  of rank  $n$  and discriminant  $d$ . If there exists a rational quadratic form  $\mathbf{g}$  such that  $\mathbf{g}_v \simeq \mathbf{q}_v \otimes \mathbb{Q}_v$  for all  $v \in \mathcal{P}$ , then there exists an integral quadratic form  $\mathbf{q}$  whose localization at  $v$  is equivalent (over  $\mathbb{Z}_v$ ) to  $\mathbf{q}_v$  for all places  $v \in \mathcal{P}$  (with the convention that  $\mathbb{Z}_\infty = \mathbb{R}$ ).*

For a proof we refer to [36, Ch. 9, Thm. 1.2]. We rephrase the preceding results using the relation between the discriminant of an integral lattice and the orders of the local discriminant groups as given in (1.19). This step is used to translate the existence criterion in terms of the local discriminant quadratic forms.

**Corollary 12.4.3.** *Let  $L$  be a free  $\mathbb{Z}$ -module of finite rank  $r \geq 2$ . Suppose that a pair  $(r_+, r_-)$  of non-negative integers is given with  $r = r_+ + r_-$ , and for every prime  $p$  a non-degenerate  $p$ -adic integral quadratic form  $\mathbf{q}_p$  on  $L_p$ .*

*There exists a non-degenerate integral quadratic form  $\mathbf{q}$  on  $L$  such that  $\mathbf{q} \otimes \mathbb{Z}_p \simeq \mathbf{q}_p$  for all primes  $p$  and with signature  $(r_+, r_-)$  (corresponding to a real form  $\mathbf{q}_\infty$  with this signature) if and only if the following conditions hold:*

1.  $L_p$  is unimodular for almost all primes  $p$ ;
2. Setting<sup>2</sup>  $d = (-1)^{r_-} \prod_{p \text{ prime}} |\text{dg}_{L_p}|$ , then up to a  $p$ -adic unit  $\text{disc}(\mathbf{q}_p) = d$  for all primes  $p$ ;
3. The product formula  $\prod_{v \in \mathcal{P}} \varepsilon_v(\mathbf{q}_v) = 1$  holds.

*Proof.* Let us first show that the conditions are necessary. If an integral quadratic lattice  $(L, \mathbf{q})$  exists, for almost all  $v \in \mathcal{P}$  the lattice  $L_v$  is unimodular, which shows item 1. If  $L_v$  is unimodular and  $v = p$  is an odd prime, by Lemma 10.4.1 its Hasse invariant is equal to 1. So  $\varepsilon_v(\mathbf{q}_v) = 1$  except for a finite set of places and the product formula makes sense. Since for a rational form  $\mathbf{q}(x) = \sum a_j x_j^2$ , by definition  $\varepsilon_v(\mathbf{q}) := \prod_{i < j} (a_i, a_j)_v$ , the Hilbert product formula (Theorem A.4.6) implies then that  $\prod_{v \in \mathcal{P}} \varepsilon_v(\mathbf{q}) = 1$ , proving 3.

<sup>2</sup>Recall that  $\text{dg}_{L_p}$  is the discriminant group of the lattice  $L_p$ .

By equations (1.18) and (1.19) we have

$$\begin{aligned} \text{disc}(L) &= (-1)^{r-} |\mathbf{d}g_L| \\ &= (-1)^{r-} \prod_{p \text{ prime}} |\mathbf{d}g_{L_p}|. \end{aligned} \tag{12.11}$$

Since  $|\mathbf{d}g_{L_q}|$  is a unit in  $\mathbb{Z}_p$  for any prime  $q$  different from a given prime  $p$ , condition 2 holds as well.

Conversely, suppose that the conditions 1–3 hold. The pair  $(r_+, r_-)$  determines  $q_\infty$  and so for all  $v \in \mathcal{P}$  we have a  $v$ -adic lattice  $(L_v, q_v)$  of rank  $r$ . Condition 2 tells us that the  $v$ -adic value of  $d$  equals  $\text{disc}(q_v)$ . So Theorem 12.4.1 then implies the existence of a  $\mathbb{Q}$ -valued form  $g$  on  $L$  with  $g_v = q_v$  (over  $\mathbb{Q}_v$ ) and such that  $\text{disc}(g_v) = d$  for all  $v \in \mathcal{P}$ . Choosing an integral basis for  $L$  we identify  $g$  with a rational form in  $r$  variables and then Theorem 12.4.2 shows that there exists an integral form  $q$  whose localization at  $v$  is isometric to  $q_v$ ,  $\forall v \in \mathcal{P}$ . Such a form endows  $L$  with the structure of an integral quadratic lattice satisfying all of the required conditions.  $\square$

The final step is a formulation of this assertion in terms of the genus and signature. Recall (cf. Propositions 11.1.3, 11.2.4) that for a given quadratic  $p$ -primary quadratic torsion form  $(G, q^\#)$  there exists a unique rank  $r = \ell(G)$  quadratic lattice  $L_{q^\#}$  whose discriminant form is  $q^\#$  if either  $p$  is an odd prime, or if  $p = 2$  and no cyclic quadratic torsion group of order two splits off from  $G$ .

**Theorem 12.4.4** (Existence of even lattices, [171, Thm. 1.10.1]). *Let  $(r_+, r_-)$  be a pair of non-negative integers and let  $(G, q^\#)$  be a non-degenerate quadratic torsion form. There exists a non-degenerate quadratic lattice  $L$  with  $\mathbf{g}(L) = (r_+, r_-, [q^\#])$  (and hence of rank  $r = r_+ + r_-$ ) if and only if all of the following conditions are fulfilled.*

1.  $r_+ - r_- \equiv \tau_8(q^\#) \pmod{8}$ ;
2.  $r \geq \ell(G)$ ;
3. For all primes  $p \neq 2$  for which  $G_p$  has length  $r$  and for  $p = 2$  in case  $G_2$  has length  $r$  but does not split off an order two cyclic summand, one has<sup>3</sup>

$$\text{disc}(L_{q_p^\#}) = (-1)^{r-} |G| \text{ in } D(\mathbb{Z}_p).$$

*Proof of the necessity.* Let  $L$  be a non-degenerate quadratic lattice with discriminant group  $G$  and discriminant form  $q^\#$ . The first condition follows from the fact that the index mod 8 for a non-degenerate quadratic torsion group  $(G, q^\#)$  (see Definition 12.2.3) is well defined as the modulo 8 index of any non-degenerate even lattice with  $q^\#$  as its discriminant form. For the second condition see (1.9). To show that the third condition holds, note that if  $G_p$  has length  $r$ , one has  $L_{q_p^\#} = L_p$ , so that  $\text{disc}(L_p) = \text{disc}(L)_p = (-1)^{r-} \cdot |G|$  in  $D(\mathbb{Z}_p)$  by localizing the first equality of (12.11).

<sup>3</sup>If  $p = 2$  and  $q^\#$  splits off an order two cyclic summand there is no extra restriction.

*Proof of the sufficiency.* The idea is to invoke Corollary 12.4.3. Its input consists of a collection of local lattices of the *same* rank  $r$  obeying conditions 1–3 mentioned there, which are phrased in terms of their local invariants. The crucial remark is that these conditions are satisfied for any even integral lattice. We make use of it by invoking Theorem 12.1.1 which states the existence of a non-degenerate even integral lattice, say  $L'$ , whose discriminant form is  $q^\#$ . However, its signature  $(r'_+, r'_-)$  need not be equal to  $(r_+, r_-)$ . We shall first remedy this using that  $L'$  is only unique up to unimodular summands.

**Step 1.** By adding a suitable number of copies of the even lattice  $U$  of signature  $(1, 1)$  to  $L'$ , one may assume that  $L'$  is an even lattice for which

$$\begin{aligned} r' &= \text{rank}(L') \geq r = r_+ + r_- \\ r'_\pm &\equiv r_\pm \pmod{8}. \end{aligned} \tag{12.12}$$

As for the second equality, note that since by condition 1 the differences  $r_+ - r_-$  and  $r'_+ - r'_-$  are fixed modulo 8, if  $r'_+ - r_+$  is made divisible by 8, this also holds for  $r'_- - r_-$ . This equality implies that  $(-1)^{r'_-} = (-1)^{r'_+}$  and so the required condition 2 of Corollary 12.4.3 also holds for the lattice  $L'$ . Conditions 1 and 3 of Corollary 12.4.3 hold automatically, since  $L'$  is an even integral lattice. We presently do not further make use of Corollary 12.4.3 since we still have to adapt the rank of  $L'$ .

**Step 2.** For each prime  $p$  we construct a local lattice of the correct rank  $r$  from the localization  $L'_p$  of the lattice  $L'$  we just constructed and in such a way that this new local lattice still satisfies the conditions of Corollary 12.4.3. The main idea here is that the conditions given in the statement of the theorem enable us to drop off a unimodular lattice of rank  $r' - r$  from  $L'_p$  in such a way that first of all the Hasse invariant remains unchanged (so that the product formula holds), and, secondly, the local discriminant remains unchanged so that condition 2 of Corollary 12.4.3 remains true. We achieve this by either dropping off a suitable number of trivial summands  $\langle 1 \rangle$  or, if  $p = 2$ , by dropping off a suitable even number of hyperbolic planes  $U$ . Indeed, for trivial lattices both the local discriminant and the Hasse invariant are equal to 1, while  $\text{disc}(\oplus^k U) = (-1)^k$  and  $\varepsilon_2(\oplus^k U) = 1$ .

We start with the normal form decomposition for the lattice  $L'_p$  as given by Propositions 11.1.4 and 11.2.6.

**Case 1:  $p$  is an odd prime.**

$$L'_p = \begin{cases} L_{q_p^\#} \oplus \oplus^{t'_p} \langle 1 \rangle, & v'_p = 0 \\ L_{q_p^\#} \oplus \langle \varepsilon \rangle \oplus \oplus^{t'_p-1} \langle 1 \rangle, & v'_p = 1. \end{cases} \tag{12.13}$$

The two cases, which are distinguished by the value of  $\text{disc}(L'_p)$ , have been labeled by  $v'_p \in \{0, 1\}$ . Explicitly,

$$\begin{aligned} t'_p &= r' - \ell(G_p) \\ v'_p &= t'_p - \text{rank}(\text{trivial summand in } L'_p). \end{aligned}$$

We now compare  $t'_p$  with

$$t_p = r - \ell(G_p).$$

Suppose first that  $t_p \geq 1$ . Since by construction  $r' \geq r$ , this implies that

$$t'_p - v'_p = r' - v'_p - \ell(G_p) \geq r - v'_p - \ell(G_p) \geq r - 1 - \ell(G_p) = t_p - 1 \geq 0.$$

In this case, since  $v'_p \in \{0, 1\}$ , certainly  $v'_p \leq t_p$ . Hence  $r' - r = t'_p - t_p \leq t'_p - v'_p$ , i.e.,  $r' - r$  is at most equal to the number of trivial summands in  $L'_p$  so that we can drop off enough trivial summands to make the rank  $r'$  of  $L'_p$  equal to  $r$ .

Finally, if  $t_p = 0$  we show that  $v'_p = 0$  by considering the discriminant of  $L'_p$  in  $D(\mathbb{Z}_p)$ :

$$\begin{aligned} \text{disc}(L'_p) &= (-1)^{r^-} \cdot |G| \\ &= \text{disc}(L_{q_p^\#}) \text{ (in } D(\mathbb{Z}_p)\text{)}. \end{aligned}$$

The first equality is based on equation (12.11), the second is assumption 3. But then  $v'_p = 0$  because if not, the normal form (12.13) shows that  $\text{disc}(L'_p)/\text{disc}(L_{q_p^\#})$  would be a non-square in  $\mathbb{Z}_p^\times$ . Consequently, we can modify  $L'_p$  by dropping off  $r' - \ell(G_p)$  trivial summands.

**Case 2:**  $p = 2$ . Here we have the normal decompositions

$$\begin{aligned} \text{Case (2a)} \quad L'_2 &= \begin{cases} L_{q_2^\#} \oplus \oplus \frac{1}{2} t'_2 U, & v'_2 = 0, \\ L_{q_2^\#} \oplus V \oplus \oplus \frac{1}{2} t'_2 - 1 U, & v'_2 = 1, \end{cases} \\ \text{Case (2b)} \quad L_2^{(i)} &= L_{q_2^\#}^{(i)} \oplus \oplus \frac{1}{2} t'_2 U, \quad i = 1, 2, \end{aligned}$$

with

$$\begin{aligned} v'_2 &= \frac{1}{2} t'_2 - \#(\text{summands } U) \\ t'_2 &= r' - \ell(G_2). \end{aligned}$$

Case (2a) occurs if and only if no cyclic quadratic torsion group of order 2 can be split off from  $q_2^\#$ . Here the same argument as for  $p$  odd can be applied in order to make  $r'$  equal to  $r$ , but now we drop off  $\frac{1}{2}(t'_2 - t_2)$  copies of  $U$ . For case (b), since  $t'_2 \geq t_2$ , we can drop off  $\frac{1}{2}(t'_2 - t_2)$  copies of  $U$  in order to make  $r'$  equal to  $r$ . In view of the remarks made at the beginning of the proof, we only need observe that  $\frac{1}{2}(t'_2 - t_2) = \frac{1}{2}(r' - r)$  is even by (12.12).

**Case 3: the place at  $\infty$ .** We replace  $L'_\mathbb{R}$  with an inner product space  $L_\mathbb{R}$  of dimension  $r$  and signature  $(r_+, r_-)$ . Since, again by (12.12),  $\frac{1}{2}r'_-(r'_- - 1) \equiv \frac{1}{2}r_-(r_- - 1) \pmod{4}$ , we have  $\varepsilon_\infty(L') = (-1)^{\frac{1}{2}r'_-(r'_- - 1)} = (-1)^{\frac{1}{2}r_-(r_- - 1)} = \varepsilon_\infty(L_\mathbb{R})$  and  $\text{disc}(L'_\mathbb{R}) = (-1)^{r'_-} = (-1)^{r_-} = \text{disc}(L_\mathbb{R})$ . Once again, all the conditions 1-3 of Corollary 12.4.3 hold.

**Final step.** For clarity we denote the new local lattices of rank  $r$  by  $M_v, v \in \mathcal{P}$ . Let  $L$  be a free  $\mathbb{Z}$ -module of rank  $r$  whose localizations at  $v$  shall be identified with  $M_v$  as  $\mathbb{Z}_v$ -modules. On each  $M_v$  we have constructed a  $\mathbb{Z}_v$ -valued quadratic form  $q_v$  (with the convention that  $\mathbb{Z}_\infty = \mathbb{R}$ ). The preceding steps ensure that the conditions needed to apply Corollary 12.4.3 hold. Consequently, an integral

quadratic form  $q$  on  $L$  exists having signature  $(r_+, r_-)$  and whose localization at each place  $v$  is isometric to  $q_v$ . Taking discriminant quadratic forms, this finally shows that  $q_L^\# = \bigoplus_p q_{L_p}^\# = \bigoplus_p q_p^\# = q^\#$ .  $\square$

*Remark 12.4.5. 1.* Existence of a genus does not imply uniqueness of the lattice itself. We have seen that for instance non-isometric definite lattices exist in the same genus (see e.g. Table 1.12.1).

**2.** Let us illustrate what limitations condition 3 puts on a genus.

- First, assume  $p$  is an odd prime. For example, assume that  $p \equiv -1 \pmod{8}$ . Then  $-1$  is a non-square in  $\mathbb{Z}_p$  (see e.g. [204, Ch. I, Theorem 5]). Suppose that  $G$  is  $p$ -primary of length  $r$  and homogeneous of odd degree  $k$  carrying the torsion form  $q^\#$  of the lattice  $L_{q^\#} = L(p^k)$ ,  $L = \langle -1 \rangle \oplus \bigoplus^{r-1} \langle 1 \rangle$ . From the table of Proposition 12.3.2, we see that  $\tau_8 = -2 + 2(r-1) = 2r-4 \pmod{8}$ . But  $2r_-(L) = r - \tau(L) \equiv -r + 4 \pmod{8}$  and so  $r$  has to be even and the parity of  $r_-(L)$  is the parity of  $\frac{1}{2}r$ . So, if  $\frac{1}{2}r$  is even,  $(-1)^{r_-(L)} = 1$ . This shows that condition 3 does not hold unless  $\frac{1}{2}r$  is odd. So one cannot weaken this condition to  $\text{disc}(L_{q^\#}) = \pm|G|$ .
- For the prime 2 this is different. It turns out that if  $\text{disc}(L_{q^\#}) = \pm|G|$  and  $q^\#$  does not have cyclic order 2 factors, the sign is automatically equal to  $(-1)^{r_-}$ . For this reason V. Nikulin in [171, Thm. 1.10.1] stated that in this situation the condition  $\text{disc}(L_{q^\#}) = \pm|G|$  is necessary and sufficient.

To indicate why this is the case, it is helpful to distinguish two types of normal forms: Let us say that we have type *I* if the discriminant equals  $\pm|G|$  and type *II* in case the discriminant is  $\pm 3|G|$ . For type *I* one calculates as before that  $r_- = \frac{1}{2}(r - \tau) \pmod{4}$ , from which the parity of  $r_-$  follows. Comparing with the sign of  $\text{disc}(L_{q^\#})$  then shows that this sign equals  $(-1)^{r_-}$ . For type *II* one gets the opposite sign while  $\text{disc}(L_{q^\#}) = \pm 3 \cdot |G|$ . Since the latter lattice cannot be isometric to the 2-adic localization of an integral lattice of the same rank, this shows that in the homogeneous situation the signs match. It also shows that in general an even number of type *II* homogeneous summands must be present. Since the parities of  $r_-$  for the various homogeneous summands add, while the discriminants multiply (an even number giving  $\pm 1$ ), one easily checks that the signs match in general.

For example, consider first a homogeneous lattice in normal form,  $L_{q^\#} = L(2^k)$ ,  $k$  odd, with  $L = \langle 3 \rangle \oplus \bigoplus^{c-1} U \oplus V$ , a lattice of rank  $2c+1$ . From the table of Proposition 12.3.3 we see that  $\tau_8(q^\#) = 3$ . Since  $\text{disc}(L) = \pm 1$  we have a type *I* lattice and so  $r_- \equiv c+1 \pmod{2}$ . In fact,  $\text{disc}(L) = (-1)^{c+1}$ , and so the signs match.

To give an example of an inhomogeneous normal form, consider  $M_k \oplus M_{k+2}$  with  $k$  odd and  $M = \langle 1 \rangle \oplus \bigoplus^{c-1} U \oplus V$  so that  $M_k$  and  $M_{k+2}$  are both of type *II*. One has  $r(M) = 2c+1$ , and from the table of Proposition 12.3.3, one sees that  $\tau_8(q^\#(M_k)) = \tau_8(q^\#(M_{k+2})) = -3$ . One calculates  $r_-(M_k) = r_-(M_{k+1}) \equiv c-1 \pmod{2}$ . Then  $\text{disc}(L) = 3 \cdot 3|G| = |G|$  since  $\text{disc}(M) = 3(-1)^c$ , while  $r_- \equiv 2(c-1) \equiv 0 \pmod{2}$ . So, again, the signs match.

- 3.** The theorem implies that unimodular even lattices of index  $(r_+, r_-)$  exist if

and only if  $r_+ - r_-$  is divisible by 8. We saw this already in Chapters 1 and 2: That even unimodular lattices have index divisible by 8 is part of the statement of Theorem 2.4.2, existence in the indefinite case is Corollary 2.4.3, while the definite case follows from the existence of  $E_8$ .

4. Observe that the existence proof is not constructive at all. Consider for instance the genus given by signature  $(8, 0)$  and zero torsion form. The proof starts out with  $L' = 0$  and enlarges it to  $L' = \mathfrak{O}^8 U$ . Then  $L'_p$  is replaced by a trivial rank 8 lattice for all odd  $p$  as well as for the place  $\infty$ , while  $L'_2$  is replaced by  $\mathfrak{O}^4 U$ . Then existence is deduced from the modified Hasse principle. Of course we know the required lattice exists:  $L = E_8$ , but it never comes up during the proof.

We shall mostly use the following consequence of Theorem 12.4.4 which uses the relation  $\ell(G) = \max_p \ell(G_p) \leq r = \text{rank}(L)$  so that condition 3 in the above theorem only applies in case  $\text{rank}(L) = \ell(G)$ .

**Corollary 12.4.6.** *Let  $(r_+, r_-)$  be a pair of non-negative integers and let  $(G, q)$  be a non-degenerate quadratic torsion group. There exists a non-degenerate even lattice  $L$  of rank  $r = r_+ + r_-$ , signature  $(r_+, r_-)$  and with discriminant form  $(G, q)$  if the following two conditions are fulfilled.*

1.  $r_+ - r_- \equiv \tau_8(q) \pmod{8}$ ,
2.  $r > \ell(G)$ .

## 12.5 Applications to Odd Lattices

**12.5.A The Genus of an Odd Lattice.** The first goal is to search for a reformulation of the genus in terms of discriminant forms similar to what we did in Theorem 11.3.1 for even lattices. Since parity is detected at the prime 2, we shall focus on symmetric  $\mathbb{Z}_2$ -lattices and their symmetric discriminant forms. As a consequence of the classification (cf. Proposition 11.2.3) every 2-primary symmetric torsion form is a polar form, but it can be the polar form of several non-isometric quadratic torsion forms. So, despite the similarity of the normal forms in the symmetric and the quadratic situation, several non-isometric normal forms may have isometric polar forms. For the basic building blocks this is already demonstrated in Table 10.3.1. We extract the relevant information:

**Lemma 12.5.1.** *The following pairs of 2-primary quadratic forms have isometric polar forms:*

1.  $\langle 2^{-1} \rangle$  and  $\langle 3 \cdot 2^{-1} \rangle$  have polar form  $\langle 2^{-1} \rangle$ ,
2.  $\langle 2^{-2} \rangle$  and  $\langle -3 \cdot 2^{-2} \rangle$  have polar form  $\langle 2^{-2} \rangle$ ,  $\langle 3 \cdot 2^{-2} \rangle$  and  $\langle -1 \cdot 2^{-2} \rangle$  have polar form  $\langle -1 \cdot 2^{-2} \rangle$ ,
3.  $\mathbf{u}_1$  and  $\mathbf{v}_1$  have polar form  $\langle \mathbf{u}_1 \rangle$ .



If the normal form of a 2-primary quadratic torsion form does not contain either one of the above forms, then it is the polar form of a unique quadratic torsion form.

For composite forms, the result is as follows:

**Proposition 12.5.2.** *Two non-degenerate 2-primary quadratic torsion forms with isometric polar forms are themselves isometric if and only if they have the same index modulo 8.*

Before proving this, we describe some consequences using the following concept:

**Definition 12.5.3.** The *index set* of a non-degenerate 2-primary symmetric torsion form  $b$  is defined as the following subset of  $\mathbb{Z}/8\mathbb{Z}$

$$\mathcal{T}_8(b) = \{\tau_8(q) \in \mathbb{Z}/8\mathbb{Z} \mid q \text{ a non-degenerate quadratic torsion form with } b_q \simeq b\}.$$

If  $\mathcal{T}_8(b) \subset \{\bar{0}, \pm\bar{2}, \bar{4}\}$ , respectively  $\mathcal{T}_8(b) \subset \{\pm\bar{1}, \pm\bar{3}\}$ , one calls  $\mathcal{T}_8(b)$  an *even-index set*, respectively an *odd-index set*. If equality holds, we say that  $\mathcal{T}_8(b)$  is a complete even-index set, respectively a complete odd-index set.

**Example 12.5.4.** The polar forms of Lemma 12.5.1 have the following index sets  $\mathcal{T}_8(\langle 2^{-1} \rangle) = \{\bar{1}, -\bar{1}\}$ ,  $\mathcal{T}_8(\langle 2^{-2} \rangle) = \{\bar{1}, -\bar{3}\}$ ,  $\mathcal{T}_8(\langle -2^{-2} \rangle) = \{-\bar{1}, \bar{3}\}$ ,  $\mathcal{T}_8(u_1) = \{\bar{0}, \bar{4}\}$ . Moreover, Lemma 12.5.1 also implies that if the normal form of  $b$  does not contain any of such forms, then  $b$  is the polar form of a unique quadratic form  $q$  and  $\mathcal{T}_8(b) = \{\tau_8(q)\}$ .

Index sets can be added using addition in  $\mathbb{Z}/8\mathbb{Z}$ :

$$\mathcal{T}_8(b) + \mathcal{T}_8(b') = \{\tau + \tau' \mid \tau \in \mathcal{T}_8(b), \tau' \in \mathcal{T}_8(b')\}.$$

If  $b = b_q$  and  $b' = b_{q'}$ , we have  $\tau(q \oplus q') = \tau(q) + \tau(q')$  and hence  $\mathcal{T}_8(b) + \mathcal{T}_8(b') \subset \mathcal{T}_8(b \oplus b')$ . Obviously, in this process the parities (being an odd-index set or an even-index set) add like the addition in  $\mathbb{F}_2$ .

We formulate an elementary property of even- and odd-index sets.

**Lemma 12.5.5.** *Let  $(G, b)$  be a non-degenerate 2-primary symmetric torsion form. If  $\ell(G)$  is even (odd), then  $\mathcal{T}_8(b)$  is an even-index (odd-index) set.*

*Proof.* From Proposition 12.3.3 we deduce that for any length 1 quadratic torsion form  $q$ , we have  $\tau_8(q) \equiv 1 \pmod{2}$ , while for the length two forms  $u_k, v_k$  we have  $\tau_8(u_k) \equiv \tau_8(v_k) \equiv 0 \pmod{2}$ . The additivity of the parity then shows the result.  $\square$

The proof of Proposition 12.5.2 requires some further reductions for the dyadic normal forms where adjacent weights are involved.

**Lemma 12.5.6.** *Let  $u, u', u''$  be units in  $\mathbb{Z}_2$ . Then the following relations hold between non-homogeneous dyadic lattices.*

$$\langle u \cdot 2^{k-1} \rangle \oplus U_k \simeq \langle -3u \cdot 2^{k-1} \rangle \oplus V_k \text{ for } k \geq 1 \quad (\text{V})$$

$$U_{k-1} \oplus \langle u \cdot 2^k \rangle \simeq \langle -3u \cdot 2^k \rangle \oplus V_{k-1} \text{ for } k \geq 1 \quad (\text{VI})$$

$$\langle u \cdot 2^{k-1} \rangle \oplus \langle u' \cdot 2^k \rangle \simeq \langle (u + 2u') \cdot 2^{k-1} \rangle \oplus \langle (u' + 2u) \cdot 2^k \rangle \text{ for } k \geq 1 \quad (\text{VII})$$

$$(\langle u \rangle \oplus \langle u' \rangle)(2^{k-1}) \oplus \langle 2^k \rangle \simeq (\langle u + 2 \rangle \oplus \langle u' - 2 \rangle)(2^{k-1}) \oplus \langle -3 \cdot 2^k \rangle \quad (\text{VIII})$$

$$\text{if } u \equiv u' \pmod{4} \quad k \geq 1$$

$$\langle u \cdot 2^{k-2} \rangle \oplus \langle u' \cdot 2^k \rangle \simeq \langle -3u \cdot 2^{k-2} \rangle \oplus \langle -3u' \cdot 2^k \rangle, \text{ for } k \geq 3. \quad (\text{IX})$$

Similar relations hold for their quadratic torsion forms, that is, for the 2-primary quadratic torsion groups where the exponents  $2^j$  are replaced by  $2^{-j}$  and for  $u_k$  and  $v_k$  instead of  $U_k$  and  $V_k$ .

The proofs of these relations have been placed in Appendix C.3.B.

*Proof of Proposition 12.5.2.* The proof of the non-trivial implication is by induction on the length  $\ell$  of the torsion group and uses the normal form decomposition for symmetric torsion forms. On the cyclic groups  $\mathbb{Z}/2^k\mathbb{Z}$ ,  $k \geq 3$ , by Lemma 12.5.1 every non-degenerate symmetric form  $b$  is the polar form of a unique quadratic form, i.e.  $\#\mathcal{T}_8(b) = 1$ , and so the result holds trivially in this case.

In case of the three pairs of non-isometric quadratic cyclic groups with the same polar form given by Lemma 12.5.1, the two have different indexes mod 8 (see Example 12.5.4) which finishes the proof of the proposition for  $\ell = 1$ .

Assuming the result has been proven for all quadratic torsion forms on 2-primary groups of length  $\leq \ell$ , let  $q, q'$  be such torsion forms on a 2-primary group of length  $\ell + 1$ . We may assume that  $b = b_q = b_{q'}$  is in normal form and we assume that  $\tau_8(q) = \tau_8(q')$ .

Suppose first that  $b = b_1 \oplus b_2$  where  $b_1$  is one of the forms  $\langle u \cdot 2^{-k} \rangle$ ,  $k \geq 3$ ,  $u_k$ ,  $k \geq 2$ , or  $v_k$ ,  $k \geq 2$ . In this case  $b_1$  is the polar form of a unique quadratic form  $q_1$ . Suppose  $b_2 = b_{q_2} = b_{q'_2}$  for some quadratic forms  $q_2$  and  $q'_2$ . Then  $b$  is the polar form of  $q = q_1 \oplus q_2$  as well as of  $q' = q_1 \oplus q'_2$ . Indeed, using the correspondence between normal forms mentioned in Proposition 11.2.3, any 2-primary quadratic form in normal form with  $b$  as polar form splits off  $q_1$ . Assuming that  $\tau_8(q) = \tau_8(q')$ , one has  $\tau_8(q_2) = \tau_8(q'_2)$ , and so, by induction  $q_2 \simeq q'_2$  and hence  $q \simeq q'$ . This shows the result in case the normal form of  $b = b_q$  splits off a summand which is the polar form of a unique quadratic form.

If  $b$  does not split as above, the normal form of  $b_q = b_{q'}$  splits off one of the following three types of symmetric torsion forms (consult also Table 11.2.1):

Type 1:  $\oplus^{a_1} \langle 2^{-1} \rangle$ ,  $a_1 \leq 2$ ,    Type 2:  $\oplus^{a_2} \langle u \cdot 2^{-2} \rangle$ ,  $a_2 \leq 2$ ,    Type 3 :  $\oplus^c u_1$  .

- We first consider the case of type 3 forms with  $c \geq 2$ , that is, where two copies of  $u_1$  split off from  $b_q$ . Then on the level of quadratic forms we may assume that  $q \simeq \oplus^2 u_1 \oplus q_2$  and  $q' \simeq \oplus^2 u_1 \oplus q'_2$  or  $q' \simeq u_1 \oplus v_1 \oplus q'_2$ , since  $u_1 = v_1$  in the symmetric situation. Suppose that  $\tau_8(q) = \tau_8(q')$ . Taking away  $u_1$ , it

follows that  $\tau_8(u_1 \oplus q_2) = \tau_8(v_1 \oplus q'_2)$  or  $\tau_8(u_1 \oplus q_2) = \tau_8(u_1 \oplus q'_2)$ , and so, by induction  $u_1 \oplus q_2 \simeq v_1 \oplus q'_2$  or  $u_1 \oplus q_2 \simeq u_1 \oplus q'_2$  and hence  $q \simeq q'$ , as desired.

- We next consider type 2 forms with  $a_2 = 2$ , so two cyclic copies of order 4 are present as direct summands of  $b_q \simeq b_{q'}$ . Table 6.1.1 shows that the non-isometric quadratic forms  $\langle 2^{-2} \rangle = [2^{-3}]$  and  $\langle -3 \cdot 2^{-2} \rangle = [-3 \cdot 2^{-3}]$  have the same polar form, and, similarly, for  $\langle 3 \cdot 2^{-2} \rangle = [3 \cdot 2^{-3}]$  and  $\langle -1 \cdot 2^{-2} \rangle = [-1 \cdot 2^{-3}]$ . However an orthogonal sum of two cyclic such forms changes the situation, since by relation III given in Appendix C.3.A, one has isometries

$$\langle u \cdot 2^{-2} \rangle \oplus \langle u' \cdot 2^{-2} \rangle \simeq \langle -3u \cdot 2^{-2} \rangle \oplus \langle -3u' \cdot 2^{-2} \rangle$$

on the level of quadratic torsion forms, eliminating the ambiguity. Assuming that  $b_q \simeq b_{q'}$  and  $\tau_8(q) = \tau_8(q')$ , splitting off the same type 2 component from both quadratic forms gives quadratic forms of lower ranks with the same index mod 8 and with isometric polar form. Hence, by induction these quadratic forms are isometric, and so also  $q$  and  $q'$  are.

- In the same way one can treat the situation where a type 2 form with  $a_2 = 1$  combined with  $u_1$  is present, i.e. if  $\langle u \cdot 2^{-2} \rangle \oplus u_1$  splits off. Here we use relation VI stating that on the level of quadratic torsion forms,  $\langle u \cdot 2^{-2} \rangle \oplus v_1 \simeq \langle -3u \cdot 2^{-2} \rangle \oplus u_1$ .
- The case  $(a_1, a_2) = (2, 1)$ , that is, where three cyclic copies  $\oplus^2 \langle 2^{-1} \rangle \oplus \langle u' \cdot 2^{-2} \rangle$  split off from  $b_q$ .

The possible quadratic forms are  $q_{u,u',u''} = \langle u \cdot 2^{-1} \rangle \oplus \langle u' \cdot 2^{-1} \rangle \oplus \langle u'' \cdot 2^{-2} \rangle$  and  $q'_{u,u',u''} = \langle u \cdot 2^{-1} \rangle \oplus \langle u' \cdot 2^{-1} \rangle \oplus \langle -3u'' \cdot 2^{-2} \rangle$ ,  $u', u', u'' \equiv 1, 3 \pmod{4}$ . Using VIII these can be reduced to  $q_{1,1,u''}$  and  $q'_{1,1,-3u''}$ . Hence in both cases we can split off  $\oplus^2 \langle 2^{-1} \rangle$  and then  $b = b_q \simeq b_{q'}$ ,  $q = \oplus^2 \langle 2^{-1} \rangle \oplus q_2$ ,  $q' = \oplus^2 \langle 2^{-1} \rangle \oplus q'_2$ , and assuming  $\tau_8(q) = \tau_8(q')$ , we find that  $\tau_8(q_2) = \tau_8(q'_2)$  and so, by induction,  $q \simeq q'$ .

- The case  $(a_1, c) = (2, 1)$ , that is,  $\oplus^2 \langle 2^{-1} \rangle \oplus u_1$  splits off from  $b_q$ .

The possibilities for  $q$  are  $q_{u,u'} = \langle u \cdot 2^{-1} \rangle \oplus \langle u' \cdot 2^{-1} \rangle \oplus u_1$  and  $q'_{u,u'} = \langle u \cdot 2^{-1} \rangle \oplus \langle u' \cdot 2^{-1} \rangle \oplus v_1$  with  $(u, u') = (1, 1), (1, 3), (3, 3)$ . Using the isometries III we can write these as a direct sum of four terms  $\langle u \cdot 2^{-1} \rangle$  with at least one  $u$  equal to 1 mod 4 and splitting off this term we may apply induction.

A limited number of cases remain to be discussed. We already discussed length 1. From the length  $\geq 2$  cases, only  $b = \oplus^2 \langle 2^{-1} \rangle$ ,  $b = \langle 2^{-1} \rangle \oplus \langle u \cdot 2^{-2} \rangle$ ,  $b = u_1$  and  $b = \langle 2^{-1} \rangle \oplus u_1$  remain. One checks that all of the non-isometric quadratic torsion forms  $q$  with the same polar form  $b = b_q$  have distinct indexes mod 8, completing the proof of the proposition.  $\square$

As a consequence, using also Proposition 11.2.4, we can count the number of non-isometric dyadic lattices with given symmetric discriminant form and of rank equal to the length of the discriminant group:

**Corollary 12.5.7.** *If  $b$  is the symmetric discriminant form of some non-degenerate dyadic lattice, there are  $\#\mathcal{I}_8(b)$  non-isometric non-degenerate dyadic lattices of*

rank equal to the length of the discriminant group for which  $\mathbf{b}$  appears as discriminant form, unless  $\langle 2^{-1} \rangle$  splits off from  $\mathbf{b}$ . In that case the number is twice as big.

We shall next link even and odd integral lattices at the level of their genus:

**Proposition 12.5.8.** *A non-degenerate lattice  $(L, \mathbf{b})$  is odd if and only if  $\mathbf{L} = L(2)$  is an even non-degenerate lattice having the properties*

1.  $\mathbf{L}_2$  splits off a summand  $\langle \mathbf{u} \cdot 2 \rangle$ ,  $\mathbf{u}$  a unit;
2.  $\text{dg}_{\mathbf{L}_2}$  has length equal to the rank of  $L$ , or, equivalently, with  $L_2^{(0)}$  the exponent 0 summand in the Jordan splitting of  $L_2$ , one has

$$\text{rank}(L) - \text{rank}(L_2^{(0)}) = \ell(\text{dg}_{L_2}).$$

*Proof.* If  $L$  is odd,  $L(2) = \mathbf{L}$  is even and  $L_2$  must split off  $\langle \mathbf{u} \cdot 2 \rangle$ ,  $\mathbf{u} \in \mathbb{Z}_2^\times$ , by Proposition 10.2.2, otherwise  $L$  would be even. The exponent 0 summand in the normal form of  $L_2$  gives the exponent 1 summand in  $\mathbf{L}_2$  and so the discriminant group of  $\mathbf{L}$  has length equal to  $\text{rank}(\mathbf{L})$ .

Conversely, if  $\mathbf{L} = L(2)$  has the stated properties, the bilinear form on  $L_2$  is divisible by 2 and so  $L_2 = L_2(\frac{1}{2})$  is a dyadic lattice. Since for odd primes  $p$ , 2 is a unit and  $L_p = L_p(\frac{1}{2})$ , all localizations of  $L$  are  $p$ -adic lattices. But then  $L$  is an integral lattice. It is odd, since  $L_2$  is odd.  $\square$

The above observation motivates the following notation for a non-degenerate symmetric lattice  $(L, \mathbf{b})$ :

$$\begin{aligned} \mathbf{L} &= L(2), & \mathbf{q}_2 &:= \mathbf{b}_{L_2}^\#, & \mathbf{q}_2 &:= \mathbf{q}_{L_2}^\#, \\ L_2 &= L_2^{(0)} \oplus L_2^{\geq 1}, & \mathbf{b}_2 &:= \mathbf{b}_{L_2}^\#, & & \\ L_2 &= L_2^{(1)} \oplus L_2^{\geq 2}, & L_2^{(1)} &= L_2^{(0)}(2), & L_2^{\geq 2} &= L_2^{\geq 1}(2), \\ \mathbf{b}_2 &= \mathbf{b}_2^{(1)} \oplus \mathbf{b}_2^{\geq 2}, & \mathbf{b}_2^{(1)} &= \mathbf{b}_{L_2^{(0)}(2)}^\#, & \mathbf{b}_2^{\geq 2} &= \frac{1}{2}\mathbf{b}_2, \end{aligned} \tag{12.10}$$

where the upper indices indicate exponents of the Jordan splitting. The last line uses the "halving" procedure explained in Definition 9.3.10.

We can now formulate Nikulin's characterization of the genus in the case of odd lattices:

**Theorem 12.5.9** ([171, Cor. 1.16.3]). *Let  $(L, \mathbf{b})$  be a non-degenerate odd symmetric integral lattice. Then the genus  $\mathfrak{g}(L)$  is determined by the discriminant symmetric form of  $L$  together with the signature of  $L$ .*

*Proof.* We show that the locations of  $L$  are determined by its discriminant symmetric form and its signature. In order to invoke the previous results on even lattices, we use  $\mathbf{L} = L(2)$  introduced above.

As noted at the start of this subsection, for  $p$  odd, there is no difference between symmetric and quadratic  $p$ -adic lattices. So  $\mathbf{b}_{L_p}^\#$  determines  $\mathbf{q}_{L_p}^\#$  and conversely.

Note that  $\mathbf{q}_{L_p}^\# = \mathbf{q}_{L_p}^\#(2)$  in this case.

We now concentrate on  $p = 2$ . Recall from Table 11.2.1 the various homogeneous normal forms and recall also that  $\mathbf{u}_1 = \mathbf{v}_1$  for symmetric forms. So  $\mathbf{b}_2^{(1)}$  has normal form  $\mathbb{O}^a \langle 2^{-1} \rangle \oplus^b \mathbf{u}_1$  with  $a = 1$  or  $a = 2$ . From Proposition 12.5.8.2 we find that  $a + 2b = r - \ell(\mathrm{dg}_{L_2^{\geq 2}})$ ,  $r = \mathrm{rank}(L)$ . So, if this number is odd,  $a = 1$  and  $b = \frac{1}{2}(r - 1 - \ell(\mathrm{dg}_{L_2^{\geq 2}}))$ , and otherwise  $a = 2$  and  $b = \frac{1}{2}(r - 2 - \ell(\mathrm{dg}_{L_2^{\geq 2}}))$ . This determines the symmetric form  $\mathbf{b}_2^{(1)}$  up to isometry if we know  $r$  and the form  $\mathrm{dg}_{L_2^{\geq 2}} = \mathbf{b}_2(2^{-1})$ . Hence, given  $r$ , the forms  $\mathbf{b}_2$  and  $\mathbf{b}_2^{(1)}$  determine each other up to isometry.

We next show that  $\tau_8(\mathbf{q}_2)$  is completely determined by the discriminant bilinear form and the signature of  $L$ . First remark that the indexes of  $L$  and  $\mathbf{L}$  are the same and so  $\tau_8(\mathbf{q}_L^\#)$ , the index mod 8 of the quadratic discriminant form of  $\mathbf{L}$ , is completely determined by the index of  $L$ . From  $\mathbf{q}_L^\# = \bigoplus_{p \text{ prime}} \mathbf{q}_{L_p}^\# \simeq \bigoplus_{p \neq 2} \mathbf{q}_{L_p}^\# \oplus \mathbf{q}_{L_2}^\#$ , we infer that  $\tau_8(\mathbf{q}_L^\#) = \sum_{p \neq 2} \tau_8(\mathbf{q}_{L_p}^\#) + \tau_8(\mathbf{q}_{L_2}^\#)$  and so  $\tau_8(\mathbf{q}_{L_2}^\#)$  is indeed completely determined by the discriminant symmetric form and the signature of  $L$ . Here we use that for odd primes  $p$  the mod 8 index of  $\mathbf{q}_{L_p}^\#$  is determined from the localization at  $p$  of the discriminant symmetric form since  $\mathbf{b}_{L_p}^\# \simeq \mathbf{q}_{L_p}^\#$ .

Combining the preceding two observations, Proposition 12.5.2 implies that the isometry class of the discriminant quadratic form for  $\mathbf{L}_2$  is completely determined by the discriminant symmetric form of  $L$  and its signature. Since we know all the other local discriminant forms as well as the index of the lattice  $\mathbf{L}$ , by Theorem 11.3.1 the genus of  $\mathbf{L}$  is determined by the discriminant symmetric form of  $L$  together with its signature. Hence the genus of  $L$  is determined by the same data.  $\square$

*Remark 12.5.10.* Defining the *genus invariant of the odd lattice*  $L$  as the triple  $\mathbf{g}(L) := (r_+, r_-, [b_L^\#])$ , where  $(r_+, r_-)$  is the signature of  $L$  and  $[b_L^\#]$  is the isometry class of the discriminant bilinear form  $b_L^\#$  of  $L$ , the preceding result can be rephrased by saying that the genus of an odd lattice is completely determined by its genus invariant.

**12.5.B Existence Results.** The next goal is to prove Nikulin's existence result for odd lattices. In the proof an index-like invariant  $t_8(\mathbf{b})$  for certain 2-primary symmetric torsion forms  $\mathbf{b}$  plays a decisive role. It is defined using any quadratic torsion form  $\mathbf{q}$  with polar form  $\mathbf{b}$ . So a priori this depends on  $\mathbf{q}$ , but, as it turns out, only if  $\mathbf{b}$  splits off  $\langle 2^{-1} \rangle$ . Its definition uses the expression  $\omega(\delta(\mathbf{q}))$ , where, we recall from § 9.1.B,  $\delta(\mathbf{q}) \in D(\mathbb{Z}_2)$  is the reduced discriminant. So, if we identify  $D(\mathbb{Z}_2)$  with  $(\mathbb{Z}/8\mathbb{Z})^\times$ , the expression  $\omega(\delta(\mathbf{q}))$  makes sense.<sup>4</sup>

<sup>4</sup>Recall (cf. (12.8)) that  $\omega(t) = 0$  if  $t \equiv \pm 1 \pmod{8}$  and  $\omega(t) = 1$  if  $t \equiv \pm 3 \pmod{8}$ .

Table 12.5.1: Mod 8 invariants

$q$	$[2^{-2}]$	$[3 \cdot 2^{-2}]$	$u_1, v_1$	$u_2, v_2$	$[2^{-3}], [-3 \cdot 2^{-3}]$	$[-2^{-3}], [3 \cdot 2^{-3}]$
$b = b_q$	$\langle 2^{-1} \rangle$	$\langle 2^{-1} \rangle$	$u_1$	$u_2, v_2$	$\langle 2^{-2} \rangle$	$\langle -2^{-2} \rangle$
$\tau_8(q)$	1	-1	0, 4	0, 0	1, -3	-1, 3
$4\omega \cdot \delta(q)$	0	4	0, 4	0, 0	0, 4	0, 4
$t_8(b)$	1	3	0	0, 0	1	-1

**Lemma 12.5.11.** 1. For a non-degenerate 2-primary quadratic torsion form  $q$  one has  $\tau_8(q(2^{-1})) \equiv \tau_8(q) + 4\omega(\delta(q)) \pmod 8$ .  
 2. Suppose  $b$  is a (not necessarily 2-primary) non-degenerate symmetric torsion form which does not split off  $\langle 2^{-1} \rangle$  and let  $q$  be a quadratic torsion form  $q$  with polar form  $b$ . Then the quantity  $\tau_8(q) + 4\omega(\delta(q_2)) \pmod 8$  only depends on  $b$  and so

$$t_8(b) := \tau_8(q) + 4\omega(\delta(q_2)) \pmod 8 \tag{12.11}$$

is well defined. Moreover, for any such choice of  $q$  and any prime  $p$  one has  $t_8(b_p) = \tau_8(q_p(2^{-1}))$ .

*Proof.* 1. The proof of this formula is given in Remark 12.3.4.

2. Note that for any odd prime  $p$  the  $p$ -primary part of  $b$  is the polar form of the form  $q_p$  and so one may as well assume that  $b$  is 2-primary. It suffices further to consider the Jordan summands of exponent 1 and 2 since for higher exponents there is a unique (non-degenerate) quadratic torsion form whose polar form is a given (non-degenerate) symmetric torsion form. But in these cases the assertion follows from the table.  $\square$

Recall the notation 12.10 which is tied to a given odd lattice  $L$ . The 2-adic localization of  $L = L(2)$  has discriminant symmetric form  $b_2$ . We consider the collection  $\mathcal{T}_8(b_2)$  of torsion quadratic forms with  $b_2$  as its polar form in an abstract manner:

**Proposition 12.5.12.** Let  $b_2$  be a non-degenerate torsion symmetric form on a 2-primary group  $G_2$  such that  $b_2^{(1)}$  splits off  $\langle 2^{-1} \rangle$ .

1. For  $b_2^{(1)}$  the following normal forms occur:

- (a) If  $b_2^{(1)} = \langle 2^{-1} \rangle$ , then  $\mathcal{T}_8(b_2^{(1)}) = \{1, -1\}$ .
- (b) If  $b_2^{(1)} = \oplus^2 \langle 2^{-1} \rangle$ , then  $\mathcal{T}_8(b_2^{(1)}) = \{0, 2, -2\}$ .
- (c) If  $b_2^{(1)} = \langle 2^{-1} \rangle \oplus \oplus^b u_1$ ,  $b \geq 1$ , then  $\mathcal{T}_8(b_2^{(1)}) = \{1, -1, 3, -3\}$ , a complete set of odd parity<sup>5</sup>.
- (d) If  $b_2^{(1)} = \oplus^2 \langle 2^{-1} \rangle \oplus^b u_1$ ,  $b \geq 1$ , then  $\mathcal{T}_8(b_2^{(1)}) = \{0, 2, -2, 4\}$ , a complete set of even parity.

<sup>5</sup>See Definition 12.5.3,

2. If  $\mathbf{b}_2^{\geq 2} = \mathbf{b}_2(2^{-1})$  for some 2-primary torsion symmetric form  $\mathbf{b}_2$  which does not split off  $\langle 2^{-1} \rangle$ , then  $t_8(\mathbf{b}_2) = \tau_8(\mathbf{q}_2^{\geq 2})$ , where  $\mathbf{q}_2^{\geq 2}$  is a quadratic form with polar form  $\mathbf{b}^{\geq 2}$ .

*Proof.* Item 1 follows from Table 12.5.1.

2. This is a consequence of Lemma 12.5.11.  $\square$

The above results lead to

**Theorem 12.5.13** (Existence for odd lattices [171, Thm. 1.16.5]). *Let there be given two non-negative integers  $(r_+, r_-)$  and a non-degenerate symmetric torsion group  $(G, \mathbf{b}^\#)$ . There exists a non-degenerate odd lattice  $(L, \mathbf{b})$  of rank  $r = r_+ + r_-$ , signature  $(r_+, r_-)$  and with discriminant bilinear form  $(G, \mathbf{b}^\#)$  if and only if all of the following conditions are fulfilled.*

- a)  $r \geq \ell(G_p)$  for odd primes  $p$ ,  $r \geq \ell(G_2) + 1$  (recall that  $G_p$  is the  $p$ -primary part of  $G$ ).
- b) For every odd prime  $p$  with  $r = \ell(G_p)$  we have  $(-1)^{r-|G_p|} = \text{disc}(\mathbf{b}_p^\#) \cdot (\mathbb{Z}_p^\times)^2$  in  $D(\mathbb{Z}_p)$ .
- c) Suppose that  $r = \ell(G_2) + 1$  and no non-degenerate cyclic rank 2 torsion quadratic form splits off from  $\mathbf{b}_2^\#$ . Then  $r_+ - r_- \equiv t_8(\mathbf{b}^\#) + \delta \pmod{8}$ ,  $\delta \in \{1, -1\}$ .
- d) Suppose that  $r = \ell(G_2) + 2$  and no non-degenerate cyclic rank 2 torsion quadratic form splits off from  $\mathbf{b}_2^\#$ . Then  $r_+ - r_- \equiv t_8(\mathbf{b}^\#) + \delta \pmod{8}$ ,  $\delta \in \{0, 2, -2\}$ .

*Proof.* We first assume that conditions a)–d) hold. The strategy is to construct a suitable quadratic torsion group  $\mathbf{q}$  which is the discriminant quadratic form of an even lattice  $\mathbf{L} = L(2)$ , where  $L$  is odd, has discriminant symmetric form  $\mathbf{b}^\#$  and signature  $(r_+, r_-)$ . Since the only prime that matters is 2, we start with  $\mathbf{b}_2^\#$  and we aim to first construct  $\mathbf{b}_2$ , the discriminant symmetric form of the localization  $\mathbf{L}_2$  of the purported lattice  $\mathbf{L}$ . To define  $\mathbf{b}_2$ , we start by setting (cf. Definition 9.3.10)

$$\mathbf{b}_2^{\geq 2} := \frac{1}{2}\mathbf{b}_2^\#.$$

By construction, its underlying torsion group, the halving of  $G_2$ , has the same length as  $G_2$ , the group underlying  $\mathbf{b}_2^\#$ .

By Proposition 12.5.8, the length of the searched for  $\mathbf{b}_2^{(1)}$  satisfies the relation

$$\ell(\mathbf{b}_2^{(1)}) = r_+ + r_- - \ell(\mathbf{b}_2^{(\geq 2)}) = r_+ + r_- - \ell(G_2).$$

If the last number (determinable from the data) is odd, i.e.,  $r_+ + r_- - \ell(G_2) = 1 + 2b$  for some  $b \geq 0$ , we set

$$\mathbf{b}_2^{(1)} := \langle 2^{-1} \rangle \oplus \oplus^b u_1. \tag{12.12}$$

If it is even, say  $r_+ + r_- - \ell(G_2) = 2 + 2b$ , set

$$\mathbf{b}_2^{(1)} := \oplus^2 \langle 2^{-1} \rangle \oplus \oplus^b \mathbf{u}_1. \tag{12.13}$$

Here we have used condition a) for  $p = 2$  and that, again by Proposition 12.5.8  $\langle 2^{-1} \rangle$  must split off from  $\mathbf{L}_2$ . Now set

$$\mathbf{b}_2 := \mathbf{b}_2^{(1)} + \mathbf{b}_2^{\geq 2}$$

so that the length of the group underlying  $\mathbf{b}_2$  is then precisely  $r$  as it should.

The primes  $p \neq 2$  do not play an essential role since  $\mathbf{b}_p^\#$  is the polar form of a unique quadratic torsion form  $\mathbf{q}_p^\#$ . The essential part of the proof consists in constructing  $\mathbf{q}_2$  with polar form  $\mathbf{b}_2$  so that the mod 8 index of

$$\mathbf{q} := \mathbf{q}_2 \oplus_{p \neq 2} \mathbf{q}_p^\#(2^{-1}),$$

satisfies  $r_+ - r_- \equiv \tau_8(\mathbf{q}) \pmod 8$ . We distinguish several cases:

1.  $r - \ell(G_2) \geq 3$ . In other words, we are in one of the cases (12.12) or (12.13) with  $b \geq 1$ . By Proposition 12.5.12,  $\mathcal{T}_8(\mathbf{b}_2^{(1)})$  then consists of a complete set of odd or even parity, so that it is always possible to choose  $\mathbf{q}_2^{(1)}$  with  $\tau_8(\mathbf{q}) \equiv r_+ - r_- \pmod 8$ .
2. If  $r - \ell(G_2) \in \{1, 2\}$  and  $\langle 2^{-1} \rangle$  splits off from  $\mathbf{b}_2^\#$ , then  $b = 0$ , i.e., either  $\mathbf{b}_2^{(1)} = \langle 2^{-1} \rangle$  (and so  $\mathbf{b}_2^{(2)} = \langle 2^{-2} \rangle$ ), or  $\mathbf{b}_2^{(1)} = \oplus^2 \langle 2^{-1} \rangle$  (and so  $\mathbf{b}_2^{(2)} = \oplus^2 \langle 2^{-2} \rangle$ ). In other words, we are in case 1(a) or 1(b) of Proposition 12.5.12. Since  $\mathcal{T}_8(\langle 2^{-1} \rangle) = \{1, -1\}$  and  $\mathcal{T}_8(\langle 2^{-2} \rangle) = \{1, -3\}$ , it follows that  $\mathcal{T}_8(\langle 2^{-1} \rangle \oplus \langle 2^{-2} \rangle) = \{0, 2, -2, 4\}$ , a complete set of even indexes mod 8. If  $\mathbf{b}_2^{(1)} = \langle 2^{-1} \rangle$ , we can choose  $\mathbf{q}_2^{(1)}$  and  $\mathbf{q}_2^{(2)}$  in such a way that all possible even or odd indexes mod 8 for  $\mathbf{q}$  can be realized. A similar argument applies if  $\mathbf{b}_2^{(1)} = \oplus^2 \langle 2^{-1} \rangle$ .
3. If  $r - \ell(G_2) \in \{1, 2\}$  and  $\langle 2^{-1} \rangle$  does not split off from  $\mathbf{b}_2^\#$ , then item 2 of Proposition 12.5.12 states that  $t_8(\mathbf{b}_2^\#) = \tau_8(\mathbf{q}_2^{\geq 2})$ . By definition (cf. (12.11)),  $t_8(\mathbf{b}_p^\#) = \tau_8(\mathbf{q}_p^\#)$  for odd primes  $p$ . So  $\tau_8(\mathbf{q}) = t_8(\mathbf{b}_2^\#) + \tau_8(\mathbf{q}_2^{(1)})$ . Items 1(a) and 1(b) of Proposition 12.5.12 enumerate the choices we have for  $\tau_8(\mathbf{q}_2^{(1)})$  and these match exactly the values of  $\delta$  given by condition c) or d). So the value of  $\delta$  determines the form  $\mathbf{q}_2^{(1)}$  we must choose.

We now can apply Theorem 12.4.4 which shows the existence of the purported even lattice  $\mathbf{L}$ .

Conversely, assume that an odd non-degenerate  $L$  exists with the stated properties and let  $\mathbf{L} = L(2)$ . For odd  $p$  we have  $L_p \simeq \mathbf{L}_p$  and so for those primes the conditions a) and b) of the present theorem hold since these hold for the even lattice  $\mathbf{L}$ . For the prime 2 condition a) holds since  $L_2$  splits off a rank one unimodular



lattice. To verify the remaining conditions, observe first that the index of  $\mathbf{L}$  is the same as the index of  $(L, b)$  and so

$$\begin{aligned} r_+ - r_- &\equiv \sum_{p \neq 2} \tau_8(\mathbf{q}_p) + \tau_8(\mathbf{q}_2^{\geq 2}) + \tau_8(\mathbf{q}_2^{(1)}) \pmod{8} \\ &\equiv t_8(\mathbf{b}^\#) + t \pmod{8}, \quad t \in \mathcal{T}_8(\mathbf{b}_2^{(1)}) \text{ (by Proposition 12.5.12, item 2),} \end{aligned}$$

and so conditions c) and d) follow from Proposition 12.5.12 items 1(a) and 1(b).  $\square$

**Corollary 12.5.14.** *Let  $(r_+, r_-)$  be a pair of non-negative integers and let  $(G, b)$  be a non-degenerate symmetric torsion group. There exists a non-degenerate odd lattice  $L$  of rank  $r$ , signature  $(r_+, r_-)$  and with discriminant form  $(G, b)$  if  $r \geq \ell(G) + 3$ .*

**Historical and Bibliographical Notes.** The existence of lattices with given discriminant quadratic form was first shown by C.T.C. Wall in [245]. In Section 12.1 we have given his proof, of which the crucial ingredient, the euclidean algorithm and its consequences, was already discussed in Section 4.3.

Uniqueness up to stable equivalence dates back to A. Durfee's thesis [56], which we have closely followed. The concept of "index mod 8" is due to V. Nikulin [171] who attributes its calculation to C.T.C. Wall. Our version as given in Section 12.3 is inspired by the calculations used to prove Theorem 8.14 in the book [99] by F. Hirzebruch, W. Neumann and S. Koh.

The insight that the classical existence results Theorems 12.4.1 and 12.4.2 can be reformulated in terms of the discriminant form (cf. Theorems 12.4.4, 12.5.13) is due to V. Nikulin and has been elaborated in his article [171]. It also contains the characterization of the genus in the case of odd lattices which is stated here as Theorem 12.5.9.

## The Spin Group

### Introduction

The spin group of a quadratic vector space  $(V, q)$  over a field  $k$  is defined by means of its Clifford algebra  $C(q)$ . As a vector space this is just the exterior algebra  $\Lambda(V)$  and it contains  $V$ . The algebra structure comes from  $q$ . For us its importance lies in the action of the algebra conjugation. Firstly, conjugation with a non-isotropic vector  $u \in V$  preserves  $V$  and, secondly, in  $V$  this gives the hyperplane reflection  $\sigma_u$  up to a sign. This property for  $u$  can be extended to a "large" subgroup of  $C(q)$ . To do this properly, one makes use of a canonical splitting of  $C(q)$  into even and odd elements. The even elements form a subalgebra, the even Clifford algebra. The conjugation with  $u$  receives a sign according to whether  $u$  is odd or even. The Clifford group consists of the invertible elements  $u$  of the Clifford algebra which have the property that twisted conjugation with  $u$  preserves  $V$ .

The classical Hamilton quaternions form the even Clifford algebra for the standard inner product on  $\mathbb{R}^3$ , as we shall see in Example 13.1.3.2; the non-zero quaternions give the special Clifford group as shown in Example 13.2.1.1. In Example 13.1.3.2 we show that, surprisingly, the classification of real Clifford algebras is equivalent to the classification of symmetric forms on  $F_2$ -vector spaces having an at most 1-dimensional radical. So the Arf invariant reappears here. Remarkably, the Arf invariant also comes up in § 13.1.B where the center of the Clifford algebra is calculated.

In the remainder of the chapter the field  $k$  has characteristic different from 2. In Section 13.2 some essential properties of the Clifford group are established. These are used to make sense of the spinor norm, a certain  $k^\times$ -valued function on  $\text{Clif}(q)$ , which is introduced in Section 13.3. Now one makes use of two observations: any element in the Clifford group is an algebra product of non-isotropic vectors in  $V$  and secondly, the Clifford algebra acts on  $V$  through a twisted adjoint action which for  $u \in V$  is given by the reflection  $\sigma_u$ . Combining the two, one defines the spinor norm of a product of such reflections as the spinor norm of the corresponding  $u$ . The Cartan–Dieudonné theorem implies that in this way we can define the spinor norm for any isometry. Since the decomposition of an isometry into reflections is not unique, this is ambiguous. To take this into account, we do not take  $k$  as the value group of this spinor norm, but  $D(k) = k^\times / (k^\times)^2$ . This version of the spinor norm shall play an essential role in establishing the classification of indefinite lattices given in Chapter 14.<sup>1</sup> In the final Section 13.4 we define all of

<sup>1</sup>For this last application only the even Clifford algebra and the untwisted adjoint action is of importance. We have chosen to involve the full Clifford algebra since it makes the presentation more coherent.

the preceding concepts in the setting of lattices.

### 13.1 The Clifford Algebra

In this section  $k$  is a field of any characteristic,  $V$  a  $k$ -vector space and  $q$  a (possibly degenerate) quadratic form on  $V$ .

**13.1.A Basic properties.** Recall that the exterior algebra  $\Lambda(V)$  is the quotient of the tensor algebra  $T(V)$  by the two-sided ideal generated by the tensors  $x \otimes x$ ,  $x \in V$ . This is a  $k$ -vector space of dimension  $2^{\dim V}$ . In the presence of a quadratic form we consider another (non-commutative) unital  $k$ -algebra, the Clifford algebra  $\mathbf{C}(q)$  of  $(V, q)$ , which might be viewed as a deformation of  $\Lambda(V)$  in that the generating relations  $x \otimes x = 0$  have been replaced by

$$x \otimes x = q(x) \cdot \mathbf{1}, \quad x \in V, \quad (13.1)$$

where we denote the unit by  $\mathbf{1}$  in  $\mathbf{C}(q)$  and the product with a dot. One finds back  $\Lambda(V)$  in case  $q = 0$  and in that sense  $\mathbf{C}(q)$  is a deformation of the exterior algebra and so both vector spaces have the same dimension. This is elaborated below resulting in Lemma 13.1.2.

The Clifford algebra  $\mathbf{C}(q)$  contains  $V$  (see below). The defining rule (13.1) implies first of all that non-isotropic vectors  $x \in V$  are invertible within  $\mathbf{C}(q)$  with two-sided inverse  $q(x)^{-1}x$ . Secondly, using the algebra rules, the commutation rule for two vectors  $x, y \in V$  is completely determined by (13.1):

$$\begin{aligned} b_q(x, y) \cdot \mathbf{1} &= q(x+y) \cdot \mathbf{1} - q(x) \cdot \mathbf{1} - q(y) \cdot \mathbf{1} \\ &= (x+y) \cdot (x+y) - x \cdot x - y \cdot y \\ &= x \cdot y + y \cdot x. \end{aligned}$$

It follows in particular that  $x \cdot y + y \cdot x = 0$  whenever  $x$  and  $y$  are orthogonal. Surprisingly, using this commutation rule, conjugation within  $\mathbf{C}(q)$  by a non-isotropic  $u \in V$  preserves  $V$  and induces in  $V$  the reflection  $\sigma_u$  up to sign:<sup>2</sup>

$$\begin{aligned} u \cdot x \cdot u^{-1} &= (u \cdot x + x \cdot u)u^{-1} - x, \quad x \in V \\ &= b_q(x, u)u^{-1} - x, \\ &= b_q(x, u)q(u)^{-1}u - x \\ &= -\sigma_u(x). \end{aligned} \quad (13.2)$$

If the characteristic is different from 2, the Cartan–Dieudonné theorem 7.2.4 then implies that all orthogonal transformations up to sign extend to the algebra  $\mathbf{C}(q)$  as conjugations. This shows the relevance of this algebra. Its formal definition is as follows:

<sup>2</sup>In the calculation the unit has been dropped.

**Definition 13.1.1.** The *Clifford algebra*  $C(q)$  is defined as the quotient of the tensor algebra  $T(V)$  on  $V$  by the two-sided ideal  $I(q)$  generated by  $x \otimes x - q(x) \cdot \mathbf{1}$ ,  $x \in V$ , and with multiplication induced by the multiplication in  $T(V)$ . We denote the multiplication in the Clifford algebra by a dot.

The natural composition

$$\iota : V \rightarrow T(V) \rightarrow T(V)/I(q) = C(q)$$

is a map of  $k$ -vector spaces for which  $\iota(x) \cdot \iota(x) = q(x) \cdot \mathbf{1}$ . One can show that  $\iota$  is injective. We refer to [137, Ch. I.1] for a proof. To simplify notation we shall identify  $V$  with its image  $\iota(V)$ .

Alternatively, we may use the Bourbakist definition of this algebra which is as follows: the Clifford algebra on  $q$  is a pair  $(C(q), \iota)$  of a  $k$ -algebra  $C(q)$  with unit  $\mathbf{1}$  together with a  $k$ -linear map  $\iota : V \rightarrow C(q)$  for which  $\iota(x) \cdot \iota(x) = q(x) \cdot \mathbf{1}$  and which satisfies the following universality property: any  $k$ -linear map  $u : V \rightarrow A$  to a  $k$ -algebra  $A$  such that  $u(x) \cdot u(x) = q(x) \cdot \mathbf{1}$  extends to  $C(q)$ . For the statement and proof that the preceding construction implies universality, see [137, Ch. I, Prop 1.1].

The grading on  $T(V)$  does not descend to  $C(q)$  since the ideal  $I(q)$  is not homogeneous. However, it is generated in even degrees only, which implies that  $C(q)$  gets a  $\mathbb{Z}/2\mathbb{Z}$ -grading, that is

$$C(q) = C^0(q) \oplus C^1(q), \quad C^i(q) \cdot C^j(q) \subset C^{i+j}(q),$$

where the indices are taken modulo 2. In particular  $C^0(q)$  is a subalgebra, the *even Clifford algebra*. The universality property for the Clifford algebra applied to  $u = -\iota$  shows for example that there exists an involution  $\alpha$  restricting to  $-\text{id}$  on  $V \subset C^1(q)$ . It satisfies

$$\alpha : C(q) \rightarrow C(q), \quad \begin{cases} \alpha|_{C^0(q)} &= \text{id}, \\ \alpha|_{C^1(q)} &= -\text{id}. \end{cases} \quad (13.3)$$

This gives the Bourbakist definition of the even and odd Clifford algebra as eigenspaces of  $\alpha$ .

We claimed above that  $C(q)$  is a deformation of the exterior algebra  $\Lambda(V)$ . This can be made more precise. The tensor-degree defines an obvious filtration  $F^\bullet$  on  $T(V)$  which descends to  $C(q)$ . It preserves the algebra structure in the sense that  $F^i \cdot F^j \subset F^{i+j}$  and the associated grading gives  $C(q)$  the structure of a graded algebra. The graded algebra  $\Lambda V$  is canonically isomorphic to this graded algebra through the map which sends  $v_1 \wedge \cdots \wedge v_k$  to the class of  $v_1 \cdots v_k$ . This map is clearly surjective and one can show by induction on the degree that it is also an injective map. See e.g. [137, Ch 1.1, Prop. 1.2].

This shows:

**Lemma 13.1.2.** *There is a canonical vector space isomorphism  $\Lambda(V) \xrightarrow{\cong} C(q)$ . In particular,  $\dim_k C(q) = 2^{\dim V}$ .*

**Examples 13.1.3. 1. Hamiltonian quaternions revisited.** Consider the standard diagonal form  $x_1^2 + x_2^2 + x_3^2$  on  $\mathbb{R}^3$ . Its Clifford algebra has as a vector space basis  $\{1, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{i} = \mathbf{e}_2\mathbf{e}_3, \mathbf{j} = \mathbf{e}_3\mathbf{e}_1, \mathbf{k} = \mathbf{e}_1\mathbf{e}_2, \mathbf{e}_1\mathbf{e}_2\mathbf{e}_3\}$ , where  $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$  is the standard basis of  $\mathbb{R}^3$ . Since for  $i, j = 1, 2, 3$  we have  $\mathbf{e}_i\mathbf{e}_j = -\mathbf{e}_j\mathbf{e}_i$  for  $i \neq j$ , and  $\mathbf{e}_i^2 = 1$ , it follows that  $\mathbf{i} \cdot \mathbf{j} = \mathbf{e}_2\mathbf{e}_3\mathbf{e}_3\mathbf{e}_1 = \mathbf{e}_2\mathbf{e}_1 = \mathbf{k}$  and similarly for the cyclic permutations of  $\mathbf{i}, \mathbf{j}, \mathbf{k}$ . Moreover,  $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ . So the vector space with basis  $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$  generates the algebra of the Hamilton quaternions  $\mathbb{H}$  which we already encountered in § 5.4.A. This is the even Clifford algebra for the dot product form on  $\mathbb{R}^3$ . As a special case of the second example below we shall see that  $\mathbb{H}$  also figures as the full Clifford algebra of the form  $-x_1^2 - x_2^2$  on  $\mathbb{R}^2$ .

Recall also that we explained in Section 5.4 how to associate a ternary quadratic form to any quaternion algebra  $D = \left(\frac{a,b}{k}\right)$ , namely the norm form restricted to the subspace  $D^{(0)}$  of the quaternions of trace 0. For the Hamilton quaternions this is the dot product form on  $\mathbb{R}^3$  where  $\mathbb{R}^3$  is identified with the real space with basis  $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$ , the so-called pure quaternions. In general the even Clifford algebra of the norm form on  $D^{(0)}$  is precisely  $D$ .

**2. Real Clifford algebras (cf. [68, 179])** By Sylvester's law 8.1.3 non-degenerate real forms are classified by their signature  $(r, s)$  with representing diagonal quadratic forms  $\sum_{i=1}^r x_i^2 - \sum_{i=r+1}^n x_i^2$ ,  $n = r + s$ . The corresponding Clifford algebra  $C_{r,s}$  is then generated by the standard basis  $\{\mathbf{e}_1, \dots, \mathbf{e}_{r+s}\}$  subject to the relations

$$\mathbf{e}_i^2 = \begin{cases} 1 & \text{if } i \leq r \\ -1 & \text{if } i > r \end{cases} \quad \text{and} \quad \mathbf{e}_i \cdot \mathbf{e}_j + \mathbf{e}_i \cdot \mathbf{e}_j = 0 \text{ if } i \neq j.$$

For example,  $C_{0,0} = \mathbb{R}$ ,  $C_{1,0} = \mathbb{R} \oplus \mathbb{R}$ , while  $C_{0,1} = \mathbb{C}$ . We shall now show that the isomorphism class of the Clifford algebra of a real quadratic form does not determine the signature. To do so we make basic use of quadratic forms over  $\mathbb{F}_2$  as suggested by the signs that appear in the above relations. We start by considering the group ring  $\mathbb{R}[G]$ ,  $G = \prod^n C_2$ , where  $C_2$  is the cyclic group of order 2. Viewing  $C_2$  as the field  $\mathbb{F}_2$  and switching to additive notation and identifying group-elements of  $G$  with vectors  $\mathbf{x} \in \mathbb{F}_2^n$ , this group ring becomes the real vector space  $V := \bigoplus_{\mathbf{x} \in G} \mathbb{R} \cdot \mathbf{e}_{\mathbf{x}}$  with algebra structure induced by the additive group structure, i.e., the product  $*$  is given by  $\mathbf{e}_{\mathbf{x}} * \mathbf{e}_{\mathbf{y}} = \mathbf{e}_{\mathbf{x}+\mathbf{y}}$ . As vector spaces  $V$  and  $C_{r,s}$  are isomorphic: identify  $\mathbf{e}_{\mathbf{x}} \in V$  with the element  $\mathbf{e}_{i_1} \cdots \mathbf{e}_{i_k} \in C_{r,s}$  where  $\mathbf{x}$  has  $i$ -th coordinate 1 precisely if  $i \in \{i_1, \dots, i_k\}$ . In particular, if  $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$  is the standard basis of  $\mathbb{F}_2^n$ ,

$$\mathbf{e}_{\mathbf{e}_k} \text{ corresponds to } \mathbf{e}_k. \tag{13.4}$$

The possibly non-commutative Clifford algebra  $C_{r,s}$  comes from the twisted group action

$$\mathbf{e}_{\mathbf{x}} \cdot \mathbf{e}_{\mathbf{y}} = (-1)^{\beta^{r,s}(\mathbf{x},\mathbf{y})} \mathbf{e}_{\mathbf{x}} * \mathbf{e}_{\mathbf{y}}, \tag{13.5}$$

where  $\beta^{r,s}$  is the  $\mathbb{F}_2$ -valued (in general non-symmetric) bilinear form on  $\mathbb{F}_2^n$ , which in coordinates with respect to the standard basis  $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$  is given by  $\mathbf{x} \mathbf{A}^{r,s} \mathbf{y}^T$ ,

where  $A$  is the upper-triangular matrix

$$A^{r,s} = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ \vdots & 0 & \ddots & \vdots \\ \vdots & \cdots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 \end{pmatrix} + \left( \begin{array}{c|c} \mathbf{0}_r & \mathbf{0}_{r \times s} \\ \hline \mathbf{0}_{s \times r} & \mathbf{1}_s \end{array} \right) \tag{13.6}$$

By the correspondence (13.4) the relations  $(-1)^{A_{ij}^{rs}} = -1$  for  $j > i$  and  $(-1)^{A_{ij}^{rs}} = 1$  for  $j < i$  imply that the desired anti-commutation relations hold, while  $(-1)^{A_{ii}^{rs}} = 1$  for  $i \leq r$  and  $(-1)^{A_{ii}^{rs}} = -1$  for  $i > r$ , proving the remaining two relations.

Observe that as in equation (1.1) in Chapter 1, a bilinear form defines a unique quadratic form on  $\mathbb{F}_2^n$ . Conversely, given a basis for a  $\mathbb{F}_2$ -vector space, a quadratic form  $q$  determines an upper-triangular bilinear form  $\beta$  which can be used to define a twisted product (13.5). The resulting associative algebra is denoted  $C_{\mathbb{R}}[\mathbb{F}_2^n, q]$ . This algebra has a special structure: either the generators  $\mathbf{e}_i$  and  $\mathbf{e}_j$  for  $i \neq j$  anti-commute (namely if  $\beta_{ij} = 1$  for  $i < j$  since then  $\mathbf{e}_i \cdot \mathbf{e}_j = -\mathbf{e}_i * \mathbf{e}_j$  and  $\mathbf{e}_j \cdot \mathbf{e}_i = \mathbf{e}_j * \mathbf{e}_i$ ), or they commute (if  $\beta_{ij} = 0$  for  $i < j$ , since then  $\mathbf{e}_i \cdot \mathbf{e}_j = \mathbf{e}_j \cdot \mathbf{e}_i = \mathbf{e}_i * \mathbf{e}_j$ ). It follows that isometric forms  $q$  give isomorphic algebras.

So the classification of the real Clifford algebras follows from the classification of the quadratic forms on the vector spaces  $\mathbb{F}_2^n$  as given in Example 8.2.7. The non-degenerate forms live on even-dimensional spaces and come in two types depending on the Arf invariant. The ones with zero Arf invariant are the form  $q_0 = \bigoplus^m U$ ,  $n = 2m$ , the ones with Arf invariant 1 are of the form  $q_1 = \bigoplus^{m-1} U \oplus \bigoplus^2 \langle 1 \rangle$ ,  $n = 2m$ . On odd dimensional spaces, say of dimension  $n = 2m + 1$ , one has three types with  $\dim \text{rad}(q) \leq 1$ , namely  $q'_0 = \bigoplus^m U \oplus 0$ ,  $q'_1 = \bigoplus^{m-1} U \oplus \bigoplus^2 \langle 1 \rangle \oplus 0$  and  $q_2 = \bigoplus^m U \oplus [1]$ . We shall show that these types indeed give all the real Clifford algebras  $C_{r,s}$ .

Note however, to identify  $C_{\mathbb{R}}[\mathbb{F}_2^n, q]$  with some  $C_{r,s}$ , one has to transform each of the 5 types of quadratic forms  $q(\mathbf{x})$  into the desired shape  $\mathbf{x}A^{r,s}\mathbf{x}^T$ , where  $A^{r,s}$  is as in formula (13.6). This poses no problem for  $C_{\mathbb{R}}[\mathbb{F}_2^2, q_i]$ ,  $i \in \{0, 1\}$ : these are the 4-dimensional Clifford algebras  $C_{2,0}, C_{0,2}$  with generators  $\mathbf{e}_1, \mathbf{e}_2$  subject to

$$\mathbf{e}_1^2 = \mathbf{e}_2^2 = 1, \quad \mathbf{e}_1 \cdot \mathbf{e}_2 = -\mathbf{e}_2 \cdot \mathbf{e}_1 \text{ for } q_0 \tag{13.7}$$

$$\mathbf{e}_1^2 = \mathbf{e}_2^2 = -1, \quad \mathbf{e}_1 \cdot \mathbf{e}_2 = -\mathbf{e}_2 \cdot \mathbf{e}_1 \text{ for } q_1. \tag{13.8}$$

Next, since  $x_1x_2 + x_2^2$  has Arf invariant 0 it is isometric to  $x_1x_2$  (in fact  $(x_1, x_2) \mapsto (x_1 + x_2, x_2)$  is an isometry). The first corresponds to  $C_{1,1}$  and the second to  $C_{2,0}$ , which indeed shows that the Clifford algebra does not determine the signature.

To continue, one checks that  $C_{2m,0} = C_{\mathbb{R}}[\mathbb{F}_2^{2m}, q_0]$  since  $A^{2m,0}$  corresponds to  $q_0$ . Likewise  $C_{0,2m} = C_{\mathbb{R}}[\bigoplus^{2m} \mathbb{F}_2, q_1]$ . The forms  $q'_0, q'_1$  correspond to  $C_{2m+1,0}$ , respectively  $C_{0,2m+1}$  and  $q_2$  corresponds to  $C_{m,m+1}$ . The resulting 2 types of  $2^{2m}$ -dimensional real Clifford algebras and 3 types of  $2^{2m+1}$ -dimensional real Clifford algebras fit in a remarkable periodic table of period 8 displayed as [137, Table II in §I.4]. This table makes use of an identification of these Clifford algebras with familiar matrix algebras as follows. The relations (13.7) show that the assignments

$\mathbf{e}_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $\mathbf{e}_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  give an algebra-isomorphism of  $C_{2,0}$  with  $\text{Mat}(2, \mathbb{R})$ .

Similarly, the map induced by  $\mathbf{e}_1 \mapsto \mathbf{i}$ ,  $\mathbf{e}_2 \mapsto \mathbf{j}$  (13.8) identifies the Clifford algebra  $C_{0,2}$  with the Hamiltonian quaternions. It follows that  $C_{2m,0} = C_{\mathbb{R}}[\mathbb{F}_2^{2m}, \mathbf{q}_0]$  leads to  $\otimes^m \text{Mat}(2, \mathbb{R}) = \text{Mat}(2^m, \mathbb{R})$  and  $C_{0,2m} = C_{\mathbb{R}}[\oplus^{2m} \mathbb{F}_2, \mathbf{q}_1]$  to  $\text{Mat}(2, \mathbb{R}) \otimes \mathbb{H} \simeq \text{Mat}(2^{m-1}, \mathbb{H})$ . Finally, the Clifford algebras  $C_{2m+1,0}$ ,  $C_{0,2m+1}$  and  $C_{m,m+1}$  are isomorphic to  $\text{Mat}(2^m, \mathbb{R}) + \text{Mat}(2^m, \mathbb{R})$ ,  $\text{Mat}(2^{m-1}, \mathbb{H}) + \text{Mat}(2^{m-1}, \mathbb{H})$ , respectively  $\text{Mat}(2^m, \mathbb{C})$ .

### 13.1.B The center of the Clifford Algebra.

**Proposition 13.1.4** ( $\text{char}(k) \neq 2$ ). *Let  $(V, q)$  be a  $k$ -quadratic space with an orthogonal basis  $\{e_1, \dots, e_n\}$ . Setting  $e = e_1 \cdots e_n \in C(q)$ , we have:*

- The center of  $C(q) = \begin{cases} k & \text{if } n \text{ is even} \\ k + k \cdot e & \text{if } n \text{ is odd} \end{cases}$
- The center of  $C^0(q) = \begin{cases} k & \text{if } n \text{ is odd} \\ k + k \cdot e & \text{if } n \text{ is even} \end{cases}$

*Proof.* The relations  $e_i e_j = -e_j e_i$ ,  $i \neq j$ , imply that  $e_J = e_{j_1} \cdots e_{j_k}$ ,  $J = \{j_1, \dots, j_k\} \subset \{1, \dots, n\}$  having  $k$  distinct elements, commutes with  $e_i e_j$  if either both or none of  $i$  and  $j$  belong to  $J$ . Otherwise there is a minus sign. It follows that  $e$  commutes with all products  $e_i e_j$ . But if  $\emptyset \neq J \neq \{1, \dots, n\}$ , taking  $i \notin J$  and  $j \in J$ , we see that  $e_J$  does not commute with  $e_i e_j$ . Since every element of  $C(q)$  is a  $k$ -linear combination of such elements  $e_J$ , we conclude that

$$C(q)_{C^0(q)} = \{x \in C(q) \mid xy = yx \text{ for all } y \in C^0(q)\} = k + ke.$$

Since  $e \cdot e_i = (-1)^{n-1} e_i \cdot e$ , for  $n$  odd  $e$  commutes with all elements in  $C(q)$  which shows the assertion for  $C(q)$ . Since  $C(q)_{C^0(q)} \cap C^0(q)$  is the center of  $C^0(q)$ , the second assertion follows as well.  $\square$

In characteristic two the situation is different (note the striking reappearance of the Arf invariant):

**Proposition 13.1.5.** *Suppose that  $\text{char}(k) = 2$ . Let  $q$  be a non-degenerate quadratic form, and let  $\{e_1, \dots, e_{2n}\}$  be a symplectic basis such that  $q = \sum_{j=1}^n x_i x_{n+i} + \sum_{j=1}^{2n} a_j x_j^2$ . Setting  $\mathbf{z} = e_1 e_{n+1} + \cdots + e_n e_{2n} \in C^0(q)$ , the center of  $C(q)$  is  $k$  and the center of  $C^0(q)$  equals  $k + k\mathbf{z}$ .*

*Moreover,  $\mathbf{z}$  satisfies the relation  $\mathbf{z}^2 + \mathbf{z} \equiv \mathbf{a}(q) \pmod{\wp(k)}$ , where we recall that  $\mathbf{a}(q)$  is the Arf invariant of  $q$ .*

*Proof.* In the Clifford algebra one has the relations

$$\begin{aligned} e_i^2 &= a_i, & i &= 1, \dots, n, \\ e_i e_j &= e_j e_i, & i, j &= 1, \dots, n, \text{ or } i, j = n+1, \dots, 2n, \\ e_i e_{n+j} + e_{n+i} e_j &= \delta_{ij}, & i, j &= 1, \dots, n. \end{aligned}$$

From these relations one sees that  $\mathbf{z} \cdot e_i = e_i \cdot \mathbf{z} + e_i$  and  $\mathbf{z} \cdot e_j e_i = e_j e_i \cdot \mathbf{z}$  for all  $i, j$ , and so  $\mathbf{z}$  centralizes  $C^0(q)$  but not  $C(q)$ . If we have any odd product, say  $e_J = e_{j_1} \cdots e_{j_k}$  of the  $e_i$ , then  $e_J \mathbf{z} = \mathbf{z} e_J + e_J$ . This proves that the center of  $C(q)$  consists of  $k$  while that of  $C^0(q)$  equals  $k + k \cdot \mathbf{z}$ . The final relation follows from  $\mathbf{z}^2 + \mathbf{z} = \sum_{i=1}^n a_i a_{i+n}$ .  $\square$

## 13.2 The Clifford Group

In this section  $V$  is a vector space over a field  $k$  of characteristic  $\neq 2$  and  $q : V \rightarrow k$  is a non-degenerate quadratic form, i.e.  $(V, q)$  is a quadratic inner product space.

The Clifford group, to be defined below, is a subgroup of the group  $C(q)^\times$  of the invertible elements of the Clifford algebra  $C(q)$  of  $q$ . Examples of invertible elements are the non-isotropic vectors  $u \in V$ , whose inverses are, we recall, given by  $q(u)^{-1}u$ . In that case,  $\text{Ad}_u$ , conjugation by  $u$  within the Clifford algebra, preserves  $V$  and  $-\text{Ad}_u|_V = \sigma_u$  by equation (13.2). It is convenient for our purposes to extend  $-\text{Ad}$ , which leads to the twisted adjoint

$$\widetilde{\text{Ad}} : C(q)^\times \longrightarrow \text{Aut}(C(q)), \quad \widetilde{\text{Ad}}_u x = \alpha(u) \cdot x \cdot u^{-1},$$

where  $\alpha$  is the involution (13.3). In other words, if  $u \in C^0(q)$ , this is the usual adjoint, but for  $u \in C^1(q)$  this is minus the adjoint. The **Clifford group** consists of *all* invertible elements of the Clifford algebra whose twisted adjoint action preserves  $V$ :

$$\text{Clif}(q) := \{u \in C(q)^\times \mid \widetilde{\text{Ad}}_u(V) \subset V\}.$$

Note that  $\text{Clif}(q)$  contains  $k^\times$  and is indeed a group. For instance, if  $u \in \text{Clif}(q)$  then  $u^{-1} \in \text{Clif}(q)$ . To see this, observe that  $v \in V$  can be written in the form  $v = \alpha(u) \cdot v' \cdot u^{-1}$ , since  $\widetilde{\text{Ad}}_u$  is an automorphism, and then  $\alpha(u^{-1}) \cdot v \cdot u = \alpha(u^{-1})\alpha(u) \cdot v' \cdot u^{-1} \cdot u = v' \in V$ .

The **special Clifford group** is given by  $\text{Clif}^0(q) := \text{Clif}(q) \cap C^0(q)$ .

**Examples 13.2.1. 1. Hamilton quaternions (II).** With  $q$  the standard dot product on  $\mathbb{R}^3$  spanned by  $e_1, e_2, e_3$ , we have seen that  $C^0(q) = \mathbb{H}$ , the Hamilton quaternion algebra (cf. Example 13.1.3.2). The involution  $\mathbf{x} \mapsto \mathbf{x}^*$  sending  $\mathbf{x} = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$  to  $\mathbf{x}^* = x_0 - x_1\mathbf{i} - x_2\mathbf{j} - x_3\mathbf{k}$  (the usual extension of complex conjugation to quaternions) can be used to define the norm  $\text{Nm}(\mathbf{x}) = \mathbf{x}\mathbf{x}^* = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbb{R}$  of a quaternion  $\mathbf{x}$ . A non-zero element  $\mathbf{x} \in \mathbb{H}$  has  $\text{Nm}(\mathbf{x})^{-1}\mathbf{x}$  as its inverse. It is easy to verify that conjugating by  $\mathbf{x}$  preserves the span of  $e_1, e_2, e_3$ . So  $\mathbb{H} - \{0\}$  is the special Clifford group. Now identify the pure quaternions, i.e. those with  $x_0 = 0$ , with (another copy of)  $\mathbb{R}^3$ . These are preserved under conjugation with a non-zero quaternion, as one easily verifies. This gives a representation of the special Clifford group on  $\mathbb{R}^3$  by means of orthogonal transformations. In fact, one can show that it gives a surjection onto the rotation group  $\text{SO}(3)$  with kernel  $\mathbb{R}^\times$ , whence a finite surjective homomorphism

$$\text{Spin}(3) = \{\mathbf{x} \in \mathbb{H} \mid \text{Nm}(\mathbf{x}) = 1\} \rightarrow \text{SO}(3).$$



The left-hand side is the classical spin group. The map turns out to have degree 2 and gives the universal cover of  $\mathrm{SO}(3)$ . See also Remark 13.3.6.3.

2. Let us consider the Lorentzian type inner product space  $\mathbb{R}^3$  with standard basis  $\{e_1, e_2, e_3\}$  and quadratic form given by  $q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$ . Then  $C^0(q)$  is spanned by  $\mathbf{i} = e_3e_2$ ,  $\mathbf{j} = e_1e_3$  and  $\mathbf{k} = e_2e_1$ , but now  $\mathbf{i}^2 = \mathbf{j}^2 = 1$ ,  $\mathbf{k}^2 = -1$ ,  $\mathbf{ij} = -\mathbf{ji} = -\mathbf{k}$  and similarly for cyclic permutations of  $\mathbf{i}, \mathbf{j}, \mathbf{k}$ . This algebra has a representation as a matrix algebra, where  $x + \mathbf{i}y + \mathbf{j}z + \mathbf{k}w$  corresponds to the matrix  $\begin{pmatrix} x+y & z-u \\ z+u & x-y \end{pmatrix}$ .

The twisted adjoint is not a faithful representation. Its kernel is going to play a central role in Section 13.3.

**Proposition 13.2.2.** *The kernel of the homomorphism  $\mathrm{Clif}(q) \rightarrow \mathrm{Aut}(V)$  given by  $u \mapsto \widetilde{\mathrm{Ad}}_u|_V$  is equal to  $k^\times \cdot \mathbf{1}$ .*

*Proof.* We follow the proof of [137, Prop. 2.4]. Suppose that for some  $u \in \mathrm{Clif}(q)$  twisted conjugation by  $u$  induces the identity in  $V$ . Since  $q$  is non-degenerate, there is an orthogonal basis  $\{e_1, \dots, e_n\}$  of  $V$ . Write  $u = u_0 + u_1$  with  $u_0$  even and  $u_1$  odd. So for all  $v \in V$  we have

$$\alpha(u) \cdot v = v \cdot u \implies \begin{cases} v \cdot u_0 &= u_0 \cdot v \\ v \cdot u_1 &= -u_1 \cdot v. \end{cases} \quad (13.9)$$

If one writes  $u_0$  as a (non-commuting) polynomial in the basis elements and uses orthogonality to rearrange terms, one finds an expression of the form

$$u_0 = a_0 + e_1 \cdot a_1, \quad a_0 \in C^0(q), \quad a_1 \in C^1(q), \quad \text{both polynomials in } e_2, \dots, e_n.$$

In particular  $e_1$  commutes with  $a_0$  and anti-commutes with  $a_1$ . Now apply the first equation of (13.9) with  $v = e_1$  and we get

$$e_1 \cdot a_0 + e_1^2 \cdot a_1 = a_0 \cdot e_1 + e_1 \cdot a_1 \cdot e_1 = e_1 \cdot a_0 - e_1^2 \cdot a_1,$$

and so<sup>3</sup>  $0 = 2e_1^2 \cdot a_1 = 2q(e_1)a_1$  which implies that  $a_1 = 0$ . So  $u_0$  does not involve  $e_1$ . Inductively, one shows that  $u_0$  does not involve any of the  $e_j$  and so  $u_0 \in k$ . Doing the same for  $u_1$  we find that  $u_1$  does not involve any of the  $e_j$  and so, since it is odd, it must be zero. We conclude that  $u = t \cdot \mathbf{1}$  and hence  $u \in k^\times \cdot \mathbf{1}$ .  $\square$

There is a second fundamental involution on  $C(q)$  induced by the order reversal map  $x_1 \otimes \dots \otimes x_r \mapsto x_r \otimes \dots \otimes x_1$  on  $T(V)$ . Since this map preserves the ideal  $I(V)$ , it descends to an involution on the Clifford algebra, the *canonical involution*, denoted by  $u \mapsto u^*$ . This is in fact an anti-involution with respect to the product in the sense that  $(u \cdot v)^* = v^* \cdot u^*$  and  $(u^*)^* = u$ , which is immediate from the definitions. Note that  $u^* = u$  whenever  $u \in V$ . Moreover, since the canonical involution respects the  $\mathbb{Z}/2\mathbb{Z}$ -grading,  $\alpha(u^*) = \alpha(u)^*$ . In other words, the two fundamental involutions commute. We shall use two more properties:

<sup>3</sup>Here we clearly see that we need to assume  $\mathrm{char}(k) \neq 2$

**Lemma 13.2.3.** *The two involutions  $\alpha$  and  $*$  preserve the Clifford group  $\text{Clif}(q)$ .*

*Proof.* Let  $v \in V$  be arbitrary. Since  $\alpha$  is an involution and  $\alpha(v) = -v$  we have

$$\alpha(\alpha(u))v\alpha(u)^{-1} = uv\alpha(u^{-1}) = -\alpha^2(u)\alpha(v)\alpha(u^{-1}) = -\alpha(\alpha(u))v\alpha(u^{-1}) \in V.$$

A similar proof holds for the second fundamental involution  $*$ .  $\square$

**Example 13.2.4.** For Examples 13.2.1 we find that  $1^* = 1$  and  $\mathbf{i}^* = -\mathbf{i}$ ,  $\mathbf{j}^* = -\mathbf{j}$  and  $\mathbf{k}^* = -\mathbf{k}$ . This shows that the notation is consistent with the notation for the classical Hamiltonians. For the latter we have seen that  $\mathbf{x} \cdot \mathbf{x}^* \in \mathbb{R}$ . This is also true for the second example: we find that  $\mathbf{x} \cdot \mathbf{x}^* = x^2 - y^2 - z^2 + w^2$ . However, for mixed degree elements in a Clifford algebra this need not be the case as is shown by the example  $\mathbf{x} = e_1 + e_1e_2$ , where  $\mathbf{x} \cdot \mathbf{x}^* = (e_1 + e_1e_2)(e_1 + e_2e_1) = 2 - 2e_2$ .

### 13.3 The Spin Group and Spinor Norm

In this section  $(V, q)$  is a quadratic inner product space over  $k$ ,  $\text{char}(k) \neq 2$ .

For vectors  $v \in V \subset C(q)$  we have  $v \cdot v = q(v)$  which we may rewrite as  $v \cdot \alpha(v^*) = -q(v)$ . Although Example 13.2.4 shows that for  $u \in C(q)$  the product  $u \cdot u^*$  need not belong to  $k$ , we shall show that the product does belong to  $k$  if  $u \in \text{Clif}^0(q)$ . In fact, we show that the *spinor norm*

$$\text{Nm}_{\text{spin}}(u) := u \cdot \alpha(u^*), \quad u \in \text{Clif}(q),$$

belongs to  $k^\times$  and so the spinor norm, by Lemma 13.2.3 a priori only  $\text{Clif}(q)$ -valued, is a  $k$ -valued function and which extends the quadratic form  $q$  (restricted to non-isotropic vectors):

**Proposition 13.3.1.** *The spinor norm is a homomorphism from  $\text{Clif}(q)$  to  $k^\times$ .*

*Proof.* We follow the arguments in [137, Ch. 1.2]. Let us first show that for  $u \in \text{Clif}(q)$ ,  $\text{Nm}_{\text{spin}}(u) \in k^\times$ .

By definition,  $\alpha(u) \cdot v \cdot u^{-1} \in V$  whenever  $v \in V$ . It suffices to show that the twisted adjoint of  $\text{Nm}_{\text{spin}}(u)$  induces the identity in  $V$  since then the result follows from Proposition 13.2.2. Let us elaborate this. Since  $u \in \text{Clif}(q)$  implies  $u^* \in \text{Clif}(q)$  (see Lemma 13.2.3), the element  $\alpha(u^*) \cdot v \cdot (u^*)^{-1}$  is in  $V$ . Applying the homomorphism  $\alpha$  then yields that  $u^* \cdot v \cdot \alpha(u^*)^{-1} \in V$ . Since the canonical involution is the identity on  $V$ , we then find that

$$u^* \cdot v \cdot \alpha(u^*)^{-1} = (u^* \cdot v \cdot \alpha(u^*)^{-1})^* = \alpha(u^{-1}) \cdot v \cdot u. \quad (13.10)$$

On the other hand, setting  $w = \text{Nm}_{\text{spin}}(u) = u \cdot \alpha(u^*)$ , we find

$$\widetilde{\text{Ad}}_w v = \alpha(w) \cdot v \cdot w^{-1} = \alpha(u) \cdot u^* \cdot v \cdot \alpha(u^*)^{-1} \cdot u^{-1} \stackrel{(13.10)}{=} v.$$

This completes the proof that the twisted adjoint of  $\text{Nm}_{\text{spin}}(u)$  induces the identity in  $V$

To check that the spinor norm is a group homomorphism, note that  $uv \cdot \alpha((uv)^*) = uv \cdot \alpha(v^*u^*) = u \cdot (v \cdot \alpha(v^*)) \cdot \alpha(u^*) = (u \cdot \alpha(u^*)) \cdot (v \cdot \alpha(v^*))$ , since the middle term  $v \cdot \alpha(v^*)$  belongs to  $k$  and hence commutes with all elements in the Clifford algebra.  $\square$

*Remark 13.3.2.* For non-isotropic vectors  $v \in V$ ,  $\text{Nm}_{\text{spin}}(v) = -q(v)$ .

**Corollary 13.3.3.** 1. For  $u \in \text{Clif}(q)$  the induced map  $\widetilde{\text{Ad}}_u$  on  $V$  is an orthogonal transformation, and if  $u \in \text{Clif}^0(q)$ , it is a rotation.  
2.  $u \in \text{Clif}(q)$  can be written as a product  $u = v_1 \cdots v_r$  with non-isotropic  $v_j \in V$ ,  $j = 1, \dots, r$ . Consequently

$$\text{Nm}_{\text{spin}}(u) = u \cdot \alpha(u^*) = (-1)^r q(v_1) \cdots q(v_r) \in k^\times. \quad (13.11)$$

If  $u \in \text{Clif}^0(q)$ , then  $r$  can be taken even.

3.  $\widetilde{\text{Ad}}$  induces isomorphisms  $\text{Clif}(q)/k^\times \xrightarrow{\cong} \text{O}(q)$  and  $\text{Clif}^0(q)/k^\times \xrightarrow{\cong} \text{SO}(q)$ .

*Proof.* 1. We first prove that the  $k$ -linear automorphism  $\widetilde{\text{Ad}}_u|_V$  is an isometry on non-isotropic vectors. First we show that this map indeed preserves non-isotropic vectors  $v \in V$ . If  $u \in \text{Clif}(q)$ , then  $\widetilde{\text{Ad}}_u$ , being an automorphism of  $\mathbb{C}(q)$ , preserves invertible elements so that  $w = \widetilde{\text{Ad}}_u(v) \in V$  is invertible in the Clifford algebra. Hence  $q(w) = -w \cdot w \neq 0$  (see Remark 13.3.2). We use this in the following computation:

$$\begin{aligned} q(\widetilde{\text{Ad}}_u v) &= -\text{Nm}_{\text{spin}}(\widetilde{\text{Ad}}_u v) \\ &= -\text{Nm}_{\text{spin}}(\alpha(u) \cdot v \cdot u^{-1}) \\ &= -\text{Nm}_{\text{spin}}(\alpha(u)) \cdot \text{Nm}_{\text{spin}}(v) \cdot \text{Nm}_{\text{spin}}(u^{-1}) \\ &= -\text{Nm}_{\text{spin}}(u) \cdot -q(v) \cdot \text{Nm}_{\text{spin}}(u^{-1}) \\ &= q(v) \text{Nm}_{\text{spin}}(u) \text{Nm}_{\text{spin}}(u^{-1}) = q(v) \quad (\text{since } q(v) \in k). \end{aligned}$$

We also used that  $\text{Nm}_{\text{spin}}(\alpha(u)) = \text{Nm}_{\text{spin}}(u)$ . This is the case since  $\alpha(u) \cdot \alpha(\alpha(u)^*) = \alpha(u \cdot (\alpha(u)^*)) = \alpha \text{Nm}_{\text{spin}}(u) = \text{Nm}_{\text{spin}}(u)$ .

Since the inverse  $\widetilde{\text{Ad}}_{u^{-1}}|_V$  of the map  $\widetilde{\text{Ad}}_u|_V$  also preserves non-isotropic vectors, both must send isotropic vectors to isotropic vectors, completing the proof of 1.

2. By the Cartan–Dieudonné theorem all orthogonal transformations of  $V$  are products of reflections in non-isotropic vectors, say  $\widetilde{\text{Ad}}_u|_V = \sigma_{v_1} \circ \cdots \circ \sigma_{v_r}$ . On the other hand, for the restrictions to  $V$  we have  $\widetilde{\text{Ad}}_{v_j} = -\sigma_{v_j}$ , and so  $\widetilde{\text{Ad}}_u = (-1)^r \widetilde{\text{Ad}}_{v_1} \circ \cdots \circ \widetilde{\text{Ad}}_{v_r} = (-1)^r \widetilde{\text{Ad}}_{v_1 \cdots v_r}$ . Hence by Proposition 13.2.2,  $u$  and  $v_1 \cdots v_r$  differ by a multiplicative non-zero constant in  $k$  which we use to adjust  $v_1$ . So every orthogonal transformation comes from twisted conjugation with elements of the Clifford algebra and the rotations from conjugation with elements in the even Clifford algebra.

Assertion 3 follows directly from these considerations.  $\square$

We next define the (s)pin groups as the following kernels of  $Nm_{\text{spin}}$ :

**Definition 13.3.4.** The *(s)pin group* is the group

$$\begin{aligned} \text{Pin}(q) &= \ker(Nm_{\text{spin}} : \text{Clif}(q) \rightarrow k^\times), \text{ respectively,} \\ \text{Spin}(q) &= \ker(Nm_{\text{spin}} : \text{Clif}^0(q) \rightarrow k^\times). \end{aligned}$$

that is, the subgroup of those  $u \in \text{Clif}(q)$ , respectively  $u \in \text{Clif}^0(q)$ , for which  $u\alpha(u^*) = 1$ .

Since  $Nm_{\text{spin}}$  restricted to  $k^\times$  is given by squaring, the spinor norm does not descend directly to the orthogonal group  $O(q) = \text{Clif}(q)/k^\times$ . It does descend if we replace  $k^\times$  by  $D(k) = k^\times/(k^\times)^2$ . Explicitly, write  $\varphi \in O(q)$  as a product of reflections,  $\varphi = \sigma_{v_1} \circ \dots \circ \sigma_{v_r}$ . Then one defines

$$Nm_{\text{spin}}(\varphi) := Nm_{\text{spin}}(v_1 \cdots v_r) \in k^\times.$$

However, this does not depend just on  $\varphi$ , but also on the way  $\varphi$  is written as a product of reflections. By Corollary 13.3.3.3, another choice leads to a scalar multiple of  $v_1 \cdots v_r$  and so  $Nm_{\text{spin}}(\varphi)$  is well defined as an element of  $k^\times/(k^\times)^2$ , that is:

$$\varphi = \sigma_{v_1} \circ \dots \circ \sigma_{v_r} \in O(q) \implies Nm_{\text{spin}}(\varphi) = q(v_1) \cdots q(v_r) \in D(k). \tag{13.12}$$

As for the intersection of  $k^\times$  and the (s)pin group: Clearly, any  $u \in k^\times$  gives  $u \cdot 1 \in \text{Clif}^0(q)$  with spinor norm 1 if and only if  $u^2 = 1$ , which implies  $u = \pm 1$ . So we can summarize the above discussion as follows.

**Theorem 13.3.5.** *The (s)pin group maps in a 2-to-1 fashion onto a normal subgroup of the appropriate orthogonal group:*

$$\begin{aligned} O^+(q) &= \text{Im}(\widetilde{\text{Ad}}|_V : \text{Pin}(q) \rightarrow O(q)), \\ \text{SO}^+(q) &= \text{Im}(\widetilde{\text{Ad}}|_V : \text{Spin}(q) \rightarrow \text{SO}(q)), \end{aligned}$$

*the reduced orthogonal groups. These groups appear in commutative diagrams all of whose rows and columns are exact; for the spin group this diagram is as follows:*

$$\begin{array}{ccccccc} & & 1 & & 1 & & 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \{1, -1\} & \longrightarrow & \text{Spin}(q) & \xrightarrow{\text{Ad}|_V} & \text{SO}^+(q) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & k^\times & \longrightarrow & \text{Clif}^0(q) & \xrightarrow{\text{Ad}|_V} & \text{SO}(q) \longrightarrow 1 \\ & & \downarrow x & & \downarrow Nm_{\text{spin}} & & \downarrow Nm_{\text{spin}} \\ & & x^2 & & k^\times & & D(k) \\ 1 & \longrightarrow & (k^\times)^2 & \longrightarrow & k^\times & \longrightarrow & D(k) \longrightarrow 1 \end{array}$$

and so

$$\mathrm{SO}^+(\mathfrak{q}) = \{\sigma_{v_1} \circ \cdots \circ \sigma_{v_r} \in \mathrm{SO}(\mathfrak{q}) \mid \mathfrak{q}(v_1) \cdots \mathfrak{q}(v_r) \in (k^\times)^2\}.$$

For the pin group there is an analogous diagram involving the twisted adjoint,  $\mathrm{Clif}(\mathfrak{q})$ ,  $\mathrm{O}^+(\mathfrak{q})$  and  $\mathrm{O}(\mathfrak{q})$ .

The image of the spinor norm on the rotation group is a subgroup of  $\mathrm{D}(k)$  which might be a proper subgroup as shown in Remark 13.3.6.1 below. We introduce a shorthand notation for this group:

$$\mathrm{S}_V = \mathrm{Im}(\mathrm{Nm}_{\mathrm{spin}} : \mathrm{SO}(\mathfrak{q}) \rightarrow \mathrm{D}(k)). \quad (13.13)$$

*Remark 13.3.6. 1.* For  $k = \mathbb{R}$  the group  $\mathrm{D}(k)$  is the cyclic group  $\mathrm{C}_2$  represented by the real numbers  $\{1, -1\}$ . Often we use these representatives instead of their classes. Note that if  $\mathfrak{q}$  is positive definite, the spinor norm is always 1 and so  $\mathrm{Nm}_{\mathrm{spin}}$  is not surjective in this case. In particular,  $\mathrm{SO}^+(\mathfrak{q}) = \mathrm{SO}(\mathfrak{q})$  and  $\mathrm{O}^+(\mathfrak{q}) = \mathrm{O}(\mathfrak{q})$ .

*2.* Suppose  $k$  is a topological field. Then the orthogonal groups  $\mathrm{O}(\mathfrak{q})$  and  $\mathrm{SO}(\mathfrak{q})$  are in a natural way topological groups. The preceding constructions give the Clifford group  $\mathrm{Clif}(\mathfrak{q})$  and the spin group  $\mathrm{Spin}(\mathfrak{q})$  the structure of a topological group. The adjoint representation as well as the spinor norm are continuous. So all the maps in the preceding diagram are continuous. This holds for instance for the fields  $\mathbb{R}, \mathbb{C}$  with the usual topology, or for  $\mathbb{Q}_p$  endowed with the  $p$ -adic topology.

The topological structure of the groups over  $\mathbb{R}$  is classical (see e.g. [96, Ch. IX.4], [137, Theorem 2.10]). If  $\mathfrak{q}$  has signature  $(r, s)$  one writes  $\mathrm{O}(r, s)$ ,  $\mathrm{SO}(r, s)$ ,  $\mathrm{Spin}(r, s)$  instead of  $\mathrm{O}(\mathfrak{q})$ , etc. If  $s = 0$ , one writes of course  $\mathrm{O}(n)$  and  $\mathrm{SO}(n)$ . We shall occasionally use this:

**Proposition 13.3.7** (Topological structure of orthogonal groups). *1.*  $\mathrm{SO}(n)$ ,  $n \geq 2$ . is connected, but not simply connected:

- $\mathrm{SO}(2)$  is the circle group and thus  $\pi_1(\mathrm{SO}(2)) = \mathbb{Z}$ ;
- for  $n \geq 3$ , one has  $\pi_1(\mathrm{SO}(n)) = \mathbb{Z}/2\mathbb{Z}$  and the universal cover of  $\mathrm{SO}(n)$  is the group  $\mathrm{Spin}(n)$ .

*2.* The groups  $\mathrm{SO}(r, s)$  have two connected components in case  $r, s \geq 1$ . The component of the identity is  $\mathrm{SO}^+(r, s)$ .

- $\mathrm{SO}(1, s)$ ,  $s \geq 1$  has fundamental group  $\mathbb{Z}/2\mathbb{Z}$  and the universal cover is  $\mathrm{Spin}(r, s)$ ;
- $\mathrm{SO}(r, s)$ ,  $r, s \geq 2$  has fundamental group  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  and the universal cover is an unramified double cover of  $\mathrm{Spin}(r, s)$ .

## 13.4 The Spin Group: Lattice Aspects

In this section  $R$  is an integral domain and  $Q(R)$  its field of fractions of characteristic different from 2.

As before, we let  $(V, q)$  be a quadratic  $Q(R)$ -space. In this section we investigate how the spinor norm construction relates to  $R$ -lattices  $L \subset V$ , i.e.  $R$ -modules for which  $V = L \otimes_R Q(R)$ . We assume that  $q|_L$  and hence  $b|_L$  are  $R$ -valued. If 2 is a unit in  $R$  then of course  $b$  is  $R$ -valued if and only if  $q$  is  $R$ -valued, but it need not be true otherwise. In particular, assuming  $b(L \times L) \subset R$  allows to treat odd lattices as well as even lattices.

To start, observe that the isometries of  $L$  are precisely the isometries of  $V$  preserving  $L$ :

$$\mathbf{O}(L, b) = \{g \in \mathbf{O}(V, q) \mid g(L) = L\}.$$

So we may restrict the spinor norm map to the subgroup  $\mathbf{O}(L, b)$  of  $\mathbf{O}(V, q)$ :

$$\mathrm{Nm}_{\mathrm{spin}} : \mathbf{O}(L, b) \longrightarrow \mathbf{D}(Q(R)) = Q(R)^\times / (Q(R)^\times)^2.$$

Analogous to Definition 13.3.4 we set

$$\begin{aligned} \mathbf{O}^+(L) &= \ker(\mathrm{Nm}_{\mathrm{spin}} : \mathbf{O}(L, b) \rightarrow \mathbf{D}(Q(R))) \\ \mathbf{SO}^+(L) &= \ker(\mathrm{Nm}_{\mathrm{spin}} : \mathbf{SO}(L) \rightarrow \mathbf{D}(Q(R))). \end{aligned} \tag{13.14}$$

Only the image

$$\mathbf{S}_L = \mathrm{Im}(\mathrm{Nm}_{\mathrm{spin}} : \mathbf{SO}(L) \rightarrow \mathbf{D}(Q(R))) \tag{13.15}$$

is going to play a role in Chapter 14. There is a subtle point here: the spinor norm for an isometry  $\sigma$  of a quadratic  $R$ -module is calculated using a decomposition of  $\sigma$  as a product of reflections within the vector space  $L \otimes Q(R)$  and so the spinor norm does not necessarily take values in  $\mathbf{D}(R)$ . For the analysis of indefinite lattices in Section 14.2 we make use of lattices for which  $\mathbf{S}_L$  contains the image of  $R^\times$  in  $\mathbf{D}(Q(R))$ . This is for instance the case if reflections exist, say  $\sigma_x$ ,  $x \in L$ , with  $q(x)$  any given unit in  $R$  as demonstrated in the next example.

**Example 13.4.1** (*p*-adic lattices). Let  $R = \mathbb{Z}_p$  in which case  $L$  is a *p*-adic lattice. We consider various examples where  $\mathbf{S}_L$  contains all *p*-adic units.

1. A homogeneous rank 2 sublattice  $M$  splits off from  $L$ , say  $M = M_0(k)$  with  $M_0$  unimodular and, if  $p = 2$ , even. In Corollary 10.1.4 we have seen that  $\mathbf{O}(M_0)$  contains reflections  $\sigma_{x_u}$  with  $q(x_u) = u$  any given unit. Since  $\mathbf{O}(M_0) = \mathbf{O}(M) \subset \mathbf{O}(L)$ , this implies that the spinor norm takes on all *p*-adic units. Hence the image of the spinor norm then contains  $\mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2$ . This is clear for the orthogonal group while for the special orthogonal group we take products of the form  $\sigma_{x_1} \circ \sigma_{x_u}$ .

2. In case  $p = 2$  and a homogeneous rank 3 lattice of exponent  $k$  splits off, by Proposition 10.2.2 either  $U_k, V_k$  splits off or the lattice is diagonal. It suffices to consider this last case separately. As before, we may assume that  $k = 0$ . By Lemma 11.2.1, the lattice is isometric to either a lattice splitting off  $U$ , or a lattice splitting off  $V$ , which brings us to the previous situation.

A vector space isometry  $f : V \rightarrow V$  sending  $L$  to the  $R$ -lattice  $L'$  induces a canonical rotation preserving isomorphism between  $\mathbf{O}(L)$  and  $\mathbf{O}(L')$ . It is given by sending  $\gamma \in \mathbf{O}(L)$  to  $\gamma' = f \circ \gamma \circ f^{-1} \in \mathbf{O}(L')$ . Since the spinor norm takes values in an abelian group,  $\gamma$  and  $\gamma'$  have the same spinor norm. Hence:

**Lemma 13.4.2.**  $S_L$ , the image of  $\text{Nm}_{\text{spin}} : \text{SO}(L) \rightarrow \text{D}(Q(R))$ , is an isometry invariant.

*Remark 13.4.3.* Since for integral lattices the spinor norm takes values in  $\text{D}(\mathbb{Q}) = \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ , this spinor norm is a more refined invariant than the real spinor norm which, as we have explained above, only takes values 1 or  $-1$ .

To extend the definition of the (s)pin group itself to the setting of lattices, we define

$$\begin{aligned} \mathbb{C}(L) &:= \text{subring of } \mathbb{C}(q) \text{ generated by } 1 \text{ and the elements } x \in L, \\ \mathbb{C}^0(L) &= \mathbb{C}(L) \cap \mathbb{C}^0(q), \\ \text{Pin}(L) &= \mathbb{C}(L) \cap \text{Pin}(q), \\ \text{Spin}(L) &= \mathbb{C}(L) \cap \text{Spin}(q). \end{aligned}$$

A word of warning here: the map  $\text{Ad}|_L : \text{Spin}(L) \rightarrow \text{SO}^+(L)$  is not necessarily surjective any more (and likewise for the image of the twisted adjoint map on  $\text{Pin}(L)$ ). See [36, Ch 10.4].

**Historical and Bibliographical Notes.** The importance of a group like the spin group seems to have been observed already by W. Hamilton (1805–1865) when he invented the quaternions in [90]. In connection to this, we mention that W. Clifford (1845–1879) in [39] relates the quaternion algebra to the group of space rotations. Here the article [141] by R. Lipschitz (1832–1903) should also be mentioned. See the amusing letter [248, Appendix II], purportedly written by him from Hades.

There are many books and papers that give expositions of the Clifford algebra. Ours follows mainly [137, Ch. 1] and [104, Ch. 11.4]. The relation with the Arf invariant is explained in J. Dieudonné's paper [48]. For the interplay with lattices we have followed §10.4 in J.W. Cassels's book [36].

## Spinor Equivalence

In this chapter  $L, L', L'', M$  are free  $\mathbb{Z}$ -modules of full rank within a quadratic inner-product space  $(V, q)$  over  $\mathbb{Q}$ . In particular,  $V = L_{\mathbb{Q}} = L'_{\mathbb{Q}} = L''_{\mathbb{Q}} = M_{\mathbb{Q}}$ . We write  $b, b', \dots$ , for the polar forms of  $q, q', \dots$ . Moreover the forms  $b, b', \dots$ , induced on  $L, L', \dots$  are assumed to be integer-valued. The localizations of  $V$  are  $(V_p, q_p)$  containing the local lattices  $L_p, L', L'_p, \dots$ .

### Introduction

The main goal of this chapter is to arrive at criteria guaranteeing that a non-degenerate indefinite lattice has class number one, that is, its genus has only one isometry class. With Nikulin's criterion of Section 11.3 in mind, we aim for criteria in terms of the genus invariant, that is, the signature and the discriminant form of the lattice.

As explained in Section 14.1, the appropriate way to compare integral lattices in a given genus is to consider these as a full rank lattice of a fixed (quadratic) inner product space over the rational numbers, say  $V$ . Observe that this fixes the signature so that the place at infinity does not play a role. Isometric lattices  $L, L'$  have isometric localizations  $L_v \simeq L'_v$  and so by definition belong to the same genus and belong to the localization  $V_v$  of  $V$ .

The notion of spinor equivalence, introduced in Section 14.2, is a subtle equivalence that uses the spinor norm, and which is intermediate between equivalence(=isometry) and genus equivalence. Two lattices of the same genus need not be spinor equivalent but there is a "computable" group that measures the difference. It follows for instance that the latter group is trivial if the primes in the prime power decomposition of the discriminant of the quadratic form appear with a sufficiently small exponent (see Corollary 14.2.6).

For *indefinite* lattices we can say much more: contrary to the definite case, here spinor equivalence coincides with equivalence. This is a consequence of the strong approximation theorem for the spin group. We explain the statement of this theorem in Section 14.3. The proof of this result is strongly number theoretic in spirit and falls outside the scope of this treatise. We refer to [36, Ch. 10.7] for an elementary demonstration. Combining this fact with the results of Section 14.2, one obtains useful criteria guaranteeing that an indefinite lattice has class number 1. This is the subject of Section 14.4. The same techniques are applied in Section 14.5 and yield criteria for the surjectivity of the reduction homomorphism



$r_L : \mathcal{O}(L, q) \rightarrow \mathcal{O}(q_L^\#)$  for quadratic lattices.

The chapter ends with a section on applications to  $p$ -elementary lattices.

## 14.1 The Genus Revisited

An integral lattice  $L$  with  $L_{\mathbb{Q}} = V$  underlies a free  $\mathbb{Z}$ -submodule of  $V$  of maximal rank. We first consider these.

**Proposition 14.1.1.** *Let  $L, M \subset V$  be free  $\mathbb{Z}$ -submodules of  $V$  of maximal rank. Then*

1.  $M = \gamma(L)$  for some vector space isomorphism  $\gamma : V \rightarrow V$ .
2.  $L_p = M_p$  for almost all primes  $p$ .
3.  $L_p = M_p$  for all primes  $p$  if and only if  $L = M$ .

*Proof.* If  $\{e_1, \dots, e_n\}$  is a basis for  $L$  and  $\{e'_1, \dots, e'_n\}$  a basis for  $M$ , then the linear map determined by sending  $e_i$  to  $e'_i$ ,  $i = 1, \dots, n$ , is as required in 1. Next, write

$$e'_i = \sum A_{ij} e_j, \quad A = (A_{ij}) \in \mathrm{GL}_n(\mathbb{Q}). \quad (14.1)$$

Let  $S$  be the finite set of primes dividing the denominators of the entries of  $A$  and  $A^{-1}$ . Hence, for the primes  $p \notin S$  the matrix  $A$  belongs to  $\mathrm{GL}_n(\mathbb{Z}_p)$ , and for those primes  $\{e'_1, \dots, e'_n\}$  is just another basis for  $L_p$ , that is  $L_p = M_p$ . This proves 2.

To show 3, observe that if  $L_p = M_p$ , localizing (14.1) in  $p$  shows that the assumption implies that every  $A_{ij}$  is a  $p$ -adic integer for all primes  $p$  and so is an integer. Hence  $L = M$ .  $\square$

We also have a criterion for glueing local lattices which we state without proof:

**Theorem 14.1.2** (Glueing local lattices, [36, Ch.11, Thm. 1.1]). *Let  $V$  be a finite dimensional vector space over  $\mathbb{Q}$  and let  $L$  be a free  $\mathbb{Z}$ -submodule of  $V$  of maximal rank. For every prime  $p$ , let  $M^{(p)}$  be a  $p$ -adic free  $\mathbb{Z}_p$ -module of maximal rank in the localization  $V_p$  of  $V$ . Then there exists a free  $\mathbb{Z}$ -submodule  $M$  of  $V$  of maximal rank whose localizations are  $M^{(p)}$  if and only if*

$$M^{(p)} = L_p \quad \text{for almost all primes } p.$$

*If  $M$  exists, it is uniquely determined by the condition  $M^{(p)} = M_p$  for all primes  $p$ .*

For the purpose of this chapter it is useful to be able to view lattices of the same genus as sublattices of a fixed quadratic space over  $\mathbb{Q}$ . This is possible since we have seen in Chapter 3 that quadratic spaces over  $\mathbb{Q}$  are isometric if and only if their localizations are isometric. Let us explain this in more detail. Recall from Section 1.9 that two integral lattices  $L', L''$  (so not necessarily in the same vector

space) whose localizations at all places are isometric, by definition belong to the same genus. Hence, as we just recalled,  $L'_0$  and  $L''_0$  are isometric and so can indeed be identified with some fixed quadratic  $\mathbb{Q}$ -vector space  $(V, q)$ .

If we follow the preceding convention, first of all, two sublattices  $L', L''$  of  $V$  are isometric precisely if there is a vector space isometry sending  $L'$  to  $L''$  in which case we call  $L'$  and  $L''$  **equivalent lattices**. Secondly,  $L'$  and  $L''$  belong to the same genus precisely if for all primes  $p$  local isometries  $g_p$  of  $V_p$  exist with  $g_p L'_p = L''_p$ .

It is natural to consider a more restricted form of equivalence between sublattices  $L', L''$  of  $V$ , namely equivalence under the rotation group  $\text{SO}(V, q)$  in which case we call the sublattices **properly equivalent**. The isometry group of the vector space  $V$  always contains isometries other than rotations, e.g., if  $\{e_1, \dots, e_n\}$  is an orthogonal basis, the linear map  $\tau$  sending  $e_1$  to  $-e_1$  and fixing all other basis elements is such an isometry. Then, by definition, the lattices  $L$  and  $L' = \tau(L)$  are equivalent, but they need not be properly equivalent as shown in Example 3 below.

**Examples 14.1.3. 1.** The above argument shows that any form equivalent to a diagonal form is also properly equivalent to it.

**2.** If  $\dim V$  is odd, the isometry  $-\text{id}$  has determinant  $-1$  and all lattices are preserved by it. So in this case there is no difference between proper equivalence classes and equivalence classes.

**3.** In Example 6.5.5.4 we showed that  $\pm \text{id}$  are the only isometries of the integral quadratic form  $q(x, y) = ax^2 + 2xy + cy^2$  on  $\mathbb{Z}^2$  with  $a, c \in \mathbb{Z}$  and  $a \geq 2$  and  $c > a$ . Hence  $\text{SO}(q) = \text{O}(q)$ . Now  $V = \mathbb{Q}e_1 \oplus \mathbb{Q}(e_1 - ae_2)$  and the reflection  $\tau$  in  $V$  with matrix  $\tau = \begin{pmatrix} -1 & -2a^{-1} \\ 0 & 1 \end{pmatrix}$  with respect to  $e_1, e_2$  is in  $\text{O}(V, q)$ , so maps  $\mathbb{Z}^2$  to the equivalent lattice  $\tau(\mathbb{Z}^2)$  with basis  $\{e_1, -(2/a)e_1 + e_2\}$ , and form (in corresponding coordinates)  $q' = au^2 - 2uv + cv^2$ . It is, however, not properly equivalent to  $q$ .

This last example leads to the following observation.

**Lemma 14.1.4.** *Let  $L$  be a sublattice of  $V$  of maximal rank. If every automorphism of  $L$  is a rotation, the equivalence class of  $L$  splits into two proper equivalence classes. If on the contrary  $L$  admits an isometry with determinant  $-1$ , then every lattice equivalent to  $L$  is also properly equivalent to it.*

*In particular, if the genus of  $L$  consists of one equivalence class, then  $\text{SO}(L)$  is of index 2 in  $\text{O}(L)$ .*

The same argument shows that for  $p$ -adic lattices  $L_p$  there is no difference between equivalence and proper equivalence since by (7.1) there exists a reflection preserving  $L_p$ . Let us tie this in with genus equivalence:

$$\mathfrak{g}(L') = \mathfrak{g}(L'') \iff \forall v \in \mathcal{P} \exists g_v \in \text{SO}(V_v, q_v) \text{ such that } L''_v = g_v L'_v. \quad (14.2)$$

Modulo these observations, Theorem 14.1.2 implies:

**Corollary 14.1.5.** *Let  $L'$  be a lattice in  $V$  of maximal rank.*

1. For every prime  $p$  let  $g'_p \in \text{SO}(V_p, q_p)$ . If  $g'_p \in \text{SO}(L'_p)$  for almost all  $p$ , then there is a unique lattice  $L''$  in  $V$  for which

$$L''_p = g'_p L'_p \quad \text{for all } p.$$

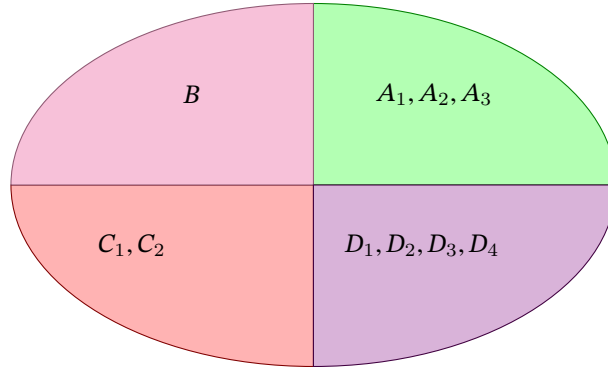
In particular  $L'$  and  $L''$  belong to the same genus.

2. Conversely, if  $L'$  and  $L''$  belong to the same genus, then for every prime  $p$  there exists  $g'_p \in \text{SO}(V_p, q_p)$  with  $L''_p = g'_p L'_p$ , and  $g'_p \in \text{SO}(L'_p)$  for almost all  $p$ .

## 14.2 The Spinor Genus

In this section we introduce the concept of spinor equivalence, intermediate between genus equivalence and lattice equivalence. We illustrate this in Figure 14.2.1, where one genus is depicted containing four spinor genera labeled  $A, B, C, D$ , and each contains one or more proper equivalence classes labeled  $A_1, \dots, B, C_1, \dots$ , etc.

Figure 14.2.1: Genus, spinor genus, proper equivalence



**Definition 14.2.1.** We say that two sublattices  $L', L''$  of  $(V, q)$  (maximal rank) are *spinor-equivalent* or belong to the same *spinor genus* if there exist  $\gamma' \in \text{SO}(V, q)$  and  $g_p \in \text{SO}^+(V_p, q_p)$  for all primes  $p$ , such that

$$L''_p = \gamma' \circ g_p(L'_p) \quad \text{for all primes } p.$$

Here  $\gamma'$  is interpreted as the induced localization at  $p$ .

This is indeed an equivalence relation, e.g., transitivity is shown as follows. If  $L, L'$  and  $L', L''$  are spinor equivalent, there exist  $\gamma, \gamma' \in \text{SO}(V, q)$  and  $g_p, g'_p \in$

$\mathrm{SO}^+(V_p, q_p)$  for all primes  $p$  such that  $L'_p = \gamma \circ g_p(L_p)$ ,  $L''_p = \gamma' \circ g'_p(L'_p)$ . Writing

$$\gamma' \circ g'_p \circ \gamma \circ g_p = \gamma' \circ \underbrace{\gamma \circ \gamma^{-1} \circ g'_p \circ \gamma \circ g_p}_{g''_p},$$

one observes that the spinor norm of  $g''_p$  is 1 since the spinor norm is a group homomorphism onto an abelian group, and  $g_p$  as well as  $g'_p$  have spinor norm 1.

This equivalence relation is indeed intermediate between proper equivalence and genus equivalence:

- Lemma 14.2.2.**    1. *Properly equivalent lattices are spinor equivalent;*  
 2. *Spinor equivalent lattices are in the same genus.*

*Proof.* 1. If  $\gamma L' = L''$  with  $\gamma \in \mathrm{SO}(V, q)$ , we take all  $g_p$  to be the identity maps.  
 2. Assume  $\gamma'$  and  $g_p$  are such that  $L''_p = \gamma' \circ g_p(L'_p)$  for all primes  $p$ . Then  $g_p$  sends the localization  $L'_p$  to the corresponding localization of  $\gamma'^{-1}L''$  and so, by (14.2), the lattices  $\gamma'^{-1}L''$  and  $L'$  are in the same genus. Since  $L''$  and  $\gamma'^{-1}L''$  are isometric, also  $L'$  and  $L''$  are in the same genus.  $\square$

In this section we focus on comparing genus equivalence and spinor equivalence. To do so we need to understand the image of the spinor norm on the level of vector spaces  $V, V_p$  over  $\mathbb{Q}, \mathbb{Q}_p$ , respectively, and integral lattices  $L$ , respectively  $p$ -adic lattices  $L_p$ . Accordingly, we extend the notation (13.15) as follows:

$$\begin{aligned} S_V &= \mathrm{Nm}_{\mathrm{spin}} \mathrm{SO}(V) \subset \mathrm{D}(\mathbb{Q}) & S_{V_p} &= \mathrm{Nm}_{\mathrm{spin}} \mathrm{SO}(V_p) \subset \mathrm{D}(\mathbb{Q}_p) \\ S_L &= \mathrm{Nm}_{\mathrm{spin}} \mathrm{SO}(L) \subset \mathrm{D}(\mathbb{Q}) & S_{L_p} &= \mathrm{Nm}_{\mathrm{spin}} \mathrm{SO}(L_p) \subset \mathrm{D}(\mathbb{Q}_p). \end{aligned}$$

Let us first consider the spinor norm image for  $\mathbb{Q}$ -vector space rotations:

**Lemma 14.2.3.** *Suppose that  $n = \dim V \geq 3$ . Then  $S_V$  contains  $\mathbb{Q}_{>0} \cdot (\mathbb{Q}^\times)^2$ . If  $q$  is indefinite, the spinor norm map is surjective:  $S_V = \mathrm{D}(\mathbb{Q})$ .*

*Proof.* Recall that (cf. (13.11)) to calculate  $\mathrm{Nm}_{\mathrm{spin}}(g)$  for  $g \in \mathrm{SO}(V, q)$ , we write  $g$  as an even product of reflections  $\sigma_x$ ,  $x \in V$ , and then  $\mathrm{Nm}_{\mathrm{spin}}(g)$  is the product of the  $q(x)$  up to squares. So, to show the assertions of the lemma, it suffices to consider products  $\sigma_x \circ \sigma_y$  of two reflections and solve equations of the form

$$q(x)q(y) = \begin{cases} a \in \mathbb{Q}, & a > 0 & \text{if } q \text{ is definite} \\ a \in \mathbb{Q}^\times & & \text{if } q \text{ is indefinite.} \end{cases} \quad (14.3)$$

The idea is to solve this locally and then use a suitable Hasse principle to deduce that global solutions exist. We first choose  $b, c \in \mathbb{Q}^\times$  so that  $a = bc$ . Choosing the sign of  $b$  (and hence of  $c$ ) appropriately we can solve these equations also at the place  $\infty$ .

To treat finite places in the case  $\dim V \geq 4$  is easy. Since by Theorem 3.2.5 the localized form on  $V_p$  represents all values, the equations  $q(x) = b$  and  $q(y) = c$

are locally soluble in  $V_p$  at all primes  $p$ . By the corollary to the Hasse–Minkowski theorem 3.3.3, solutions then exist globally.

For  $\dim V = 3$  this is slightly more involved. In this case Remark 3.2.6 states the set  $q(V_p) \cdot (\mathbb{Q}_p^\times)^2$  in  $D(\mathbb{Q}_p)$  misses at most one single element  $e_p \cdot (\mathbb{Q}_p^\times)^2$ ,  $e_p = -\text{disc}(q_p)$ . This happens for at most a finite set  $P$  of primes. We aim to write  $a = bc$  such that for all  $p \in P$  both  $b$  and  $c$  are such that their cosets in  $D(\mathbb{Q}_p)$  are different from  $e_p \cdot (\mathbb{Q}_p^\times)^2$ . This is indeed possible since by Theorem A.2.1 the group  $D(\mathbb{Q}_p)$  is either isomorphic to the product of two or three cyclic groups of order 2. Hence we have enough elements left in  $D(\mathbb{Q}_p)$  to write, for  $p \in P$ ,  $a = b_p \cdot c_p$  with the cosets of  $b_p$  and  $c_p = a/b_p$  different from that of  $e_p$ . Now apply Corollary A.3.2 to find  $b \in \mathbb{Q}^\times$  such that its localizations at the primes  $p \in P$  are equal to  $b_p$ . Then we can solve  $q(x_p) = b_p$  and  $q(y_p) = a/b_p$  in  $V_p$ . For a prime not in  $P$  there is no such subtlety. The rest of the argument proceeds as before.  $\square$

Next, consider the images  $S_L$  for lattices  $L \subset V$  and  $S_{L_p}$  for the local lattices  $L_p \subset V_p$ . By Lemma 13.4.2, if  $L$  and  $L'$  are equivalent lattices, then  $S_L = S_{L'}$ , and if  $L$  and  $L'$  are genus-equivalent, then  $S_{L_p} = S_{L'_p}$  for all primes  $p$ . So, to gather information on the number of spinor genera in the genus of  $L$  it makes sense to consider the subgroups  $S_{L_p}$  for all primes  $p$ . These are small abelian subgroups of  $D(\mathbb{Q}_p)$ . E.g. for  $p$  odd,  $D(\mathbb{Q}_p)$  is isomorphic to the Klein group and consists of the cosets of  $1$ ,  $p$ ,  $\epsilon$  and  $\epsilon \cdot p$ , where  $\epsilon$  is a non-square mod  $p$  and so  $S_{L_p}$  is either the full group, the trivial group or one of the three cyclic groups of order 2 generated by the cosets of  $\epsilon$ ,  $p$  or  $\epsilon \cdot p$ . These small groups form the basic source of information about the number of spinor genera in the genus of  $L$ . We shall ultimately prove (see Theorem 14.4.2) that the class number of the genus of  $L$  is one if for all primes  $p$  the group  $S_{L_p}$  contains the subgroup of  $D(\mathbb{Q}_p)$  generated by units.

First some examples where such groups are calculated. We use Example 13.4.1 for information about a typical binary lattice which leads to:

**Examples 14.2.4. 1.** If  $L$  is a binary  $p$ -adic unimodular quadratic lattice, then  $S_L$  contains the classes of all  $p$ -adic units. This is a direct consequence of Corollary 10.1.4. If  $p$  is odd this holds for any  $p$ -adic lattice of rank  $\geq 2$  since such lattices are diagonalizable by Proposition 10.2.2. Moreover, in this case, by the Cartan–Dieudonné theorem in the shape of Corollary 7.2.5, this is the full image, that is,  $S_L = \mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2$ .

**2.** Consider the integral lattice  $L = A_2$  with quadratic form  $x^2 + xy + y^2$ . This lattice is positive definite and has discriminant 3. For primes  $p \neq 3$  the lattice  $L_p$  is unimodular and then, by the argument of example 1,  $S_{L_p} = \mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2$ .

For the prime 3 the situation is different since the lattice  $L_3$  is not unimodular. The basis  $e_1 = (1, 0)$ ,  $e_2 = (-1, 2)$  exhibits  $L_3 \simeq [1] \oplus [3]$  and the corresponding reflections  $\sigma_{e_1}$  and  $\sigma_{e_2}$  have spinor norm 1, respectively 3. Since  $q(xe_1 + ye_2) = x^2 + 3y^2$  cannot be of the form  $-z^2$  in  $\mathbb{Q}_3$  (a square is 1 modulo 3), the group  $S_{L_3}$  is the cyclic group of order 2 generated by the class of  $1 \cdot 3$  and so again is strictly smaller than  $D(\mathbb{Q}_3)$ .

The next result demonstrates how to use information about the images of the local spinor norms to deduce that the genus of  $L$  contains only one spinor genus:

**Theorem 14.2.5** (Spinor equivalence = genus equivalence). *Let  $(V, q)$  be a quadratic inner product space of dimension  $\geq 3$  over  $\mathbb{Q}$  and let  $L \subset V$  be a maximal rank sublattice with  $b_q(L, L) \subset \mathbb{Z}$ . If for all primes  $p$  the coset in  $D(\mathbb{Q}_p)$  of every  $p$ -adic unit is the spinor norm of some rotation of  $L_p$ , all lattices in the genus of  $L$  are spinor equivalent. In other words, every lattice in the same genus as  $L$  is spinor equivalent to it if*

$$S_{L_p} = \text{Nm}_{\text{spin}}(\text{SO}(L_p)) \supset \mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2 \text{ within } D(\mathbb{Q}_p) \text{ (for all primes } p). \quad (14.4)$$

For a **given prime**  $p$  the inclusion (14.4) holds if a collection of  $p$ -adic units  $u_j$ , and vectors  $x_j \in L_p$ ,  $j \in J$ , exists such that

- (a)  $q(x_j) = u_j p^k$  for all  $j \in J$ , and some fixed  $k$ , and all reflections  $\sigma_{x_j}$  preserve the lattice  $L_p$ ;
- (b) the set of pairwise products  $u_{j_1} u_{j_2}$  generate  $\mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2$ .

This occurs for instance in the following cases:

1. **In case  $p \neq 2$ :** at least one homogeneous summand of exponent  $k$  and rank  $\geq 2$  splits off from  $L_p$ . This holds if for example  $\ell(\text{dg}_{L_p}) \leq \text{rank}(L) - 2$ .

2. **In case  $p = 2$ :**

(a) If  $L$  (and hence  $L_2$ ) is an even lattice, at least one homogeneous summand of exponent  $k$  and rank  $\geq 2$  splits off from  $L_2$ , for example in case  $\ell(\text{dg}_{L_2}) \leq \text{rank}(L) - 2$ .

(b) If  $L$  (and hence  $L_2$ ) is an odd lattice and a summand of one of the following three types splits off from  $L_2$ :

- either one of the rank two lattices  $U_k, V_k$ ;
- any homogeneous summand of exponent  $k$  and rank  $\geq 3$ ;
- a rank 3 lattice of the form  $M = \langle u^{(1)} \cdot 2^k \rangle \oplus \langle u^{(2)} \cdot 2^k \rangle \oplus \langle u^{(3)} \cdot 2^{k+1} \rangle$  for some dyadic units  $u^{(i)}$ ,  $i = 1, 2, 3$ .

This is the case if for example  $\ell(\text{dg}_{L_2}) \leq \text{rank}(L) - 3$  or if  $u_k$  or  $v_k$ ,  $k \geq 1$ , splits off from  $q_L^\#$ .

*Proof.* We show first that the assumption (14.4) implies that a lattice  $L'$  in the genus of  $L$  is spinor equivalent to  $L$ . Being in the same genus implies (as noted below Lemma 14.1.4) that for all primes  $p$  there exists  $g_p \in \text{SO}(V_p)$  such that  $L'_p = g_p L_p$ , and so one may write

$$\text{Nm}_{\text{spin}}(g_p) = u_p p^{r_p} \cdot (\mathbb{Q}_p^\times)^2, \quad u_p \in \mathbb{Z}_p^\times, r_p \in \mathbb{Z}.$$

To prove spinor-equivalence, we adapt the  $g_p$ . By Proposition 14.1.1.2, for almost all primes  $p$  we have  $L'_p = L_p$  and so for those we may replace  $g_p$  by  $g'_p = \text{id}$  with  $r_p = 0$ . There remains a finite set  $S$  of primes and we put  $a = \prod_{p \in S} p^{r_p} \in \mathbb{Q}$ . Since  $a > 0$ , by Lemma 14.2.3 there is some  $\gamma \in \text{SO}(V, q)$  with  $\text{Nm}_{\text{spin}}(\gamma) = a$  up to squares and hence for  $p \in S$

$$\text{Nm}_{\text{spin}}(\gamma^{-1} \cdot g_p) = v_p \cdot (\mathbb{Q}_p^\times)^2, \quad v_p \in \mathbb{Z}_p^\times.$$

By assumption (14.4) for every  $p \in S$  there exists  $w_p \in \mathrm{SO}(L_p)$  with  $\mathrm{Nm}_{\mathrm{spin}}(w_p) = v_p^{-1} \cdot (\mathbb{Q}_p^\times)^2$  and hence, since  $L'_p = \gamma(\gamma^{-1} \circ g_p)L_p$ , we find

$$L'_p = \underbrace{\gamma \circ (\gamma^{-1} g_p) \circ}_{g'_p} w_p L_p, \text{ with } \mathrm{Nm}_{\mathrm{spin}}(g'_p) = 1 \cdot (\mathbb{Q}_p^\times)^2.$$

This precisely means that  $g'_p$  belongs to the kernel  $\mathrm{SO}^+(V_p)$  of the spinor norm map for all primes  $p$  and so, by definition,  $L'$  and  $L$  are spinor equivalent.

Now suppose that for a fixed prime  $p$  vectors  $x_j$  and units  $u_j$ ,  $j \in J$ , exist with the properties (a) and (b). To show that (14.4) holds, note that by (a)  $\mathrm{Nm}_{\mathrm{spin}}(\sigma_{x_{j_1}} \sigma_{x_{j_2}}) = u_{j_1} u_{j_2} p^{2k} \cdot (\mathbb{Q}_p^\times)^2 = u_{j_1} u_{j_2} \cdot (\mathbb{Q}_p^\times)^2$ , and thus by assumption (b), modulo  $(\mathbb{Q}_p^\times)^2$  units in  $\mathbb{Z}_p$  are spinor norms as asserted.

To deal with the further special cases, assume first  $p \neq 2$  or  $p = 2$  and  $L$  even. Example 13.4.1 implies that such vectors  $x_j$  exist if a homogeneous summand of exponent  $k$  and rank  $\geq 2$  splits off from  $L_p$ . Next, assuming  $L$  odd and  $p = 2$ , the first two cases of 2(b) are also direct consequences of Example 13.4.1. Finally, we check the claim for the lattice  $M$  occurring in the third case of 2(b). This lattice admits the 4 reflections  $\sigma_x$ , for  $x = e_1, e_1 + 2e_2, e_2, e_2 + e_3$ , where  $e_1, e_2, e_3$  generate the three summands of  $M$ . Since in  $D(\mathbb{Z}_2)$  one has

$$\begin{aligned} q(e_1 + 2e_2)q(e_1) &= \frac{q(e_1 + 2e_2)}{q(e_1)} = q(e_1)/q(e_1) + 4q(e_2)/q(e_1) = 1 + 4u^{(2)}/u^{(1)} \\ q(e_2 + e_3)q(e_2) &= \frac{q(e_2 + e_3)}{q(e_2)} = q(e_2)/q(e_2) + q(e_3)/q(e_2) = 1 + 2u^{(3)}/u^{(2)}, \end{aligned}$$

the generators  $\{5, 3\}$  of the group  $D(\mathbb{Z}_2)$  – and hence all dyadic units – belong to the image of the spinor norm.

To complete the proof, recall that  $L_p$  determines  $b_{L_p}^\#$  and so for odd primes  $p$  the condition  $\ell(\mathrm{dg}_{L_p}) \leq \mathrm{rank}(L) - 2$  implies that we are in situation 1. If  $L_2$  is even and if  $\ell(\mathrm{dg}_{L_2}) \leq \mathrm{rank}(L) - 2$ , then, by Proposition 11.2.6,  $U$  or  $V$  splits off and situation 2 occurs. This is also the case if  $u_k$  or  $v_k$ ,  $k \geq 1$ , splits off from  $q_L^\#$ . If  $L_2$  is odd, and  $\ell(\mathrm{dg}_{L_2}) \leq \mathrm{rank}(L) - 3$ , we are again in (another instance of) situation 2.  $\square$

**Corollary 14.2.6.** *Let  $(W, q)$  be a quadratic inner product space over  $\mathbb{Q}$  of dimension  $n \geq 3$  and let  $L, L'$  be maximal rank quadratic sublattices of  $W$  with the same discriminant  $d$ . Suppose that the factorization of  $d$  contains the prime 2 to the power  $< \lfloor \frac{1}{2}(n^2 + 1) \rfloor$  and any odd prime to the power  $< \frac{1}{2}(n(n-1))$ . Then  $L, L'$  are spinor equivalent if and only if they are in the same genus.*

*In the case of odd symmetric lattices, the estimate for the power of 2 dividing  $d$  can be replaced by  $< \lfloor \frac{1}{2}((n-1)^2 + 1) \rfloor$ .*

*Proof.* Consider first an odd prime  $p$ . Since  $L_p$  is diagonalizable (Proposition 10.2.2) it is isometric to  $\mathbb{Q}_{i=1}^n \langle u_i \cdot p^{r_i} \rangle$  and we may assume  $0 \leq r_1 \leq r_2 \leq \dots \leq r_n$ . If all the exponents are distinct we have  $\sum r_i \geq 0 + 1 + \dots + (n-1) = \frac{1}{2}n(n-1)$ . Hence

$$\sum r_i < \frac{1}{2}n(n-1) \tag{14.5}$$

implies that at least two of the exponents must coincide and  $L_p$  contains a rank 2 lattice of the form  $M(p^s)$ , which is the condition described in the statement of Theorem 14.2.5.1 for an odd prime  $p$ . On the other hand condition (14.5) is equivalent to  $\text{disc}(L)_p = \text{disc}(L_p) = \prod_i u_i \cdot p^{\sum r_i}$  being not divisible by  $p^{\frac{1}{2}n(n-1)}$ .

For the prime 2 we may assume that  $L_2$  is diagonalizable, since otherwise some  $U_k$  or  $V_k$  splits off and Theorem 14.2.5 directly gives the result. So we suppose that  $L_2 = \bigoplus_{i=1}^n \langle u_i \cdot 2^{r_i} \rangle$ . As we observed before, every  $r_i \geq 1$  and we may assume  $1 \leq r_1 \leq r_2 \leq \dots \leq r_n$ . If for all odd  $j$  one has  $r_j \geq j$  it follows that  $\sum r_j \geq 1 + 1 + 3 + 3 + \dots = \lfloor \frac{1}{2}n^2 + 1 \rfloor$  which is equivalent to  $\text{disc}(L_2) = \prod_i u_i \cdot 2^{\sum r_i}$  being divisible by  $2^k$  where  $k = \lfloor \frac{1}{2}(n^2 + 1) \rfloor$ . On the other hand, if this is not the case, at least one  $r_j$  with  $j$  odd must be  $< j$  and so there is a triplet  $\{r_{i-2}, r_{i-1}, r_i\}$ ,  $i \leq j$ , with  $r_i - r_{i-2} \leq 1$ , i.e., two of these numbers are equal and the third differs from it by at most 1. Then the last mentioned condition in case 2 of Theorem 14.2.5 applies.

If the lattice  $L$  is odd,  $L_2$  contains at least one summand of the form  $\langle u \rangle$ ,  $u \in \mathbb{Z}_2$ , which means that in the above argument the rank  $n$  can be replaced by  $n - 1$ .  $\square$

*Remark 14.2.7.* The theory of binary forms (lattices of rank 2) cannot be treated with the above approach. See [36, Chapter 14 and Section 13.3] for a method to classify the latter.

J. Cassels gives in [36, Section 11.3] a constructive way to calculate the number of spinor genera in a given genus as the order of a certain computable finite group  $G(L)$  of exponent 2. The latter is defined as follows. Fix a finite set  $P$  of prime numbers such that  $2 \in P$  and  $\text{Nm}_{\text{spin}}(\text{SO}(L_p)) = \mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2$  for all  $p \notin P$ . Such sets exist: Take for  $P$  the set of primes dividing  $\text{disc}(L)$  and add 2 if  $\text{disc}(L)$  happens to be odd. This follows from Example 14.2.4.1 since  $L_p$  is unimodular for all  $p \in P$  and  $p \neq 2$ . Making use of  $P$ , introduce the groups

$$S = \prod_{p \in P} S_{L_p}, \quad S_{L_p} = \text{Nm}_{\text{spin}}(\text{SO}(L_p)), \quad R = \prod_{p \in P} D(\mathbb{Q}_p)$$

$$T = \{(t, \dots, t) \in R \mid t \in D(\mathbb{Q}) \text{ such that } \left. \begin{array}{l} t \in D(\mathbb{Z}_p) \text{ simultaneously for all } p \notin P \\ t > 0 \text{ in case } q \text{ is definite} \end{array} \right\}.$$

Here we make use of the map  $D(\mathbb{Q}) \rightarrow D(\mathbb{Q}_p)$  induced by the embedding  $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$  (which preserves units and squares). Finally set  $G(L) = R/ST$ . The result alluded to is as follows:

**Theorem 14.2.8** (Cassels, [36, §11.3]). *The (finite commutative) group  $G(L)$  does not depend on the choice of  $P$ . It has exponent 2. The set of spinor genera in the genus of  $(L, b)$  forms a principal space under  $G(L)$  and so its number is equal to the order of the group  $G(L)$  and hence a power of 2.*

The group  $G(L)$  can be understood as follows. We have seen that the groups  $D(\mathbb{Q}_p)$  for odd  $p$  are isomorphic to the Klein 4-group generated by  $p$  and a non-square unit  $\epsilon$ , and that  $D(\mathbb{Q}_2)$  is the product of three order 2 cyclic groups generated by  $-1, -3$  and  $2$ . The group  $T$  consists of diagonally embedded cyclic groups of



order two generated by the primes  $p \in P$  (and by  $-1$  if  $q$  is indefinite). Multiplication by  $p \in T$  takes care of the odd powers of the prime  $p \in P$  in the corresponding factor of  $R$ , but changes the units in the other factors and so might enlarge  $ST$  so that  $G(L)$  becomes smaller. But in any case, if for all  $p \in P$  the  $p$ -adic units are contained in  $S_{L_p}$ , the group  $G(L)$  is the trivial group, confirming Theorem 14.2.5 stating the uniqueness of the spinor genus in that case.

In general,  $G(L)$  is a product of at most as many cyclic groups of order 2 as there are odd primes  $p \in P$  for which  $S_{L_p}$  is either trivial or a cyclic group generated by  $p$ , and possibly at most two more cyclic groups of order two depending on the behaviour at the prime 2 (here the (in)definiteness of the form is also of influence). We give an example in the positive definite case from [36, Chap. 11, Examples] where many more examples can be found.

**Example 14.2.9.** We enlarge the lattice of Example 14.2.4.2 to a rank 3 even lattice as follows. The Gram matrix

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 18 \end{pmatrix}$$

defines a quadratic lattice isometric to  $M = L \oplus \langle 2 \cdot 3^2 \rangle$ ,  $L \simeq A_2$ , (with quadratic form  $q(x, y, z) = x^2 + xy + y^2 + 3^2 z^2$ ). It has discriminant  $2 \cdot 3^3$ . We can take  $P = \{2, 3\}$ . The local lattice  $M_3$  is isometric to  $\langle 2 \rangle \oplus \langle 2 \cdot 3 \rangle \oplus \langle 2 \cdot 3^2 \rangle$ . The corresponding reflections in  $e_1, e_2, e_3$  have spinor norms  $1, 3, 1$ . Note that  $q(x, y, z) = x^2 + 3y^2 + 3^2 z^2$  does not represent  $-1 \cdot (\mathbb{Q}^\times)^2$  since squares modulo 3 are 1. So  $S_{M_3}$  is the group generated by the class  $3 \cdot (\mathbb{Q}_3^\times)^2$ .

The local lattice  $M_2$  is isometric to  $L_2 \oplus \langle 2 \rangle$  and so, by Theorem 14.2.5,  $S_{M_2}$  contains all units. In fact, it is not larger: any reflection has to preserve the indecomposable summands and we have seen in Example 14.2.4.2 that reflections from  $L_2$  have spinor norm a unit, while the reflection  $e_3 \rightarrow -e_3$  has spinor norm 1. There is a subtle interaction between  $S$  and  $T$  in this example. Here  $R = D(\mathbb{Q}_2) \times D(\mathbb{Q}_3)$  contains 32 elements and the group  $ST$  contains 16 elements: the 8 elements  $(\pm 1, 1), (\pm 3, 1), (\pm 1, 3), (\pm 3, 3)$  and (via the diagonal action of  $\{(2, 2), (3, 3)\} \subset T$  by coordinate-wise multiplication) we obtain the supplementary set  $\{(\pm 2, -1), (\pm 6, -1), (\pm 2, -3), (\pm 6, -3)\}$  also consisting of 8 elements. Hence  $G(M) = R/ST$  is cyclic of order two and so there are two spinor genera. A representing quadratic form for the second spinor genus is given by  $q'(x, y, z) = z^2 + 3(x^2 + xy + y^2)$ . To show this, observe first of all that  $q'$  and  $q$  are in the same genus (they are positive definite and have the same localizations at 2 and 3). On the other hand  $q$  and  $q'$  are not isometric. This can be seen using the unique splitting of positive definite forms into indecomposable forms (Eichler's theorem 1.12.3). Indeed, the form  $x^2 + xy + y^2$  is indecomposable, since this is the case for its localization  $L_2$  (see Section 10.1) and so is  $3(x^2 + xy + y^2)$ . So the forms  $q$  and  $q'$  are already given as sums of indecomposable summands, and these are different.

### 14.3 Strong Approximation for the Spin Group

Let  $L \subset V$  be an integral lattice in a quadratic inner product space  $(V, q)$  over the rational numbers  $\mathbb{Q}$ . We recall that we have the reduced orthogonal groups

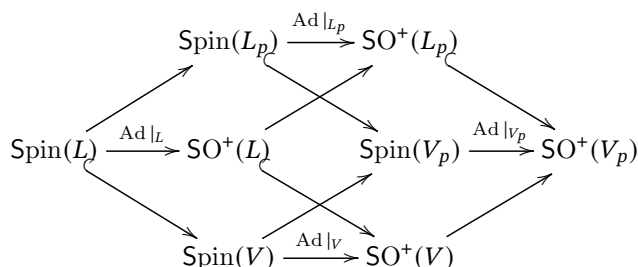
$$\mathrm{SO}^+(L) = \{\sigma_{u_1} \cdots \sigma_{u_{2r}} \in \mathrm{SO}(L_{\mathbb{Q}}) \cap \mathrm{O}(L) \mid q(u_1) \cdots q(u_{2r}) \in (\mathbb{Q}^\times)^2\},$$

where the  $\sigma_{u_j}$  are hyperplane reflections in hyperplanes orthogonal to non-isotropic vectors  $u_j \in L$ ,  $j = 1, \dots, 2r$ .

The inclusions  $\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p$  and  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{Q}_p$  induce inclusions

$$L \subset L_p \subset V_p, \quad L \subset V \subset V_p.$$

Using the  $p$ -adic topology described in Appendix A.3, these induce natural continuous homomorphisms fitting into commutative diagrams



Since we work both with lattices  $L, L_p, \dots$  and vector spaces  $V, V_p, \dots$ , we have written  $\mathrm{Spin}(V), \mathrm{Spin}(L)$  etc., instead of  $\mathrm{Spin}(q)$ . Under the slant arrows coming from extension of scalars we identify  $u \in \mathrm{Spin}(L)$  with  $u \otimes 1 \in \mathrm{Spin}(L_p)$ , etc., and  $g \in \mathrm{SO}^+(L)$  with  $g \otimes 1 \in \mathrm{SO}^+(L_p)$ , etc. In what follows we need to remember (see Appendix A.3) that in the  $p$ -adic topology the lattice  $L_p$  is an open subset of the vector space  $V_p$ . Also the group  $\mathrm{Spin}(L_p)$  is an open subgroup of the group  $\mathrm{Spin}(V_p)$ .

We can now state the strong approximation theorem. For a proof we refer to [36, Ch. 10.7]. It uses in an essential way another approximation theorem, stated as Theorem A.3.6 in Appendix A.3. For the latter result indefiniteness of the quadratic form is essential.

**Theorem 14.3.1** (Strong approximation for the spin group). *Let  $(V, q)$  be a quadratic inner product space over  $\mathbb{Q}$  of dimension  $\geq 3$  with  $q$  indefinite and let  $L \subset V$  be a maximal rank integral lattice in  $V$ . For all prime numbers  $p$  let  $U_p \subset \mathrm{Spin}(V_p, q_p)$  be a non-empty open subset such that*

$$U_p = \mathrm{Spin}(L_p) \text{ for almost all } p.$$

*Then there exists  $u \in \mathrm{Spin}(V, q)$  such that its localization  $u_p$  belongs to  $U_p$  for all primes  $p$ .*

By continuity of the maps in the above diagrams, we conclude:

**Corollary 14.3.2.** *Under the assumptions on  $(V, q)$  and  $L$  of Theorem 14.3.1, suppose that for all primes  $p$  we have a non-empty open subset  $W_p \subset \mathrm{SO}^+(V_p, q_p)$  with the property that*

$$W_p = \mathrm{SO}^+(L_p) \text{ for almost all } p.$$

*Then there is a  $\delta \in \mathrm{SO}^+(V, q)$  such that  $\delta$  belongs to  $W_p$  for all primes  $p$ .*

*Remark 14.3.3.* 1. There is no analog of Corollary 14.3.2 for the larger group  $\mathrm{SO}(V, q)$ . This is explained in [36] on page 187.

2. In subsequent sections we shall use the above corollary to show that spinor equivalence and equivalence coincide in the indefinite case.

## 14.4 Genus, Spinor Genus and Equivalence

Recall that we assume that sublattices  $L$  of a quadratic inner product space vector space  $(V, q)$  over  $\mathbb{Q}$  are integer valued in the strong sense that  $b_q(L, L) \subset \mathbb{Z}$ . For simplicity of notation, in the remainder of this section we will write  $b$  instead of  $b_q$ . Recall also that two sublattices  $L', L''$  of  $V$  are properly equivalent, respectively spinor-equivalent, if there exist  $\gamma, \gamma' \in \mathrm{SO}(V, q)$  and  $g'_p \in \mathrm{SO}^+(V_p, q_p)$  (for all primes  $p$ ) such that  $\gamma(L') = L''$ , respectively

$$L''_p = \gamma' \circ g'_p(L'_p) \quad \text{for all primes } p. \quad (14.6)$$

As announced, the strong approximation theorem implies that in the indefinite case in dimension  $\geq 3$  spinor equivalence and proper equivalence are the same:

**Theorem 14.4.1** (Spinor equivalence = proper equivalence). *Let  $(V, q)$  be an indefinite quadratic inner product space over  $\mathbb{Q}$  of dimension  $\geq 3$ . Then spinor equivalence for integer valued lattices in  $V$  is the same as proper equivalence.*

*Proof.* That proper equivalence implies spinor equivalence was already proved in Lemma 14.2.2. Now let  $L', L''$  be two lattices that are spinor-equivalent via  $\gamma' \in \mathrm{SO}(V)$  and  $g'_p \in \mathrm{SO}^+(V_p)$ , that is, (14.6) holds. To show that  $L'$  and  $L''$  are properly equivalent, we shall use the strong approximation theorem for the spin group to find some global vector space rotation inducing the local isometries  $\gamma' \circ g'_p$ . If we achieve this, by Proposition 14.1.1 the lattices  $L'$  and  $L''$  are properly equivalent. To carry this out, we choose the open sets in Corollary 14.3.2 to be

$$W_p = g'_p \mathrm{SO}^+(L'_p) \subset \mathrm{SO}^+(V_p).$$

As in the proof of Proposition 14.1.1.2, for all primes  $p$  except for those in a finite set we have  $g'_p \in \mathrm{SO}^+(L'_p)$ , and for these  $W_p = \mathrm{SO}^+(L'_p)$ . Hence, we can apply Corollary 14.3.2 to conclude that there exists a (vector space) rotation  $\delta \in \mathrm{SO}^+(V)$  with  $\delta \in g'_p \mathrm{SO}^+(L'_p)$  for all primes  $p$ , implying  $\delta(L'_p) = g'_p(L'_p)$  for all primes  $p$ . But then

$$(\gamma' \circ \delta(L'))_p = \gamma' \circ \delta(L'_p) = \gamma' \circ g'_p(L'_p) = L''_p \quad \text{for all } p.$$

So indeed, we found a vector space rotation  $\gamma' \circ \delta$  inducing  $\gamma' \circ g'_p$  for all primes  $p$ .  $\square$

We can now use Theorem 14.4.1 together with the result on the uniqueness of isometry classes in a spinor genus, cf. Theorem 14.2.5. Recall also (cf. Lemma 14.1.4) that if there is only one isometry class in a genus, equivalence coincides with proper equivalence which implies in turn that the isometry group of the lattice contains isometries that are not rotations. All of these considerations taken together prove the following important criterion:

**Theorem 14.4.2** (Criterion for class number 1). *Let  $(L, b)$  be an indefinite non-degenerate symmetric lattice of rank  $\geq 3$ . If*

$$\mathrm{Nm}_{\mathrm{spin}}(\mathrm{SO}(L_p)) \supset \mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2 \text{ for all primes } p,$$

then  $L$  has class number 1.

The above inclusion holds for a given prime  $p$  if a collection of  $p$ -adic units  $u_j$ , and vectors  $x_j \in L_p$ ,  $j \in J$ , exist such that

1.  $q(x_j) = u_j p^k$  for all  $j \in J$ , and some fixed  $k$ , and all reflections  $\sigma_{x_j}$  preserve the lattice  $L_p$ ;
2. the set of pairwise products  $u_{j_1} u_{j_2}$  generate  $D(\mathbb{Z}_p)$ .

This is in particular true in case we are in one of the situations 1 or 2 of Theorem 14.2.5.

In these cases a lattice isometric to  $L$  is also properly isometric to  $L$  and  $\mathrm{SO}(L)$  is of index two in  $\mathrm{O}(L)$ . In other words,  $L$  admits isometries that are not rotations.

This proves Theorem 1.13.2 from Section 1.13:

**Corollary 14.4.3.** *Let  $L$  be an even non-degenerate indefinite lattice of rank  $r \geq 3$ . Assume that the minimal number of generators of the discriminant group  $\mathrm{dg}_L = L^*/L$  is at most  $r-2$ . Then  $L$  has class number 1. In other words: if  $\ell(\mathrm{dg}_L) \leq r-2$ , then the isometry class of  $L$  is determined by  $r$ , the index  $\tau(L)$  and the discriminant form  $q_L^\#$ .*

*If  $L$  is odd, a similar statement is true provided  $\ell(\mathrm{dg}_L) \leq r-3$  and we replace  $q_L^\#$  with  $b_L^\#$ .*

The last assertion of the corollary follows from an application of Nikulin's characterization for the genus, Theorem 11.3.1 in the even case and Theorem 12.5.9 for the odd case.

Another practical test, stated in terms of discriminants only, follows from combining Theorem 14.4.1 with Corollary 14.2.6

**Corollary 14.4.4.** *Let  $L, L'$  be non-degenerate indefinite lattices of rank  $r \geq 3$  with the same discriminant. Suppose that  $\mathrm{disc}(L) \in \mathbb{Z}$  contains the prime 2 to the power  $< \lfloor \frac{1}{2}r^2 + 1 \rfloor$  if  $L$  is even, or, if  $L$  is odd, to the power  $< \lfloor \frac{1}{2}(r-1)^2 + 1 \rfloor$ , and any odd prime to the power  $< \frac{1}{2}r(r-1)$ . Then  $L$  and  $L'$  are isometric if and only if they are in the same genus.*

## 14.5 Lifting Isometries of the Discriminant Group

In this section  $(L, q)$  is a quadratic integral lattice and  $(L_p, q_p)$  denotes its localization at  $p$ .

Since we are working with even integral lattices, we shall focus on the reduction homomorphism  $r_L^q$  given in (6.9) which for simplicity will be denoted as  $r_L$ . In other words,

$$r_L : \mathcal{O}(L, q) \rightarrow \mathcal{O}(q_L^\#)$$

is the homomorphism that sends a lattice isometry to the induced isometry on the discriminant quadratic group. The central question in this section is: when is this map surjective? To arrive at a criterion, we first show lifting isometries can be done locally:

**Proposition 14.5.1.** *The local reduction maps  $r_{L_p}$  are surjective for every prime  $p$ , that is, every isometry of the discriminant quadratic form of  $L_p$  can be lifted to an isometry of  $L_p$ .*

*Proof.* We have seen in Section 10.2 that for  $p$  odd all (symmetric or quadratic) forms on  $L_p$  are diagonalizable, while for  $p = 2$  such forms split orthogonally into rank 1 pieces and rank 2 pieces of the form  $U_k$  and  $V_k$ .

For  $p$  odd, we can pick an orthogonal basis  $\{g_1, \dots, g_n\}$  of  $\text{dg}_{L_p}$ . By Proposition 10.3.2, writing  $L_p = L_0 \oplus L_1$  with  $L_0$  a maximal unimodular sublattice of  $L_p$ , there is an orthogonal basis  $\{e_1, \dots, e_n\}$ ,  $j = 1, \dots, n$ , of  $L_1$  such that

$$b_p(e_k, e_k) = u_k p^{j_k}, \quad b_{L_p}^\#(\bar{g}_k, \bar{g}_k) = u_k p^{-j_k}, \quad u_k \in \mathbb{Z}_p^\times, k = 1, \dots, n.$$

Let  $\bar{\sigma}$  be an isometry of  $b_{L_p}^\#$ . The orthogonal basis  $\{\bar{\sigma}(g_1), \dots, \bar{\sigma}(g_n)\}$  gives another diagonalisation of the discriminant form and, applying Proposition 10.3.2 again, there is a corresponding orthogonal basis  $\{e'_1, \dots, e'_n\}$ ,  $j = 1, \dots, n$ , of  $L_1$ . Since then  $b_p(e_k, e_k) = b_p(e'_k, e'_k)$ , the isomorphism  $\sigma$  of  $L_p$  defined by  $\sigma|_{L_0} = \text{id}$  and  $\sigma(e_k) = e'_k$ ,  $k = 1, \dots, n$ , is an isometry of  $L_p$  that obviously induces  $\bar{\sigma}$ .

If  $p = 2$ , essentially the same argument applies, except that for the rank two indecomposable summands  $U_k, V_k$  we choose a basis. If we define  $\sigma$  using this basis, we can no longer guarantee that  $\sigma$  induces  $\bar{\sigma}$ . However we can always adapt our choice since by Examples 6.5.5.2–3, any isometry of  $u_k$  or  $v_k$  can be lifted.  $\square$

For the global lifting problem isometries inducing the identity on the discriminant group play a decisive role. This motivates introducing the kernel of the reduction homomorphism (6.8) and of the reduction homomorphism restricted to the rotation group:

$$\begin{aligned} \mathcal{O}^\#(L, q) &= \ker \left( r_L : \mathcal{O}(L, q) \rightarrow \mathcal{O}(q_L^\#) \right), \\ \text{SO}^\#(L, q) &= \ker \left( r_L' : \text{SO}(L, q) \rightarrow \mathcal{O}(q_L^\#) \right). \end{aligned} \tag{14.7}$$

Similarly, we use the local versions  $O^\#(L_p, q_p)$  and  $SO^\#(L_p, q_p)$ , the kernels of the local reduction maps. We often drop the  $q$  or  $q_p$  in the notation. Standard examples of isometries inducing the identity on the discriminant group are the reflections in  $-2$ -roots (Cf. Lemma 7.1.1.3). Example 13.4.1 shows that the image of the spinor norm evaluated on these smaller (local) groups already contains all units:

**Lemma 14.5.2.** *Let  $L_p$  be a non-degenerate  $p$ -adic lattice,  $p \neq 2$ . Suppose that a homogeneous rank 2 sublattice splits off. Then the image of the spinor norm restricted to  $SO^\#(L_p)$  contains  $\mathbb{Z}_p^\times \cdot (\mathbb{Q}^\times)^2$ . The same holds if  $p = 2$  and  $L_2$  is even. If no homogeneous rank 2 lattice splits off, assume instead that a homogeneous rank 3 sublattice splits off.*

Later in this section this local result will be used in conjunction with the following result:

**Proposition 14.5.3.** *Let  $(L, q)$  be a non-degenerate indefinite quadratic integral lattice of rank  $\geq 3$ . Suppose that*

$$\text{Nm}_{\text{spin}}(SO^\#(L_p)) \supset \mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2 \quad \text{for all primes } p. \tag{14.8}$$

*Then the reduction map  $r'_L : SO(L, q) \rightarrow O(q_L^\#)$  is surjective. Moreover, the map  $r'_L$  is then already surjective on the subgroup of  $SO(L, q)$  consisting of rotations with real spinor norm 1.*

*Proof.* Let  $\bar{\sigma} \in O(q_L^\#)$  with  $p$ -primary component  $\bar{\sigma}_p$ . By Proposition 14.5.1 we can find  $\sigma_p \in SO(L_p)$  that induces  $\bar{\sigma}_p$ .

In order to apply the strong approximation theorem (cf. Section 14.3), we view the lattice  $L$  as a sublattice of the  $\mathbb{Q}$ -vector space  $V = L_{\mathbb{Q}}$  and  $L_p$  as a sublattice of the localization  $V_p$  of  $V$ . For almost all primes  $p$  the lattice  $L_p$  is unimodular and so we may assume  $\sigma_p = \text{id}$  for primes  $p$  outside some finite set  $S$ . If  $\text{Nm}_{\text{spin}}(\sigma_p) = u_p p^{\alpha_p} \cdot (\mathbb{Q}_p^\times)^2$ ,  $u_p \in \mathbb{Z}_p^\times$ , set  $a = \prod_{p \in S} p^{\alpha_p}$ . By Lemma 14.2.3, there is a rotation  $\gamma$  of  $V$  with  $\text{Nm}_{\text{spin}}(\gamma) = a$ . By Proposition 14.1.1, we may also enlarge  $S$  if needed so that  $\gamma_p$  preserves the lattice  $L_p$  for all primes  $p \notin S$ . In  $\mathbb{Q}_p$  one may write  $a = v_p p^{\alpha_p}$ ,  $v_p \in \mathbb{Z}_p^\times$ . By assumption there exists a rotation  $\tau_p \in SO^\#(L_p)$  with  $\text{Nm}_{\text{spin}}(\tau_p) = u_p^{-1} v_p$  and so, by construction,  $\text{Nm}_{\text{spin}}(\gamma^{-1} \circ \sigma_p \circ \tau_p) = 1$ . Define

$$W_p = \gamma^{-1} \circ \sigma_p \circ \tau_p \left( SO^+(L_p) \cap SO^\#(L_p) \right) \subset SO^+(V_p).$$

For  $p \notin S$  the lattice  $L_p$  is unimodular and so in particular  $SO^\#(L_p) = SO(L_p)$ . Since  $\gamma$  preserves  $L_p$  for those primes, it follows that  $W_p = SO^+(L_p)$  for almost all primes  $p$  and we can apply Corollary 14.3.2 in our situation. So there is a spinor norm 1 rotation  $\delta \in SO^+(V)$  whose localizations belong to  $W_p$ . This means that for all primes  $p$  one has  $\delta_p = \gamma^{-1} \circ \sigma_p \circ \tau_p \circ w_p$  for some  $w_p \in SO^+(L_p) \cap SO^\#(L_p)$ , or, equivalently,

$$(\gamma \circ \delta)_p = \sigma_p \circ \tau_p \circ w_p \quad \text{for all primes } p.$$

Since the right-hand side preserves  $L_p$ , Proposition 14.1.1 implies that the isometry  $\sigma := \gamma \circ \delta$  preserves the lattice  $L$ .

We claim that  $\sigma$  induces the isometry  $\bar{\sigma} \in \mathcal{O}(q_L^\#)$  we started out with. To show this, it suffices to prove this on every  $p$ -primary part of the discriminant group. By construction, the localization of  $\sigma$  at  $p$  equals  $\sigma_p \circ \tau_p \circ \omega_p$  and since  $\tau_p \circ \omega_p \in \mathcal{SO}^\#(L_p)$ , the subgroup of  $\mathcal{SO}(L_p)$  acting as the identity on  $\text{dg}_{L_p}$ , this shows the claim.

The last assertion follows since  $\gamma$  has  $\mathbb{Q}$ -spinor norm  $\mathbf{a} \cdot (\mathbb{Q}^\times)^2$ ,  $\mathbf{a} = \prod_{p \in S} p^{\alpha_p} > 0$ , and so has real spinor norm 1, while  $\delta$  already has rational spinor norm 1.  $\square$

*Remark 14.5.4.* Of course, the same conditions as stated in the previous proposition imply surjectivity of the reduction homomorphisms for the full orthogonal groups. A priori these conditions can be weakened but this leads to very technical considerations. See [156, Ch. VIII, 5] where the failure of surjectivity of the reduction map is captured in an explicit group.

Now notice the similarity of the containment (14.4) in Theorem 14.2.5 and the containment (14.8) in Proposition 14.5.3. Since Lemma 14.5.2 gives a condition ensuring that the two conditions are in fact the same, we arrive at the main result of this section:

**Theorem 14.5.5.** 1. *Let  $L$  be a non-degenerate indefinite quadratic lattice of rank  $\geq 3$ . Suppose that for all primes  $p$  a homogeneous rank 2 sublattice splits off from  $L_p$  which is the case if for instance  $\ell(\text{dg}_L) \leq \text{rank}(L) - 2$ . Then*

- $L$  has class number 1;
- the reduction homomorphism  $r'_L : \mathcal{SO}(L, \mathfrak{q}) \rightarrow \mathcal{O}(q_L^\#)$  is surjective, as well as its restriction to the subgroup  $\mathcal{SO}^+(L, \mathfrak{q})$  of  $\mathcal{SO}(L, \mathfrak{q})$  consisting of isometries having real spinor norm 1.

2. *For odd non-degenerate indefinite lattices a similar assertion holds provided one sharpens the condition for the prime  $p = 2$  to demand that a homogeneous rank 3 sublattice splits off from  $L_2$ . All conditions are satisfied in this case if e.g.  $\ell(\text{dg}_L) \leq \text{rank}(L) - 3$ .*

**Examples 14.5.6.** 1.  $L = \mathcal{O}^k U(2)$ ,  $k \geq 3$ , satisfies the conditions of the above theorem.

2. Sometimes the condition  $\ell(\text{dg}_L) \leq \text{rank}(L) - 2$  is not satisfied but can be remedied by adding a non-trivial even unimodular lattice.

## 14.6 Uniqueness of $p$ -Elementary Lattices

Recall (Section 1.7.B) that  $L$  is  $p$ -elementary if  $pL^* \subset L \subset L^*$ . The discriminant group of the  $p$ -elementary lattice  $L$  is a  $p$ -primary group, and so  $L$  is determined by the localization  $L_p = L \otimes \mathbb{Z}_p$ . We have seen in loc. cit. that  $W_L = L^*/L$  and  $V_L = L/pL^*$  are  $\mathbb{F}_p$ -inner product spaces. We start by observing:

**Lemma 14.6.1.** *Let  $(L, b)$  be a non-degenerate  $p$ -elementary lattice. Then*

1.  $\text{disc}(L) = \pm p^w$ ,  $w = \dim W_L$ . If  $b$  is an even form and  $p$  is odd,  $\text{rank}(L)$  is even;
2. There is a splitting  $L_p = L^{(0)} \oplus L^{(1)}(p)$ , where  $L^{(0)}$  and  $L^{(1)}$  are unimodular,  $\text{rank}(L^{(0)}) = \dim V_L$  and  $\text{rank}(L^{(1)}) = \dim W_L$ .

*Proof.* 1. Since  $W_L = \text{dg}_L$ , we have  $\text{disc}(L) = \pm |W_L| = \pm p^w$ . If  $b$  is even and  $p$  is odd,  $\text{disc}(L) = \pm p^w$  is odd and by Corollary 10.2.8 this implies that  $\text{rank}(L)$  is even.

2. Note that since  $pL_p^* \subset L_p$ , there is a canonical projection map  $L_p \rightarrow L_p/pL_p^* \simeq L/pL^* = V_L$ . We let  $L^{(0)}$  be a primitive sublattice of  $L_p$  spanned by vectors  $\{e_1, \dots, e_v\}$ ,  $v = \dim V_L$ , that map to a basis of  $V_L$  under the above projection. Since the pairing on  $V_L$  is non-degenerate, the matrix  $(e_i \cdot e_j \pmod p)$  has non-zero determinant. Hence, the determinant of the matrix  $(e_i \cdot e_j)$  is a unit in  $\mathbb{Z}_p$ , and so the product on  $L_p$  restricts to a unimodular pairing on  $L^{(0)}$ . Consequently,  $L^{(0)}$  splits off, say  $L_p = L^{(0)} \oplus L'$ . Now  $\text{rank}(L') = w$  and one has  $L' \subset pL_p^*$ . To see this, let  $x \in L'$  and  $\bar{x}$  its class in  $L_p/pL_p^* = V_L$ . If  $\bar{x} \neq \bar{0}$ , then there exists  $\bar{y} \in V_L$  such that  $\bar{x} \cdot \bar{y} \neq 0$ . Since we may lift  $\bar{y}$  to  $y \in L^{(0)}$  (which is orthogonal to  $L'$ ), this is impossible. So  $x \in pL_p^*$  and therefore  $L' \subset pL_p^*$ . If  $x, z \in L'$ , then  $x \in pL_p^*$  and  $z \in L_p$ , and so  $x \cdot z \in p\mathbb{Z}_p$ . In other words, making use of (1.15),  $L' = L^{(1)}(p)$  for some  $\mathbb{Z}_p$ -lattice  $L^{(1)}$ . Calculating discriminants we find  $\text{disc}(L') = \text{unit} \cdot p^w = \pm p^w \text{disc}(L^{(1)})$ , and so  $L^{(1)}$  is unimodular.  $\square$

From now on we assume that  $L$  is even of rank  $\geq 4$ . This assumption implies that at least one of the unimodular lattices  $L^{(0)}$  or  $L^{(1)}$  must have rank  $\geq 2$ . Then Theorem 14.2.5 implies that the genus of  $L$  contains one spinor equivalence class. If, moreover,  $L$  is indefinite, by Theorem 14.4.1 there is only one isometry class in the genus and then, using Nikulin's characterization of the genus, Theorem 11.3.1, we deduce:

**Corollary 14.6.2.** *Let  $L$  be an even indefinite  $p$ -elementary lattice of rank  $\geq 4$ . Then the class number of  $L$  is at most one. Up to isometry  $L$  is thus determined by its signature and its discriminant quadratic form.*

So, classification of even  $p$ -elementary lattices of rank  $\geq 4$  is now reduced to classifying the possible discriminant quadratic forms of even  $p$ -elementary lattices. The basic invariant here is  $\tau_8(q^\#)$ , the index mod 8 of a torsion quadratic form  $q^\#$ . By Proposition 9.4.1, for odd  $p$  the torsion quadratic form is isometric to

$p \pmod 8$	$u$ square	$u$ non-square
1	0	4
-1	$2w$	$2w + 4$
3	$-2w$	$-2w + 4$
-3	$4w$	$4w + 4$

Table 14.6.1: Values of  $\tau_8(q_{w,u}^\#)$



$q_{w,u}^\# = \langle u \cdot p^{-1} \rangle \oplus \langle p^{-1} \rangle^{\oplus w-1}$  and by Proposition 12.3.2 the values of its index mod 8 are determined by  $p \bmod 8$  and  $w$ . This yields Table 14.6.1.

For  $p = 2$ , recall the subdivision of 2-elementary lattices in type I and II (Section 1.7). The normal forms for  $q^\#$  are enumerated in Table 11.2.2. Type I lattices always split off length 1 torsion groups. The indices mod 8 of the building blocks are given by Proposition 12.3.3. Combining this, we arrive at Table 14.6.2.

$q^\#$	$w$	$u$	$u'$	$\tau_8$
$[u \cdot 2^{-2}] \oplus u_1^{\oplus \frac{1}{2}(w-1)}$	odd	1 3		1 -1
$[u \cdot 2^{-2}] \oplus u_1^{\oplus \frac{1}{2}(w-1)} \oplus v_1$	odd	1 3		-3 3
$[u \cdot 2^{-2}] \oplus [u' \cdot 2^{-2}] \oplus u_1^{\oplus \frac{1}{2}(w-2)}$	even	1 3 1	3 3 1	0 -2 2
$[u \cdot 2^{-2}] \oplus [u' \cdot 2^{-2}] \oplus u_1^{\oplus \frac{1}{2}(w-4)} \oplus v_1$	even	1 * *	3 1 3	4 -2 2

Table 14.6.2: Type I lattices

In this table the two last rows containing a "\*" give the same index mod 8 as the possibilities in rows 6 and 7. These can be eliminated by making use of relation (IV) (see Appendix C.3.A) which in terms of quadratic torsion forms reads:

$$u_1 \oplus [u \cdot 2^{-2}] \oplus [u' \cdot (2^{-2})] \simeq v_1 \oplus [(u - 2) \cdot 2^{-2}] \oplus [(u' + 2) \cdot 2^{-2}], \text{ if } u \equiv u' \pmod{4}.$$

Indeed, using this relation to replace the occurrence of  $v_1$  in the normal form by  $u_1$  in case there are also two copies of  $[2^{-2}]$  or two copies of  $[3 \cdot 2^{-2}]$  present. This procedure yields lattices isometric to those of rows 6 and 7 respectively. The above tables can be used to show:

**Proposition 14.6.3.** *Let  $(L, b)$  be an indefinite, even  $p$ -elementary lattice of rank  $\geq 4$  and  $\text{disc}(L) = \pm p^w$  (so that  $w = \ell(\text{dg}_L)$ , the length of  $\text{dg}_L$ ).*

1. *For  $p \neq 2$  the isometry class of  $L$  is uniquely determined by its signature and  $w$ .*
2. *For  $p = 2$  the class of  $L$  is determined by its type,  $w$  and the signature. Moreover, in case  $L$  is of type II,  $w$  must be even and two types occur according to whether the Arf invariant of  $q^\#$  equals 0 or 1. In the first case,  $q^\# \simeq \oplus^{\frac{1}{2}w} u_1$  with  $\tau_8 \equiv 0 \pmod{8}$ , and in the second case  $q^\# \simeq \oplus^{\frac{1}{2}(w-2)} u_1 \oplus v_1$  with  $\tau_8 \equiv 4 \pmod{8}$ .*

*Proof.* 1. By Proposition 9.4.1, for  $p \neq 2$  the discriminant quadratic form is isometric to either  $\mathbb{Q}^w\langle p^{-1} \rangle$  with reduced discriminant 1, or to  $\mathbb{Q}^{w-1}\langle p^{-1} \rangle \mathbb{Q}\langle \varepsilon \cdot p^{-1} \rangle$  with reduced discriminant  $\varepsilon$ . The first of the above tables shows that for all values of  $p \bmod 8$  and  $w$ , the invariant  $\tau_8$  determines which of the two forms appear. So the discriminant form is determined by  $\tau_8$  and  $w$ . Since in this situation the lattice is up to isometry uniquely determined by its discriminant quadratic form and its signature, the result follows for  $p$  odd.

2. For  $p = 2$  we argue as follows. From Table 11.2.2 we see that type II forms have discriminant quadratic forms  $\mathbb{Q}^w u_1$  or  $\mathbb{Q}^{w-2} u_1 \mathbb{Q} v_1$  with signature mod 8 equal to 0, respectively 4. This shows the assertion for type II forms.

Table 14.6.2 demonstrates that the values of  $\tau_8$  and  $w$  determine the equivalence class of the discriminant quadratic form completely, which shows the claim in this case as well.  $\square$

As to existence, we invoke Theorem 12.4.4 to obtain the following result.

**Theorem 14.6.4.** *Let there be given a pair of two positive integers  $(r_+, r_-)$ , a non-negative integer  $w$ , an element  $\tau_8 \in \mathbb{Z}/8\mathbb{Z}$ , and, in case  $p = 2$ , a “type”  $\in \{I, II\}$ . Then a (necessarily indefinite)  $p$ -elementary quadratic lattice  $L$  of rank  $r = r_+ + r_- \geq 4$  and signature  $(r_+, r_-)$  exists for which  $L_p = L^{(0)} \mathbb{Q} L^{(1)}(\mathfrak{p})$  with  $L^{(0)}$  and  $L^{(1)}$  unimodular,  $\dim L^{(1)}(\mathfrak{p}) = w$ , if and only if the following conditions hold simultaneously:*

1.  $w \leq r$ ,  $r_+ - r_- \equiv \tau_8 \pmod{8}$ ;
- 2a. in case  $p$  is odd, then
  - $r$  must be even,
  - $\tau_8$  has to match one of the two values for  $p$  as given in Table 14.6.1,
  - if  $w = r$  in addition we must have  $u = (-1)^{r_-}$
- 2b. in case  $p = 2$ , then
  - the lattice  $L$  is of type I or of type II,
  - $\tau_8 \equiv 0, 4 \pmod{8}$  if  $w \neq r$ ,
  - $\tau_8 \equiv 0 \pmod{8}$  if  $w = r$ .

**Historical and Bibliographical Notes.** For Sections 14.1–14.4 on spinor equivalence in relation to genus equivalence and equivalence we have largely followed Chapters 10 and 11 in J. Cassels’s book [36] as well as Kapittel VIII in M. Kneser’s book [122].

As indicated in Remark 14.5.4, surjectivity of the reduction homomorphism  $r_L$  or failure thereof has been extensively studied in Ch. VIII of the preprint [156] by R. Miranda and D. Morrison. We only elaborate a simple case ensuring surjectivity.

The applications to  $p$ -elementary lattices are based on V. Nikulin’s approach in [169].

## Lattice Embeddings

### Introduction

In Subsection 1.7.C of Chapter 1 we showed that overlattices of a non-degenerate lattice correspond bijectively to isotropic submodules of its discriminant form and that an isometry between two non-degenerate lattices extend to isometries between overlattices if it induces a homomorphism between the corresponding isotropic submodules. This chapter is devoted to overlattices of the orthogonal sum of two non-degenerate lattices  $S \oplus T$ . In Section 15.1 we show that overlattices of  $S \oplus T$  exist in which  $S$  and  $T$  embed primitively if a certain glueing criterion on the discriminant forms of  $S$  and  $T$  holds. The question whether  $S$  can be primitively embedded in a given lattice  $L$  is harder to decide using these techniques, since we then should first find a candidate for  $T$ . For unimodular lattices  $L$  this problem is solved in Section 15.2, and, with the help of these results, in Section 15.3 for non-unimodular lattices. Here we use most of the techniques and results obtained in previous chapters. In § 15.2.C we apply the results of Section 15.2 to lattice involutions.

### 15.1 Primitive Embeddings of Lattices

Recall from Subsection 1.7.C that an overlattice of a non-degenerate symmetric or quadratic lattice  $N$  is an integral lattice  $L$  containing  $N$  as a finite index sublattice. Here we consider overlattices  $L$  of lattices of the form  $N = S \oplus T$  with  $S$  and  $T$  proper sublattices. The inclusions  $L \subset L^* \subset N^*$  induce in this case inclusions  $L/(S \oplus T) \subset L^*/(S \oplus T) \subset S^*/S \oplus T^*/T = \text{dg}_S \oplus \text{dg}_T$  such that  $L/(S \oplus T)$  is an isotropic subspace of  $\text{dg}_S \oplus \text{dg}_T$ . We require also that  $S$  and  $T$  embed primitively in the overlattice  $L$ . By Remark 1.3.2 this is equivalent to  $S = T^\perp$  and  $T = S^\perp$ .

We aim to reverse the construction, i.e., given non-degenerate lattices  $S$  and  $T$ , find a criterion allowing to construct an overlattice  $L$  of  $S \oplus T$  in which  $S$  and  $T$  embed primitively such that  $T = S^\perp$  and  $S = T^\perp$ . Before we do this, we first show that the compositions of the inclusion  $L/(S \oplus T) \hookrightarrow \text{dg}_S \oplus \text{dg}_T$  with the projections on the first, respectively the second summand of the right-hand side are injective. It suffices to verify this for the composition  $p : L/(S \oplus T) \rightarrow \text{dg}_T$ . To see this, let  $\bar{x} \in L/(S \oplus T)$ ,  $x \in L$ , be in the kernel of  $p$ . Writing  $x$  as  $x_1 + x_2$  with  $x_1 \in S^*$  and  $x_2 \in T^*$ , then  $p(\bar{x}) = 0$  just means that  $x_2 \in T$ . Then  $x - x_2 = x_1 \in S^* \cap L = S$ . So  $x \in S \oplus T$ . In other words, we have shown that the image of  $L/(S \oplus T)$  in  $\text{dg}_S \oplus \text{dg}_T$

is the "graph"<sup>1</sup> of an injective homomorphism  $\psi_{S,T} : H_S \hookrightarrow \text{dg}_T$  where  $H_S \subset \text{dg}_S$  is the first embedded copy of  $L/(S \oplus T)$ . This is summarized in the commutative diagram

$$\begin{array}{ccccc}
 & & \text{dg}_S \oplus \text{dg}_T & & \\
 & \swarrow & \uparrow & \searrow & \\
 & & L/(S \oplus T) & & \\
 & \swarrow \cong & & \searrow p & \\
 \text{dg}_S & \longleftarrow & H_S & \xrightarrow{\psi_{S,T}} & \text{dg}_T.
 \end{array} \tag{15.1}$$

If  $L$  is unimodular, using (1.8), Lemma 1.3.1 shows that  $|\text{dg}_S| = |\text{dg}_T| = [L : S \oplus T]$ . Since also  $[L : S \oplus T] = |H_S|$ , we conclude that  $H_S = \text{dg}_S$  and that  $\psi_{S,T}$  maps  $\text{dg}_S$  isomorphically onto  $\text{dg}_T$ .

Returning to the general setting, recall from Proposition 1.7.4 that the form on  $L$  becomes zero on the quotient  $L/(S \oplus T)$  which means that the graph of  $\psi_{S,T}$  is an isotropic subspace of  $\text{dg}_S \oplus \text{dg}_T$ . Phrasing this differently, one has:

**Proposition 15.1.1.** *Let  $L$  be a non-degenerate symmetric (respectively quadratic) lattice,  $S$  a primitive non-degenerate sublattice and  $T = S^\perp$ . With the notation of diagram (15.1), the following equivalent properties hold:*

1. on  $H_S \subset \text{dg}_S$  the **glueing criterion**  $b_T^\#(\psi_{S,T}^-, \psi_{S,T}^-) + b_S^\#(-, -) = 0$ , respectively  $q_T^\# \circ \psi_{S,T} + q_S^\# = 0$  holds;
2. up to a sign the embedding  $\psi_{S,T}$  is an isometry of torsion forms;
3.  $H := \text{graph of } \psi_{S,T} \subset \text{dg}_S \oplus \text{dg}_T$  is an isotropic subspace.

If  $L$  is unimodular, then  $H_S = \text{dg}_S$ ,  $\psi_{S,T}$  is an isomorphism and the glueing condition becomes  $b_S^\# \simeq -b_T^\#$  (respectively  $q_S^\# \simeq -q_T^\#$ ).

**Example 15.1.2.** An example illustrating Proposition 15.1.1 is the following. Let  $L = U \oplus U$  be the sum of two copies of the hyperbolic plane  $U$ , the first one with the usual basis  $e, f$  (so  $b(e, e) = b(f, f) = b(e, f) - 1 = 0$ ) and the second one with similar basis  $e', f'$ . Take  $S$  to be the span of  $e + f, e' + f'$  in  $L$ , and let  $T$  be the span of  $e - f, e' - f'$  in  $L$ . Then  $L$  is an even unimodular overlattice of  $S \oplus T$ . The discriminant groups of  $S$  and  $T$  are  $\text{dg}_S = \frac{1}{2}S/S = \langle u = \frac{1}{2}(e+f) + S, u' = \frac{1}{2}(e'+f') + S \rangle$  and  $\text{dg}_T = \frac{1}{2}T/T = \langle v = \frac{1}{2}(e-f) + T, v' = \frac{1}{2}(e'-f') + T \rangle$ . The image of  $L/(S \oplus T)$  in  $\text{dg}_S \oplus \text{dg}_T$  equals  $\{0, (u, v), (u', v'), (u + u', v + v')\}$ , which is the graph of the isomorphism  $\psi_{S,T} : \text{dg}_S \rightarrow \text{dg}_T$  determined by  $\psi_{S,T}(u) = v$  and  $\psi_{S,T}(u') = v'$ . Note that  $b_S^\#(u, u) = \frac{1}{2} + \mathbb{Z} = -b_T^\#(v, v)$ , etc. Also, for the associated quadratic form  $q(x) = \frac{1}{2}b(x, x)$  we have  $q_S^\#(u) = \frac{1}{2} \cdot \frac{1}{2} + \mathbb{Z} = \frac{1}{4} + \mathbb{Z}$  and  $q_T^\#(v) = \frac{1}{2} \cdot -\frac{1}{2} + \mathbb{Z} = -\frac{1}{4} + \mathbb{Z}$ , etc.

<sup>1</sup>Since the map  $\psi_{S,T}$  is not defined on all of  $S$ , the correct notion is that of the "push-out" of the maps  $H_S \hookrightarrow \text{dg}_S$  and  $\psi_{S,T}$  (modulo some identifications), but we prefer the terminology "graph" in this situation.

Now we are ready to reverse the construction starting with two lattices  $S$  and  $T$ .

**Proposition 15.1.3.** *Let  $S$  and  $T$  be non-degenerate symmetric (respectively quadratic) lattices,  $H_S \subset \text{dg}_S$  a subgroup, and  $\psi_{S,T} : H_S \hookrightarrow \text{dg}_T$  an injective homomorphism. Suppose that the glueing criterion of Proposition (15.1.1) holds. Then, setting  $N := S \oplus T$ , we have*

1. *The lattice  $L = \{y \in N^* \mid y \bmod N \in H\}$ , where  $H$  is the graph of  $\psi_{S,T}$ , is a symmetric (respectively quadratic) overlattice of  $N$  satisfying  $[L : N] = |H_S|$ ;*
2.  *$S$  and  $T$  embed primitively in  $L$  and  $T = S^\perp$ ,  $S = T^\perp$ ;*
3. *If  $H_S = \text{dg}_S$  and  $\psi_{S,T}$  is an isomorphism, then  $L$  is unimodular.*

*Proof.* Item 1 is implied by Proposition 1.7.4. The equality  $[L : N] = |H_S|$  follows from the isomorphism  $L/(S \oplus T) \simeq H_S$ . Moreover, if  $H_S = \text{dg}_S$  and  $\psi_{S,T}$  is an isomorphism, then  $[L : N] = |\text{dg}_S| = |\text{disc}(S)| = |\text{dg}_T| = |\text{disc}(T)|$ , and Lemma 1.3.1 implies that  $L$  is unimodular, proving item 3.

2. The assumptions imply that the composition of the embedding  $L/(S \oplus T) \xrightarrow{\cong} H \subset \text{dg}_S \oplus \text{dg}_T$  with the projection onto either one of the summands of  $\text{dg}_S \oplus \text{dg}_T$  is injective. We claim that this implies that  $S$  and  $T$  are primitive in  $L$ . If for instance  $S$  were not primitive in  $L$ , there would exist a vector  $x \in L$ ,  $x \notin S$ , such that  $nx \in S$  for some integer  $n > 1$ . Since then  $x \in S^*$ , this would give a non-zero element in the kernel of the composition  $L/(S \oplus T) \hookrightarrow \text{dg}_S \oplus \text{dg}_T \rightarrow \text{dg}_T$ . As before, by Remark 1.3.2, then  $S = T^\perp$ .  $\square$

Surprisingly, if  $S$  embeds primitively in an even lattice  $L$  which is unique in its genus, also any lattice in the genus of  $S$  can be embedded primitively in  $L$ :

**Corollary 15.1.4.** *Let  $L$  be a non-degenerate even lattice with one isometry class in its genus and suppose that the non-degenerate lattice  $S$  embeds primitively in  $L$ . Then any lattice  $S'$  in the same genus as  $S$  embeds primitively in  $L$ .*

*Proof.* Let  $T$  be the orthogonal complement of  $S$  in  $L$  and  $N = S \oplus T$ . The subgroup  $H = L/N$  of  $\text{dg}_N$  is then isotropic with respect to the discriminant quadratic form. By Lemma 1.9.4 the discriminant quadratic form of  $S$  only depends on the genus of  $S$  and so  $N$  and  $N' = S' \oplus T$  have isometric discriminant quadratic forms (with an isometry respecting the summands). Therefore, the isotropic graph  $H$  of  $\psi_{S,T}$  (as in Proposition 15.1.3) can be transported to a graph  $\psi_{S',T}$ , which is isotropic in  $\text{dg}_{S'} \oplus \text{dg}_T$ . So by Proposition 1.7.4.3 it determines a unique even overlattice  $L'$  of  $N'$ . Moreover, by Proposition 1.7.4.2 the discriminant form of  $L'$  is the same as that of  $L$ . Lastly,  $L$  and  $L'$  have the same signature – as this is the case for  $N'$  and  $N$ . This shows that  $L$  and  $L'$  have the same genus invariants and so they are in the same genus (cf. Theorem 11.3.1). Hence, by assumption,  $L$  and  $L'$  are isometric and so  $S'$  also embeds primitively in  $L$ .  $\square$

**Example 15.1.5.** Here is an example of two non-isometric lattices in the same genus that embed in the same even unimodular lattice. The lattices  $E_8 \oplus E_8$  and  $\Gamma_{16}$  are in the same genus, but are not isometric (see Examples 1.5.1 and 11.3.2). The indefinite unimodular lattices  $\bigoplus^k U \oplus E_8 \oplus E_8$  and  $\bigoplus^k U \oplus \Gamma_{16}$ ,  $k = 1, 2, \dots$ , however, are both even and have the same signature, and so are isometric by Theorem 2.4.1. Note that Corollary 15.1.4 applies in this case, but is not needed.

**Application: Extending isometries to overlattices.** In Subsection 1.7.C we discussed the problem of extending a lattice isometry  $N \rightarrow N'$  to an isometry between overlattices  $L \rightarrow L'$ . Applying this in the situation of overlattices of an orthogonal direct sum  $N = S \oplus T$ , Proposition 15.1.3 gives a second extension criterion:

**Proposition 15.1.6** (Extending isometries, II). *Let  $S, S', T, T'$  be non-degenerate quadratic lattices related by isometries  $\sigma : S \xrightarrow{\sim} S'$  and  $\tau : T \xrightarrow{\sim} T'$ . Suppose  $L, L'$  are quadratic overlattices of  $S \oplus T, S' \oplus T'$ , respectively. Assume that  $S$  and  $T$  are primitively embedded in  $L$ , and similarly for  $S'$  and  $T'$ .*

*Then the isometry  $\lambda = \sigma \oplus \tau$  extends to an isometry  $L \xrightarrow{\sim} L'$  if and only if (the map induced by)  $\lambda$  sends the subgroup  $L/(S \oplus T)$  of  $\text{dg}_S \oplus \text{dg}_T$  to the subgroup  $L'/(S' \oplus T')$  of  $\text{dg}_{S'} \oplus \text{dg}_{T'}$ . In other words, using the notation of diagram (15.1),  $\lambda$  extends if and only if there is a commutative diagram*

$$\begin{array}{ccccc}
 \text{dg}_S & \longleftarrow & H_S & \xrightarrow{\psi_{S,T}} & \text{dg}_T \\
 r_{S,S'}(\sigma) \downarrow & & \downarrow & & \downarrow r_{T,T'}(\tau) \\
 \text{dg}_{S'} & \longleftarrow & H_{S'} & \xrightarrow{\psi_{S',T'}} & \text{dg}_{T'}
 \end{array} \tag{15.2}$$

where  $r_{S,S'}(\sigma)$  and  $r_{T,T'}(\tau)$  are induced by  $\sigma$  and  $\tau$ , respectively. In particular, if  $L$  (and hence  $L'$ ) is unimodular, using Propositions 15.1.1, 15.1.3, this reduces to the glueing criterion exhibited by the commutative diagram

$$\begin{array}{ccc}
 \text{dg}_S & \xrightarrow{\cong} & \text{dg}_T \\
 r_{S,S'}(\sigma) \downarrow & & \downarrow r_{T,T'}(\tau) \\
 \text{dg}_{S'} & \xrightarrow{\cong} & \text{dg}_{T'}
 \end{array} \tag{15.3}$$

The preceding result for embeddings in the same lattice  $L = L'$  is a version of Witt's theorem 7.2.8 and as in that case we speak of **equivalent embeddings**:

**Theorem 15.1.7** (Witt's extension theorem for lattices). *1. Let  $L$  be a non-degenerate even lattice and let  $i, i' : S \hookrightarrow L$  be two primitive embeddings. Then these embeddings are equivalent if and only if an isometry  $T = i(S)^\perp \xrightarrow{\sim} T' = i'(S)^\perp$  exists inducing a commutative diagram like (15.2).*

*2. Suppose in addition that  $L$  is unimodular, then two primitive embeddings of  $S$*

in  $L$  with isometric orthogonal complements are equivalent if the reduction homomorphism  $r_T : \mathcal{O}(T) \rightarrow \mathcal{O}(q_T^\#)$  is surjective, where  $T$  is the orthogonal complement of an embedded copy of  $S$ .

*Proof.* The first assertion follows directly from Proposition 15.1.6.

2. Identify  $S$  with the image under the first embedding, let  $S'$  be the image of the second embedding. This yields the isometry  $\sigma : S \rightarrow S'$  which relates the embeddings. Setting  $T = S^\perp$ ,  $T' = S'^\perp$ , one seeks an isometry  $\tau : T \xrightarrow{\sim} T'$  such that  $\sigma \oplus \tau$  extends to an isometry of  $L$ . Since  $L$  is unimodular  $\psi_{S,T}$  and  $\psi_{S',T'}$  are isomorphisms by Proposition 15.1.1, hence so is  $\bar{\tau} := \psi_{S',T'} \circ r_{S,S'}(\sigma) \circ \psi_{S,T}^{-1} : \mathfrak{dg}_T \xrightarrow{\sim} \mathfrak{dg}_{T'}$ . It is even an isometry since  $\psi_{S,T}$  and  $\psi_{S',T'}$  reverse signs of the discriminant forms and  $r_{S,S'}(\sigma)$  is an isometry. Since  $T$  and  $T'$  are isometric, the assumption that the reduction homomorphism  $r_T$  is surjective implies that the isometry  $\bar{\tau} : \mathfrak{dg}_T \rightarrow \mathfrak{dg}_{T'}$  lifts to an isometry  $\tau : T \xrightarrow{\sim} T'$ . By construction the resulting diagram (15.3) is commutative and then  $\sigma \oplus \tau$  extends.  $\square$

The weakness of the above result is twofold. First, if  $S$  is a given lattice we would like to know if it embeds primitively in  $L$ . Secondly, we are using properties of  $T$ , the orthogonal complement of  $S$ . In the next section we arrive at a more manageable condition in the case of unimodular lattices. In Section 15.3 we treat the general case.

## 15.2 Primitive Embeddings into Unimodular Quadratic Lattices

In this section we assume that  $(L, q)$  is a unimodular quadratic lattice.

**15.2.A Existence of Embeddings.** Suppose now that we are given a non-degenerate quadratic lattice  $S$  which we want to embed primitively in a unimodular quadratic lattice  $L$ . In order to apply the preceding results, we need to find all candidate orthogonal complements  $T$  in  $L$ . By Propositions 15.1.1, 15.1.3 we should in any case have  $q_T^\# \simeq -q_S^\#$ . By Theorem 11.3.1 this implies that the genus of such a lattice  $T$  is completely determined if, in addition, we know the signature  $(r_+, r_-)$  of the resulting overlattice. In other words, to be able to embed  $S$  primitively in *some* unimodular lattice of signature  $(r_+, r_-)$  there should exist a lattice  $T$  with genus invariant  $\mathfrak{g}(T) = (r_+ - s_+, r_- - s_-, [-q_S^\#])$ . There is however an additional condition since the signature of an even unimodular lattice is divisible by 8 (cf. Corollary 2.4.3). This leads to the following criterion:

**Proposition 15.2.1** ([171, Theorem 1.12.2 & Cor. 1.12.3]). *Let  $(r_+, r_-)$  be a pair of non-negative integers for which  $r_+ - r_- \equiv 0 \pmod{8}$  and let  $S$  be a non-degenerate even lattice of signature  $(s_+, s_-)$  with  $s_+ \leq r_+$  and  $s_- \leq r_-$ , discriminant group  $\mathfrak{dg}_S$*

and discriminant quadratic form  $q^\#$ . Suppose that, moreover,  $(r_+ + r_-) - \text{rank}(S) \geq \ell(\text{dg}_S)$ . Then the following conditions are equivalent.

1.  $S$  can be primitively embedded in some even unimodular lattice  $L$  of signature  $(r_+, r_-)$  ( $L$  is unique up to isometry in case  $r_+ > 0$  and  $r_- > 0$ );
2. A (non-degenerate) even lattice  $T$  of signature  $(r_+ - s_+, r_- - s_-)$  with discriminant quadratic form  $-q^\#$  exists;
3. A (non-degenerate) even lattice  $T'$  of signature  $(r_- - s_-, r_+ - s_+)$  with discriminant quadratic form  $q^\#$  exists;
4. The equality<sup>2</sup>  $\text{disc}(L_{q^\#}) = (-1)^{r_- - s_-} |\text{dg}_S|$  in  $D(\mathbb{Z}_p)$  holds in the following cases:
  - for any prime  $p \neq 2$  for which  $\text{dg}_{S_p}$ , the  $p$ -primary part of  $\text{dg}_S$ , has length equal to  $(r_+ + r_-) - \text{rank}(S)$ ;
  - for  $p = 2$  in case  $\ell(\text{dg}_{S_2}) = (r_+ + r_-) - \text{rank}(S)$  and  $\text{dg}_{S_2}$  does not split off a cyclic order 2 module.

In particular, all of these these conditions are satisfied if  $(r_+ + r_-) - \text{rank}(S) > \ell(\text{dg}_S)$ .

*Proof.* From the discussion so far 1) implies 2), while item 3 is equivalent to item 2 (just reverse the sign of the form). To show that 2) implies 1), first observe that, assuming 2), there exists an isomorphism from  $\text{dg}_S$  onto  $\text{dg}_T$  such that the glueing condition holds for the quadratic forms. Then Proposition 15.1.3 implies that there exists an even overlattice  $L$  of  $S \oplus T$  such that  $[L : S \oplus T] = |\text{dg}_S| = |\text{disc}(S)| = |\text{disc}(T)|$ . By Lemma 1.3.1 this implies that  $L$  is unimodular as required.

Item 4 is the existence criterion of Theorem 12.4.4 applied to  $T'$ . The penultimate assertion follows from Corollary 12.4.6 since the stated condition implies the existence of an even lattice  $T'$  as in item 3. The seemingly missing condition on the signature modulo 8 is automatic since  $r_+ - r_- \equiv 0 \pmod 8$ , so that  $\tau_8(q^\#) \equiv s_+ - s_- \equiv r_- - s_- - (r_+ - s_+) \equiv \tau(T') \pmod 8$ .

Since even indefinite unimodular lattices are determined up to isometry by their signature as demonstrated in Chapter 2, the lattice  $L$  in item 1 is unique if  $r_+ > 0$  and  $r_- > 0$ . □

*Remark 15.2.2.* If  $S$  is definite, the preceding embedding result is less interesting since the uniqueness of  $L$  need not hold. For instance  $E_8$  embeds trivially in  $E_8 \oplus E_8$  but does not embed in  $\Gamma_{16}$ .

We apply the preceding results to show embeddability for a large class of lattices.

**Theorem 15.2.3** (Universal Embeddability). *Let  $(r_+, r_-)$  be a pair of non-negative integers for which  $r_+ - r_- \equiv 0 \pmod 8$  and let  $(s_+, s_-)$  be a pair of non-negative integers with  $s_+ \leq r_+$  and  $s_- \leq r_-$ .*

---

<sup>2</sup>Recall that we have shown in Chapter 11 that every  $p$ -primary quadratic torsion form  $(G, q^\#)$  comes from a unique  $p$ -adic lattice  $L_{q^\#}$  of rank  $\ell(G)$  in case  $p$  is odd, or if  $p = 2$  and  $G$  does not split off a cyclic group of order 2.



Then every even non-degenerate lattice  $S$  of signature  $(s_+, s_-)$  satisfying  $r_+ + r_- - \text{rank}(S) \geq \ell(\text{dg}_S)$  can be primitively embedded in some even unimodular lattice  $L$  of signature  $(r_+, r_-)$  if

$$s_+ + s_- \leq \frac{1}{2} \text{rank}(L). \quad (15.4)$$

In case  $r_+ > 0$  and  $r_- > 0$ , the unimodular lattice  $L$  is unique up to isometry.

*Proof.* Assume we have an even non-degenerate lattice  $S$  of signature  $(s_+, s_-)$  with discriminant form  $q^\#$  for which (15.4) holds. We want to show that  $S$  embeds in some (non-specified) unimodular even lattice  $L$  of signature  $(r_+, r_-)$ . Again, by Theorem 12.4.4.2 we have  $\text{rank}(S) = s_+ + s_- \geq \ell(\text{dg}_S)$  and hence, using the assumption (15.4),

$$\text{rank}(L) - \text{rank}(S) \geq \text{rank}(S) \geq \ell(\text{dg}_S).$$

If one of these inequalities is strict,  $S$  can be embedded primitively in such a lattice  $L$  as follows from Proposition 15.2.1. It remains to consider the situation where one has equality everywhere, that is,

$$\text{rank}(S) = \frac{1}{2} \text{rank}(L) = \ell(\text{dg}_S). \quad (15.5)$$

To show that  $S$  embeds in  $L$ , by Proposition 15.2.1.3 it suffices to show that a lattice  $T'$  with signature  $(r_- - s_-, r_+ - s_+)$  and quadratic torsion group  $(G = \text{dg}_S, q^\#)$  exists. We want to apply the existence criterion of Theorem 12.4.4.

- First of all, condition (1) on the signature holds since  $(r_- - r_+) - (s_- - s_+) \equiv s_+ - s_- \pmod{8} \equiv \tau_8(q^\#) \pmod{8}$  (since  $q^\#$  is the discriminant form of  $S$ ).
- Equality (15.5) implies that  $\text{rank}(L) - \text{rank}(S) = \text{rank}(S) \geq \ell(G_p)$  for all primes  $p$  so that condition 2 holds.
- The verification of the remaining condition is more involved. First observe that equality (15.5) yields

$$\begin{aligned} r_+ - s_+ &= r_+ - (s_+ + s_-) + s_- \\ &= r_+ - \frac{1}{2}(r_+ + r_-) + s_- \\ &= \frac{1}{2}(r_+ - r_-) + s_-, \end{aligned}$$

and since by assumption  $r_+ - r_-$  is divisible by 8, we have  $r_+ - s_+ \equiv s_- \pmod{2}$  and so

$$(-1)^{s_-} = (-1)^{r_+ - s_+}. \quad (15.6)$$

Let  $p$  be a prime for which  $\ell(G) = \ell(G_p)$ . Then (15.5) gives  $\text{rank}(S) = \ell(G_p)$ . We invoke item 3 of Theorem 12.4.4 applied to  $S$  and  $G$ , and use (15.6) which leads to the equality

$$(-1)^{r_+ - s_+} \cdot |G| = \text{disc}(L_{q^\#}) \text{ in } D(\mathbb{Z}_p),$$

which is valid for odd  $p$  and for  $p = 2$  if no cyclic summand of order two splits off from  $G_2$ . Hence, also the remaining condition for the existence of  $T'$  is satisfied, and so in the case where (15.5) holds  $S$  can also be embedded.  $\square$

We tie this in with the embedding criterion we found in Section 1.8 and its generalization, Proposition 6.3.12. Recall that it states that any even lattice  $S$  of rank  $s$  can be embedded in  $\mathbb{Q}^s U$  with  $S^\perp \simeq S(-1)$ . This can be used to embed  $S$  in an arbitrary even unimodular lattice  $L$  whose Witt-index is at least  $s$ . Indeed, by the classification theorem 2.4.1 an indefinite even unimodular lattice is isometric to an orthogonal sum of say  $t$  hyperbolic planes and a number of copies of  $E_8$  or  $E_8(-1)$ . The number  $t$  is the Witt index. So, clearly,  $S$  embeds in such a lattice which leads to rephrase the result as follows:

**Lemma 15.2.4.** *An even lattice  $S$  can be embedded in an indefinite even unimodular lattice  $L$  if the Witt index of  $L$  is  $\geq \text{rank}(S)$ . In particular,  $S$  embeds in  $\mathbb{Q}^s U$ ,  $s = \text{rank}(S)$ , with  $S^\perp \simeq S(-1)$ .*

We see that in case  $S$  is non-degenerate Theorem 15.2.3 states that  $S$  can be primitively embedded in  $L = \mathbb{Q}^a U \oplus \mathbb{Q}^b E_8(\pm 1)$  if  $\text{rank}(S) \leq \frac{1}{2} \text{rank}(L) = a + 4b$ , while Lemma 15.2.4 just provides the condition  $\text{rank}(S) \leq a$ .

**Example 15.2.5.** We discuss under what condition an even non-degenerate lattice  $T$  of rank  $a + e$  with  $e > 0$  can be embedded in the hyperbolic lattice  $\mathbb{Q}^a U$ . Clearly, if  $e$  copies of  $U$  can be split off, say  $T = \mathbb{Q}^e U \oplus S'$ , then the lattice  $S'$  – which has rank  $a - e$  – can be primitively embedded in  $\mathbb{Q}^{a-e} U$  and hence  $T$  embeds primitively in  $\mathbb{Q}^a U$ .

We claim that the converse holds. To see this, let the signature of  $T$  be  $(k, a + e - k)$ . Assume that  $T$  embeds primitively in  $\mathbb{Q}^a U$ . Then  $a \geq a + e - k$  so that  $k \geq e$  and  $S := T^\perp$  has signature  $(a - k, k - e)$  and index  $a + e - 2k$ . The lattice  $\mathbb{Q}^e U \oplus S(-1)$  has index  $2k - a - e$  and rank  $a + e$ , just as  $T$ , and since  $q_S^\# = -q_T^\#$ , it has also the same discriminant form. It follows that  $\mathbb{Q}^e U \oplus S(-1)$  and  $T$  are in the same genus by Theorem 11.3.1. Since  $\ell(\text{dg}_T) = \ell(\text{dg}_S) \leq \text{rank}(T) - 2e$ , Corollary 14.4.3 implies that  $T$  and  $\mathbb{Q}^e U \oplus S(-1)$  are isometric. So we conclude that indeed  $T$  embeds primitively in  $\mathbb{Q}^a U$  if and only if  $\mathbb{Q}^e U$  is an orthogonal direct summand of  $T$ .

**15.2.B Uniqueness of Embeddings.** While up to now we only invoked Nikulin’s existence results 12.4.4, we can say more using Nikulin’s theorems about uniqueness of the isometry class in a genus as we now explain. More precisely, we shall use Corollary 14.4.3 stating that a non-degenerate indefinite quadratic lattice  $S$  is unique in its genus if  $\ell(\text{dg}_S) \leq \text{rank}(S) - 2$ , and Theorem 14.5.5 which asserts that under this condition the reduction map  $r_S : \text{O}(S) \rightarrow \text{O}(q_S^\#)$  is surjective. Proposition 15.2.1 can be paraphrased by saying that  $S$  embeds primitively in an indefinite unimodular quadratic lattice  $L$  with  $T = S^\perp$  if  $\ell(\text{dg}_S) < \text{rank}(T)$ . Replacing this condition with  $\ell(\text{dg}_S) \leq \text{rank}(T) - 2$  the just stated results imply the following:

**Theorem 15.2.6.** *Let  $L$  be an indefinite even unimodular lattice and  $(S, q)$  a non-degenerate quadratic lattice with  $\ell(\text{dg}_S) \leq \text{rank}(L) - \text{rank}(S) - 2$ . Let  $L$  and  $S$  have signature  $(r_+, r_-)$ ,  $(s_+, s_-)$ , respectively, and assume that  $r_+ > s_+$ ,  $r_- > s_-$ . Then*

1. the orthogonal complement of a primitively embedded  $S \hookrightarrow L$  has genus invariant  $(r_+ - s_+, r_- - s_-, -[q_S^\#])$ ;
2.  $S$  admits a primitive embedding in  $L$  and such primitive embeddings are unique up to equivalence, i.e.,  $O(L)$  acts transitively on primitive embeddings of  $S$  in  $L$ .

*Proof.* Let  $\mathfrak{g}(S) = (s_+, s_-, q_S^\#)$ . As observed just before the statement of this theorem, Proposition 15.2.1 shows that there exists an isometry class of a lattice  $T$  with genus invariant  $\mathfrak{g}(T) = (r_+ - s_+, r_- - s_-, [-q_T^\#])$ . Theorem 14.5.5 shows that the reduction map  $r_T : O(T) \rightarrow O(q_T^\#)$  is surjective. Hence Theorem 15.1.7 implies unicity of the embedding  $S \hookrightarrow L$ . Moreover, since  $S^\perp$  has the same genus invariant as  $T$ , the two are isometric.  $\square$

Since  $\ell(\text{dg}_S) \leq \text{rank}(S)$ , Theorem 15.2.6 implies:

**Corollary 15.2.7.** *Let  $L$  be an indefinite even unimodular lattice of rank  $\geq 4$ , and signature  $(r_+, r_-)$ . A non-degenerate even lattice  $S$  of signature  $(s_+, s_-)$ ,  $(s_\pm \leq r_\pm)$ , admits a primitive embedding in  $L$  which is unique up to equivalence if  $\text{rank}(S) \leq \frac{1}{2} \text{rank}(L) - 1$ ,*

**Examples 15.2.8. 1.** Let  $L = \Lambda_{K3} = U \oplus U \oplus U \oplus E_8(-1) \oplus E_8(-1)$ , the K3-lattice. Then any non-degenerate even lattice of rank  $\leq 2$  can be embedded uniquely as a primitive lattice in  $\Lambda_{K3}$ . This holds more generally for any non-degenerate even lattice of rank  $r \leq 10$  which has signature  $(0, r)$ ,  $(1, r - 1)$  or  $(2, r - 2)$ . For the same reason, if  $L = U^{\oplus a} \oplus E_8(-1)^{\oplus b}$ , then any non-degenerate lattice of rank  $\leq a - 1$  or of rank  $r \leq a + 4b - 1$  and signature  $(s, r - s)$ ,  $s \leq a - 1$  can be embedded uniquely in  $L$  as a primitive lattice.

**2.** Again  $L = \Lambda_{K3}$  but now  $S = A_{k_1}(-1) \oplus A_{k_2}(-1) \oplus \cdots \oplus A_{k_\ell}(-1)$ . If  $\sum k_j \leq 10$  conditions 1 and 2 hold.

**15.2.C Applications.** We first give an application to the group of isometries of a unimodular lattice  $L$  that preserve a given sublattice  $S$ .

**Proposition 15.2.9.** *Let  $L$  be a quadratic unimodular lattice,  $S \subset L$  a primitive non-degenerate sublattice,  $T = S^\perp$  and  $\sigma \in O^\#(S)$ .*

*The isometry  $\sigma \oplus \text{id}_T$  of  $S \oplus T$  extends to an isometry  $e_S(\sigma)$  of  $L$ . The assignment  $\sigma \mapsto e_S(\sigma)$  defines an injective homomorphism  $e_S : O^\#(S) \rightarrow O(L)$  with image contained in the subgroup  $O^\#(L)_S$  of the stabilizer  $O(L)_S$  of  $S$  in  $O(L)$  given by*

$$O^\#(L)_S := \{\gamma \in O(L)_S \mid r_S(\gamma) = r_T(\gamma)\}.$$

*In other words, there is an exact sequence*

$$1 \rightarrow O^\#(S) \xrightarrow{e_S} O^\#(L)_S \xrightarrow{\rho_T} O(T),$$

*where  $\rho_T$  is the restriction map. If the reduction map  $r_S : O(S) \rightarrow O(q_S^\#)$  is surjective, then also  $\rho_T$  is surjective.*

*Proof.* If  $\sigma \in \mathcal{O}^\#(S)$ , then  $\sigma \oplus \text{id}_T$  induces the identity on  $\text{dg}_S \oplus \text{dg}_T$  and hence preserves its subspace  $L/S \oplus T$  and so it extends to  $L$  by Proposition 15.1.6. Clearly this gives an injective homomorphism  $e_S$  and  $e_S(\sigma)$  preserves  $S$ . Since  $e_S(\sigma)$  is the identity on  $T$ , we have  $\rho_T \circ e_S(\sigma) = \text{id}_T$ .

The kernel of the map  $\rho_T$  consists of isometries inducing the identity on  $T$ . These isometries act trivially on  $\text{dg}_T \simeq \text{dg}_S$  and so their restrictions to  $S$  by definition belong to  $\mathcal{O}^\#(S)$ . Finally, if  $r_S$  is surjective, then for any  $\psi \in \mathcal{O}(T)$ , some  $\varphi \in \mathcal{O}(S)$  exists with  $r_S(\varphi) = r_T(\psi)$  since  $\mathcal{O}(q_S^\#) \simeq \mathcal{O}(q_T^\#)$ . So, by the glueing condition (Proposition 15.1.6),  $\varphi \oplus \psi$  extends as an isometry of  $L$  which by construction preserves  $S$  and  $T$  and by construction belongs to  $\mathcal{O}^\#(L)_S$ . □

Next, we give an application to lattice involutions, making use of the invariant lattice.

**Proposition 15.2.10** (Comparing lattice involutions). *Let  $L$  and  $L'$  be isometric indefinite quadratic unimodular lattices admitting lattice involutions  $i$ , respectively  $i'$ . Suppose that*

- *the corresponding invariant lattices  $S, S'$  are isometric,*
- *$T = S^\perp, T' = S'^\perp$  are indefinite and have rank  $\geq 4$ .*

*then there is an isometry  $\lambda : L \xrightarrow{\cong} L'$  intertwining  $i$  and  $i'$ , that is, there is a commutative diagram*

$$\begin{array}{ccc} L & \xrightarrow[\lambda]{\cong} & L' \\ \downarrow i & & \downarrow i' \\ L & \xrightarrow[\lambda]{\cong} & L' \end{array}$$

*Proof.* Since  $S$  and  $S'$  are invariant lattices, they are also non-degenerate (see Example 1.7.3), and then so are  $T$  and  $T'$ . By the same example these four lattices are 2-elementary. Also the lattices  $T$  and  $T'$  are isometric since first of all they have the same genus by Theorem 11.3.1 (their signatures are the same and  $q_T^\# \cong q_S^\#(-1) \cong q_{S'}^\#(-1) \cong q_{T'}^\#$ ), and, secondly, by Corollary 14.6.2, 2-elementary lattices of rank  $\geq 4$  in the same genus are isometric.

Let  $\sigma : S \rightarrow S'$  be an isometry. We will construct an isometry  $\tau : T \rightarrow T'$  such that  $\sigma \oplus \tau$  extends to a global isometry  $\lambda : L \rightarrow L'$ . Since  $\lambda$  commutes with  $i$  and  $i'$  on the finite index sublattice  $S \oplus T$ , it does so on  $L$ . By Proposition 15.1.6 the desired isometry  $\tau$  should satisfy  $r_{T,T'}(\tau) = \psi_{S,T} \circ r_{S,S'}(\sigma) \circ \psi_{S,T}^{-1}$ . The right-hand side is an isometry (see the proof of Theorem 15.1.7) and if the reduction map  $r_T : \mathcal{O}(T) \rightarrow \mathcal{O}(q_T^\#)$  is surjective, then as in loc. cit. an isometry  $\tau$  as desired exists.

To show that  $r_T$  is surjective, note that, using the notation of Lemma 14.6.1 and observing that  $T$  is 2-elementary, we can write  $T_2 = T^{(0)} \oplus T^{(1)}(2)$ , where  $T^{(0)}$  and  $T^{(1)}$  are unimodular. Since  $\text{rank}(T) \geq 4$  at least one of the two summands has rank  $\geq 2$  and surjectivity of  $r_T$  follows from Theorem 14.5.5. □

### 15.3 Primitive Embeddings Into Non-Unimodular Quadratic Lattices

Let  $S, M$  be non-degenerate quadratic lattices. We aim to find a criterion to embed  $S$  primitively in  $M$ . If  $M$  is unimodular, we have made use of the isometry  $q_S^\# = -q_K^\#$ , where  $K = S^\perp \subset M$ , but it is not immediate how to determine  $q_K^\#$  from the discriminant quadratic forms of  $S$  and  $M$  in general. Making use of a suitable unimodular lattice in which  $M$  embeds, we show how the isometry classes of all possible  $q_K^\#$  can be calculated. At the same time this provides a criterion:

**Proposition 15.3.1.** *Let  $S$  and  $M$  be non-degenerate quadratic lattices with genus invariants  $\mathbf{g}(S) = (s_+, s_-, [q_S^\#])$ ,  $\mathbf{g}(M) = (m_+, m_-, [q_M^\#])$ , and satisfying  $s_\pm \leq m_\pm$ . Primitive embeddings  $S \hookrightarrow M$  are determined by quadruples  $(H_S, \psi, K, \gamma_K^\psi)$ , where*

- $H_S \subset \mathbf{dg}_S$  is a subgroup,  $\psi : H_S \hookrightarrow \mathbf{dg}_M$  an embedding of quadratic torsion groups, that is,  $\psi(H_S)$  is a subgroup of  $\mathbf{dg}_M$  and  $q_S^\#(x) = q_M^\#(\psi(x))$  for all  $x \in H_S$ ;
- $K$  is a quadratic lattice with genus-invariant  $(m_+ - s_+, m_- - s_-, [-\kappa^\psi])$ ,  $\kappa^\psi := \Gamma_\psi^\perp / \Gamma_\psi$ , where  $\Gamma_\psi \subset \mathbf{dg}_S \oplus \mathbf{dg}_M$  is the graph of  $\psi$  and  $\Gamma_\psi^\perp$  its orthogonal complement with respect to the polar form of  $q_S^\# \oplus q_M^\#$ ;
- $\gamma_K^\psi : q_K^\# \xrightarrow{\sim} -\kappa^\psi$  is an isometry.

The orthogonal complement of  $S$  in  $M$  in this embedding is isometric to  $K$ .

Two embeddings  $i : S \hookrightarrow M$  and  $i' : S \hookrightarrow M$  given by  $(H_S, \psi, K, \gamma)$  and  $(H'_S, \psi', K', \gamma')$  are equivalent if and only if the following two conditions hold simultaneously:

- $H_S = H'_S$  and there exists an isometry  $\lambda$  of  $\mathbf{dg}_M$  such that  $\lambda \circ \psi = \psi'$ ;
- there is an isometry  $\varphi : K \xrightarrow{\sim} K'$  such that  $\mathbf{dg}_\varphi \circ \gamma = \gamma' \circ \lambda'$ , where the isometry  $\lambda' : -\kappa^\psi \xrightarrow{\sim} -\kappa^{\psi'}$  is induced by  $\lambda$ .

*Proof.* As we just explained, we look first for a suitable even unimodular lattice  $L$  in which  $M$  embeds primitively. By Theorem 15.2.6 there exist even unimodular lattices  $L$  in which  $M$  embeds primitively. Such a lattice then has signature  $(m_+ + t_+, m_- + t_-)$  for some non-negative integers  $t_+$  and  $t_-$ . The pair  $(t_+, t_-)$  is the signature of  $T = M^\perp$  in  $L$  and its discriminant quadratic form is the one of  $M$  with a minus sign.

By the existence criterion, Theorem 12.4.4, a lattice  $T$  in the genus of  $M^\perp$  with  $t_+ + t_- \geq \ell(\mathbf{dg}_M) + 2$  and where the condition on the index is satisfied exists, provided we replace  $(t_+, t_-)$  by  $(t_+ + k, t_- + k)$  for large enough  $k$ . Then Theorem 14.5.5 implies

$$\left. \begin{array}{l} \text{the class number of } T \text{ is one,} \\ r_T : \mathcal{O}(T) \rightarrow \mathcal{O}(q_T^\#) \text{ is onto} \end{array} \right\} \quad (15.7)$$

This then implies that all primitive embeddings of  $T$  in  $L$  are equivalent and in particular that

$$M \simeq T^\perp. \tag{15.8}$$

Now giving a primitive embedding  $S \hookrightarrow M$  is equivalent to giving a primitive embedding  $S \oplus T \hookrightarrow L$ . Here  $i : S \hookrightarrow M$  and  $i' : S \hookrightarrow M$  are considered as isomorphic if they are related by an isometry of  $L$ .

Embeddings  $S \hookrightarrow M$  can thus be obtained in two stages. To ensure that  $S \oplus T$  is primitively embedded in  $M \oplus T$  we shall consider the primitive closure  $V'$  of  $S \oplus T$  in  $M \oplus T$  and then embed  $V'$  primitively in  $L$ . To capture  $V'$  we shall list all overlattices  $V$  of  $S \oplus T$  such that  $S$  and  $T$  are primitively embedded in  $V$  up to isometries of  $T$ . Next, we shall list the primitive embeddings of such a  $V$  in  $L$  up to isometries of  $V$  and  $L$ . Note that some of those  $V$  may not be embeddable in  $L$ . To ensure this we use the supplementary assumptions.

By Proposition 15.1.3 an overlattice  $V$  of  $S \oplus T$  is determined by a subgroup  $H_S \subset \text{dg}_S$  and an injection  $\psi : H_S \hookrightarrow \text{dg}_T$  satisfying the glueing condition. Because of (15.8),  $\text{dg}_T \simeq \text{dg}_M$  with opposite forms and so we consider the graph  $\Gamma_\psi \subset \text{dg}_S \oplus \text{dg}_T$  of  $\psi$  as a subgroup of  $\text{dg}_S \oplus \text{dg}_T$  equipped with the form  $q_S^\# \oplus -q_M^\#$ . In fact, this subgroup is isotropic and Proposition 1.7.4 tells us that  $\kappa^\psi = \Gamma_\psi^\perp / \Gamma_\psi$  is the discriminant quadratic form of the overlattice  $V$ .

Next, we note that by Proposition 15.2.1 the lattice  $V$  embeds primitively in  $L$  if and only if a lattice with genus-invariant  $(m_+ - s_+, m_- - s_-, [-q_V^\#])$  exists. By assumption, one has an isometry  $\gamma_K^\psi : q_K^\# \xrightarrow{\sim} -\Gamma_\psi^\perp / \Gamma_\psi = -\kappa^\psi$  and so  $K$  has the required genus invariant. Consequently, a primitive embedding  $j : V \hookrightarrow L$  exists and under this embedding  $V^\perp$  and  $K$  are isometric. As to unicity of the embedding  $j$ , observe that since  $t_+ + t_- \geq \ell(\text{dg}_M) + 2 = \ell(\text{dg}_T) + 2$ , one has

$$\begin{aligned} \ell(\text{dg}_V) &\leq \ell(\text{dg}_S) + \ell(\text{dg}_T) \\ &\leq \text{rank}(S) + \text{rank}(T) + 2 \\ &= \text{rank}(V) + 2, \end{aligned}$$

and so by Proposition 15.1.6 the lattice  $V$  uniquely embeds in  $L$  up to isometries of  $L$ . Moreover, since we have chosen  $T$  in such a way that  $T$  is unique in its genus and such that  $r_T : \mathcal{O}(T) \rightarrow \mathcal{O}(q_T^\#)$  is onto, this proposition also implies that the embedding  $S \oplus T \hookrightarrow V$  is unique up to isometries of  $T$ .

Observe that this procedure shows that the orthogonal complement of  $S$  in  $M$  in this embedding is as claimed, since  $K \simeq V^\perp(\text{in } L) = S^\perp(\text{in } M)$ .

Next, we compare two primitive embeddings. Clearly, if two primitive embeddings of  $S$  in  $M$  are equivalent, the comparison conditions hold. For the converse, observe first that Proposition 1.7.4 implies that  $\kappa_\psi$  is isometric to the discriminant quadratic form of  $M$  since  $M$  is the overlattice of  $S \oplus K$  given by the embedding  $\psi$ . The glueing criterion for  $(S, K = S^\perp)$  in  $M$  is equivalent to the existence of the isometry  $\gamma_K$ . If  $(S', K' = (S')^\perp)$  is coming from another primitive embedding of  $S$  in  $M$ , the compatibility of the glueing data given by the diagram (15.2) is equivalent

to the existence of a commutative diagram

$$\begin{array}{ccc}
 -\kappa_\psi & \xrightarrow[\sim]{\gamma_K^{-1}} & \mathfrak{q}_K^\# \\
 \downarrow \lambda' & & \downarrow \text{dg}_\varphi \\
 -\kappa_{\psi'} & \xrightarrow[\sim]{\gamma_{K'}^{-1}} & \mathfrak{q}_{K'}^\#
 \end{array} \tag{15.9}$$

where the meaning of  $\varphi$  and  $\lambda'$  is as stated in the comparison criterion. Since this is assumed to hold, Proposition 15.1.6 implies that the two embeddings are equivalent. □

*Remark 15.3.2.* **1.** The case  $H_S = 0$  is allowed and serves for instance to cover unimodular lattices  $M$ . Similarly, if  $M = L \oplus M'$ , where  $L$  is unimodular and  $S$  embeds primitively in  $L$ , then  $H_S = 0$ .

**2.** If other lattices genus equivalent to  $K$  exist, these give rise to non-isomorphic embeddings of  $S$  in  $M$ . Moreover, different subgroups of  $\text{dg}_S$  may embed in  $\text{dg}_M$  and a given subgroup  $H_S \subset \text{dg}_S$  may embed in non-isomorphic ways in  $\text{dg}_M$ . These all give rise to non-isomorphic embeddings of  $S$  in  $M$ .

**Corollary 15.3.3.** *Let  $S, M$  be non-degenerate quadratic lattices and  $H$  a subgroup of  $\text{dg}_S$ . Primitive embeddings of  $S$  in  $M$  determined by isometric embeddings  $\psi, \psi' : H \hookrightarrow \text{dg}_M$  are equivalent, i.e., they are related by an isometry of  $M$ , in case the following conditions hold simultaneously:*

1. *The isometric embeddings  $\psi, \psi' : H \hookrightarrow \text{dg}_M$  are related by an isometry  $\lambda$  of  $\text{dg}_M$ ;*
2. *Up to isometry there is a unique lattice  $K$  with genus-invariant  $(\mathfrak{m}_+ - \mathfrak{s}_+, \mathfrak{m}_- - \mathfrak{s}_-, [-\Gamma_\psi^{-1}/\Gamma_\psi])$ .*
3. *For every primitive embedding of  $S$  in  $M$ ,  $S^\perp$  is isometric to  $K$ ; identifying  $S^\perp$  with  $K$ , the reduction map  $r_K : \text{O}(K) \rightarrow \text{O}(\mathfrak{q}_K^\#)$ ,  $K = S^\perp$ , is surjective.*

*Conditions 2 and 3 hold if  $\text{rank}(K) \geq 3$ ,  $K$  is indefinite and the conditions of Theorem 14.5.5 hold, e.g., if  $\ell(\text{dg}_K) \leq \text{rank}(K) - 2 = \text{rank}(M) - \text{rank}(S) - 2$ .*

*Proof.* We compare the two primitive embeddings  $i, i' : S \hookrightarrow M$  with  $i(S)^\perp = K$ ,  $i'(S)^\perp = K' \simeq K$  induced by  $\psi, \psi' : H \rightarrow \text{dg}_M$ . These give rise to a diagram such as (15.9) where  $\lambda' : \text{dg}_K \xrightarrow{\sim} \text{dg}_{K'}$  is the isometry induced by  $\lambda$ . The rightmost vertical isometry,  $\gamma_{K'}^{-1} \circ \lambda' \circ \gamma_K$ , making the diagram commutative, comes from an isometry  $K \simeq K'$ . So the comparison conditions of Proposition 15.3.1 are fulfilled. □

*Remark 15.3.4.* Observe that for a non-degenerate quadratic lattice  $S$ , and  $L$  unimodular, taking  $H_S = 0$ , Theorem 15.2.6 and Corollary 15.3.3 give identical conditions.

**Examples 15.3.5. 1.** Consider the action of  $O(M)$  on vectors  $x \in M$  of given length, say  $q(x) = p^k$  where  $p$  is an odd prime. In this case  $S = \langle 2p^k \rangle$  and  $dg_S \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/p^k\mathbb{Z}$ . If the Sylow-decomposition of  $dg_M$  does not contain 2-primary or  $p$ -primary components, the only possibility for  $H_S$  is the trivial group and then  $dg_K = -dg_M$ . The two conditions of Corollary 15.3.3 hold if for instance  $\ell(dg_M) \leq \text{rank}(M) - 3$ .

**2.** Let  $M = L \oplus L'(-2)$  with  $L$  and  $L'$  indefinite unimodular quadratic lattices. Consider the  $O(M)$ -orbits of vectors  $x \in M$  with  $q(x) = -2$ . Then  $S = \langle -4 \rangle$  and hence  $dg_S = \frac{1}{4}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z}$ . So  $H_S = 0$  or  $H_S = \mathbb{Z}/2\mathbb{Z}$ . By the classification of even indefinite unimodular forms as given in Section 2.4, the lattice  $M$  splits off  $U \oplus U(-2)$ , and so the lattice  $K = S^\perp$  is indefinite of rank  $\geq 3$ . As follows from Example 1.6.8.2 and 11.2.5.3, the discriminant quadratic form of  $L'(2)$  is isometric to a number of copies of  $u_1$ , say  $\oplus^m u_1$ , where  $2m = \text{rank}(L')$ .

If  $H_S = 0$ ,  $q_K^\# = q_{L'(2)}^\#$  which splits off a copy of  $u_1$  and hence Theorem 14.5.5 shows that conditions 2 and 3 are satisfied. Condition 1 being trivially satisfied, the preceding theorem shows that there is a unique orbit of  $x$  of this type. Since  $L$  contains a copy of  $U$ , the orbit contains  $e - 2f$ , where  $\{e, f\}$  is the standard basis of  $U$ . This deals with the case  $H_S = 0$ .

Assume now that  $H_S = \mathbb{Z}/2\mathbb{Z}$ . We can view  $dg_M$  as a symplectic  $\mathbb{F}_2$ -space and so by an argument as in the proof of Proposition A.5.2 we may assume that  $H_S$  embeds in the first copy of  $u_1$  as  $\langle \bar{e} + \bar{f} \rangle$ , where  $\{\bar{e}, \bar{f}\}$  is the standard basis of  $u_1$ . Then  $q_K^\# \simeq \langle 2^{-1} \rangle \oplus^{m-1} u_1$ . In this case

$$\ell(dg_K) = \text{rank}(L') - 1 = \text{rank}(M) - \text{rank}(L) - 1 \leq \text{rank}(M) - 3,$$

and hence conditions 2 and 3 are satisfied.

Note that the two types of orbits of  $x$  can be characterized as follows: for  $H_S = 0$  one must have  $x \cdot M = \mathbb{Z}$  (since  $x$  can be assumed to be in the unimodular lattice  $L$ ). For  $H_S = \mathbb{Z}/2\mathbb{Z}$  for similar reasons one must have  $x \cdot M = 2\mathbb{Z}$ .

## 15.4 On Embeddings into Odd Unimodular Lattices

Let  $S$  be a non-degenerate symmetric lattice of signature  $(s_+, s_-)$ . We want to investigate whether  $S$  can be primitively embedded in some *odd* unimodular lattice  $L$ , say of signature  $(r_+, r_-)$ . As in the even case, a necessary condition is  $s_\pm \leq r_\pm$ . We consider two cases:

**Case 1:  $S$  or  $T = S^\perp$  is odd, where  $S$  is assumed to be primitively embedded in some odd unimodular lattice  $L$ .** For the sake of the argument, we assume that  $S$  is odd and search for conditions that  $T$  be odd, respectively even. Taking into account that, by Proposition 15.1.1,  $b_S^\# \simeq -b_T^\#$ , one sees that the following analog of Proposition 15.2.1 holds (with analogous proof, but now also invoking Corollary 12.5.14):

**Proposition 15.4.1.** *Let  $(r_+, r_-)$  be a pair of non-negative integers and let  $S$  be*



a non-degenerate odd lattice of signature  $(s_+, s_-)$  with  $s_+ \leq r_+$  and  $s_- \leq r_-$  and discriminant bilinear form  $\mathbf{b}^\#$ . The following conditions are equivalent.

1.  $S$  can be primitively embedded in some odd unimodular lattice  $L$  of signature  $(r_+, r_-)$  and such that  $T = S^\perp$  is odd, respectively even;
2. A (non-degenerate) odd, respectively even lattice  $T$  of signature  $(r_+ - s_+, r_- - s_-)$  with discriminant form  $-\mathbf{b}^\#$ ;
3. A (non-degenerate) odd respectively even lattice  $T'$  of signature  $(r_- - s_-, r_+ - s_+)$  with discriminant form  $\mathbf{b}^\#$  exists.

If, moreover, both  $r_+ > 0$  and  $r_- > 0$ , the unimodular lattice  $L$  is unique up to isometry.

These conditions hold in particular if  $\ell(\mathrm{dg}_S) \leq \mathrm{rank}(L) - \mathrm{rank}(S) - 3$ .

**Case 2:  $S$  and  $T$  are both even.** Proposition 15.1.1 in addition forces the existence of an isomorphism  $\theta : \mathrm{dg}_S \xrightarrow{\sim} \mathrm{dg}_T$  with  $b_S^\# \circ \theta(-, -) = -b_T^\#(-, -)$ , but for which  $q_S^\# \circ \theta \neq -q_T^\#$ , since otherwise  $L$  would be even. This implies that we need the inclusion  $\mathrm{O}(q_S^\#) \hookrightarrow \mathrm{O}(b_S^\#)$  to be strict. These considerations then imply:

**Proposition 15.4.2.** *Let  $(r_+, r_-)$  be a pair of non-negative integers and let  $S$  be a non-degenerate even lattice of signature  $(s_+, s_-)$  with  $s_+ \leq r_+$  and  $s_- \leq r_-$ , discriminant quadratic form  $q^\#$  with polar form  $\mathbf{b}^\#$ . The following conditions are equivalent.*

1.  $S$  can be primitively embedded in some odd unimodular lattice  $L$  of signature  $(r_+, r_-)$  and such that  $T = S^\perp$  is even;
2. Either  $r_+ - r_- \not\equiv 0 \pmod{8}$ , or else,  $\mathrm{O}(q^\#)$  is properly included in  $\mathrm{O}(b^\#)$  and a (non-degenerate) even lattice  $T$  of signature  $(r_+ - s_+, r_- - s_-)$  with discriminant form  $-\mathbf{b}^\#$  exists;
3. Either  $r_+ - r_- \not\equiv 0 \pmod{8}$ , or else,  $\mathrm{O}(q^\#)$  is properly included in  $\mathrm{O}(b^\#)$  and a (non-degenerate) even lattice  $T'$  of signature  $(r_- - s_-, r_+ - s_+)$  with discriminant form  $\mathbf{b}^\#$  exists.

If, moreover, both  $r_+ > 0$  and  $r_- > 0$ , the unimodular lattice  $L$  is unique up to isometry.

These conditions hold if  $\ell(\mathrm{dg}_S) \leq \mathrm{rank}(L) - \mathrm{rank}(S) - 3$  and either  $\tau(L)$  is not divisible by 8 or  $\mathrm{O}(q_S^\#)$  is properly included in  $\mathrm{O}(b_S^\#)$

**Examples 15.4.3. 1.**  $L = \mathbb{Q}^{a+b}\langle 1 \rangle \oplus \mathbb{Q}^{b+c}\langle -1 \rangle$ , where  $a, b, c > 0$  and let  $S = \mathbb{Q}^a\langle 1 \rangle \oplus \mathbb{Q}^b\langle A_1(-2) \rangle$ . Then  $\mathrm{rank}(L) - \mathrm{rank}(S) = b + c = \ell(\mathrm{dg}_S) + c$  and so, if  $c \geq 3$ ,  $S$  can be primitively embedded in  $L$  with  $S^\perp$  odd or even.

**2.** Let  $L = \mathbb{Q}^{a+b}\langle 1 \rangle \oplus \mathbb{Q}^{b+c}\langle -1 \rangle$ ,  $a, b, c > 0$  with  $a \equiv c \pmod{8}$ . Let  $S$  be an even unimodular lattice of signature  $(a, c)$ . Then  $S$  cannot be embedded in  $L$  with even orthogonal complement, but if  $a + c \geq 3$  the lattice  $S$  can be embedded in  $L$  with  $S^\perp = \mathbb{Q}^b\langle 1 \rangle \oplus \mathbb{Q}^b\langle -1 \rangle$ . If instead  $S = \mathbb{Q}^b U(2)$ , then  $b_S^\# \simeq \mathbb{Q}^b \mathbf{u}_1$  is

isometric to a symplectic form  $b_q$  on an  $\mathbb{F}_2$ -vector space of rank  $2b$  and hence  $O(q)$  is strictly contained in  $O(b_q)$ . Such  $S$  can be embedded in  $L$  with even orthogonal complement as soon as  $2b \leq a + c - 3$ .

Recall that using Theorem 14.5.5, the existence criterion Corollary 12.4.6 for even lattices yields Theorem 15.2.6, which is a version of Witt's extension theorem for embeddings in even unimodular lattices. Similarly, using the above existence criterion for odd lattices one deduces a version of Witt's theorem for embeddings of odd or even lattices  $S$  in indefinite odd unimodular lattices. We only state the version for  $S$  odd, leaving the even case to the reader:

**Theorem 15.4.4.** *Let  $L$  be an indefinite odd unimodular lattice and  $S$  a non-degenerate odd lattice with  $\ell(\mathbf{dg}_S) \leq \text{rank}(L) - \text{rank}(S) - 3$ . Then  $S$  admits a primitive embedding into  $L$  and such primitive embeddings are unique up to equivalence, i.e.,  $O(L)$  acts transitively on primitive embeddings of  $S$  in  $L$ . Furthermore, for each primitive embedding of  $S$  with  $T = S^\perp$  odd, respectively even,  $T$  has genus invariant  $(r_+ - s_+, r_- - s_-, [-b_S^\#])$ , respectively  $(r_+ - s_+, r_- - s_-, [-q_S^\#])$ , where  $(r_+, r_-)$ ,  $(s_+, s_-)$  are the signatures of  $L$  and  $S$ , respectively.*

**Historical and Bibliographical Notes.** The material of this chapter is largely based on V. Nikulin's results from [171]. The embedding results are generalizations of much older results of C.T.C. Wall [244] and of D.G. James [109].

---

## The Structure of Orthogonal Groups I, Vector spaces

### Introduction

The first three sections of this chapter are devoted to isometries of vector spaces. In Section 16.1 sign structures are considered in relation to the spinor norm. In Section 16.2 special attention is given to characteristic 2 where a proper definition of a rotation is given with the help of the Dickson invariant. We determine the size of the orthogonal groups over finite fields in Section 16.3 along the lines of [122, §13].

In Section 16.4 we give an application of the Arf invariant to the classical subject of theta characteristics. These have been widely studied in relation to theta functions. We give a very short synopsis of this vast subject. We discuss also the connection with the 28 bitangents of a plane quartic curve.

### 16.1 Vector Space Isometries and Sign Structures

Let  $(V, b)$  be a real inner product space and write  $q(x) = \frac{1}{2}b(x, x)$  so that  $b$  is the polar form of  $q$ . Recall (cf. Section 7.1) that by definition rotations have determinant 1 and constitute the group  $SO(V)$ , while an isometry  $g \in O(V)$  with  $\det(g) = -1$  is called a reflection. Special examples of reflections are the hyperplane reflections  $\sigma_x$  given by

$$v \xrightarrow{\sigma_x} v - \frac{b(x, v)}{q(x)}x, \quad q(x) \neq 0.$$

We come back to the reduced orthogonal group, i.e., the kernel of the real spinor norm,

$$O^+(V) = \{g \in O(V) \mid \text{Nm}_{\text{spin}} g = 1\}.$$

Recall that  $\text{Nm}_{\text{spin}} g$  can be calculated upon writing  $g = \sigma_{x_1} \circ \cdots \circ \sigma_{x_r}$  as a product of hyperplane reflections (see (13.12)) and then  $\text{Nm}_{\text{spin}} g = q(x_1) \cdots q(x_r)$  up to squares. So the real spinor norm only takes at most two values which for brevity are identified with the real numbers 1 and  $-1$  which represent their classes.

A signed variant of the spinor norm turns out to be useful. The real spinor norm of  $g = \sigma_{x_1} \circ \cdots \circ \sigma_{x_r}$  is 1 precisely if  $q(x_j) < 0$  for an even number of indices. Note that for rotations  $g$  then also  $q(x_j) > 0$  for an even number of indices, but for

reflections there is a difference which leads to a useful distinction: one can impose that the number of indices  $j$  for which  $q(x_j) < 0$  is even or that the number of indices  $j$  for which  $q(x_j) > 0$  is even. This leads to the *signed spinor norm*, also called  $\epsilon$ -*spinor norm*, where  $\epsilon \in \{+1, -1\}$ :

$$\text{Nm}_{\text{spin}}^\epsilon(\sigma_{x_1} \circ \dots \circ \sigma_{x_r}) = \begin{cases} 1 & \text{if } \#\{j \in \{1, \dots, r\} \mid \epsilon q(x_j) < 0\} \text{ is even} \\ -1 & \text{otherwise.} \end{cases} \quad (16.1)$$

So, for rotations  $g$  we have  $\text{Nm}_{\text{spin}}^+(g) = \text{Nm}_{\text{spin}}^-(g)$  and for reflection  $\text{Nm}_{\text{spin}}^+(g) = -\text{Nm}_{\text{spin}}^-(g)$ . Since these cardinalities depend only on the determinant and the ordinary spinor norm, this definition is independent of the way  $g$  is decomposed into hyperplane reflections. We immediately deduce:

**Lemma 16.1.1.** *Let  $(V, q)$  be a quadratic vector space and let  $x \in V$  and  $\epsilon \in \{1, -1\}$  be such that the sign of  $q(x)$  equals  $\epsilon$ . Then  $\text{Nm}_{\text{spin}}^\epsilon(\sigma_x) = 1$ .*

The signed spinor norm is a homomorphism, as can be easily seen from the definition, and so its kernel is a group

$$\text{O}^\epsilon(V) := \{g \in \text{O}(V) \mid \text{Nm}_{\text{spin}}^\epsilon(g) = 1\}.$$

This notation is consistent with the previous definition of the spinor norm (cf. (13.11)) since for  $\epsilon = +1$ , one has  $\text{Nm}_{\text{spin}}^\epsilon(g) = \text{Nm}_{\text{spin}}(g)$  and hence  $\text{O}^+(V)$  has the same meaning as in Equation (13.12).

By convention we shall use  $\text{Nm}_{\text{spin}}^\epsilon$  if  $q$  is an  $\epsilon$ -definite form, that is, if  $q(\epsilon)$  is positive definite. Hence the  $\epsilon$ -spinor norm is equal to 1 for isometries of  $\epsilon$ -definite forms.

For indefinite forms  $\text{Nm}_{\text{spin}}^\epsilon$  makes it possible to focus solely on the contribution of “positive” reflections  $\sigma_x$ , that is, for which  $q(x) > 0$ , by switching between  $V$  and  $V(-1)$ . Indeed, automorphisms of  $V$  that preserve  $q$  also preserve  $q(-1)$  but the  $+1$ -spinor norm for  $q$  corresponds to the  $(-1)$ -spinor norm for  $q(-1)$ . This is especially useful when dealing with Picard–Lefschetz reflections (see Section 18.2).

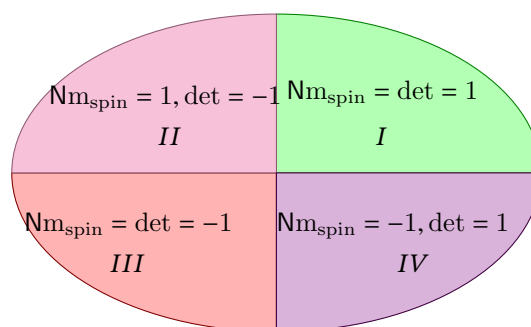
Next, in the case of indefinite forms, we shall give an alternative way to describe the above subgroups using  $q^\pm$ -orientations, also called *sign structures*. To define these, recall that all maximal subspaces of  $V$  on which  $q > 0$  or  $q < 0$  have the same dimension, say  $n_+ > 0$ , respectively  $n_- > 0$  (Sylvester’s law, Corollary 8.1.3). The relevant Grassmann variety

$$\text{G}(V) = \{W \subset V \mid \dim W = n_+, \quad q|_W > 0\} \simeq \{W' \subset V \mid \dim W' = n_-, \quad q|_{W'} < 0\},$$

is a differentiable manifold. To see this, remark that  $\text{G}(V)$  is homogeneous under the Lie group  $G = \text{O}(V, q) \simeq \text{O}(n_+, n_-)$  with isotropy group (isomorphic to)  $\text{O}(n_+) \times \text{O}(n_-)$ . This manifold is connected since by Proposition 13.3.7 the group  $\text{O}(n_+, n_-)$  has four components each containing one of the four components of  $\text{O}(n_+) \times \text{O}(n_-)$ . We use this to explain the notions of a  $q^+$ - and  $q^-$ -orientation. Recall that an *orientation* of a vector space  $W$  is an equivalence class of ordered bases of  $W$  where two ordered bases define the same orientation if and only if they are related

by a linear transformation with positive determinant. A vector space of dimension  $> 0$  has two orientations. Choosing an orientation for a maximal subspace on which  $q > 0$  induces an orientation on all such subspaces since  $G(V)$  is connected. A choice of such a coherent system of orientations is called a  $q^+$ -*orientation*. Switching to the second description for the Grassmann variety  $G(V)$ , one obtains the definition of a  $q^-$ -*orientation*.

Figure 16.1.1



Giving  $V$  both a  $q^+$ - and a  $q^-$ -orientation amounts to giving  $V$  an orientation. The four components of  $O(n_+, n_-)$  can be described using the homomorphism  $(Nm_{\text{spin}}, \det)$  on  $O(n_+, n_-)$  as in Figure 16.1.1. The corresponding subgroups of  $O(n_+, n_-)$  all contain the connected component of the identity which is component  $I$ . The subgroup of rotations is the union of components  $I$  and  $IV$ . A further description of the components is as follows.

**Lemma 16.1.2.** *Let  $n_{\pm}$  be positive (i.e., the form is indefinite).*

1. *The connected component of  $O(n_+, n_-)$  is the group  $SO^+(n_+, n_-)$ . It is the subgroup of  $O(n_+, n_-)$  preserving a given  $q^+$ -orientation as well as a given  $q^-$ -orientation.*
2. *The group  $O^+(n_+, n_-)$  of spinor norm 1 elements is the subgroup of  $O(n_+, n_-)$  preserving a given  $q^-$ -orientation. It is the union of the components  $I$  and  $II$  in Figure 16.1.1.*
3. *The subgroup of elements with  $Nm_{\text{spin}}^- = 1$  is the subgroup of  $O(n_+, n_-)$  preserving a given  $q^+$ -orientation. It is the union of the components  $I$  and  $III$ .*

*Proof.* 1. Since  $O(n_+, n_-)$  has four components and since by Remark 13.3.6.2 the map  $(Nm_{\text{spin}}, \det)$  is continuous, its kernel is connected. This is precisely  $SO^+(n_+, n_-)$ . The second assertion of item 1 will be shown after we investigate the relation with the  $q^{\pm}$ -orientations.

2 and 3. Consider a vector  $x$  belonging to a maximal subspace  $W$  on which  $q > 0$ . Since  $\sigma_x$  changes the orientation of  $W$ , we see that  $\sigma_x$  switches the two distinct

$q^+$ -orientations. The hyperplane orthogonal to  $x$  contains some maximal subspace  $W'$  with  $q|_{W'} < 0$  and so  $\sigma_x$  preserves the orientation of  $W'$ , i.e.,  $\sigma_x$  preserves  $q^-$ -orientations. Similarly, if  $q(y) < 0$  the reflection  $\sigma_y$  switches  $q^-$ -orientations and preserves the  $q^+$ -orientations.

An isometry  $g \in O(n_+, n_-)$  preserves  $q^-$ -orientations if and only if  $g$  is a product of an even number of reflections  $\sigma_x$  with  $q(x) < 0$ , which is equivalent to  $\text{Nm}_{\text{spin}} g = 1$ . This completes the proof of 2.

Using  $\text{Nm}_{\text{spin}}^-$  a similar assertion holds for isometries preserving  $q^+$ -orientations, showing item 3.

Since  $\text{SO}^+(n_+, n_-)$  is the intersection of the groups described in items 2 and 3, this entails the remaining assertion of 1.  $\square$

Let us consider the special case of a hyperbolic vector space whose definition we recall. Suppose  $V$  has a basis  $\{e_0, e_1, \dots, e_n\}$  such that the polarization of the quadratic form is given by

$$x \cdot y = x_0 y_0 - \sum_{i=1}^n x_i y_i, \quad x = \sum_{i=0}^n x_i e_i, \quad y = \sum_{i=0}^n y_i e_i.$$

We call  $V$  with this inner product a *hyperbolic vector space*.

**Lemma 16.1.3.** *Let  $V$  be a hyperbolic vector space. The "light cone"  $\{x \in V \mid x \cdot x > 0\}$  is a disjoint union  $C_V \cup -C_V$  of two convex cones where  $C_V$  is contained in the half space  $x_0 > 0$ . For points  $x, y$  in the light cone we have:*

$$x \cdot y > 0 \iff x, y \in C_V \text{ or } x, y \in -C_V. \quad (16.2)$$

If  $x \neq 0$  and  $x \in \overline{C_V}$ ,  $y \in C_V$ , then we still have  $x \cdot y > 0$ .

*Proof.* To prove (16.2), it suffices to prove the "if"-part. We use that  $x_0 > \sqrt{x_1^2 + \dots + x_n^2}$  for  $x \in C_V$ . Then combine this with the Cauchy-Schwarz inequality  $\sum_{i=1}^n x_i y_i \leq \sqrt{x_1^2 + \dots + x_n^2} \cdot \sqrt{y_1^2 + \dots + y_n^2}$ . If  $x \neq 0$  and  $x \in \overline{C_V}$ , then  $0 < x_0 = \sqrt{x_1^2 + \dots + x_n^2}$ . From  $y_0 > \sqrt{y_1^2 + \dots + y_n^2}$  we then infer  $x \cdot y > 0$  in this case as well.

Using the equivalence (16.2), convexity of  $C_V$  follows from a straightforward computation involving  $(tx + (1-t)y) \cdot (tx + (1-t)y)$  and  $tx_0 + (1-t)y_0 > 0$ ,  $0 \leq t \leq 1$ .  $\square$

Observe that positive lines, i.e., lines on which the form is positive definite, are exactly those lines that, apart from the origin, belong to the light cone. Hence the subgroup of the Lorentz group  $O(1, n)$  preserving the components of the light cone is the subgroup preserving a fixed orientation of such lines, that is the subgroup of isometries with  $\text{Nm}_{\text{spin}}^- = 1$ :

$$O^-(V) = \{g \in O(V) \mid g(C_V) \subset C_V\}. \quad (16.3)$$

## 16.2 Orthogonal Groups in Characteristic Two

Let  $(V, q)$  be a quadratic space over a field  $k$  of characteristic 2. Non-degeneracy of  $q$  means that  $b_q$  has zero radical and so  $b_q$  is a non-degenerate symplectic form which implies that  $\dim V$  is even, say  $\dim V = 2n$  (see also Section 8.2). Let the corresponding symplectic basis be  $\mathbf{E} = \{e_1, \dots, e_{2n}\}$  and let the quadratic form in this basis be  $q = \sum_{j=1}^n x_j x_{n+j} + \sum_{j=1}^{2n} a_j x_j^2$ . Proposition 13.1.5 implies that the vector

$$\mathbf{z}_E = e_1 e_{n+1} + \dots + e_n e_{2n} \in C^0(q)$$

together with 1 spans the center of the even Clifford algebra  $C^0(q)$ . Moreover, we established in Proposition 13.1.5 a relation involving the Arf invariant:

$$\mathbf{z}_E^2 + \mathbf{z}_E = \text{arf}(q), \quad \text{where } \text{arf}(q) \equiv \sum_{i=1}^n a_i a_{n+i} \pmod{\wp(k)}. \quad (16.4)$$

Recall that  $C(q)$  is generated by 1 and the vector space basis  $\mathbf{E}$ , with relations

$$\begin{cases} e_i^2 &= a_i, & i = 1, \dots, 2n \\ e_i e_j &= e_j e_i, & e_{i+n} e_{j+n} = e_{j+n} e_{i+n}, & i, j = 1, \dots, n \\ e_i e_{n+j} + e_{n+i} e_j &= \delta_{ij}, & i, j = 1, \dots, n. \end{cases} \quad (16.5)$$

We shall aim at finding a criterion for a symplectic transformation  $s$  to preserve  $q$ . Since  $s$  preserves symplectic bases for  $V$ , the elements  $s(e_i)$ ,  $i = 1, \dots, 2n$ , form a system of generators for the Clifford algebra  $C^0(q)$  but with the relations (16.5) with respect to the transformed quadratic form  $x \mapsto q(sx)$ . The corresponding element

$$\mathbf{z}_{sE} = s(e_1)s(e_{n+1}) + \dots + s(e_n)s(e_{2n})$$

belongs to the center of  $C^0(q)$  as well and hence it can be expressed as a  $k$ -linear combination of the generators 1 and  $\mathbf{z}_E$ , say

$$\mathbf{z}_{sE} = p(s) + r(s) \cdot \mathbf{z}_E. \quad (16.6)$$

To determine the coefficients in this linear combination, write

$$s(e_i) = \sum_{j=1}^n a_{ij} e_j + \sum_{j=1}^n b_{ij} e_{j+n}, \quad s(e_{i+n}) = \sum_{j=1}^n c_{ij} e_j + \sum_{j=1}^n d_{ij} e_{j+n}.$$

In the first expression for  $\mathbf{z}_{sE}$  observe that only the combinations  $e_i^2, e_i e_{i+n}, e_{n+i} e_i$ ,  $i = 1, \dots, n$ , can occur. The relations (16.5) can be used to rewrite  $\mathbf{z}_{sE}$  as an expression involving 1 and the monomials  $e_i^2, e_i e_{n+i}$ . Taking all of this into account, this yields the searched for coefficients in the relation 16.6:

$$\begin{aligned} p(s) &= \sum_{1 \leq i, j \leq n} a_j a_{ij} c_{ij} + \sum_{1 \leq i, j \leq n} a_{j+n} b_{ij} d_{ij} + \sum_{1 \leq i, j \leq n} b_{ij} c_{ij}, \quad a_i = q(e_i). \\ r(s) &= \sum_{i=1}^n a_{i1} d_{i1} + b_{i1} c_{i1} = \dots = \sum_{i=1}^n a_{in} d_{in} + b_{in} c_{in}. \end{aligned}$$

On the other hand,  $s$  being symplectic implies that  $1 = b(s(e_i), s(e_{i+n}))$ , where  $b$  is the standard symplectic form. Writing this out gives  $1 = \sum_{i=j}^n (a_{ij}d_{ij} + b_{ij}c_{ij}) = r(s)$  and so

$$\mathbf{z}_{sE} - \mathbf{z}_E = p(s) = \sum_{1 \leq i, j \leq n} a_j a_{ij} c_{ij} + \sum_{1 \leq i, j \leq n} a_{j+n} b_{ij} d_{ij} + \sum_{1 \leq i, j \leq n} b_{ij} c_{ij}. \quad (16.7)$$

This motivates the following definition.

**Definition 16.2.1.** Let  $s$  be a symplectic transformation whose matrix with respect to  $E$  is given by

$$\begin{pmatrix} (a_{ij})_{1 \leq i, j \leq n} & (c_{ij})_{1 \leq i, j \leq n} \\ (b_{ij})_{1 \leq i, j \leq n} & (d_{ij})_{1 \leq i, j \leq n} \end{pmatrix} \in \mathrm{Sp}(n).$$

Then the *Dickson invariant* of the triple  $(q, s, E)$  is the element in the field  $k$  given by

$$D(q, s, E) = \mathbf{z}_{sE} - \mathbf{z}_E = p(s) = \sum_{1 \leq i, j \leq n} a_j a_{ij} c_{ij} + \sum_{1 \leq i, j \leq n} a_{j+n} b_{ij} d_{ij} + \sum_{1 \leq i, j \leq n} b_{ij} c_{ij}.$$

Observe that (16.7) implies

$$\begin{aligned} \wp(D(q, s, E)) &= \wp(p(s)) = \mathbf{z}_{sE}^2 + \mathbf{z}_{sE} - \mathbf{z}_E^2 - \mathbf{z}_E \\ &\equiv \mathrm{arf}(q^{(s)}) - \mathrm{arf}(q), \quad q^{(s)}(x) := q(sx), \end{aligned}$$

which gives another proof that the Arf invariant is independent of the choice of a symplectic basis. Moreover, since  $\wp(p(s)) = 0$  if and only if  $p(s) = 0$  or  $p(s) = 1$ , applying this when  $q^{(s)} = q$ , we obtain:

**Corollary 16.2.2.** *An isometry of the quadratic form  $q$  has Dickson invariant 0 or 1.*

**Example 16.2.3.** Let  $\varepsilon = t_{u,a}$  be a transvection where  $u = \sum u_i e_i$ . Comparing with (8.5) we find

$$D(q, \varepsilon, E) = a \cdot \left[ q(u) + (aq(u) + 1) \cdot \sum_{i=1}^n u_i u_{i+n} \right].$$

Of course this can also be found by direct calculation. Observe that  $\varepsilon$  preserves the quadratic form  $q$  if and only if  $q(u) = a^{-1}$ , and if so, its Dickson invariant equals 1. Such transvections are the orthogonal reflections.

We cannot expect the Dickson invariant to be additive on the entire symplectic group. In fact, writing as before  $q^{(s)}$  for the quadratic form  $x \mapsto q(sx)$ , we have

$$D(q, t \circ s, E) = D(q, s, E) + D(q^{(s)}, t, sE). \quad (16.8)$$



To see this, we use the transformation law (16.7) for  $t \circ s$  which gives  $\mathbf{z}_{ts(E)} + \mathbf{z}_E = D(q, t \circ s, \mathbf{E})$ , but since  $D(q, t, s\mathbf{E}) = \mathbf{z}_{ts(E)} + \mathbf{z}_{s\mathbf{E}}$ , one gets

$$\begin{aligned} D(q, s, \mathbf{E}) + D(q^{(s)}, t, s\mathbf{E}) &= \mathbf{z}_{s\mathbf{E}} + \mathbf{z}_E + \mathbf{z}_{ts(E)} + \mathbf{z}_{s\mathbf{E}} \\ &= \mathbf{z}_E + \mathbf{z}_{ts(E)} \\ &= D(q, t \circ s, \mathbf{E}). \end{aligned}$$

Suppose now that  $s$  is  $q$ -orthogonal. Then  $q^{(s)} = q$ . The matrix of  $t$  with respect to the basis  $s\mathbf{E}$  is the same as the matrix of  $s^{-1}ts$  with respect to  $\mathbf{E}$  and so  $D(q^{(s)}, t, s\mathbf{E}) = D(q, s^{-1}ts, \mathbf{E})$ . So, if we replace  $t$  with  $sts^{-1}$  in the formula (16.8), we obtain

$$D(q, s \circ t, \mathbf{E}) = D(q, s, \mathbf{E}) + D(q, t, \mathbf{E}).$$

So on transformations that preserve  $q$  the Dickson invariant gives an additive homomorphism  $O(q) \rightarrow \{0, 1\} = \mathbb{F}_2$ . The kernel of this homomorphism then is a subgroup of  $O(q)$  of index 2, by definition the subgroup of rotations:

**Definition 16.2.4.** Let  $(V, q)$  be a quadratic space over a field of characteristic 2. A *rotation* is an orthogonal transformation with Dickson invariant 0.

**Examples 16.2.5. 1.** Since an orthogonal transvection is just a reflection and has Dickson invariant 1, an even product of reflections is a rotation.

**2.** Consider the hyperbolic plane  $U$ . We have seen in Example 6.5.5.2 that the only isometries are  $i_a$  and  $j_b$ . These have Dickson invariant 0, respectively 1. Since  $j_1 \circ j_b = i_b$ , a rotation is a product of two reflections.

**3.** As we observed before (cf. Remark 7.2.6), almost all quadratic spaces have the property that orthogonal transformations are products of reflections and for those spaces rotations are even products of reflections. This leads to an alternative interpretation of the Dickson invariant  $D(q, s, \mathbf{E})$  for orthogonal transformations  $s$ , namely  $D(q, s, \mathbf{E}) = \dim(\text{Im}(s - \text{id})) \bmod 2$  (see [223, p. 160]). Indeed, the Dickson invariant being a homomorphism, it suffices to observe that a reflection hyperplane in a (non-degenerate) symplectic space has odd dimension.

The exceptional quadratic space is  $N \oplus N$  where  $N = \mathbb{F}_2^2$  with quadratic form  $x^2 + xy + y^2$ . The isometry  $s$  exchanging the two copies of  $N$  is not a product of two reflections. Its Dickson invariant is 0 but here again  $\dim(\text{Im}(s - \text{id}))$  is even, so the above interpretation of the Dickson invariant is uniformly valid.

**4.** Let  $k = \mathbb{F}_2$  and  $K = k(\xi)$  the unique separable quadratic extension of  $k$ . Then  $\xi^2 + \xi + 1 = 0$  and the norm form  $N_{K/k}$  is the quadratic form  $x^2 + xy + y^2$  on  $k^2$ . As we saw in § 6.3.B, example 6, multiplication with a norm 1 element  $a + b\xi$  in  $K$  gives an isometry with matrix  $M_{a,b} = \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}$  and the Dickson invariant equals  $ab + b(a+b) + b^2 = 0$ . Hence this is a rotation. We also saw that all other orthogonal transformations have matrix  $M'_{a,b} = \begin{pmatrix} a & a+b \\ b & a \end{pmatrix}$  and those have Dickson invariant equal to  $ab + a(a+b) + b(a+b) = a^2 + ab + b^2 = 1$ . So half the orthogonal transformations are rotations and the other half are not. Since  $M'_{a,b} \circ M'_{1,0} = M_{a,b}$ , also in this example all rotations are products of two reflections.

### 16.3 Orthogonal Groups of Quadratic Spaces over Finite Fields

We consider quadratic forms  $(V, q_V)$  with  $\text{rad}(q_V) = 0$  over finite fields  $k$ , referring for odd characteristics to Theorem 8.3.3 (then  $q_V$  is unimodular) and for characteristic 2 to Proposition 8.2.5 (then  $q_V$  is unimodular or semi-unimodular). Isometry classes of such forms are collected in Table 16.3.1 together with the number  $s(V)$  of isotropic vectors in the quadratic space  $V$  as well as the number  $s_\alpha(V) = \{v \in V \mid q_V(v) = \alpha\}$  for  $\alpha \neq 0$ . The number  $s(V)$  will be computed below and turns out to be an essential ingredient in the determination of the size of the orthogonal groups.

Table 16.3.1: Types of quadratic spaces

Type	isometry class	$s(V) = s_0(V) - 1$	$s_\alpha(V), \alpha \neq 0$
I	$U^{\oplus m}$	$(q^m - 1)(q^{m-1} + 1)$	$q^{2m-1} - q^{m-1}$
II	$U^{\oplus m-1} \oplus N_{K/k}$	$(q^m + 1)(q^{m-1} - 1)$	$q^{2m-1} + q^{m-1}$
III char( $k$ ) = 2	$U^{\oplus m} \oplus [a]$ semi-unimodular	$q^{2m} - 1$	$q^{2m}$
III char( $k$ ) $\neq$ 2	$U^{\oplus m} \oplus [a]$ unimodular	$q^{2m} - 1$	$q^{2m} + q^m, a^{-1}\alpha \in (k^\times)^2$ $q^{2m} - q^m, a^{-1}\alpha \notin (k^\times)^2$

We set apart the values for  $s_1(V)$  and  $s_0(V)$  for the case  $k = \mathbb{F}_2$  in Table 16.3.2.

Table 16.3.2: Values of  $s_0, s_1$  if  $q = 2$

Type	Arf invariant	$s_0(V)$	$s_1(V)$
I	0	$2^{m-1}(2^m + 1)$	$2^{m-1}(2^m - 1)$
II	1	$2^{m-1}(2^m - 1)$	$2^{m-1}(2^m + 1)$

This table shows an amusing consequence, first noted by F. Browder [31], namely it gives an alternative definition of the Arf invariant for non-degenerate quadratic forms  $q_V$  over  $\mathbb{F}_2$ : the Arf invariant is the value  $q_V$  takes on for most points of  $V$ . Therefore the Arf invariant is also called the **democratic invariant** of  $q_V$ .

The calculation of  $s(V)$  is performed by induction. So suppose  $V = U \oplus W$  with  $\dim W = n$ . Let  $\{e, f\}$  be the standard basis of  $U$  and write an isotropic vector in  $V$  as  $x \cdot e + y \cdot f + w, w \in W$ . We have the following possibilities:

- $q_W(w) = 0, xy = 0$  which gives  $2q - 1$  possibilities with  $w \neq 0$  leading to  $(2q - 1)s(W)$  possible vectors, and  $2q - 2$  in the case that  $w = 0$ ;
- $q_W(w) \neq 0$  and  $xy = q_W(w)$ . This gives  $(q^n - s(W) - 1)(q - 1)$  possibilities since  $x \in \mathbb{F}_q^\times$  together with each of the  $(q^n - 1) - s(W)$  possible vectors  $w$  determine  $y$ .

This sums up to give  $s(U \oplus W) = q \cdot s(W) + (q^n + 1)(q - 1)$ . From this one finds  $s(U^{\oplus m})$  by induction. Applying it to type II we find for  $m = 1$  the stated number

$(q^2 + 1)(q - 1)$ , and then for arbitrary  $m$  it follows by induction. For type III the proof proceeds in the same way with induction starting from  $m = 1$  with  $q^2 - 1$ .

The value of  $s(V)$  also gives the value  $s_\alpha(V)$ ,  $\alpha \in k^\times$ , the number of vectors  $x$  in  $V$  with  $q(x) = \alpha$ . In the cases I, II, and in case III for characteristic 2, this follows since then  $V(\alpha) \simeq V$  if  $\alpha \neq 0$ . This is easily verified for  $U$  – and hence for  $\bigoplus^m U$  – using the bijective map  $xe + yf \mapsto xe + y\alpha f$ ; for the surjective norm map  $N_{K/k} : K^* \rightarrow k^*$  use that the cosets of the kernel have equal size; for  $[a]$  in characteristic 2 use that  $\alpha$  is a square in  $k$ . It follows that  $s_1(V) = s_\alpha(V)$  for all  $\alpha \neq 0$ . Hence, if  $n = \dim V$ , we have

$$s_\alpha(V) = \frac{q^n - s_0(V)}{q - 1} = \frac{q^n - 1 - s(V)}{q - 1}, \quad \alpha \neq 0.$$

For case III, characteristic  $p \neq 2$ , this is slightly more involved since the result depends on whether  $\alpha^{-1}\alpha$  is a square or a non-square. The square case is as before, but for the non-square case the calculation is a bit different. See [122, §13] for details.

We next calculate  $O(V)$  for the various types, again using the method of splitting off a hyperbolic plane. By Remark 7.2.9.2 the Witt extension theorem holds for isotropic vectors and so  $O(V)$  acts transitively on these. Suppose as before that  $V = U \oplus W$  with  $\dim W = n$  and  $\{e, f\}$  the standard basis of  $U$ . It follows that

$$|O(V)| = s(V) \cdot |O_e(V)|.$$

Decompose  $\gamma \in O_e(V)$  according to  $U \oplus W$  (here we also use the polar form):

$$\gamma = \left( \begin{array}{cc|c} 1 & -q(\mathbf{w}) & \phi^T \mathbf{w} \\ 0 & 1 & 0 \\ \hline 0 & \mathbf{w} & \phi \end{array} \right), \quad \mathbf{w} \in W, \phi \in O(W).$$

Hence  $|O_e(V)| = q^n \cdot |O(W)|$ . To start the induction we have to calculate the number of elements in  $O(W)$  for  $W = N_{K/k}$  and for  $[a]$ . For the norm form we do this separately for even and odd characteristics using the remarks in § 6.3.B, example 4, respectively Examples 16.2.5.

Case 1:  $p$  odd. The rotations correspond precisely to the elements of norm 1. There are exactly  $(q^2 - 1)/(q - 1) = q + 1$  of those and so  $|O(N_{K/k})| = 2(q + 1)$ .

Case 2:  $p = 2$ . Here rotations have Dickson invariant 0 and form a subgroup of index 2 in the group of all orthogonal transformations and so the same result holds.

For one-dimensional spaces the isometries are just multiplication by  $\pm 1$  which explains the difference in the results for odd and even characteristics in the next table. The results in this table are calculated inductively as before.

isometry class $V$	$ O(V) $
$U^{\oplus m}$	$2q^{m(m-1)}(q^m - 1) \prod_{i < m} (q^{2i} - 1)$
$U^{\oplus m-1} \oplus N_{K/k}$	$2q^{m(m-1)}(q^m + 1) \prod_{i < m} (q^{2i} - 1)$
$U^{\oplus m} \oplus [a]$	$q^{m^2} \prod_{i \leq m} (q^{2i} - 1) \cdot \begin{cases} 2 & \text{if char}(k) \neq 2 \\ 1 & \text{if char}(k) = 2. \end{cases}$

## 16.4 Application: Theta Characteristics

This section comprises some preliminaries on curves, divisors and theta functions before, in Subsection 16.4.D, we apply the theory of quadratic forms over the field  $\mathbb{F}_2$ . For background on curves the reader may consult e.g. [2, Ch. 1], [88, Ch. 2].

**16.4.A Curves and divisors.** We start by recalling some basic properties of divisors on smooth curves. On a smooth curve  $C$ , a divisor is just a formal finite sum  $D = \sum n_x x$ ,  $n_x \in \mathbb{Z}$ ,  $x \in C$ . The union of all points  $x \in C$  for which  $n_x \neq 0$  is called the support of  $D$ , the sum,  $\sum n_x$  its degree. The set of divisors admits an obvious addition, making it into an abelian group. A non-zero rational function  $f$  on  $C$  defines a divisor  $\text{div}(f) = (f)_0 - (f)_\infty$ , where  $(f)_0$ ,  $(f)_\infty$  is the zero divisor, respectively the pole divisor of  $f$ . Such a divisor has degree 0. Two divisors  $D_1, D_2$  are linearly equivalent if  $D_1 - D_2 = \text{div}(f)$  for some rational function  $f$ . This is indeed an equivalence relation. The **Picard group** of  $C$  is the group of divisors modulo linear equivalence. The equivalence class of the divisor  $D$  is usually denoted by  $[D]$ . Classes of degree  $d$  divisors make up the subset  $\text{Pic}^d(C)$  of the Picard group. This is not a subgroup, unless  $d = 0$ , but a principal homogeneous space under  $\text{Pic}^0(C)$ , since, fixing any degree  $d$  divisor  $D_0$ , we have  $\text{Pic}^d(C) = [D_0] + \text{Pic}^0(C)$ . The group  $\text{Pic}^0(C)$  is called the **Picard variety**. It is known to be an abelian variety of dimension equal to the genus of  $C$  as we shall explain in Subsection 16.4.B.

For a rational function  $f$  on  $C$  with support disjoint from the support of  $D$  we define

$$f(D) := \prod_{x \in \text{support } D} f(x)^{n_x} \in \mathbb{C}^\times.$$

This is well behaved under morphisms: if  $\varphi : C \rightarrow C'$  is a morphism and  $f : C' \rightarrow \mathbb{P}^1$  a non-constant rational function on  $C'$ ,  $D$  a divisor on  $C$ , then  $f_*\varphi(D) = f(\varphi_*(D))$  whenever this makes sense. Here  $\varphi_*$  is the push forward of divisors on  $C$  to divisors on  $C'$ . **Weil reciprocity** follows from this: for all rational functions  $f$  and  $g$  whose supports are disjoint,

$$f(\text{div}(g)) = g(\text{div}(f)),$$

since on  $\mathbb{P}^1$  this is obvious and every curve maps to  $\mathbb{P}^1$ .

**16.4.B The jacobian.** The Picard variety is an abelian variety. Let us sketch how this can be shown. One first introduces  $J(C)$ , the **jacobian** of  $C$ , which is defined in a Hodge theoretic manner: One sets

$$J(C) = H^0(C, \Omega_C^1)^* / \iota(H_1(C, \mathbb{Z})),$$

where  $\iota$  send a class of a one-cycle  $\gamma$  to the functional on holomorphic one-forms  $\omega$  given by integration, i.e.  $\omega \mapsto \int_\gamma \omega$ . This is well defined (Stokes' theorem) and it turns out that the image of  $\iota$  is a discrete subgroup of rank  $2g$  of the  $g$ -dimensional complex vector space  $H^0(C, \Omega_C^1)^*$ , where  $g$  is the genus of  $C$ . Hence

$J(C)$  is indeed a torus. Using a symplectic basis  $\{\gamma_1, \dots, \gamma_{2g}\}$  for  $H_1(C, \mathbb{Z})$ , a basis  $\{\omega_1, \dots, \omega_g\}$  for  $H^0(C, \Omega_C^1)$  exists so that the matrix of periods  $(\omega_{ij})$ ,  $\omega_{ij} = \int_{\gamma_j} \omega_i$ ,  $i = 1, \dots, g, j = 1, \dots, 2g$ , has the shape  $(\mathbf{1}_g, Z)$  with  $Z$  symmetric and  $\text{Im}(Z)$  positive definite.

Divisors on tori such as  $J(C)$  come from holomorphic functions  $f$  on  $\mathbb{C}^g$  which are quasi-periodic with respect to the lattice  $\Gamma$  defining the torus, that is, for all  $\gamma \in \Gamma$  and  $\mathbf{z} \in \mathbb{C}^g$ , one has  $f(\mathbf{z} + \gamma) = \varphi_\gamma(\mathbf{z})f(\mathbf{z})$  for some non-vanishing holomorphic function  $\varphi_\gamma$ . The classical theta functions give an abundance of such functions. The simplest is **Riemann's theta function**  $\theta_Z$ , a quasi-periodic function on  $\mathbb{C}^g$  defined by the everywhere convergent series

$$\theta_Z(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{Z}^g} \exp 2\pi i \left[ \mathbf{x} \cdot (\mathbf{z} + \frac{1}{2}Z\mathbf{x}) \right], \quad \mathbf{z} \in \mathbb{C}^g, \quad (16.9)$$

where the standard dot product on  $\mathbb{C}^g$  has been used. We shall also be using a variant, the theta functions with characteristics  $\varepsilon_1, \varepsilon_2 \in \mathbb{R}^g$  which are obtained from Riemann's theta function (16.9) by replacing  $\mathbf{x}$  with  $\mathbf{x} + \varepsilon_1$  and  $\mathbf{z}$  with  $\mathbf{z} + \varepsilon_2$ :

$$\theta_Z \left[ \begin{smallmatrix} \varepsilon_1 \\ \varepsilon_2 \end{smallmatrix} \right] (\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{Z}^g} \exp 2\pi i \left[ (\mathbf{x} + \varepsilon_1) \cdot (\mathbf{z} + \varepsilon_2 + \frac{1}{2}Z(\mathbf{x} + \varepsilon_1)) \right], \quad \mathbf{z} \in \mathbb{C}^g. \quad (16.10)$$

We state some basic properties we need:

**Properties 16.4.1.** 1.  $\theta_Z \left[ \begin{smallmatrix} \varepsilon_1 \\ \varepsilon_2 \end{smallmatrix} \right]$  is the translate of Riemann's theta function by the vector  $Z\varepsilon_1 + \varepsilon_2$  up to a multiplicative factor which is a function of  $\mathbf{z}$ .

2. If  $k_1, k_2 \in \mathbb{Z}^g$ , then  $\theta_Z \left[ \begin{smallmatrix} \varepsilon_1 + k_1 \\ \varepsilon_2 + k_2 \end{smallmatrix} \right] = \theta_Z \left[ \begin{smallmatrix} \varepsilon_1 \\ \varepsilon_2 \end{smallmatrix} \right]$ .

3. One has the symmetry relation  $\theta_Z \left[ \begin{smallmatrix} \varepsilon_1 \\ \varepsilon_2 \end{smallmatrix} \right](-\mathbf{z}) = \exp 4\pi i [\varepsilon_1 \cdot \varepsilon_2] \cdot \theta_Z \left[ \begin{smallmatrix} \varepsilon_1 \\ \varepsilon_2 \end{smallmatrix} \right](\mathbf{z})$ . If  $\varepsilon_1, \varepsilon_2 \in \frac{1}{2}\mathbb{Z}^g$ , then  $\exp 4\pi i [\varepsilon_1 \cdot \varepsilon_2] \in \{1, -1\}$ . In particular,  $\theta_Z(\mathbf{z}) = \theta_Z(-\mathbf{z})$ .

*Proof.* 1. This follows by comparing the expressions for  $\theta_Z \left[ \begin{smallmatrix} \varepsilon_1 \\ \varepsilon_2 \end{smallmatrix} \right](\mathbf{z})$  and for  $\theta_Z(\mathbf{z} + Z\varepsilon_1 + \varepsilon_2)$ .

2. Replacing the summation over  $\mathbf{x} \in \mathbb{Z}^g$  with  $\mathbf{x} + k_1$  takes care of the first characteristic while  $\exp 2\pi i k_2 = 1$  takes care of the second.

3. From the expression (16.10) one sees that replacing  $\mathbf{z}$  with  $-\mathbf{z}$  can be counteracted if we replace  $\mathbf{x} + \varepsilon_1$  with  $-\mathbf{x} - \varepsilon_1$  except that the factor  $\exp 2\pi i [-\varepsilon_1 \cdot \varepsilon_2]$  comes up which differs from the factor we started with,  $\exp 2\pi i [\varepsilon_1 \cdot \varepsilon_2]$ . The factor  $\exp 4\pi i [\varepsilon_1 \cdot \varepsilon_2]$  corrects this. If  $\varepsilon_1$  and  $\varepsilon_2$  are half integral vectors, their dot product takes values in  $\frac{1}{4}\mathbb{Z}$  which means that the factor  $\exp 4\pi i [\varepsilon_1 \cdot \varepsilon_2]$  gives a sign.  $\square$

The zero locus on  $J(C)$  of Riemann's theta function is the so-called **theta divisor**  $\Theta$ . Referring to [88, Ch. II.7] for proofs, we state some of its properties:<sup>1</sup>

- $h^0(\mathcal{O}_{J(C)}(\Theta)) = 1$ , i.e., up to a multiplicative constant  $\theta_Z$  is the unique section of the line bundle  $\mathcal{O}_{J(C)}(\Theta)$ .
- $\theta_Z(0) \neq 0$ .

<sup>1</sup>We use the standard convention that  $h^i(V)$  stands for  $\dim H^i(V)$ .

- $\Theta$  is an ample divisor, and so  $J(C)$  is indeed a projective torus, i.e. an abelian variety.

The two tori  $\text{Pic}^0(C)$  and  $J(C)$  are related through the **Abel–Jacobi map**  $\alpha : C \rightarrow J(C)$  defined by integration over paths starting from a fixed point  $x_0 \in C$ , i.e.,  $\alpha(x)(\omega) = \int_{x_0}^x \omega$ . The definition of the jacobian shows that this is well defined. This map can be linearly extended to divisors on  $C$  by setting  $\alpha : \text{Pic}^d C \rightarrow J(C)$ ,  $\alpha(x_1 + \cdots + x_d) = \sum_j \alpha(x_j)$ , where the second sum is addition on the jacobian. This is known to be injective (**Abel’s theorem**) and surjective if  $d = g$  (**Jacobi inversion**). In degree 0 this gives a group isomorphism  $\text{Pic}^0(C) \xrightarrow[\alpha]{\sim} J(C)$ , which is independent of the choice of  $x_0$  and hence  $\text{Pic}^0(C)$  has indeed the structure of an abelian variety.

The theta divisor can be identified with a translate of a geometrically defined divisor  $W_{g-1}$ , the Abel–Jacobi image of the set of all effective divisors of degree  $g - 1$  on  $C$ . This is the content of **Riemann’s theorem**:

$$W_{g-1} = \Theta + \kappa, \quad 2\kappa = \alpha[K_C].$$

Here  $[K_C]$  is the class of a canonical divisor  $K_C$  on  $C$ , i.e., the divisor of a holomorphic 1-form on  $C$ . Recall that this divisor has degree  $2g - 2$  and so  $\kappa = \alpha([\vartheta_0])$ , where  $\vartheta_0$  is a degree  $g - 1$  divisor such that  $2\vartheta_0$  is linearly equivalent to  $K_C$ , also called a half-canonical divisor or a **theta characteristic**. The particular  $\kappa$  we found here is called the **Riemann constant**.

In the remainder of this section we use the shorthand notation  $h^0(C, D)$  in place of  $h^0(\mathcal{O}_C(D))$ . We say that a theta characteristic  $\vartheta$  is **even**, respectively **odd**, if  $h^0(C, \vartheta)$  is even or odd. Riemann’s constant is an even theta characteristic. This follows from **Riemann’s singularity theorem** stating that for a degree  $g - 1$  divisor  $D$ ,  $h^0(C, D)$  equals the multiplicity  $\mu_P(\Theta)$  of the point  $P = \alpha(D) - \kappa$  on the theta divisor:

$$\mu_P(\Theta) = h^0(C, D), \quad P = \alpha(D) - \kappa = \alpha(D - \vartheta_0).$$

Hence, taking for  $D$  the pre-image of the Riemann constant, we get  $\mu_0(\Theta) = 0$  since  $\theta_Z(0) \neq 0$ , confirming that  $\kappa$  is even.

A theta characteristic can be given as  $\vartheta = \vartheta_0 + \varepsilon$  where  $\alpha(\varepsilon) \in J_2(C)$ , the group of 2-torsion points of  $J(C)$ . In terms of the period matrix  $Z$ , two-torsion points on  $J(C)$  can be written as  $\varepsilon = \frac{1}{2}(\varepsilon'' + Z\varepsilon')$ ,  $\varepsilon', \varepsilon'' \in \mathbb{Z}^g/2\mathbb{Z}^g \simeq \mathbb{F}_2^g$ . Using Property 16.4.1.1, the theta divisor belonging to the theta function with characteristics  $\varepsilon_1 = \frac{1}{2}\varepsilon'$ ,  $\varepsilon_2 = \frac{1}{2}\varepsilon''$  is a translate of the Riemann theta divisor by the two-torsion point  $\varepsilon$  which we denote  $t_\varepsilon^*\Theta$ . Hence, applying Riemann’s singularity theorem, we find for the multiplicity at 0 of the translated theta-divisor

$$\mu_0(t_\varepsilon^*\Theta) = \mu_0 \text{div} \left( \theta_Z \left[ \begin{smallmatrix} \varepsilon' \\ \varepsilon'' \end{smallmatrix} \right] \right) = h^0(\mathcal{O}_C(\vartheta)).$$

To calculate this number, we make use of the symmetry relation 16.4.1.3 which in this case reads

$$\theta_Z \left[ \begin{smallmatrix} \frac{1}{2}\varepsilon' \\ \frac{1}{2}\varepsilon'' \end{smallmatrix} \right](-\mathbf{z}) = (-1)^{(\varepsilon' \cdot \varepsilon'')} \theta_Z \left[ \begin{smallmatrix} \frac{1}{2}\varepsilon' \\ \frac{1}{2}\varepsilon'' \end{smallmatrix} \right](\mathbf{z}).$$

This implies that all partial derivatives of this theta function vanish up to even, respectively odd order, if  $\varepsilon' \cdot \varepsilon''$  is even, respectively odd. But this means precisely that the parity of the multiplicity at zero of the corresponding theta divisor equals  $\varepsilon' \cdot \varepsilon''$ . Summarizing:

**Lemma 16.4.2.** *Let  $\vartheta_0$  be the theta characteristic corresponding to the Riemann constant. Using the dot product on  $\mathbb{F}_2^g$ , the theta characteristic  $\vartheta = \vartheta_0 + \varepsilon$  has parity  $\varepsilon' \cdot \varepsilon''$ , where we write  $\varepsilon = \frac{1}{2}\varepsilon'' + \frac{1}{2}Z\varepsilon'$ ,  $\varepsilon', \varepsilon'' \in \mathbb{Z}^g/2\mathbb{Z}^g \simeq \mathbb{F}_2^g$ .*

As an example, consider  $g = 1$ . Then  $\vartheta_0$  is itself a 2-torsion point which can be taken as the zero on the elliptic curve. This function has 3 zeros at the non-zero torsion points. There are 3 other theta characteristics corresponding to the functions  $\theta_Z \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ ,  $\theta_Z \begin{bmatrix} 1 \\ 0 \end{bmatrix}$  (even theta characteristic) and the function  $\theta_Z \begin{bmatrix} 1 \\ 1 \end{bmatrix}$  which has odd theta characteristic. So we have 3 even ones and 1 odd one.

We shall also be interested in the case  $g = 3$ . A similar argument shows that there are 28 odd theta characteristics and 36 even ones. This has a nice (classical) geometric interpretation for smooth plane curves  $C$  of degree 4. Since  $K_C$  is the hyperplane bundle, odd theta characteristics are precisely of the form  $\mathcal{O}_C(P + Q)$ , with  $2P + 2Q = L \cdot C$  for some line  $L$ . In other words, these are the *bitangents*. We shall see below (cf. Theorem 16.4.4) that there are  $2^{g-1}(2^g - 1)$  odd theta characteristics and  $2^2(2^3 - 1) = 28$ . This shows, as is well known, that  $C$  has 28 bitangents.

**16.4.C Weil pairing on torsion points of  $J(C)$ .** Suppose that  $D_1, D_2$  are two degree 0 divisors on the curve  $C$  with  $\alpha(D_j)$ ,  $j = 1, 2$ , a  $k$ -torsion point. Then  $kD_j = \text{div}(f_j)$  for some non-zero rational functions  $f_1, f_2$ . If  $D_1$  and  $D_2$  have disjoint supports, then so have  $f_1$  and  $D_2$  as well as  $f_2$  and  $D_1$ . Hence we can define

$$e_k(D_1, D_2) := f_1(D_2)/f_2(D_1), \quad \text{div}(f_j) = kD_j.$$

Observe that interchanging  $(D_1, f_1)$  and  $(D_2, f_2)$  replaces the right-hand side by its reciprocal, so  $\log(e_k)$  gives a skew symmetric form. A priori  $e_k(D_1, D_2)$  is only a non-zero number, but it is actually a  $k$ -th root of unity. This is the case because of Weil reciprocity:

$$\frac{f_1^k(D_2)}{f_2^k(D_1)} = \frac{f_1(kD_2)}{f_2(kD_1)} = \frac{f_1(\text{div}(f_2))}{f_2(\text{div}(f_1))} = 1.$$

Moreover, adding the divisor of a function to  $D_1$  or  $D_2$  is easily seen to leave the number  $e_k(D_1, D_2)$  unchanged. This gives the **Weil pairing** on the  $k$ -torsion points  $J_k(C)$  of  $J(C)$ :

$$e_k : J_k(C) \times J_k(C) \rightarrow \mu_k := \{z \in \mathbb{C} \mid z^k = 1\}.$$

In the remainder of this section we take  $k = 2$ , that is, we consider only two-torsion, but we shall instead use the additive version of this pairing upon writing

$$e_2(\varepsilon_1, \varepsilon_2) = (-1)^{b(\varepsilon_1, \varepsilon_2)}.$$

This gives  $J_2(C)$  the structure of a symplectic space over  $\mathbb{F}_2$ . We shall next explain that theta characteristics define quadratic forms whose polarization is the given symplectic form. To start, let  $L \in \text{Pic}^{g-1}(C)$  be a half-canonical divisor and  $\vartheta = \mathcal{O}_C(L)$  the corresponding line bundle. First, recall that, using the Abel–Jacobi map we have identified  $\varepsilon \in J_2(C)$  with a line bundle whose divisor class in  $\text{Pic}^0(C)$  corresponds to  $\varepsilon \in J(C)$  so that it makes sense to set

$$q_\vartheta(\varepsilon) = h^0(C, \vartheta) + h^0(C, \vartheta \otimes \varepsilon) \pmod{2}, \quad \varepsilon \in J_2(C). \quad (16.11)$$

That the polar form of  $q$  is the additive Weil pairing is a direct consequence of the *Riemann–Mumford relation* (cf. [92, 164]):

$$h^0(C, \vartheta \otimes \varepsilon_1 \otimes \varepsilon_2) + h^0(C, \vartheta \otimes \varepsilon_1) + h^0(C, \vartheta \otimes \varepsilon_2) + h^0(C, \vartheta) \equiv b(\varepsilon_1, \varepsilon_2) \pmod{2}.$$

Since there are as many quadratic forms on the  $\mathbb{F}_2$ -vector space  $J_2(C)$  as 2-torsion points on the jacobian, every quadratic form  $q$  whose polarization is the (additive) Weil pairing is of the form  $q = q_\vartheta$ .

**16.4.D Quadratic forms over  $\mathbb{F}_2$ .** We have studied quadratic vector spaces  $(V, q)$  over fields of characteristic 2 in Section 8.2 and showed that the polar form of  $q$  is a symplectic form and that there is a family of non-isometric quadratic forms with the same polar form. The isometry classes are determined by the Arf invariant  $\text{arf}(q)$  of  $q$ . If the field is  $\mathbb{F}_2$  the theory simplifies considerably since the Arf invariant assumes only two values, 0 or 1.

From now on assume that  $(V, J)$  is a symplectic space over  $\mathbb{F}_2$  of dimension  $2g$  and let

$$Q(V) := \{\text{quadratic forms } q : V \rightarrow k \mid b_q = J\}.$$

Observe that  $x^2 = x$  in the field  $\mathbb{F}_2$  and so a linear form on  $V$  is the same as a quadratic form which in every basis is diagonal and hence has zero polar form. Every linear form on  $V$  is of the form  $x \mapsto J(x, y)$  for some  $y \in V$  and adding such a form to  $q \in Q(V)$  defines an action of  $V$  on  $Q(V)$  which is denoted as  $t_v(q)(x) := q(x) + J(x, v)$ . To calculate its Arf invariant, write  $q(x) = \sum_{i=1}^{2g} a_i x_i^2 + q_0(x)$ ,  $q_0(x) = \sum_{i=1}^g x_i x_{i+g}$  and  $v = (v_1, \dots, v_{2g})$ . We find

$$\begin{aligned} q_v(x) &= \sum_{i=1}^{2g} a_i x_i^2 + \sum_{i=1}^g x_i v_{i+g} + \sum_{i=1}^g x_{i+g} v_i + q_0(x) \\ &= \sum_{i=1}^g (a_i + v_{i+g}) x_i^2 + \sum_{i=1}^g (a_{i+g} + v_i) x_{i+g}^2 + q_0(x). \end{aligned}$$

It follows that  $\text{arf}(t_v(q)) = \sum_{i=1}^g (a_i + v_{i+g})(a_{i+g} + v_i) = \text{arf}(q) + \sum_{i=1}^{2g} a_i v_i + \sum_{i=1}^g v_i v_{i+g}$  and, since  $v_i = v_i^2$ , we find

$$\text{arf}(t_v(q)) = \text{arf}(q) + q(v). \quad (16.12)$$

On the other hand, a sum  $q + q'$  of two quadratic forms in  $Q(V)$  is a linear form, and hence has the shape  $x \mapsto J(x, v)$  for a vector  $v = v(q, q')$  uniquely determined



by  $q$  and  $q'$ . So adding two quadratic forms  $q$  and  $q'$  defines a unique vector in  $V$ . The set  $Q(V)$  is not a vector space, since it has no zero, but the disjoint union of  $V$  and  $Q(V)$  is a vector space of dimension  $2n + 1$  if we take the original vector space structure on  $V$ , we use the  $t$ -action on  $Q(V)$  for addition of vectors  $v \in V$  and  $q \in Q(V)$ , and, finally, we define  $q + q' = v(q, q')$  whenever  $q, q' \in Q(V)$ .

The symplectic group has two orbits in  $Q(V)$ ,  $Q_0(V)$  consisting of those quadratic forms with Arf invariant 0 and  $Q_1(V)$  assembles those of Arf invariant 1.

**Proposition 16.4.3.** *There are  $2^{g-1}(2^g + 1)$  forms with Arf invariant 0 and  $2^{g-1}(2^g - 1)$  with Arf invariant 1.*

*Proof.* The quadratic form  $q_0(x) = \sum_{i=1}^g x_i x_{g+i}$  of Arf invariant 0 has  $2^{g-1}(2^g + 1)$  zeros in  $V$ . This follows from our "democratic" count which gave Table 16.3.2. Because of equation (16.12), the forms  $v + q_0$  have Arf invariant  $q_0(v)$  and so one has  $2^{g-1}(2^g + 1)$  forms with Arf invariant 0 and the remaining  $2^{g-1}(2^g - 1)$  must have Arf invariant 1.  $\square$

**16.4.E Relation with theta characteristics.** We explained that a theta characteristic  $\vartheta$  defines a quadratic form  $q_\vartheta$  on  $J_2(C)$  and, conversely, that every quadratic form on  $J_2(C)$  whose polar form is a non-degenerate symplectic form can be written in this way. The group  $J_2(C)$  acts transitively on such quadratic forms. The Riemann constant is an even theta characteristic. It comes from the theta divisor  $\Theta$  and is associated to a quadratic form  $q_0$  with Arf invariant 0. Then, by the transitivity of the action of  $J_2(C)$ , we have  $q_\vartheta = q_0 + \varepsilon$  and by (16.12) the Arf invariant of  $q_\vartheta$  equals  $q_0(\varepsilon)$ . Since (16.11) implies that  $q_0(\varepsilon) \equiv h^0(\vartheta) \pmod{2}$ , applying Proposition 16.4.3 we arrive at the main result of this section:

**Theorem 16.4.4.** *Let  $C$  be a smooth complex algebraic curve of genus  $g \geq 1$ . Then  $C$  has  $2^{g-1}(2^g + 1)$  even and  $2^{g-1}(2^g - 1)$  odd theta characteristics. The even theta characteristics correspond to quadratic forms with Arf invariant 0 and the odd ones to quadratic forms with Arf invariant 1.*

*Remark.* In [164] D. Mumford gave a geometric argument proving this result. His argument is valid for curves in all characteristics different from 2.

**Historical and Bibliographical Notes.** Sign structures have been introduced by R. Miranda and D. Morrison in Ch. 1.11 of [156]. The treatment of the Dickson invariant given in Section 16.2 is due to J. Dieudonné, c.f. [48]. The determination of the size of the orthogonal groups over finite fields in Section 16.3 follows the calculation in §13 of M. Kneser's book [122].

The material in Section 16.4 is classical and goes back to B. Riemann [194, 195] and A. Coble [40]. Modern expositions can be found in the books [2, 88].

## The Structure of Orthogonal Groups II, Lattices

### Introduction

In Section 17.1 we mainly investigate some groups of isometries preserving a lattice such as reflection groups, reduced orthogonal groups and groups acting trivially on the discriminant group.

Root lattices and their reflection groups are treated in the next section. According to the signature of the lattice these are either almost always of finite index in the full isometry group, such as for the definite lattices or those of signature  $(r, s)$  with  $r, s \geq 2$ , or this holds sparingly such as for the Lorentz type lattices. This section is somewhat cursory in that the reader is mostly referred to the literature for full proofs. This is compensated by giving several illustrative examples such as the classical root lattices, the  $T_{p,q,r}$ -lattices, the Leech lattice and the Borcherds lattice. Special attention is given in Subsection 17.2.C to a result due to M. Kneser which describes the Weyl group of lattices of Witt index  $\geq 2$  (these are not hyperbolic) since this result is going to play a decisive role in Chapter 18.

By contrast, the subject of Eichler–Siegel transformations is discussed at length in Section 17.3, since these are going to play a major role in the study of isometries of certain hyperbolic type lattices as well as in W. Ebeling’s results on vanishing lattices which we treat in the next chapter.

In this chapter  $(L, b)$  is assumed to be a non-degenerate symmetric lattice embedded in  $V = L_{\mathbb{Q}}$ . The  $\mathbb{Q}$ -bilinear extension of  $b$  to  $V$  is also denoted  $b$ . One sets  $q(x) = \frac{1}{2}b(x, x) \in \frac{1}{2}\mathbb{Z}$ . For the signed spinor norms one has  $\epsilon \in \{+, -\}$ .

### 17.1 An Overview of Lattice Isometries

The case where  $L$  is a free module of finite rank over an integral domain  $R$  has been briefly discussed in Section 6.5. Here we consider the case  $R = \mathbb{Z}$  and consider the orthogonal group  $O(L)$  of  $L$  as the group of isometries of  $V = L_{\mathbb{Q}}$  that preserve the lattice  $L$ .

We discuss first which of the standard vector space isometries of  $V$  preserve  $L$ .

1. **Reflections.** Recall from Section 1.5 that a vector space reflection  $\sigma_x$  in the hyperplane orthogonal to a non-isotropic vector  $x \in L$  preserves the lattice  $L$  if and

only if

$$\frac{b(x, y)}{q(x)} \cdot x \in L \text{ for all } y \in L.$$

We also saw that we may assume that  $x$  is primitive since the above condition is insensitive under scaling of  $x$ . The resulting vector is unique up to sign and so  $k := 2q(x) \in \mathbb{Z}$  is an invariant of the reflection, and  $x$  is called the ***k-root associated to the reflection*** and the reflection is called a ***reflection in a k-root***. Note that  $k$  is even for quadratic lattices but for odd lattices it might be odd. Since  $x$  is primitive, the function on  $L$  given by  $y \mapsto 2b(x, y)/k$  is integral valued and defines an element in the discriminant group  $\text{dg}_L$ . It is torsion of order  $\frac{1}{2}|k|$  or  $|k|$  according to whether  $k$  is even or odd respectively. In particular, for a unimodular integral lattice one can only have  $k = \pm 1$  or  $k = \pm 2$ . The sublattice of  $L$  generated by all  $k$ -roots for varying  $k$  is called its ***root sublattice***, and the group generated by reflections in the roots, the ***reflection group of L***. If  $L$  is spanned by its roots, it is called a ***root lattice***. Since roots play such a central role, it is crucial to know for which lattices there are many roots, a special case of Corollary A.3.7 from the Appendix gives an instance where this is the case:

**Proposition 17.1.1.** *Suppose  $L$  is an indefinite lattice of rank  $\geq 4$ . If  $L$  contains a  $k$ -root, it contains infinitely many  $k$ -roots.*

The set of  $\epsilon$ -roots in a lattice  $L$  is the collection of roots

$$\Delta_\epsilon(L) = \{r \in L \mid b(r, r) = \epsilon 2\}, \quad \epsilon \in \{+, -\},$$

spanning the  $\epsilon$ -root sublattice

$$L_{\epsilon\text{-root}} = \sum_{x \in \Delta_\epsilon(L)} \mathbb{Z}x \subset L. \quad (17.1)$$

The group of the reflections in the  $\epsilon$ -roots is the ***Weyl group***

$$W^\epsilon(L) = \text{group generated by } \sigma_r, \quad r \in \Delta_\epsilon(L).$$

We will mostly use this set-up in the setting of even lattices. In that case the relevant quadratic form  $q$  satisfies  $q(r) = \epsilon 1$ .

2. **Groups induced by the groups from § 16.1.** These are

$$\begin{aligned} \text{O}^\epsilon(L) &= \{g \in \text{O}(L) \mid \text{Nm}_{\text{spin}}^\epsilon g_{\mathbb{R}} = 1\}, \\ \text{SO}(L) &= \{g \in \text{O}(L) \mid \det g = 1\}, \\ \text{SO}^+(L) &= \{g \in \text{SO}(L) \mid \text{Nm}_{\text{spin}} g_{\mathbb{R}} = 1\}. \end{aligned}$$

Then there are groups that only make sense for lattices:

3. **Orthogonal transformations inducing the identity on the discriminant group.** These form the group

$$\text{O}^\#(L) = \{g \in \text{O}(L) \mid g \text{ induces id on } \text{dg}_L\}.$$

The criterion of Lemma 7.1.1 implies that a reflection  $\sigma_x$  with  $b(x, x) = \pm 2$  induces the identity on the discriminant group. Introducing the group

$$O^{\epsilon, \#}(L) = O^\epsilon(L) \cap O^\#(L) \tag{17.2}$$

we thus have an inclusion

$$W^\epsilon(L) \subset O^{\epsilon, \#}(L),$$

since the **Weyl group**  $W^\epsilon(L)$  is the subgroup of  $O(L)$  generated by the  $\epsilon$ -reflections.

Proposition 17.1.1 implies that  $W^\epsilon(L)$  is infinite as soon as  $L$  is indefinite of rank  $\geq 4$  and contains at least one  $\epsilon$ -root. This is the case since a root (up to sign) and the corresponding reflection determine each other uniquely.

**4. The level  $n$  congruence subgroups  $O(L)[n]$ .** The quotient map  $L \rightarrow L/nL$  induces a group homomorphism  $\rho_n : O(L) \rightarrow \text{Aut}(L/nL)$ , the **mod  $n$ -reduction map**. Its kernel

$$O(L)[n] = \ker(\rho_n) = \{\gamma \in O(L) \mid \gamma \equiv \text{id mod } n\} \tag{17.3}$$

is the level  $n$  congruence subgroup. If  $n = p$  is a prime number, the symmetric form  $b$  on  $L$  induces a symmetric form  $\bar{b}$  on the  $\mathbb{F}_p$ -vector space  $\bar{L} = L/pL$  given by

$$\bar{b}(x + pL, y + pL) = b(x, y) \text{ mod } p. \tag{17.4}$$

This form is  $\mathbb{F}_p$ -valued and  $\text{disc}(\bar{b}) \equiv \text{disc}(b) \pmod{p}$ . In particular,  $\bar{b}$  is unimodular if and only if  $\text{disc}(b)$  is prime to  $p$ . The mod  $p$ -reduction map  $\rho_p$  sends an isometry of  $(L, b)$  to an isometry of  $(\bar{L}, \bar{b})$ .

As we have seen in Examples 1.6.8.2, for any unimodular lattice  $(L, b)$ , the mod  $p$ -reduction is related to the discriminant group of  $L(p)$ . Indeed,  $L(p)^* = p^{-1}L$  and so  $\text{dg}_{L(p)} = p^{-1}L/L \simeq L/pL$ . The discriminant form of  $L(p)$  is  $p^{-1}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{F}_p$ -valued and after the identifications becomes the form  $\bar{b}$  on  $L/pL$ .

Let us look at some examples.

**Examples 17.1.2. 1. Rank one lattices.** For symmetric lattices  $\langle a \rangle$  over an integral domain, see Example 6.5.5.1. Here  $R = \mathbb{Z}$  and the only isometries are  $\pm \text{id}$ . If  $k \in \mathbb{Z}, k \neq 0$ , we have  $\text{SO}^+(\langle k \rangle) = \text{SO}(\langle k \rangle) = \{1\}$  and  $O^+(\langle k \rangle) = \{1\}$  if  $k < 0$  and  $O^+(\langle k \rangle) = \{1, -1\}$  otherwise.

**2. Hyperbolic lattice  $U$  over  $\mathbb{Z}$ .** Hyperbolic lattices over integral domains have been discussed in § 6.3.B, example 6. In the present case, there are only 4 isometries,  $\pm \text{id}$  and the reflections  $j_1 = \sigma_{e-f}$  with matrix  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  and  $-j_1 = \sigma_{e+f}$ . Their properties are assembled in the following table.

element	det	$\text{Nm}_{\text{spin}}^\epsilon$
id	1	1
-id	1	-1
$j_1$	-1	$-\epsilon$
$-j_1$	-1	$\epsilon$

One has  $O^\pm(U) = \langle \mp j_1 \rangle$ ,  $SO^+(U) = \{\text{id}\}$  and  $SO^-(U) = \langle -\text{id} \rangle$ . We also see that  $U$  is not a root lattice. In fact  $\mathbb{Z}(e + \varepsilon f)$  is the lattice spanned by the  $\varepsilon$ -roots and the full root sublattice is isometric to  $\langle 2 \rangle \oplus \langle -2 \rangle$ .

**3. Reduction mod 2.** We consider the A-D-E root lattices. We have assembled their discriminants in Table 4.1.1. So the reductions mod 2 give unimodular lattices for  $A_n$ ,  $n$  even,  $E_6$  and  $E_8$ . The other root lattices have null-spaces. The quadratic form for  $A_{2m}/2A_{2m}$  has the standard symplectic form as its polar form and has Arf invariant 1 as one can show inductively. One can also show that  $A_{2m+1}/2A_{2m+1} = A_{2m}/2A_{2m} \oplus \langle 0 \rangle$ . The form  $E_8$  is unimodular and so the reduction mod 2 is isometric to the discriminant form for  $E_8(2)$  which we calculated before in Example 11.2.5.4. It is the 8-dimensional quadratic  $\mathbb{F}_2$ -space with Arf invariant 0. For  $E_6$  one finds the 6-dimensional quadratic  $\mathbb{F}_2$ -space with Arf invariant 1 since there are  $72 = 2 \cdot 36$  roots. We leave the determination of the mod 2 reduction of the other root lattices as an exercise.

## 17.2 Root Lattices and Reflection Groups

In this section we shall discuss the size of the Weyl group of a lattice in relation to its signature. Of course, a lattice may be devoid of roots and then the Weyl group is just the identity. At the other extreme we have the root lattices, by definition spanned by their roots. The Weyl group may not be of finite index in the full orthogonal group as we shall see in this section. This motivates the following terminology.

**Definition 17.2.1.** A lattice  $L$  is called  *$k$ -reflective, respectively reflective*, if the group generated by the reflections in  $k$ -roots for fixed  $k$ , respectively for all  $k$ , has finite index in the group  $O(L)$ .

**17.2.A Definite lattices.** Here is a classical result describing the finite reflection groups for a definite root lattice. These results imply that all (positive) definite root lattices are 2-reflective.

**Lemma 17.2.2.** *The isometry group of a positive definite irreducible quadratic 2-root lattice  $\Gamma$  (that is  $\Gamma = A_n, D_n$  or  $E_n$ ) is a direct product of its Weyl group and the group of symmetries of the Dynkin diagram. Explicitly*

- $O(\Gamma) = W^+(\Gamma)$  for  $\Gamma = A_1, E_7, E_8$ .
- $O(\Gamma) = W^+(\Gamma) \times \{\pm \text{id}\}$  for  $\Gamma = A_n, n \geq 2, D_n, n \geq 5$ , and for  $E_6$ .
- $O(\Gamma) = W^+(\Gamma) \times \mathfrak{S}_3$  for  $\Gamma = D_4$ , where  $\mathfrak{S}_n$  is the permutation group in  $n$  letters.

We refer to [26, Planches I, II–VII] where  $A(R)$  stands for the full orthogonal group of the lattice generated by an abstract system of roots  $R$ , and  $W(R)$  denotes its Weyl group. Comparing this with the calculations in Section 4.1.D we find:

**Corollary 17.2.3.** *We have*

- $O^{+\#}(A_n) = W^+(A_n)$ .
- $O^{+\#}(D_n) = W^+(D_n)$  for  $n \geq 5$ ,  $O^{+\#}(D_4) = W^+(D_4) \times \mathbb{Z}/3\mathbb{Z}$ .
- $O^{+\#}(E_n) = W^+(E_n)$ ,  $n = 6, 7, 8$ .

*Proof.* Observe that the discriminant group of  $A_n$  is cyclic of order  $n + 1$  and only has non-trivial automorphisms if  $n \neq 1$ . By Lemma 17.2.2 there is only one non-trivial automorphism in this case,  $-\text{id}$ , which only belongs to the Weyl group if  $n = 1$ . In that case the orthogonal group is generated by one reflection in a root. It follows that in all cases  $O^{+\#}(A_n)$  coincides with the Weyl group.

For the lattices  $D_n$ ,  $n \geq 4$ , and for  $E_6$  the isometry group of the discriminant form is induced by  $-\text{id}$ , those of  $E_7$  and  $E_8$  are trivial. In these cases the Weyl group coincides with the subgroup of the orthogonal group consisting of elements acting as the identity on the discriminant group. For  $n = 4$  the Weyl group has index 3 in the latter group.  $\square$

*Remark 17.2.4.* We saw some other classical reflection groups in Examples 4.2.3 where  $k$ -roots come up for  $k \neq \pm 2$ .

Occasionally we use some standard results on the classical reflection groups for the definite 2-roots lattices  $A_n, B_n, C_n, E_n$ , or the lattices  $D_n, F_4, G_3$  with roots of other lengths. We refer to [26], [103, Chapter III] for details of what follows.

To set the stage, let  $L$  be one of these lattices and let  $W(L)$  be its Weyl group. A component of the complement of all reflection hyperplanes is called a **Weyl chamber**. The roots forming the vertices of the Dynkin diagram give a basis  $\mathbf{E} = \{\alpha_1, \dots, \alpha_n\}$  for the vector space  $L_{\mathbb{R}}$ . This basis is a so-called **root basis**, by definition a basis such that every root in  $L$  is an all non-negative or an all non-positive integral linear combination of the  $\alpha_j$ . Root bases and Weyl chambers are in one-to-one correspondence:

**Proposition 17.2.5.** *The closure of a Weyl chamber is a fundamental domain for the action of the Weyl group  $W(L)$  on  $L_{\mathbb{R}}$ .*

1. Let  $\mathcal{C}$  be a Weyl chamber. The set of roots  $\Delta_{\mathcal{C}} = \{r \in \Delta(L) \mid b(x, r) > 0 \text{ for all } x \in \mathcal{C}\}$  has the property that  $\Delta(L) = \Delta_{\mathcal{C}} \cup -\Delta_{\mathcal{C}}$ . There are precisely  $n$  roots in  $\Delta_{\mathcal{C}}$  that form a root basis and these give a Dynkin diagram whose root lattice is  $L$ .
2. Conversely, let  $\Delta(L) = \Delta \cup -\Delta$  be a partition of the set  $\Delta(L)$  such that  $\Delta$  is closed under taking sums, i.e., any non-negative integral linear combination of roots in  $\Delta$  belongs to  $\Delta$ . Then  $\{x \in (C_{L_{\mathbb{R}}} \mid b(x, r) > 0 \text{ for all } r \in \Delta)\}$  is a Weyl chamber.
3.  $W(L)$  acts simply transitively on root bases and on Weyl chambers.
4. The roots of given length form one orbit under  $W(L)$ .

**17.2.B Lorentzian Lattices.** The lattice  $L$  is of Lorentzian type if it has signature  $(1, n)$ ,  $n \geq 2$ . We consider it as a sublattice of  $V_{\mathbb{R}} = L_{\mathbb{R}}$ , so that  $V_{\mathbb{R}}$  is a hyperbolic vector space. The Lorentzian signature implies that only the hyperplanes in  $V_{\mathbb{R}}$  orthogonal to a  $k$ -root,  $k < 0$ , meet the light cone. We only consider this type of roots and the spinor norm  $\text{Nm}_{\text{spin}}^{\varepsilon}$  with  $\varepsilon = -$ . This leads to the following

**Observation.** *Reflections in  $k$ -roots with  $k < 0$  preserve the components of the light cone.*

By (16.3) the subgroup of isometries of  $L$  preserving the two components of the light cone is  $O^-(L)$ . In particular it contains the reflections in  $k$ -roots,  $k < 0$ , since these have signed spinor norm 1. The corresponding Weyl group  $W^-(L)$  is a normal subgroup of  $O^-(L)$ .

We recall some well-known properties of groups generated by reflections in the vector space  $V_{\mathbb{R}}$ . See e.g. [172, §1.1]. A connected component of the complement of the union of all reflection hyperplanes in  $C_{V_{\mathbb{R}}}$  is called a **Weyl chamber**. We just observed that reflections preserve the light cone. In other words, the Weyl group preserves the light cone. This is analogous to the positive definite case, where the role of the light cone is played by  $L_{\mathbb{R}}$ . Moreover, Proposition 17.2.5 has a direct analog:

**Proposition 17.2.6.** *Let  $\Delta(L)$  be the set of roots  $r \in L$  with  $b(r, r) < 0$ . The closure of a Weyl chamber is a fundamental domain for the action of the Weyl group  $W^-(L)$  on  $C_{V_{\mathbb{R}}}$ .*

1. *Let  $\mathcal{C}$  be a Weyl chamber. The set of roots  $\Delta_{\mathcal{C}} = \{r \in \Delta(L) \mid b(x, r) > 0 \text{ for all } x \in \mathcal{C}\}$  has the property that  $\Delta(L) = \Delta_{\mathcal{C}} \cup -\Delta_{\mathcal{C}}$ .*
2. *Conversely, let  $\Delta(L) = \Delta \cup -\Delta$  be a partition of the set  $\Delta(L)$  such that  $\Delta$  is closed under taking sums, i.e., any non-negative integral linear combination of roots in  $\Delta$  belongs to  $\Delta$ . Then  $\{x \in C_{V_{\mathbb{R}}} \mid b(x, r) > 0 \text{ for all } r \in \Delta\}$  is a Weyl chamber.*

**Corollary 17.2.7.** *The group  $O^-(L)$  of isometries preserving the light cone is the semi-direct product of  $W^-(L)$  and the stabilizer in  $O^-(L)$  of a Weyl chamber. Consequently, the latter group is isomorphic to  $O^-(L)/W^-(L)$ .*

*Remark 17.2.8.* By item 2, the Weyl group  $W^-(L)$  is generated by those roots in  $\Delta_{\mathcal{C}}$  which cannot be written as a non-trivial sum of roots in  $\Delta_{\mathcal{C}}$ . As in the positive definite case such roots are called **indecomposable**. For two different indecomposable roots  $r, s \in \Delta$  we have  $r \cdot s \geq 0$ .

Reflective Lorentzian root lattices can only have relatively small rank:

**Theorem 17.2.9** ([239, 240, 172, 72]). *A root lattice of signature  $(1, n)$  is reflective if and only if  $n \in \{1, \dots, 19, 21\}$ . If  $n = 21$  such a lattice is even: it is the unique reflective Lorentzian lattice of rank 22 (see Example 17.2.10.5 below). In particular there are no odd reflective Lorentzian lattices of rank 22.*

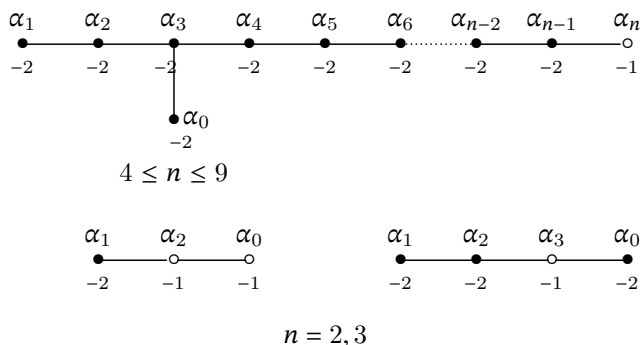
We skip the elaborate proofs. We only give some examples stating which of those are reflective and which are not, again referring to the cited works above for full details.

**Examples 17.2.10. 1.** The *Lorentz lattice*  $\mathbb{Z}^{1,n}$ ,  $n \geq 2$ , is a root lattice. Indeed, using, as before, the standard basis  $\{e_0, \dots, e_n\}$  for  $\mathbb{R}^{n+1}$  it has a new basis

$$\begin{aligned} \alpha_0 &= (1, -1, -1, -1, 0, \dots, 0), \text{ for } n \geq 3, & &= (1, -1, -1) \text{ for } n = 2, \\ \alpha_j &= e_j - e_{j+1}, & j &= 1, \dots, n-1, \\ \alpha_n &= e_n. \end{aligned}$$

The vectors  $\alpha_j$ ,  $j = 1, \dots, n-1$ , are  $(-2)$ -roots,  $\alpha_n$  is a  $(-1)$ -root and  $\alpha_0$  is a  $(-2)$ -root for  $n \geq 3$ , but a  $(-1)$ -root for  $n = 2$ .

Although the Lorentz lattice has a basis of roots, the corresponding reflections might not generate the full reflection group. E. Vinberg developed an algorithm which terminates if a finite set of roots exists such that the corresponding reflection group has finite index in  $O(\mathbb{Z}^{1,n})$ .<sup>1</sup> Termination occurs if and only if  $n \leq 19$  and so precisely then  $\mathbb{Z}^{1,n}$  is reflective. For a proof which is more in the spirit of lattice theory see [24, §6, especially Cor. 6.3 and Lemma 6.5]. These results show in particular that for  $2 \leq n \leq 9$  the above root basis suffices to generate the full reflection group. The corresponding graphs resemble the graphs  $E_{n+1}(-1)$  (cf. Eqn. (4.4)):



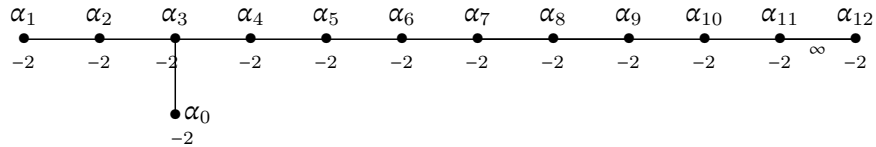
Here we denote the self-intersections of the roots below the vertices: among the depicted roots the black ones are  $(-2)$ -roots and the white ones are  $(-1)$ -roots. As mentioned before, for  $2 \leq n \leq 19$  the lattices  $\mathbb{Z}^{1,n}$  are reflective, but they might not be  $(-2)$ -reflective because of the presence of  $(-1)$ -roots in the basis. For  $2 \leq n \leq 9$  we shall show below in Example 17.3.8 that  $\mathbb{Z}^{1,n}$  is not  $(-2)$ -reflective.

**2.** Those of the lattices  $T_{2,3,n-2} = E_n(-1) \subset \mathbb{Z}^{1,n}(-1)$  which are *Lorentzian*, that is, for which  $n \geq 10$ , have been investigated in Subsection 4.1.C, where it was shown that they are even root lattices (of rank  $n$ ). For  $n = 10$  we get the Enriques lattice. For  $n = 10, 11, 12, 13$  these are reflective by [172], but for  $n > 13$  these are not reflective.

<sup>1</sup>This is equivalent to finding a Weyl chamber having finite volume in the hyperbolic space  $\mathbb{R}^{1,n}$ . This explains E. Vinberg's use of hyperbolic geometry to construct such a set of roots.



3. The *hyperbolic T-shaped lattices* from Section 4.1. Recall that the lattices  $T_{p,q,r}$  are even root lattices which for  $p^{-1} + q^{-1} + r^{-1} < 1$  are all Lorentzian. Apart from the lattices with  $(p, q, r) = (2, 3, r)$ ,  $r = 7, 8, 9$ , from Example 2, only the lattices with  $(p, q, r) = (2, 4, r)$  with  $r = 5, 6, 7$  and  $(p, q, r) = (3, 3, r)$  with  $r = 4, 5, 6$  are reflective. The roots corresponding to the vertices give a root basis only for  $(p, q, r) = (2, 3, 7), (3, 3, 4), (2, 4, 5)$ . To obtain a generating set of roots for the other root lattices, some roots have to be added to a basis. See [172] for details. Here is an example where  $\alpha_{12}$  needs to be added:



The graph for the root lattice of  $T_{2,3,8}$

Recall (cf. Table 4.2.1) that the label  $\infty$  on the extreme right edge means that the angle between the roots  $\alpha_{11}$  and  $\alpha_{12}$  is  $\pi$ . In the present situation the two corresponding reflection hyperplanes are parallel in the sense that they meet on the boundary of the light cone<sup>2</sup>. In our case this is equivalent to  $b(\alpha_{11}, \alpha_{12}) = -2$ .

4. Reflection groups related to the *Leech lattice*  $\Gamma_{24}$ . Recall (Section 5.1) that the Leech lattice is a positive definite rank 24 unimodular lattice, the unique Niemeier lattice without roots. The even unimodular Lorentzian lattice

$$II_{1,25} := U \oplus \Gamma_{24}(-1)$$

is by classification (cf. Corollary 2.4.3) isometric to  $U \oplus E_8^{\oplus 3}(-1)$ . Since  $U \oplus E_8(-1)$  and  $E_8(-1)$  are spanned by their roots (see § 4.1.C) so is  $II_{1,25}$ . The group generated by the reflections in these roots has a fundamental domain  $P$  described in [42] whose bounding hyperplanes are orthogonal to roots of the form  $e - (1 + q(v))f + v$  where  $v \in \Gamma_{24}(-1)$  and  $\{e, f\}$  is the standard basis of  $U$ . Those roots are called the *Leech roots*. The lattice  $II_{1,25}$  is not reflective: the symmetry group of  $P$  turns out to be isomorphic to  $\Gamma_{24} \ltimes \mathcal{O}(\Gamma_{24})$ , an infinite group isomorphic to  $\mathcal{O}^-(L)/W^-(L)$ .

5. The *Borcherds lattice* [24]. The sublattice  $L_{1,21} \subset E_{21}(-1)$  consisting of vectors  $\sum x_i e_i$  with  $\sum x_i$  even defines an even lattice. It is isometric to  $U \oplus D_{20}(-1)$  and turns out to be a reflective root lattice having a generating set of 210 roots. Moreover, the quotient  $\mathcal{O}^-(L_{1,21})/W^-(L_{1,21})$  is isomorphic to a finite group of order  $2^8 \cdot 3^3 \cdot 5 \cdot 7$ . It is the reflective Lorentzian lattice of maximal possible rank. We shall encounter this lattice again as an example of a supersingular K3 lattice (see Remark 19.5.3).

**17.2.C Lattices with (real) Witt index  $\geq 2$ .** One has  $W^-(L) = \mathcal{O}^{-\#}(L)$  for "most" lattices having roots provided the (real) Witt index of  $L$  is 2 or more, for instance if in addition the discriminant is prime to 6. This can be derived from a result due to M. Kneser which deals with  $W^+(L)$  and which we first discuss:

<sup>2</sup>The light cone is introduced in Lemma 16.1.3.

**Theorem 17.2.11** ([121, Satz 4]). *Let  $(L, q)$  be an integral quadratic lattice with real Witt index  $\geq 2$ , that is  $\min(r, s) \geq 2$ , where  $(r, s)$  is the signature of  $L$ . Assume that the following conditions on  $L$  hold simultaneously:*

- $L$  contains at least one root  $x$  with  $q(x) = 1$ ;
- $L$  contains a sublattice  $L_1$  of rank  $\geq 5$  with  $\text{disc}(L_1)$  not divisible by 3;
- $L$  contains a sublattice  $L_2$  of rank  $\geq 6$  with  $\text{disc}(L_2)$  odd.

Then  $W^+(L) \cap \text{SO}^+(L) = \text{SO}^+(L) \cap \text{O}^\#(L)$ .

*Sketch of the proof.* The spinor group and spinor norm make use of  $\mathbb{Q}$ -vector space isometries  $\sigma_x$  with  $q(x) \in \mathbb{Q}^\times$  and these need not preserve the lattice. Indeed,  $\text{SO}^+(L) \cap \text{O}^\#(L)$  might be strictly larger than the subgroup of rotations generated by lattice-preserving reflections  $\sigma_x$  in 2-roots  $x$ . The strategy of the proof is to localize the situation and show that for most primes  $p$  this does not happen and so the two groups locally coincide for such primes  $p$ . This is the first step of the proof:

**Step 1.** *Except for some 2-adic and 3-adic lattices, one has  $\text{O}^\#(L_p) = W^+(L_p) \cap \text{SO}^+(L)$ .* The exceptions are

- either  $p = 2$  and  $\dim_{\mathbb{F}_2} L/2L = 1, \dots, 5$ ,
- or  $p = 3$  and  $\dim_{\mathbb{F}_3} L/3L = 2, 3, 4$ .

The proof is a consequence of a detailed study of the local reflection groups. It combines three results whose assertions involve the induced bilinear form on  $L/pL \simeq L_p/pL_p$  which as in (17.4) is given by  $\bar{b}(\bar{x}, \bar{y}) = b(x, y) \pmod{p}$ .

1. "Satz 2" from [121] states that  $\text{O}^\#(L_p)$  is generated by all reflections unless  $p = 2$  and  $\bar{q}$  is a hyperbolic plane or an orthogonal direct sum of two hyperbolic planes.
2. "Lemma 1" from loc. cit. states that – unless  $p = 2$  and  $L/pL$  has rank 1, 3, 5 – the group  $W^+(L_p) \cap \text{SO}(L)$  is generated by "good" products of two reflections, i.e., products  $\sigma_x \circ \sigma_y$  with  $q(x) = q(y)$  a unit and  $\bar{x}, \bar{y}$  not in the null-space of  $\bar{b}$ .
3. "Lemma 2" from loc. cit. states that  $W^+(L_p) \cap \text{SO}(L)$  contains **all** of the "good" products except for the above exceptions for  $p = 2$  and some new exceptions for  $p = 3$  where  $L/pL$  has rank 2, 3, 4.

To reduce to this local situation, one introduces the globally defined group

$$S'(L) = \{\text{subgroup of } \text{Clif}^0(q) \text{ generated by } xy \mid x, y \in L, q(x) = q(y) = 1\} \subset \text{Spin}(L),$$

as well as the obvious local version  $S'(L_p) \subset \text{Spin}(L_p)$ .

We first discuss a crucial property of the global group  $S'(L)$  which makes reduction to the local situation possible:

**Step 2.** *The group  $S'(L)$  is a congruence subgroup of  $\text{Spin}(L)$ .* This uses a deep result proven in [120]:

**Theorem.** *If the real Witt index of  $L$  is at least 2 and a normal subgroup  $N$  of  $\text{Spin}(L)$  is not contained in the center of  $\text{Spin}(L)$ , then  $N$  is a congruence subgroup.*

This result applies to  $S'(L)$  since, first of all, it is a normal subgroup of  $\text{Spin}(L)$ : an element  $w \in \text{Clif}^0(q)$  is an even product of vectors  $x \in L$  and conjugation with  $w$

on  $L$  acts as the product of the corresponding reflections  $\sigma_x$  (see formula (13.2)) and so preserves norms. Conjugation with  $w$  sends a product of two elements  $x, y \in L$  to  $wxw^{-1} \cdot wyw^{-1}$  and so is a generator of  $S'(L)$ . Secondly,  $S'(L)$  cannot be contained in the (finite) center of  $\text{Spin}(L)$ . This is the case since by our assumptions ( $L$  is indefinite and  $\text{rank}(L) \geq 4$ ) we can apply Proposition 17.1.1 stating that there are infinitely many roots as soon as the lattice contains at least one root.

To prepare for the next step of the proof, note that a reflection  $\sigma_x$  with  $x \in L$  and  $q(x) = 1$  preserves the lattice  $L$  and so by (13.2) we have a natural map

$$\phi : S'(L) \rightarrow \text{SO}^+(L), \quad xy \mapsto \text{Ad}_{xy}|_L = \sigma_x \circ \sigma_y.$$

Now we can make the reduction to the local situation:

**Step 3. A local-global principle [121, Satz 1].**

$$\begin{aligned} \text{W}^+(L) \cap \text{SO}^+(L) &= \phi(S'(L)) = \bigcap_{p \text{ prime}} \phi(S'(L_p)) \cap \text{SO}^+(L) \\ &= \bigcap_{p \text{ prime}} \text{W}^+(L_p) \cap \text{SO}^+(L). \end{aligned} \quad (17.5)$$

Applying an appropriate approximation theorem, we show that this follows from the congruence property. First observe that the left-hand side is clearly contained in the right-hand side and so it suffices to show that every  $u \in \text{SO}^+(L)$  with the property that it belongs to  $\varpi(S'(L_p))$  for all primes  $p$ , must be of the form  $u = \phi(v)$  with  $v \in S'(L)$ . We claim that by Step 1 we may restrict our attention to a finite set of primes. Indeed, since  $S'(L)$  is a congruence  $\mathfrak{m}$  subgroup of the spinor group, for all primes *not* belonging to the finite set  $S$  of primes dividing  $\mathfrak{m}$  we have  $S'(L_p) = \text{Spin}(L_p)$ . Moreover, for any prime  $p$ ,  $S'(L_p)$  is an open subgroup of  $\text{Spin}(L_p)$ .

By assumption, if  $p \in S$ , we can write  $u = \phi(v_p)$  with  $v_p \in S'(L_p)$  and, adding trivial products  $r \cdot r$  (or  $(-r) \cdot (-r)$ ) we may assume that

$$v_p = r_p^{(1)} s_p^{(1)} r_p^{(2)} s_p^{(2)} \cdots r_p^{(N)} s_p^{(N)}, \quad q(r_p^{(i)}) = q(s_p^{(i)}) = 1, \quad i = 1, \dots, N,$$

where  $N$  is the same for all  $p \in S$ . Now apply Theorem A.3.6 which states that the local roots  $r_p^{(i)}, s_p^{(i)}$  can be approximated (in the  $p$ -adic norm) as good as we want by roots  $r^{(i)}, s^{(i)} \in L$ ,  $i = 1, \dots, N$ . The corresponding product  $\tilde{v} = \prod_{i=1}^N r^{(i)} s^{(i)}$  belongs then to  $S'(L)$ . Since  $S'(L_p)$  is an open subgroup of  $\text{Spin}(L_p)$ , we may choose the roots  $r^{(i)}, s^{(i)}$  close enough to the  $r_p^{(i)}, s_p^{(i)}$  so that  $w := \tilde{v} v_p^{-1} \in S'(L)_p$  for all  $p \in S$ . But for primes  $p \notin S$  one has  $v_p \in S(L_p) = S'(L_p)$  and so  $w \in S'(L_p)$  for *all* primes  $p$ . In other words,  $w$  belongs to  $S'(L)$ . Consequently,  $u = \phi(v_p) = \phi(\tilde{v} \cdot w^{-1}) \in \phi(S'(L))$ .

**Concluding argument.** The conditions on  $L$  imply that  $\dim_{\mathbb{F}_2} L/2L \geq 6$  and  $\dim_{\mathbb{F}_3} L/3L \geq 5$  so that the exceptions in Step 1 do not occur and thus

$$\begin{aligned} \text{W}^+(L) \cap \text{SO}(L) &= \bigcap_p \text{W}^+(L_p) \cap \text{SO}^+(L) \quad (\text{Step 3}) \\ &= \bigcap_p \text{O}^\#(L_p) \cap \text{SO}^+(L) \quad (\text{Step 1}) \\ &= \text{O}^\#(L) \cap \text{SO}^+(L). \end{aligned} \quad \square$$

This result equally applies to  $W^-(L)$ :

**Corollary 17.2.12.** *Under the same conditions on  $(L, q)$ , one has  $W^\epsilon(L) = O^{\epsilon, \#}(L)$ .*

*Proof.* By the (proof of) Theorem 17.2.11, the group  $W^+(L) \cap \text{SO}(L)$  is generated by products  $u = \sigma_x \sigma_y$  of two reflections in roots  $x, y$  with  $q(x) = q(y) = 1$  (and so  $\text{Nm}_{\text{spin}} u = 1$ ). Since  $W^+(L) = W^+(L) \cap \text{SO}(L) \cup \sigma_x \cdot [W^+(L) \cap \text{SO}(L)]$ , one has  $W^+(L) = O^{+, \#}(L)$ . Replace  $L$  with  $L(-1)$ . The assumptions hold equally well for the lattice  $L(-1)$ . The same argument with the  $(-)$ -spinor norm gives the result for  $\epsilon = -1$ .  $\square$

*Remark 17.2.13.* The condition on the signature is necessary as we see from Theorem 17.2.9 which demonstrates that the Weyl group in a Lorentzian lattice is rarely of finite index in the full orthogonal group. See also Theorem 17.3.7 below.

## 17.3 Eichler–Siegel Transformations

**17.3.A Basic properties.** Before considering lattices, we first consider rational inner product spaces  $(V, b)$ , where  $b$  is the polar form of a quadratic form  $q$ .

**Definition 17.3.1.** Given a pair of vectors  $\{f, y\}$  in  $V$  where  $f$  is isotropic and  $b(f, y) = 0$ , the *Eichler–Siegel transformation* with respect to  $\{f, y\}$  is given by

$$\begin{aligned} \psi_{f,y} : V &\longrightarrow V \\ x &\longmapsto x + b(x, y)f - b(x, f)y - b(x, f)q(y)f. \end{aligned} \quad (17.6)$$

The linear map  $\psi_{f,y}$  is an isometry (by direct computation) with inverse  $\psi_{f,-y}$  (see Lemma 17.3.3). If  $y$  and  $f$  are linearly dependent, then  $\psi_{f,y}$  is simply the identity.

**Lemma 17.3.2.** *Assume that  $q(y) \neq 0$ . Then the Eichler–Siegel transformation  $\psi_{f,y}$  is the unique isometry of  $V$  which satisfies*

$$\psi_{f,y}z = z + b(z, y)f \quad \forall z \in \mathbb{R}f^\perp.$$

*In particular,  $\psi_{f,y}f = f$ .*

*Proof.* Since  $b$  is non-degenerate  $\dim V \geq 3$ , and so there exists a vector  $g$  with  $b(f, g) = 1$  and  $b(g, y) = 0$ . The vectors  $f, g, y$  span a three-dimensional space  $W$ , and  $g$  and  $f^\perp$  span  $V$ . Let  $\psi : V \rightarrow V$  be an isometry which acts on  $f^\perp$  in the same way as  $\psi_{f,y}$ . Then we need to verify that  $\psi(g) = \psi_{f,y}(g) = g - q(y)f - y$ . Since  $W^\perp \subset f^\perp$  and  $\psi_{f,y}|_{W^\perp} = \text{id}$ , we have  $\psi|_{W^\perp} = \text{id}$  and so  $\psi(W) \subset W$  (here we use that  $(W^\perp)^\perp = W$ , see Lemma 1.1.3). Now let  $\psi(g) = \alpha g + \beta f + \gamma y$ . Expanding the equations

$$\begin{aligned} 1 &= b(\psi(g), \psi(f)) \\ 0 &= b(\psi(g), \psi(y)) \\ b(g, g) &= b(\psi(g), \psi(g)), \end{aligned}$$

yields  $\alpha = 1, \gamma = -1$  (here we use  $q(y) \neq 0$ ), and  $\beta = -q(y)$ .  $\square$

From now on, we again suppose that  $L$  is a non-degenerate symmetric lattice and  $V = L_{\mathbb{Q}}$ . Observe that the defining equation (17.6) shows that the Eichler–Siegel transformation  $\psi_{f,y}$  of  $V$  preserves  $L$  provided  $f$  and  $y$  belong to  $L$  and  $q(y) \in \mathbb{Z}$ . We can say more:

**Lemma 17.3.3.** *Suppose  $f \in L$  is a primitive isotropic vector and suppose  $y \in L$  satisfies  $b(y, y)$  even and  $b(f, y) = 0$ . Then  $\psi_{f,y}$  induces a lattice isometry of  $L$  with the following properties.*

1.  $\psi_{f,y} \in \mathcal{O}^{\epsilon}(L)$  for  $\epsilon = -$  as well as for  $\epsilon = +$ .
2.  $\psi_{f,y}$  induces the identity on the discriminant group.
3. One has  $\psi_{f,y} = \psi_{f,y+f}$  and the map

$$\begin{array}{ccc} L_f = f^{\perp}/\mathbb{Z}f & \xrightarrow{\psi_f} & \mathcal{O}(L) \\ y + \mathbb{Z}f & \mapsto & \psi_{f,y} \end{array}$$

is a well-defined injective group homomorphism. In particular  $\psi_f(L_f)$  is an abelian subgroup of  $\mathcal{O}(L)$  whose rank equals  $\text{rank}(L_f)$ .

4.  $\psi_f(L_f)$  is a normal subgroup of  $\mathcal{O}_f(L)$ , the stabilizer of  $f$ .

*Proof.* 1. The spinor norm is continuous on  $\mathcal{O}(V_{\mathbb{R}})$  (see Remark 13.3.6.2) and the path  $t \mapsto \psi_{tf,y}$  belonging to  $\mathcal{O}(V_{\mathbb{R}})$  connects  $\psi_{f,y}$  to the identity and so  $\text{Nm}_{\text{spin}}^{\epsilon} \psi_{f,y} = 1$ .

2. Let  $u \in L^*$ , then, since  $b(u, y)$ ,  $b(u, f)$  and  $q(y)$  are integers, (17.6) shows that  $\psi_{f,y}u \equiv u \pmod{L}$  which means precisely that  $\psi_{f,y}$  induces the identity on  $\text{dg}_L$ .

3. Note that  $q(y+f) = q(y) + q(f) + b(y, f) = q(y)$ . Using this, the first assertion and the well-definedness of  $\psi_f$  follow from

$$\begin{aligned} \psi_{f,y+f}(x) &= x + b(x, y+f)f - b(x, f)(y+f) - b(x, f)q(y+f)f \\ &= x + b(x, y)f + b(x, f)f - b(x, f)y - b(x, f)f - b(x, f)q(y)f \\ &= x + b(x, y)f - b(x, f)y - b(x, f)q(y)f \\ &= \psi_{f,y}(x). \end{aligned}$$

The second assertion follows from

$$\begin{aligned} \psi_{f,y'} \circ \psi_{f,y}(x) &= \psi_{f,y'}(x + b(x, y)f - b(x, f)y - b(x, f)q(y)f) \\ &= x + b(x, y')f - b(x, f)y' - b(x, f)q(y')f \\ &\quad + b(x, y)f - b(x, f)y - b(x, f)b(y, y')f \\ &\quad \quad \quad - b(x, f)q(y)f \\ &= x + b(x, y+y')f - b(x, f)(y+y') - b(x, f)q(y+y')f \\ &= \psi_{f,y+y'}(x), \end{aligned}$$

where we have used

$$\begin{aligned}\psi_{f,y'}(f) &= f, \\ \psi_{f,y'}(y) &= y + b(y, y')f.\end{aligned}$$

That we get an injection follows since if  $\psi_{f,y} = \text{id}$ , then either  $y$  and  $f$  are dependent or  $b(x, f)y = 0$  for all  $x \in L$  in which case  $y = 0$  since  $b$  is non-degenerate.

4. This is because for all  $g \in \mathcal{O}_f(L)$  we have  $g \circ \psi_{f,y} \circ g^{-1} = \psi_{gf,gy} = \psi_{f,gy}$ .  $\square$

Property 3 shows that a non-degenerate lattice of rank  $\geq 3$  containing isotropic vectors and at least one vector  $y \in f^\perp - \mathbb{Z} \cdot f$  with  $b(y, y)$  even has an infinite isometry group. The existence of such a  $y$  with  $b(y, y)$  even can be circumvented by replacing  $L$  with  $L(2)$  which has the same isometry group as  $L$ . Hence we have shown:

**Proposition 17.3.4.** *Let  $L$  be a non-degenerate lattice of rank  $n \geq 3$  containing an isotropic vector. Then  $\mathcal{O}(L)$  contains a free abelian group of rank  $n - 2$ . In particular,  $L$  has infinitely many isometries.*

**Corollary 17.3.5.** *Let  $L$  be a non-degenerate indefinite lattice of rank  $\geq 5$ , then  $\mathcal{O}(L)$  is infinite.*

*Proof.* By Meyer's theorem 3.3.4, the rational space  $L_{\mathbb{Q}}$  has an isotropic vector and hence this is also the case for  $L$ .  $\square$

Eichler–Siegel transformations of the form  $\psi_{f,r}$  with  $r$  a  $(-2)$ -root are compositions of reflections. More is true:

**Proposition 17.3.6.** *Let  $L$  be a non-degenerate lattice of rank  $n$  containing a primitive isotropic vector  $f$  and a  $(-2)$ -root  $r \in f^\perp$ . Then*

1.  $\psi_{f,r} = \sigma_{f-r} \circ \sigma_r$ .
2. The image of the  $(-2)$ -root lattice of  $L_f$  under  $\psi_f : L_f \rightarrow \mathcal{O}(L)$  is contained in the Weyl group  $W^-(f^\perp)$  considered as the subgroup of  $W^-(L)$  generated by reflections in  $(-2)$ -roots of  $f^\perp$  (and hence preserving  $f$ ).
3. If  $y \in L_f$  is orthogonal to the  $(-2)$ -root lattice  $L_{f,\text{root}}$  of  $L_f$ , then  $\psi_f(y)$  restricts to the identity on the  $(-2)$ -root lattice of  $f^\perp$ . In particular,  $W^-(f^\perp) \cap \psi_f(L_{f,\text{root}}^\perp) = \{\text{id}\}$ .

*Proof.* 1. Given two  $(-2)$ -roots  $r, r'$  in a lattice  $(L, b)$ , one has

$$\sigma_{r'} \circ \sigma_r(x) = \sigma_r(x) + b(r', \sigma_r(x))r' = x + b(x, r)r + b(x, r')r' + b(r, r')b(x, r)r', \quad x \in L.$$

Substituting  $r' = f - r$ , one gets  $\sigma_{r-f} \circ \sigma_r(x) = x + b(x, r)f - b(x, f)r + b(x, f)f = \psi_{f,r}(x)$ .

2. From 1 we infer that if  $y = \sum a_j r_j$ , a  $\mathbb{Z}$ -linear combination of roots in  $f^\perp$ , then  $\psi_{f,y} = \prod_j (\sigma_{f-r_j} \circ \sigma_{r_j})^{a_j} \in W^-(f^\perp)$ .

3. In this situation  $\psi_{f,y}(x) = x + b(x, y)f$ . Hence, if the class of  $y$  belongs to  $L_{f,\text{root}}^\perp$ ,

then  $\psi_{f,y}$  is clearly the identity on the  $(-2)$ -root lattice of  $f^\perp$ .

Finally, suppose that  $\gamma \in W^-(f^\perp) \cap \psi_f(L_{f,\text{root}}^\perp)$ . Then  $\gamma$  is a composition of reflections in  $(-2)$ -roots of  $f^\perp$  inducing the identity on the lattice  $M := f_{\text{root}}^\perp$  spanned by all such  $(-2)$ -roots  $r$ . But then  $\gamma = \text{id}_L$  since it is the identity on the orthogonal complement of  $M$  in  $L$ , because this is the intersection of the reflection hyperplanes for the  $\sigma_r \in M$ .  $\square$

**17.3.B Application to Lorentzian lattices.** The aim is to find a criterion which ensures that a Lorentzian lattice  $L$  is not  $(-2)$ -reflective, i.e., a lattice for which the reflection group generated by reflections in  $(-2)$ -roots is not of finite index in  $O(L)$ . We start with a technical result.

**Lemma.** *Suppose that a Lorentzian lattice  $L$  contains a (primitive) isotropic vector  $f$ . Then*

$$W_f^- L = W^-(f^\perp), \quad (17.7)$$

where we recall that  $W_f^- L$  is the subgroup of the Weyl group of  $L$  fixing  $f$ , and the right-hand side,  $W^-(f^\perp)$ , is identified with the subgroup of  $W^-(L)$  generated by reflections in  $(-2)$ -roots of  $f^\perp$  (and hence preserving  $f$ ).

*Proof.* We first construct a partitioning of the  $(-2)$ -roots in  $L$  using that a root  $r$  either is contained in  $f^\perp$ , or else  $b(r, f) \neq 0$ . Choosing  $z \in f^\perp \otimes \mathbb{R}$  not belonging to the hyperplanes orthogonal to roots in  $f^\perp$ , the former can be partitioned into  $\Delta_1^+ \cup -\Delta_1^+$  where each root  $r \in \Delta_1^+$  satisfies  $b(r, z) > 0$ . A root with  $b(r, f) \neq 0$  either satisfies  $b(r, f) > 0$ ; such roots form a set  $\Delta_2^+$ . Or one has  $b(r, f) < 0$  and such roots form  $-\Delta_2^+$ . Combining the two gives a partition  $\Delta^+ \cup -\Delta^+$ ,  $\Delta^+ = \Delta_1^+ \cup \Delta_2^+$  of the roots in  $L$ . This partition is closed under taking sums: a root which is a sum of roots from  $\Delta^+$  belongs to  $\Delta^+$ . Hence, by Proposition 17.2.6 it defines a Weyl chamber and Remark 17.2.8 implies that the Weyl group is generated by reflections in indecomposable roots.

To continue, note first that  $W^-(f^\perp) \subset W_f^- L$ . Conversely, assume that  $g \in W_f^- L$  and write  $g$  as a product of reflections from  $\Delta_1^+$  and  $\Delta_2^+$ . If  $g \notin W^-(f^\perp)$  at least one reflection  $\sigma_r$ ,  $r \in \Delta_2^+$ , must appear in the product and then  $b(\sigma_r(f), f) > 0$ . Products of reflections in roots from  $\Delta_1^+$  do not alter this number. So we may assume that  $g = \sigma_{r_k} \circ \dots \circ \sigma_{r_1}$  with indecomposable roots  $r_j \in \Delta_2^+$ . Since the number  $b(g(f), f)$  does not depend on the order of the roots  $r_j$  in the expression for  $g$ , we may assume that each root appears at most once. For two different indecomposable roots  $r_i, r_j$  we have  $b(r_i, r_j) \geq 0$ . It then follows inductively that for any finite product  $g$  of different indecomposable roots in  $\Delta_2^+$  one has  $b(g(f), f) > 0$  contradicting our assumption that  $g(f) = f$ .  $\square$

This result yields the criterion we are after:

**Proposition 17.3.7** (compare [172, Prop. 1.3.1]). *For a Lorentzian type lattice  $L$  of rank  $\geq 3$  containing a primitive isotropic vector  $f$  and associated negative definite lattice  $L_f = f^\perp/\mathbb{Z}f$ , let  $\delta_f = \text{rank}(L_f) - \text{rank}(L_{f,\text{root}})$ . Then  $O(L)/W^-(L)$*

contains a normal abelian subgroup of rank  $\delta_f$ . In particular, if  $L_f$  is not spanned by its roots, the group  $O(L)/W^-(L)$  is infinite.

*Proof.* By Proposition 17.3.6 and (17.7) we have  $W_f^-(L) \cap \psi_f(L_{f,\text{root}}^\perp) = \{\text{id}\}$ . Since  $\text{Im}(\psi_f) \subset O_f(L)$ , the intersection  $W_f^-(L) \cap \text{Im}(\psi_f)$  coincides with the intersection  $W^-(L) \cap \text{Im}(\psi_f)$ . Consequently,  $\psi_f(L_{f,\text{root}}^\perp) \subset O(L)/W^-(L)$ . By Lemma 17.3.3, the Eichler–Siegel transformations  $\psi_{f,y}$ ,  $y \in \psi_f(L_f)$ , form an abelian subgroup  $\psi_f(L_f)$  of the stabilizer of  $f$  in  $O^-(L)$ . Since  $\text{rank}(\psi_f L_f) = \text{rank}(L_f)$ , it follows that  $\psi_f(L_f)/W^-(L)$  contains an abelian group of rank  $\delta_f$ .  $\square$

**Example 17.3.8.** Consider the root lattice of the Lorentz lattices  $E^{1,n}$  of Examples 17.2.10.1. If  $n = 2$ , the lattice is spanned by  $\alpha_0 = (1, -1, -1)$ ,  $\alpha_1 = (0, 1, -1)$  and  $\alpha_2 = (0, 0, 1)$ . It contains the isotropic vector  $f = \alpha_0 + \alpha_1 + \alpha_2$  and  $f^\perp/\mathbb{Z}f$  has rank 1 and is spanned by the class of  $\alpha_0$  which is a  $(-1)$ -root and not a  $(-2)$ -root. A similar calculation shows that  $E^{1,3}$  is not  $(-2)$ -reflective.

For  $n = 5, \dots, 9$  the computation is slightly different: the vector  $f = e_0 + e_n = \alpha_0 + \sum_{i=1}^n i\alpha_i$  is isotropic and  $f^\perp/f$  has root basis  $\alpha_1, \dots, \alpha_{n-2}, \alpha_{n-1} + \alpha_n$  which gives the root system  $B_{n-1}$  and so  $f^\perp/f$  is not spanned by  $(-2)$ -roots. Hence also for  $n = 5, \dots, 9$  the root-lattice for  $\mathbb{Z}^{1,n}$  is not  $(-2)$ -reflective.

### 17.3.C Application to lattices splitting off copies of the hyperbolic plane.

This situation occurs frequently in the study of singularities as we shall see in Chapter 18. Assume that we are given an even lattice  $L = U \oplus L'$  and we let  $\{e, f\}$  be the standard basis of  $U$ . Then for all  $y \in L'$  one has Eichler–Siegel transformations  $\psi_{e,y}$  as well as  $\psi_{f,y}$ . The group generated by those transformations will be denoted by

$$\psi_U(L') = \langle \psi_{e,y}, \psi_{f,y} \rangle_{y \in L'} \subset O(L).$$

As indicated by the notation, this group does not depend on the choice of basis for  $U$  (see Example 17.1.2.2). The following result shows how one can use Eichler–Siegel transformations to describe certain orbits under the isometry group.

**Lemma 17.3.9** ([144, Lemma 2.5]). *Let  $U$  be a hyperbolic plane with standard basis  $\{e, f\}$ . Consider the lattice  $U \oplus U'$  where  $U'$  is another hyperbolic plane. Then  $\psi_U U' = \psi_{U'} U \simeq \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z})$ . Moreover, every vector  $x$  is in the  $\psi_U(U')$ -orbit of some vector of the form  $ae + df$  with  $d|a$ . In particular, if  $x$  is primitive with  $q(x) = a$ , we can take  $d = 1$ .*

*Proof.* Let  $\{e', f'\}$  be a standard basis for  $U'$ , then

$$ae + df + be' + cf' \mapsto \begin{pmatrix} a & b \\ -c & d \end{pmatrix}$$

defines an isometry between  $U \oplus U'$  and  $(\text{Mat}(2 \times 2, \mathbb{Z}), \det)$ . Under this isometry the transformations  $\psi_{e,\pm e'}, \psi_{e,\pm f'}, \psi_{f,\pm e'}, \psi_{f,\pm f'}$  correspond to row and column additions and subtractions. Since  $\text{SL}_2(\mathbb{Z})$  is generated by the corresponding elementary matrices, this shows in particular that  $\psi_U U' = \psi_{U'} U \simeq \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z})$  – the



first copy acting from the left on  $2 \times 2$  integral matrices, and the second copy acting from the right. Using these elementary transformations, a given matrix  $M \in \text{Mat}(2 \times 2, \mathbb{Z})$  can be put in diagonal form  $\text{diag}(a, d)$  with  $d|a$  (use the elementary divisor theorem A.1.2 applied to the submodule of  $\mathbb{Z}^2$  generated by the column vectors  $\begin{pmatrix} a \\ -c \end{pmatrix}$  and  $\begin{pmatrix} b \\ d \end{pmatrix}$ ). In terms of a primitive vector  $x \in U \oplus U'$  this means that we can either take  $x = f$  or  $x = ae + f$ .  $\square$

**Corollary 17.3.10.** *Suppose  $L = U \oplus L'$ , with  $L' = U' \oplus L''$ ,  $L''$  even, and let  $x \in L$ . Then*

1. *there exists an isometry of  $L$  belonging to  $\psi_U(U')$  which sends  $x$  to  $\alpha e + \beta f + x''$  with  $\beta|a$  and  $x'' \in L''$ ;*
2. *if, moreover,  $b(x, L) = \mathbb{Z}$ , there is an isometry belonging to  $\psi_U(L')$  sending  $x$  to  $ae + f$ ,  $a = q(x)$ .*

*Proof.* Assume  $x = x' + x''$  with  $x' \in U \oplus U'$  and  $x'' \in L''$ .

1. This follows by applying Lemma 17.3.9 to  $x'$ . We thus may assume that  $x' = \alpha e + \beta f \in U$ , where the integer  $\beta$  divides the integer  $\alpha$ . This implies

$$b(x, u) \equiv 0 \pmod{\beta}, \quad \forall u \in U. \quad (17.8)$$

2. Suppose that  $y \in L$  satisfies  $b(x, y) = 1$  and write  $y = u + y'$ ,  $u \in U, y' \in L'$ , and apply  $\psi = \psi_{e, y'}$  to  $x$ . Then we have  $\psi(e) = e$  and  $\psi(f) = f - y' - q(y')e$ . Since  $\psi^{-1} = \psi_{e, -y'}$  we find  $\psi^{-1}(f) = f + y' - q(y')e$  and so, writing  $\psi(x) = a'e + b'f + z$ ,  $z \in L'$ , one finds

$$\begin{aligned} b' &= b(\psi x, e) = b(\psi x, \psi e) = b(x, e) = \beta \\ a' &= b(\psi x, f) = b(x, \psi^{-1} f) = b(x, f + y' - q(y')e) = \alpha + b(x, y') - q(y')\beta \\ &\equiv b(x, y') \pmod{\beta} \text{ since } \beta|a \\ &\equiv b(x, u + y') \pmod{\beta} \text{ by (17.8)} \\ &\equiv b(x, y) \pmod{\beta} \\ &\equiv 1 \pmod{\beta} \text{ by the assumption on } y. \end{aligned}$$

It follows that  $a'e + b'f \in U$  is primitive and so, again by Lemma 17.3.9, we may assume that  $b' = 1$ , that is, the  $\psi_U L'$ -orbit of  $x$  contains a vector of the form  $a'e + f + z'$ . Applying  $\psi_{e, z'}$  to this vector yields a vector of the form  $\tilde{x} = a e + f$  with  $a = q(\tilde{x}) = q(x)$ .  $\square$

In Section 18.1 we shall use some more properties of lattices that split off a hyperbolic plane:

**Lemma 17.3.11.** *Let  $L$  be an even lattice. Suppose that  $L = U \oplus L'$  and let  $\{e, f\}$  be a standard basis for  $U$ . Then*

1. *The group  $O(U)$  normalizes  $\psi_U(L')$ .*

2. Suppose that  $r \in L'$  is a  $(-2)$ -root. Then

$$\psi_{e,r} = \sigma_r \circ \sigma_{r+e} \tag{17.9}$$

$$\sigma_r = \psi_{f,r} \circ \psi_{e,-r} \circ \psi_{f,r} \circ \sigma_{e-f} \tag{17.10}$$

3. Suppose that  $L'$  is a lattice generated by  $(-2)$ -roots. Then  $\psi_U(L') \subset W^-(L)$ .

*Proof.* 1. By Example 17.1.2 we only have to consider the effect of the reflection  $\sigma_{e-f}$  interchanging  $e$  and  $f$ . For  $y \in L'$  one finds  $\sigma_{e-f} \circ \psi_{e,y} \circ \sigma_{e-f} = \psi_{f,y}$  and likewise  $\sigma_{e-f} \circ \psi_{f,y} \circ \sigma_{e-f} = \psi_{e,y}$ .

2. By Lemma 17.3.3.3 we have  $\psi_{e,r} = \psi_{e,r+e}$  which by Proposition 17.3.6.1 equals  $\sigma_{e-(r+e)} \circ \sigma_{r+e} = \sigma_{-r} \circ \sigma_{r+e}$ .

□

**Historical and Bibliographical Notes.** Isometries in hyperbolic spaces and for Lorentzian lattices have been studied by many people, especially by É. Vinberg [237, 238, 239, 240] and by V. Nikulin [170, 172]. Reflection subgroups of lattices with higher Witt index have been investigated by M. Kneser [121]. M. Eichler remarks in Kap. V.1. of [67] that his transformations  $\psi_{f,y}$  that we introduced in Section 17.3 were for the first time used by C.-L. Siegel, whence the terminology "Eichler–Siegel transformation". The present treatment is heavily influenced by W. Ebeling's book [62] and the articles [60, 61].

## Applications to Singularities

### Introduction

In this chapter we consider quadratic lattices  $(L, q)$  generated by roots  $r$  with  $q(r) = -1$ . If a spanning set  $\Delta$  of roots can be found which forms a single orbit under the Weyl group  $W^-(\Delta)$ , we speak of a vanishing lattice. As we shall see in Section 18.2, these occur in the study of monodromy of singularities and of families of hypersurfaces in projective space.

The goal of Section 18.1 is twofold. First we describe tools to recognize vanishing lattices. The second goal is to see when the Weyl group is as large as possible, that is, equal to  $O^{-\#}(L)$ . The idea is first to show that  $W^-(\Delta) = W^-(L)$  and then to apply M. Kneser's result, Theorem 17.2.11.

In practice  $L$  is often the lattice associated to a generalized Dynkin diagram  $\Gamma$ . However, in general the roots corresponding to the vertices of  $\Gamma$  do not define a vanishing lattice. Theorem 18.1.7 provides a large class of Dynkin diagrams that do not suffer from this defect. As demonstrated in Section 18.2, these can be used to determine the monodromy group of many singularities.

However, in applications we need more, namely a class of vanishing lattices which in a certain sense is stable under inclusions, the so-called complete vanishing lattices (cf. Definition 18.1.4). Many lattices associated to Dynkin diagrams yield complete vanishing lattices and so for those not only  $W^-(L) = O^{-\#}(L)$ , but this equality persists under inclusion into larger vanishing lattices. This is used in Section 18.3 to determine global monodromy groups (cf. Theorem 18.3.2).

### 18.1 Generalized Dynkin Diagrams and Vanishing Lattices

In this section  $(L, q)$  is a quadratic integral lattice with polarization  $b$ . By "root" we shall mean "(-2)-root" and accordingly we set  $\epsilon = -$ . With appropriate changes all results are valid for 2-roots and  $\epsilon = +$ . The set of roots in  $L$  is denoted  $\Delta(L)$ , the lattice generated by these  $L_{\text{root}}$ , and the Weyl group  $W^-(L)$ .

The lattices we consider in this chapter are spanned by roots which form the nodes of a graph. If  $r, r'$  are such roots and  $b(r, r') = 1$ , as usual, we connect the corresponding nodes by an unlabelled edge. In the lattices also pairs  $\{r, r'\}$  occur for which  $b(r, r') = -2$ . We connect the corresponding nodes by a doubly dashed edge. The resulting graphs  $\Gamma$  are called (*generalized*) *Dynkin diagrams* and

the corresponding even integral lattice  $L_\Gamma$  they give rise to the **associated root-lattice**. Identifying the vertices of  $\Gamma$  with roots in  $L_\Gamma$ , the **Weyl group**  $W^-(\Gamma)$  of  $\Gamma$  is the group generated by the reflections determined by  $\Gamma$ .

Let  $\Delta \subset L_\Gamma$  be a set of roots. A **1-connected path within  $\Delta$  from  $r \in \Delta$  to  $r' \in \Delta$**  is a chain  $r = r_0, r_1, \dots, r_N = r'$  of roots in  $\Delta$  such that  $b(r_j, r_{j+1}) = 1$ ,  $j = 0, \dots, N - 1$ . This defines an equivalence relation on  $\Delta$ . The equivalence classes are called the **1-connected components** of  $\Delta$ . If there is only one component,  $\Delta$  is called a **1-connected set**. The Dynkin diagrams associated to finite 1-connected sets of roots are connected. Such graphs will be called 1-connected. Similarly, one can speak of the 1-connected components of a Dynkin graph.

We also need a suitable notation to deal with orbits of a possibly infinite set of roots, say  $\Lambda \subset L$ . If  $W^-(\Lambda)$  is the group generated by the reflections  $\sigma_\lambda$ ,  $\lambda \in \Lambda$ , we shall denote the orbit of  $\Lambda$  by the corresponding bold letter:

$$\mathbf{\Lambda} = W^-(\Lambda) \Lambda \subset L_{\text{root}}.$$

**Lemma 18.1.1.** *Two roots in a 1-connected component of a set of roots  $\Delta \subset L = L_\Gamma$  belong to the same  $W^-(\Delta)$ -orbit.*

*Proof.* This follows from the observation that for any two roots  $r_i, r_j$  with  $b(r_i, r_j) = 1$ , one has  $\sigma_{r_i} \sigma_{r_j} r_i = \sigma_{r_i}(r_i + r_j) = r_j$ . □

As announced, the specific root lattices coming from singularities are the vanishing lattices, ordered under containment:

**Definition 18.1.2.** 1. A **vanishing lattice** consists of a pair  $(L, \Delta)$  of a lattice  $L$  and a set of roots  $\Delta$  spanning  $L$  and forming a single orbit under  $W^-(\Delta) = \langle \sigma_r \rangle_{r \in \Delta}$ , that is  $\Delta = \mathbf{\Delta}$ .

2. A vanishing lattice  $(L, \Delta)$  **contains the vanishing lattice**  $(L', \Delta')$  if  $L'$  is a primitive sublattice of  $L$  and  $\Delta' \subset \Delta$ .

*Remark 18.1.3.* The vertices of a generalized Dynkin diagram  $\Gamma$  form a finite set of roots, say  $\Delta$ , spanning the lattice  $L_\Gamma = \mathbb{Z} \cdot \Delta$ . If  $\Delta$  is 1-connected, by Lemma 18.1.1 all roots in  $\Delta$  are in the same orbit under the reflection group  $W^-(\Delta)$ , but  $\Delta$  need not be an entire orbit. Taking  $\mathbf{\Delta} = W^-(\Delta)$  instead of  $\Delta$  then yields a vanishing lattice. In general, if the subset  $\Delta$  of roots of  $L$  belongs to a single  $W^-(\Delta)$ -orbit, this procedure yields a vanishing lattice. Clearly, this also shows that such a vanishing lattice is determined by the lattice itself.

For a general vanishing lattice  $(L, \Delta)$ , the Weyl group  $W^-(L)$  of course contains the subgroup  $W^-(\Delta)$ , but the entire Weyl group of  $L$  might be larger. Our goal is to give a large class of vanishing lattices for which  $W^-(\Delta) = W^-(L)$ . Since in applications we need a class of vanishing lattices which is stable under containment, we shall look within the class of so-called complete vanishing lattices (see below for their definition). The basic building block for such lattices is the pair  $(L_{\min}, \mathbf{\Gamma}_{\min})$

with  $L_{\min} := U \oplus U' \oplus A_2(-1)$  and, using the standard basis  $\{e, f\}$  of  $U$ ,  $\{e', f'\}$  of  $U'$ ,  $\{\omega_1, \omega_2\}$  of  $A_2(-1)$  with

$$\Gamma_{\min} = \{r_1 = e - f, r_2 = \omega_1 - e, r_3 = \omega_1, r_4 = \omega_2, r_5 = \omega_1 - e', r_6 = e' - f'\}.$$

There are of course other choices for a spanning set of roots, e.g., we may replace  $r_2$  with  $r'_2 = -\omega_1 - \omega_2 - e - (e' + f')$  and  $r_5$  with  $r'_5 = -\omega_1 - \omega_2 - e' - (e + f)$  which gives the graph  $\Gamma'_{\min}$ . The two graphs are depicted in Fig. 18.1.1. Both graphs are connected and since the transition matrix expressing the roots in the basis is unimodular, the roots give a basis of  $L_{\min}$  and so this indeed defines vanishing lattices.<sup>1</sup>

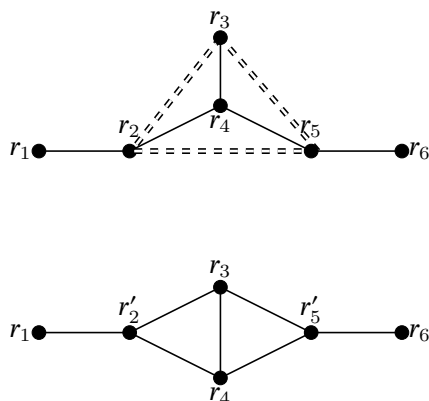


Figure 18.1.1:  $\Gamma_{\min}$  and  $\Gamma'_{\min}$

**Definition 18.1.4.** A vanishing lattice  $(L, \Delta)$  is called *complete* if it contains a copy of  $(L_{\min}, \Gamma_{\min})$ .

This concept is obviously preserved under containment of vanishing lattices; since this plays a central role later on, we set this apart.

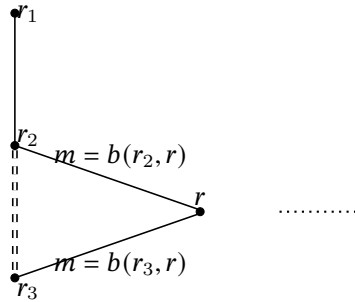
**Lemma 18.1.5.** A vanishing lattice containing a complete vanishing lattice is itself complete.

We shall further make use of some technical concepts which play a central role in the proofs that follow:

**Definition 18.1.6.** A (possibly infinite) subset  $\Lambda$  of roots in  $L$  is called a *special subset of roots* of  $L$  if it contains three roots  $r_1, r_2, r_3$ , by definition a *socle* of  $\Lambda$ , which have the following two properties:

1. The intersection behaviour of roots in the socle and with other roots  $r \in \Lambda$  is as in the following graph:

<sup>1</sup>The graph  $\Gamma'_{\min}$  is the graph used by Beauville in [18]



In other words,  $b(r_1, r_2) = 1$ ,  $b(r_2, r_3) = -2$ ,  $b(r_1, r) = 0$  for  $r \neq r_1, r_2$  and, finally,  $b(r, r_2) = b(r, r_3)$  for  $r \neq r_1, r_2, r_3$ . In particular it follows that  $r_1, r_2, r_3$  are independent (consider the Gram matrix).

2. The set  $\Lambda' = \Lambda - \{r_1, r_2\}$  is 1-connected.

We make some observations and introduce related terminology.

- If the set  $\Lambda$  contains at least 4 elements, it is 1-connected since then there exists  $r \in \Lambda'$ ,  $r \neq r_3$  for which  $b(r_3, r) = 1$  and thus  $b(r_2, r) = 1$ .
- The hyperbolic plane with standard basis  $e = -r_2 + r_3$ ,  $f = -r_1 - r_2 + r_3$  is called the **socle plane**, and the resulting decomposition  $L = U \oplus L'$  the **socle decomposition**. The lattice generated by  $\Lambda'$  belongs to  $L'$  as is easily verified.

The usefulness of these concepts and remarks is illustrated by the next result. Its formulation uses Eichler–Siegel transformations defined in Section 17.3, and the proof makes essential use of the results of § 17.3.C.

**Theorem 18.1.7** ([60, Thm 3]). *Let  $(L, q)$  be a quadratic lattice of rank at least 4 containing a special subset  $\Lambda$  of roots which span  $L$ . Then  $(L, \Lambda)$  is a vanishing lattice. If, moreover,  $L$  splits off an extra hyperbolic plane besides the socle plane, then  $W^-(L) = W^-(\Lambda)$ . More precisely, we have:*

1.
  - Let  $U$  be the socle plane and  $L = U \oplus L'$  the corresponding socle decomposition. Then  $L'$  is spanned by  $\Lambda' = \Lambda - \{r_1, r_2\}$ .
  - Conversely, let  $L$  be a quadratic lattice of rank at least 4 with a decomposition  $L = U \oplus L'$ , where  $L'$  is spanned by a 1-connected set of roots  $\Lambda'$ . Let  $\{e, f\}$  be the standard basis of  $U$  and  $r_3 \in \Lambda'$ . Then the set of roots  $r_1 = e - f, r_2 = -e + r_3, r_3, r \in \Lambda'$  forms a special subset of roots.
2. With  $\Lambda'$  as in 1, the roots  $r' \in \Lambda'$  belong to the same  $W^-(L')$ -orbit.
3.  $\psi_U L' \subset W^-(\Lambda)$ .
4. If, moreover,  $L' = U' \oplus L''$  for some hyperbolic plane  $U'$ , then  $W^-(\Lambda) = W^-(L)$ . In other words, the Weyl group of  $L$  is generated by the reflections  $\sigma_r$ , where the roots  $r$  belong to  $\Lambda$ .

*Proof.* We already observed that we get a vanishing lattice if  $\Lambda$  has at least 4 elements, since then  $\Lambda$  is 1-connected (cf. Definition 18.1.6 and use Remark 18.1.3).

1. Since  $\Lambda$  spans  $L$ ,  $L'$  is spanned by  $\Lambda'$ . Conversely, the crucial input is  $b(e, r) = b(f, r) = 0$  for  $r \neq r_1, r_2$  so that  $b(r_2, r_3) = b(-e + r_3, r_3) = b(r_3, r_3) = -2$  while  $b(r_2, r) = b(-e + r_3, r) = b(r_3, r)$  if  $r \neq r_1, r_2, r_3$ .

2. By the assumption on the 1-connectedness, Lemma 18.1.1 shows that all roots  $r \neq r_1, r_2$  are in the  $G$ -orbit of  $r_3$ , where  $G$  is the group generated by the reflections  $\sigma_r, r \neq r_1, r_2$ . This group is contained in  $W^-(L')$ .

3. The group  $\psi_U L'$  is generated by  $\psi_{e,r}$  and  $\psi_{f,r}$  where  $r$  runs through a generating set of  $L'$ . We take for the latter the set of roots  $\Lambda'$ . By equation (17.9), these isometries are products of the reflections  $\sigma_r$  and  $\sigma_{r-e}$  or  $\sigma_r$  and  $\sigma_{r-f}$  with  $r \in \Lambda'$ . Let us deduce that the above generators for  $\psi_U L'$  belong to  $W^-(\Lambda)$ .

- Since  $r_3 - e = r_2$ , the corresponding reflection is in  $W^-(\Lambda)$ .
- For  $r_3 - f = r_1 + r_2 = \sigma_{r_1} r_2$  we have  $\sigma_{r_3-f} = \sigma_{r_1} \circ \sigma_{r_2} \circ \sigma_{r_1} \in W^-(\Lambda)$ .
- Assume that  $r \in \Lambda'$ . Since  $\Lambda'$  is 1-connected, we may write  $r = g(r_3)$  for some  $g \in W^-(\Lambda')$ . But then

$$\begin{aligned}\sigma_{r-e} &= g \circ \sigma_{r_3-e} \circ g^{-1} \in W^-(\Lambda), \\ \sigma_{r-f} &= g \circ \sigma_{r_3-f} \circ g^{-1} \in W^-(\Lambda).\end{aligned}$$

4. We first show the inclusion  $W^-(L) \subset \psi_U L' \cdot \mathcal{O}(U)$ . By Corollary 17.3.9 any root  $r \in L$  can be moved to a root in  $L' = U' \oplus L''$  by an Eichler–Siegel transformation  $\psi \in \psi_U \cdot U = \psi_U U' \subset \psi_U L'$ . Applying (17.10) it follows that  $\sigma_{\psi(r)} = \psi' \circ u$  with  $\psi' \in \psi_U L'$  and  $u \in \mathcal{O}(U)$ . By Lemma 17.3.11.1 we find some  $\psi'' \in \psi_U L'$  such that

$$\begin{aligned}\sigma_r &= \psi^{-1} \circ \sigma_{\psi(r)} \circ \psi \\ &= \psi^{-1} \circ \psi' \circ u \circ \psi \\ &= \psi^{-1} \circ \psi' \circ \psi'' \circ u,\end{aligned}$$

and hence  $\sigma_r \in \psi_U L' \cdot \mathcal{O}(U)$ .

Next, since  $\text{Nm}_{\text{spin}}^\epsilon \psi = \det \psi = 1$  for all  $\psi \in \psi_U L'$  and since by Example 17.1.2 the only isometry in  $\mathcal{O}(U)$  with the same invariants is the identity, we conclude

$$W^-(L) \cap \text{SO}(L) \subset \psi_U L' \subset W^-(\Lambda), \quad (18.1)$$

where the rightmost inclusion is assertion 3. If  $\sigma \in W^-(L)$ , equation (18.1) implies that  $\sigma \circ \tau \in W^-(\Lambda)$  for all  $\tau \in W^-(\Lambda)$  and hence  $W^-(L) \subset W^-(\Lambda)$  so that these two sets coincide.  $\square$

If there exists a special subset of roots  $\Lambda$  *spanning* the lattice  $L$  then, by Remark 18.1.3,  $(L, \Lambda)$  is a vanishing lattice. Now Theorem 18.1.7 comes into play. It states that, if, besides the socle plane,  $L$  splits off a second hyperbolic plane,  $W^-(\Lambda)$  is the full Weyl group of the lattice. Let us give an important class of examples which illustrate this and serve to motivate the theorem.

**Example 18.1.8.** Consider the Dynkin diagram  $T_{p,q,r}^1$  depicted in Figure 18.1.2. The vertices define a special subset of roots. We shall show that this defines a complete vanishing lattice.

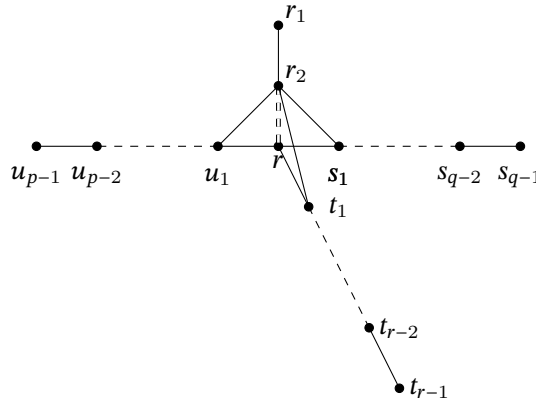


Figure 18.1.2: Vanishing lattice given by  $T_{p,q,r}^1$ ,  $p \geq 2, q \geq 3, r \geq 7$ .

The graph is 1-connected and defines a vanishing lattice by Remark 18.1.3. The vertices of the graph form a special set of roots with socle  $\{r_1, r_2, r\}$ . The three legs have lengths  $p, q, r$ , respectively. The corresponding quadratic lattice will be denoted by the same symbol. One verifies that

$$T_{p,q,r}^1 \simeq \tilde{T}_{p,q,r} \oplus U,$$

where  $U$  is the socle plane, i.e., the hyperbolic plane with basis  $e = -r_2 + r$ ,  $f = -r_1 - r_2 + r$ , and  $\tilde{T}_{p,q,r}$  is the Coxeter diagram depicted in Section 4.1. If  $p \geq 2, q \geq 3, r \geq 7$ , the diagram of  $\tilde{E}_8$  is a subgraph of  $\tilde{T}_{p,q,r}$  and a proof similar to the proof of Lemma 4.1.5 shows then that  $\tilde{T}_{p,q,r} \simeq \tilde{T}_{p,q,4} \oplus U \oplus A_{r-6}(-1)$ . Since  $\tilde{T}_{p,q,r}$  splits off a copy of the hyperbolic plane, and  $\tilde{T}_{p,q,4}$  contains  $A_2(-1)$  and so  $T_{p,q,r}^1$  contains  $L_{\min} = U \oplus U \oplus A_2(-1)$ , by Remark 18.1.3 it is a complete vanishing lattice. Its reflection group is maximal as follows from Theorem 18.1.7, but we shall prove shortly (cf. Theorem 18.1.9) that this also follows from completeness of the vanishing lattice.

We shall show now that the class of complete vanishing lattices has indeed the merit of having maximally possible Weyl groups:

**Theorem 18.1.9** ([63, Thm. 5.3.4]). *Let  $(L, \Delta)$  be a complete vanishing lattice. Then  $W^-(\Delta) = W^-(L) = O^{-\#}(L)$ .*

*Proof.* The equality  $W^-(L) = O^{-\#}(L)$  is a consequence of M. Kneser’s result, Corollary 17.2.12, since  $L$  contains  $L_2 = U \oplus U' \oplus A_2(-1)$  which has rank 6 and discriminant 3, and  $L_1 = U \oplus U' \oplus A_1(-1)$  which has rank 5 and discriminant  $-2$ .

For the leftmost equality we maneuver us in the situation of Theorem 18.1.7 and search for a special set of roots which generate the lattice. We break up the proof in the following steps.

**Connectedness:** The graph of  $\Delta$  is 1-connected. We postpone the proof, cf. Lemma 18.1.10 below.



**Characterizing  $W^-(\Delta)$ :** The Weyl group of  $\Delta$  is the group  $G$  generated by the reflections in the roots from  $\Delta$  having distance  $\leq 1$  to  $r_3$ , that is, the following set of roots

$$\Delta_0 = \{r \in \Delta \mid r = r_3 \text{ or } b(r, r_3) = 1\}. \quad (18.2)$$

Moreover, the latter set generates  $L$ . Here  $r_3 \in \Lambda_{\min}$  is as in Figure 18.1.1, a root orthogonal to the sum  $U \oplus U'$  of the hyperbolic planes spanned by  $\{e, f, e', f'\}$ .

To show the claim, first notice that by Lemma 18.1.10 we can connect  $r \in \Delta$  to  $r_3$  by a chain  $(r_3, \dots, r_k = r)$  of minimal length  $k - 2$ . Next, we show by induction on the minimal length that  $r$  is in the  $G$ -orbit of  $r_3$ . We may assume that  $k > 2$ . By the induction hypothesis, there exists  $g \in G$  such that  $g(r_{k-1}) = r_3$  and since  $b(r_3, g(r)) = b(g(r_{k-1}), g(r)) = b(r_{k-1}, r) = 1$ , we have  $g(r) \in \Delta_0$ . Hence the reflection  $\sigma_{g(r)} = g\sigma_r g^{-1}$  belongs to  $G$ . We infer

$$\begin{aligned} r &= \sigma_{r_{k-1}} \circ \sigma_{r_k}(r_{k-1}) \\ &= \sigma_{r_{k-1}} \circ g^{-1} \circ (g\sigma_r g^{-1})(r_3) \in G \cdot r_3. \end{aligned}$$

Since all roots  $r \in \Delta$  belong to  $Gr_3 \subset G\Delta_0$ , we have  $W^-(\Delta) = G = W^-(\Delta_0)$  and the lattice spanned by  $\Delta$  must be the same as the lattice spanned by  $\Delta_0$ .

**Construction of a special subset of roots:** With  $\Gamma_{\min} \subset \Delta$  as in Figure 18.1.1 and  $U = \mathbb{Z}e + \mathbb{Z}f$ ,  $U' = \mathbb{Z}e' + \mathbb{Z}f'$ , let  $\Lambda$  be the set of roots consisting of

- the roots of  $\Gamma_{\min}$ ;
- the 1-connected component  $\Lambda'$  of  $\Delta \cap U^\perp$  containing  $r_3$ .

Then  $\Lambda \subset \Delta$  is a special subset of roots of  $L$  containing  $\Gamma_{\min}$ . Moreover,  $L = U \oplus U' \oplus L''$ .

Let us prove these assertions. A root  $r \in \Lambda'$  is orthogonal to  $r_1$  and  $b(r, r_2) = b(r, r_3)$ . Since  $\Gamma_{\min}$  is 1-connected and contains  $r_3$  which belongs to the 1-connected set  $\Lambda'$ , also  $\Lambda$  is 1-connected. Hence  $\Lambda$  is a special subset of roots in  $L$ . The lattice spanned by  $\Gamma_{\min}$  contains  $U \oplus U'$  and so does  $\mathbb{Z}\Lambda$ . It remains to show that  $L$  is spanned by  $\Lambda$ . By the previous step it suffices to show that  $\Delta_0$ , the subset of roots of  $\Delta$  having distance  $\leq 1$  belongs to the lattice  $\mathbb{Z}\Delta_0$ . Let us show the latter assertion. So take  $r \in \Lambda$ ,  $r \neq r_3$ . By Corollary 17.3.10 there is some  $\psi \in \psi_U(U')$  with  $\psi(r) \in U' \oplus L''$ . Then  $\psi(r_3) = r_3$  since  $r_3$  is orthogonal to  $U \oplus U'$  and so

$$\begin{aligned} b(\psi(r), r_3) &= b(\psi(r), \psi(r_3)) \\ &= b(r, r_3) = 1, \end{aligned}$$

where the last equality holds according to the definition (18.2) of  $\Delta_0$ . So  $\psi(r) \in \Lambda'$ . Since  $\psi \in W^-(\Lambda)$ , we conclude  $r = \psi^{-1}(\psi r) \in W^-(\Lambda)\Lambda' \subset \mathbb{Z}\Lambda$ , which proves our claim that  $\Delta_0 \subset \mathbb{Z}\Lambda$ .

**Final step:** Once we have found the special subset of roots, it remains to apply Theorem 18.1.7.  $\square$

As announced, the following result completing the proof of Theorem 18.1.9 remains to be shown.

**Lemma 18.1.10.** *For a complete vanishing lattice  $(L, \Delta)$ , the set  $\Delta$  is 1-connected.*

*Proof. Step 1:* Any 1-connected component  $\Delta'$  of  $\Delta$  is a complete  $W^-(\Delta')$ -orbit. To prove this, first remark that by Lemma 18.1.1 a 1-connected subset  $\Delta'$  of  $\Delta$  belongs to a single orbit under  $W^-(\Delta')$ . On the other hand the complete  $W^-(\Delta')$ -orbit  $\Delta'$  belongs to  $\Delta'$ . To see this, one shows that for  $r, s \in \Delta'$  one has  $\sigma_r s \in \Delta'$ . We distinguish two cases.

- For  $r = s$  this just means that we need to see that  $-r \in \Delta'$ . To show this, first remark that since  $(L, \Delta)$  is a vanishing lattice,  $r$  can be moved to any other root in  $\Delta$  by means of an element of the Weyl group of  $\Delta$ . Since  $(L, \Delta)$  is complete it contains  $(L_{\min}, \Gamma_{\min})$  and hence  $r_4 \in \Delta$ . So there is some  $\gamma \in W^-(\Delta)$  for which  $\gamma(r_4) = r$ . The roots  $r_4, r_5, r_6 \in \Delta$  define a Dynkin diagram of type  $A_3$  (see Figure 18.1.1) and  $\Delta$  contains all of its roots. These form a 1-connected subset of  $\Delta$  as one can see in Figure 18.1.3. In particular,  $-r_4$

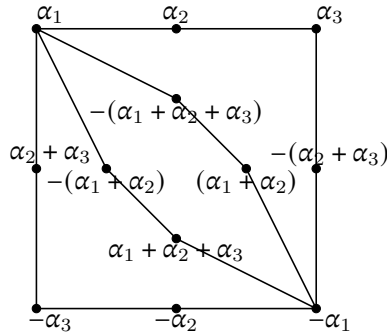


Figure 18.1.3: The root system  $A_3(-1)$  is 1-connected.

belongs to this 1-connected subset of  $\Delta$ . The same holds for the images under  $\gamma$  which then must be included in  $\Delta'$  since  $\Delta'$  is a 1-connected component of  $\Delta$  and  $A_3(-1)$  is 1-connected. But then also  $-r = \gamma(-r_4)$  belongs to  $\Delta'$ .

- For  $r \neq s$ , take a 1-connected path in  $\Delta'$  of minimal length from  $r$  to  $s$ , say  $r = s_0, s_1, \dots, s_{k-1}, s_k = s$ , and suppose that by induction we have shown that  $\sigma_r s_{k-1}$  connects within  $\Delta'$  to  $r$ . Since  $\sigma_r s_{k-1}$  belongs to the 1-connected  $\Delta'$ , and  $\sigma_r s_{k-1}$  and  $\sigma_r s_k \in \Delta$  are connected, we must have  $\sigma_r s (= \sigma_r s_k) \in \Delta'$ .

**Step 2:** We claim that reflection in a root  $r \in \Delta$  fixes some root  $r' \in \Delta'$ , that is, for which  $b(r, r') = 0$ . To show this, first remark that since we have a vanishing lattice, there is a reflection  $\gamma \in W^-(\Delta)$  which maps a root of  $\Gamma_{\min}$  to  $\Delta'$ . But then, since  $\Delta'$  is a 1-connected component of  $\Delta$  and  $\Gamma_{\min}$  is itself 1-connected,  $\gamma(\Gamma_{\min}) \subset \Delta'$ . On the other hand, by Corollary 17.3.10, we can move  $\gamma^{-1}r$  to  $U \oplus L''$  by an element  $\psi \in \psi_U(U')$  and since  $r_6 = e' - f' \in U'$  is orthogonal to  $U \oplus L''$  we have

$$\begin{aligned} 0 &= b(r_6, \psi\gamma^{-1}r) \\ &= b(\gamma\psi^{-1}(r_6), r). \end{aligned}$$

By Lemma 17.3.11, all elements of  $\psi_U(U' \oplus A_2(-1)) \subset \mathcal{O}(\Gamma_{\min})$  such as  $\psi^{-1}$  are products of reflections because  $U' \oplus A_2(-1)$  is indeed a root-lattice.<sup>2</sup> Hence, since  $\Gamma_{\min} \subset \Delta'$  we have  $\gamma(r_6) \in \Delta'$  and  $\gamma\psi^{-1}\gamma^{-1} \in W^-(\Delta')$ . Consequently  $r' = \gamma\psi^{-1}r_6 = \gamma\psi^{-1}\gamma^{-1}\gamma r_6$  belongs to the  $W^-(\Delta')$ -orbit of  $\Delta'$  and so to  $\Delta'$  as desired.

**Final step:** The Weyl group  $W^-(\Delta)$  acts transitively on the 1-connected components of  $\Delta$ . By Step 2 this group leaves the 1-connected component  $\Delta'$  invariant and so there is just one such component, that is  $\Delta$  itself is 1-connected.  $\square$

*Remark.*  $A_2(-1)$  is not 1-connected: the set of roots  $\{\alpha_1, \alpha_2, -(\alpha_1 + \alpha_2)\}$  as well as the set  $\{-\alpha_1 - \alpha_2, \alpha_1 + \alpha_2\}$  is 1-connected, but these two sets cannot be connected.

**Examples 18.1.11.** 1. The Dynkin diagram  $T_{p,q,r}^1$  from Figure 18.1.2 defines a special subset of roots in the lattice it defines and yields a vanishing lattice. As we remarked in Example 18.1.8, its reflection group is maximal. It forms a complete vanishing lattice, provided  $p \geq 2, q \geq 3, r \geq 7$  since  $T_{p,q,r}^1 = T_{p,q,4} \oplus U \oplus U' \oplus A_{r-6}(-1)$ , which contains  $U \oplus U' \oplus A_2(-1)$  (all legs of  $T_{p,q,4}$  have  $\geq 2$  nodes).

2. Every vanishing lattice containing  $T_{p,q,r}^1$  as in the first example is a complete vanishing lattice.

## 18.2 Application to the Monodromy of Singularities

In this section  $(X, x)$  is a germ of an isolated hypersurface singularity of even dimension

$$n. \text{ Furthermore, } \epsilon = \begin{cases} - \text{ or } -1 & \text{if } n \equiv 2 \pmod{4} \\ + \text{ or } 1 & \text{if } n \equiv 0 \pmod{4}. \end{cases}$$

**18.2.A Introduction to isolated hypersurface singularities.** We let  $z_1, \dots, z_{n+1}$  be the standard coordinates on  $\mathbb{C}^{n+1}$  and we shall write  $\mathbf{z} = (z_1, \dots, z_{n+1})$  for the vector with coordinates  $z_1, \dots, z_{n+1}$

We consider germs  $(X, x)$  of  $n$ -dimensional hypersurfaces with an isolated singularity at  $x$ . Such a singularity will be represented by the zero-set of a holomorphic function  $f : \mathbb{C}^{n+1} \rightarrow \mathbb{C}$  restricted to a neighborhood of the origin  $0 \in \mathbb{C}^{n+1}$ , where  $0$  corresponds to the singularity at  $x$ . To ease the presentation we assume that  $0$  is the only critical point of  $f$ . So, if  $t$  is a coordinate on the target space, the level sets  $f^{-1}(t)$  for  $t \neq 0$  are smooth hypersurfaces while  $f^{-1}(0)$  is smooth away from  $0$ . The  $t$ -disc of radius  $r$  punctured at the origin is denoted  $\Delta^*(r)$ .

The associated *Milnor fibration* is obtained by restricting  $f$  to

$$\mathcal{M} = \{|\mathbf{z}|^2 < \eta\} \cap f^{-1}[\Delta^*(r)],$$

where  $\eta$  and  $r$  are sufficiently small so that  $f : \mathcal{M} \rightarrow \Delta^*(r)$  is a locally trivial fibration. Its typical fiber,  $M_*$ , is the so-called *Milnor fiber* associated to the

<sup>2</sup>Here the extra root-lattice  $A_2(-1)$  is essential since  $U'$  is not a root-lattice.

singularity. We think of the lower index  $*$  as the “general point” of the punctured disk  $\Delta^*(r)$ . The Milnor fiber has the homotopy type of a bouquet of  $\mu$  (real) spheres of dimension  $n$ , where  $\mu$  is the **Milnor number** and hence  $H_n(M_*, \mathbb{Z})$  is a free  $\mathbb{Z}$ -module of rank  $\mu$ . The orientation induced by the complex structure defines the intersection pairing

$$H_n(M_*, \mathbb{Z}) \times H_n(M_*, \mathbb{Z}) \rightarrow \mathbb{Z},$$

which is symmetric and bilinear, but not necessarily non-degenerate. We denote this pairing with a dot. The resulting lattice

$$\Lambda_{X,x} = (H_n(M_*, \mathbb{Z}), \cdot)$$

is called the **Milnor lattice** of  $(X, x)$ . It comes equipped with the action of the **monodromy operator**  $T_{X,x}$  which is induced by moving the Milnor fiber of  $f$  once about the origin in anti-clockwise direction.

**Examples 18.2.1. 1.** The function  $f(\mathbf{z}) = z_1^2 + \dots + z_{n+1}^2$  has a single critical point at the origin. The corresponding singularity is an ordinary double point. If  $t \neq 0$ , the fiber  $f^{-1}(t)$  is the smooth hypersurface  $\sum_j z_j^2 = t$ . The Milnor number is 1 since  $H_n(M_*, \mathbb{Z}) = \mathbb{Z}$  is generated by a so-called **vanishing cycle**  $\delta$  given by  $\{x_1^2 + \dots + x_{n+1}^2 = t_*\} \cap \{|\mathbf{z}|^2 < \eta\}$ , where  $z_j = x_j + iy_j$ ,  $j = 1, \dots, n + 1$ , and  $t_*$  is the  $t$ -coordinate of the point  $*$ . It is well known (cf. e.g. [134, §6]) that  $\delta \cdot \delta = 2\epsilon$  and that the monodromy operator  $T_{X,x}$  is the reflection  $s_\delta$ , corresponding to  $\delta$ .

**2.** More generally, consider the du Val singularities of Table 4.5.1. The minimal resolution of these singularities is a connected chain of rational curves of self-intersection  $-2$  whose dual graph is one of the Dynkin diagrams  $A_k, D_k, E_6, E_7, E_8$ . The construction on page 102 shows that a tubular neighborhood of such a chain is a disc bundle over a wedge of 2-spheres, and from this it follows that the Milnor fibre has the same homotopy type as the latter wedge of 2-spheres. Du Val-type singularities occur in any dimension and are denoted by the same symbols as for dimension 2. Their Milnor lattices are given in Table 18.2.1. The Milnor number for  $A_k, D_k$  and  $E_k$  equals  $k$ .

Table 18.2.1: Milnor lattice of the du Val singularities

Name	equation	Milnor lattice
$A_k$	$z_1 z_2 + z_3^{k+1} + \sum_{j \geq 4} z_j^2 = 0$	$A_k(\epsilon)$
$D_k$	$z_1^2 + z_2^2 + z_3^{k-1} + \sum_{j \geq 4} z_j^2 = 0$	$D_k(\epsilon)$
$E_6$	$z_1^2 + z_2^3 + z_3^4 + \sum_{j \geq 4} z_j^2 = 0$	$E_6(\epsilon)$
$E_7$	$z_1^2 + z_2^3 + z_2 z_3^3 + \sum_{j \geq 4} z_j^2 = 0$	$E_7(\epsilon)$
$E_8$	$z_1^2 + z_2^3 + z_3^5 + \sum_{j \geq 4} z_j^2 = 0$	$E_8(\epsilon)$

**18.2.B Deforming hypersurface singularities.** For a proper treatment of this topic see e.g. [142, Ch. 8], [5, Ch. 1]. The basic concept is that of a *semi-universal unfolding* of the isolated singularity  $(X, x)$ . Roughly speaking a semi-universal unfolding or miniversal deformation of  $(X, x)$  is a family of hypersurfaces  $\{X_u\}_{u \in U}$ , where the base manifold  $U$  is a ball centered at 0 with  $X_0 \simeq X$  and which “contains” all deformations of  $(X, x)$ . More precisely, every deformation  $\{X_t\}_{t \in T}$  of  $(X, x)$  is the pull-back of a semi-universal unfolding by a holomorphic map  $\phi : T \rightarrow U$  which is “infinitesimally unique at 0” in the sense that the derivative of  $\phi$  at 0 is uniquely determined by the family  $\{X_t\}$ . It is well known that there exists a semi-universal unfolding of the shape

$$F(\mathbf{z}, u_0, \dots, u_{\tau-1}) = f(\mathbf{z}) + u_0 + u_1 \mathbf{z}^{\mathbf{B}_1} + \dots + u_{\tau-1} \mathbf{z}^{\mathbf{B}_{\tau-1}}. \quad (18.3)$$

The multi-index notation we use means this: if  $\mathbf{B}_j = (b_{1,j}, \dots, b_{n+1,j})$ , one sets

$$\mathbf{z}^{\mathbf{B}_j} = z_1^{b_{1,j}} \dots z_{n+1}^{b_{n+1,j}}.$$

The exponents  $\mathbf{B}_j$  are chosen so that  $\{1, \mathbf{z}^{\mathbf{B}_1}, \dots, \mathbf{z}^{\mathbf{B}_{\tau-1}}\}$  is a basis for the algebra  $J_{X,x}/\bar{f}$ , where

$$J_{X,x} = \mathbb{C}[\mathbf{z}] / (\partial f / \partial z_1, \dots, \partial f / \partial z_{n+1})$$

is the jacobian algebra and  $\bar{f} \in J_{X,x}$  is the class of  $f$  in the jacobian algebra. Write  $\mathbf{u} = (u_1, \dots, u_{\tau-1})$ . The number  $\tau$  is the *Tjurina number* of the singularity. Then the function

$$\mathbf{F} : \mathbb{C}^{n+1+\tau} \rightarrow \mathbb{C}^\tau, \quad (\mathbf{z}, u_0, \mathbf{u}) \rightarrow (F(\mathbf{z}, u_0, \mathbf{u}), \mathbf{u})$$

restricted to a suitable small neighbourhood  $V$  of 0 is a semi-universal unfolding of  $f$ . The critical points of  $\mathbf{F}$  by definition make up the *discriminant locus*  $D_{\mathbf{F}}$  of  $\mathbf{F}$ , a hypersurface in  $U$ . If  $U$  is small enough, the fibers over  $D_{\mathbf{F}}$  have isolated singularities only and the locus of a given isomorphism type of singularity  $(Y, y)$  forms a locally closed subvariety of the discriminant locus. If  $(X, x)$  is a singularity in its closure we say that  $(Y, y)$  is *adjacent* to  $(X, x)$ . Such a singularity can be viewed as less complicated than  $(X, x)$ . The ordinary double point singularities, making up an open dense stratum of the discriminant, give the simplest type of singularity while the stratum  $S_\mu$  parametrizes the most complex ones, those with Milnor number  $\mu$ . Although the singularities with fixed Milnor number are topologically the same, this need not be the case in the biholomorphic category. To see this, observe that the group of germs of biholomorphic automorphisms of  $(X, x)$  acts on  $S_\mu$ , and while the points in the orbit of 0 (corresponding to  $(X, x)$ ) are all isomorphic, those in a slice transversal to this orbit are not. The dimension  $m$  of such a slice gives the number of moduli of  $(X, x)$  and we say that  $(X, x)$  is an *m-modal singularity*. If  $m = 1$  we speak of a *unimodal* singularity.

**Examples 18.2.2. 1.** The ordinary double point  $z_1^2 + \dots + z_{n+1}^2 = 0$  of Example 18.2.1 has the function  $z_1^2 + \dots + z_{n+1}^2 - t$  as its semi-universal unfolding and so  $\tau = \mu = 1$ . The discriminant locus is the origin and the modality is 0.

**2.** The other Du Val singularities have  $\mu = \tau$  as well and the modality is 0. For instance, for  $E_6$  the jacobian ring has a basis  $\{1, z_2, z_3, z_3^2, z_2 z_3, z_2 z_3^2\}$  consisting of

6 elements and it also contains the defining polynomial.

**3.** The *hyperbolic singularities*  $T_{p,q,r}$ . In dimension 2 these singularities are given by:

$$f = 0, \quad f = x^p + y^q + z^r + axyz, \quad a \in \mathbb{C}^\times, \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

With  $J_f$  the jacobian ideal, we see that the vector space  $\mathbb{C}[[x, y, z]]/(J_f, f)$  is generated by 1 together with the monomials  $x^k, k = 1, \dots, p - 1, y^\ell, \ell = 1, \dots, q - 1, z^m, m = 1, \dots, r - 1,$  and so  $\tau(f) = p + q + r - 2.$  Because of the relation

$$p^{-1}xf_x + q^{-1}yf_y + r^{-1}zf_z - f = (p^{-1} + q^{-1} + r^{-1} - 1)axyz,$$

we find  $\mu = p + q + r - 2.$  For all non-zero  $a$  the singularities have the same Milnor number. It turns out (see [5, Ch. I.2.3]) that the isomorphism class of the singularity varies with  $a,$  and so it is a unimodal singularity.

**4.** Milnor lattices can have a non-zero null-space. The simplest are the so-called *parabolic singularities.* These are also unimodal, again by [5, Ch. I.2.3].

Table 18.2.2: Milnor lattice of the parabolic singularities

Name	equation	Milnor lattice	restriction
$\tilde{E}_6$	$z_1^3 + z_2^3 + z_3^3 + az_1z_2z_3 + \sum_{j \geq 4} z_j^2 = 0$	$\tilde{E}_6(\epsilon)$	$a^3 + 27 \neq 0$
$\tilde{E}_7$	$z_1^4 + z_2^4 + z_3^2 + az_1z_2z_3 + \sum_{j \geq 4} z_j^2 = 0$	$\tilde{E}_7(\epsilon)$	$a^4 - 64 \neq 0$
$\tilde{E}_8$	$z_1^6 + z_2^3 + z_3^2 + az_1z_2z_3 + \sum_{j \geq 4} z_j^2 = 0$	$\tilde{E}_8(\epsilon)$	$a^6 - 432 \neq 0$

**18.2.C Monodromy.** Let the base  $U \subset \mathbb{C}^\tau$  of a semi-universal unfolding  $\mathbf{F}$  of the singularity  $(X, x)$  be a small enough ball about 0 such that  $\mathbf{F}^{-1}U \subset V$  away from the discriminant locus  $D_{\mathbf{F}}$  gives a locally trivial differentiable fiber bundle

$$\mathbf{F}^{-1}[U - U \cap D_{\mathbf{F}}] \rightarrow U - U \cap D_{\mathbf{F}},$$

and such that the fiber  $\mathbf{F}_{*,0}$  of  $\mathbf{F}$  passing through the point  $(*, 0)$  intersected with the ball  $|z| < \eta$  is the Milnor fiber  $M_*$  of  $(X, x).$  By definition  $H_n(M_*, \mathbb{Z}) = \Lambda_{X,x}$  is free of rank  $\mu.$  It is generated by vanishing cycles as follows. A general line  $\ell$  intersects the discriminant hypersurface  $D_{\mathbf{F}}$  transversally. It turns out that  $\ell \cap U \cap D_{\mathbf{F}}$  consists of precisely  $\mu$  points, say  $t_1, \dots, t_\mu,$  and the fiber of  $\mathbf{F}$  over each of these points has exactly one ordinary double point, say  $s_j,$  and no other singular points. In Example 18.2.1 we found a vanishing cycle  $\delta'_j$  in the fibre near  $s_j.$  We want to transport it to  $(*, 0) \in U$  along a well-chosen path.

To this end we introduce a distinguished set of generators of the fundamental group  $\pi_1(U - U \cap D_{\mathbf{F}}, (*, 0)),$  namely the loops  $\gamma_j, j = 1, \dots, \mu,$  which start at  $(*, 0) \in U \cap \ell,$  follow the straight line segment  $\ell_j$  from  $(*, 0)$  to the first point of intersection with a little circle  $\sigma_j$  about  $t_j,$  traverse this circle in anti-clockwise

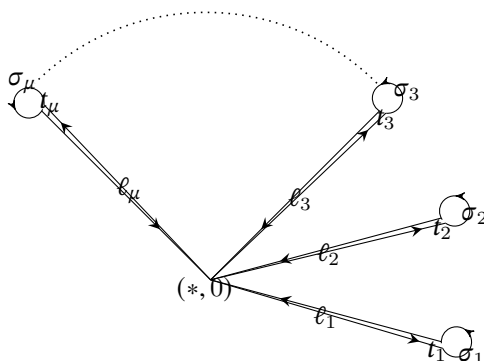


Figure 18.2.1: Generators of the fundamental group

direction and then go back to  $(*, 0)$  along  $\ell_j$  as in Figure 18.2.1. We assume that the loops are numbered consecutively as in the figure and that any two of them only have  $(*, 0)$  in common. These loops generate the fundamental group of  $U \cap \ell - \{t_1, \dots, t_\mu\}$  (recall that  $U \cap \ell$  is a disc containing all of the points  $t_j$ ). The vanishing cycle  $\delta_j$  in  $H_n(M_*, \mathbb{Z})$  for  $j = 1, \dots, \mu$ , is obtained by transporting  $\delta'_j$  along the path  $\ell_j$  to the fiber over  $(*, 0) \in U$ . The monodromy representation associated to (an unfolding of) the singularity is by definition the representation of the fundamental group  $\pi_1(U - U \cap D_{\mathbb{F}}, (*, 0))$  on  $\Lambda_{X,x} = H_n(\mathbb{F}_{*,0}, \mathbb{Z})$  with image the *monodromy group associated to the singularity*, denoted

$$\text{Mon}(\Lambda_{X,x}) \subset \text{O}(\Lambda_{X,x}).$$

Since by [142, Chap. 7] the inclusion  $U \cap \ell \hookrightarrow U$  induces a surjection

$$\pi_1(U \cap \ell - \{t_1, \dots, t_\mu\}, (*, 0)) \twoheadrightarrow \pi_1(U - \Delta, (*, 0)), \quad (18.4)$$

the action of the monodromy group is completely described by the automorphism  $T_i$  on  $H_n(M_*)$  resulting from moving vanishing cycles around the loops  $\gamma_i$ ,  $i = 1, \dots, \mu$ . From what we have seen in the case of an ordinary double point,  $T_i$  is a reflection in the hyperplane  $\delta_i^\perp \subset H_n(M_*)$ . One can show that the discriminant locus is a connected hypersurface and then, by the arguments in [134, §7], [142, Chap. 7], it follows that all vanishing cycles are in the same orbit under the reflection group they generate:

**Theorem 18.2.3.** *The set  $\Delta_{X,x} = \{\delta_1, \dots, \delta_\mu\}$  of vanishing cycles is a basis for the Milnor lattice  $\Lambda_{X,x}$ . All of these vanishing cycles are in the same orbit under the action of the monodromy group. In particular  $(\Lambda_{X,x}, \Delta_{X,x})$  is a vanishing lattice.*

For the actual calculation of vanishing lattices such as for the following examples, we refer to [5, Ch.2] and [63].

**Examples 18.2.4. 1.** Let us continue with the hyperbolic singularities of Example 18.2.2 (3). The associated vanishing lattices are *not* given by the Dynkin

diagrams  $\widetilde{T}_{p,q,r}$  from Section 4.1.A, but are obtained from  $T_{pqr}^1$  by deleting the root  $r_1$ . Since then  $r_2 - r$  is orthogonal to itself and all other roots, the lattice is isometric to  $\widetilde{T}_{p,q,r} \oplus 0$ .

2. The 14 exceptional unimodal families of Arnold [4] as given in Table 18.2.3. The

Table 18.2.3: Exceptional unimodal singularities

Notation	Normal Form	Milnor number $\mu$	Dynkin Diagram
$K_{12}$	$x^3 + y^7 + z^2 + axy^5$	12	$T_{2,3,7}^1$
$K_{13}$	$x^3 + xy^5 + z^2 + ay^8$	13	$T_{2,3,8}^1$
$K_{14}$	$x^3 + y^8 + z^2 + axy^6$	14	$T_{2,3,9}^1$
$Z_{11}$	$x^3y + y^5 + z^2 + axy^4$	11	$T_{2,4,5}^1$
$Z_{12}$	$x^3y + xy^4 + z^2 + ax^2y^3$	12	$T_{2,4,6}^1$
$Z_{13}$	$x^3y + y^6 + z^2 + axy^5$	13	$T_{2,4,7}^1$
$W_{12}$	$x^4 + y^5 + z^2 + ax^2y^3$	12	$T_{2,5,5}^1$
$W_{13}$	$x^4 + xy^4 + z^2 + ay^5$	13	$T_{2,5,6}^1$
$Q_{10}$	$x^3 + y^4 + yz^2 + axy^3$	10	$T_{3,3,4}^1$
$Q_{11}$	$x^3 + y^5 + yz^2 + az^5$	11	$T_{3,3,5}^1$
$Q_{12}$	$x^3 + y^3z + xz^3 + axy^4$	12	$T_{3,3,6}^1$
$S_{11}$	$x^4 + y^2z + xz^2 + ax^3z$	11	$T_{3,4,4}^1$
$S_{12}$	$x^2y + y^2z + xz^3 + az^5$	12	$T_{3,4,5}^1$
$U_{12}$	$x^3 + y^3 + z^4 + axyz^2$	12	$T_{4,4,4}^1$

vanishing lattice  $T_{p,q,r}^1$  is given in Figure 18.1.2 by means of a Dynkin diagram with  $\mu$  vertices. The "modulus"  $a$  is any complex number. In Example 18.1.11.1 we have shown that the vanishing lattices of these singularities are complete (cf. Definition 18.1.4) and by Theorem 18.1.9 we have  $\text{Mon}(\Lambda_{X,x}) = W^\epsilon(\Lambda_{X,x}) = O^{\epsilon,\#}(\Lambda_{X,x})$ .

3. For the Du Val singularities the monodromy groups are as large as possible. Indeed, the quotient of full the isometry group by the monodromy group is isomorphic to the group of symmetries of the Dynkin diagram as shown in Table 18.2.2.

Table 18.2.4: Monodromy of the Du Val singularities

Name	monodromy	index in full isometry group
$A_k$	$W^\epsilon(A_k(\epsilon)) = O^\#(A_k(\epsilon))$	1
$D_k$	$W^\epsilon(D_k(\epsilon)) = O^\#(D_k(\epsilon))$	2 if $k \neq 4$ 4 if $k = 4$
$E_6$	$W^\epsilon(E_6(\epsilon)) = O^\#(E_6(\epsilon))$	2
$E_7$	$W^\epsilon(E_7(\epsilon)) = O^\#(E_7(\epsilon))$	1
$E_8$	$W^\epsilon(E_8(\epsilon)) = O^\#(E_8(\epsilon))$	1

4. If  $(Y, y)$  is adjacent to  $(X, x)$ , the vanishing lattice of the former is contained in



that of the latter. In particular, the lattice  $(\Lambda_{X,x}, \Delta_{X,x})$  is complete whenever this is the case for  $(\Lambda_{Y,y}, \Delta_{Y,y})$ . This remark can be used to prove completeness in a great number of cases. See [61].

### 18.3 Application to Global Monodromy

We now consider the global situation of the universal family of degree  $d$  hypersurfaces  $\sum_{|I|=d} a_I \mathbf{z}^I = 0$  in  $\mathbb{P}^{n+1}$ ,  $\mathbf{z} = (z_0, \dots, z_{n+1})$ . The base manifold is the projective space  $\mathbb{P}_{n,d}$  with homogeneous coordinates  $(\dots, a_I, \dots)$ , where  $I$  runs over multi-indices of length  $n+1$  and total degree  $d$ . Let us write  $X_t$  for the hypersurface corresponding to  $t \in \mathbb{P}_{n,d}$  and  $F_{n,d}$  for the total manifold. The singular hypersurfaces correspond to points of the discriminant hypersurface  $D_d \subset \mathbb{P}_{n,d}$  and so its complement

$$U_{n,d} = \mathbb{P}_{n,d} - D_d$$

parametrizes the smooth hypersurfaces. A generic line  $\ell \subset \mathbb{P}_{n,d}$  meets  $D_d$  transversally in points  $P$  corresponding to hypersurfaces with exactly one ordinary double point. Every such point  $P$  gives rise to a vanishing cycle  $\delta_P$  in a nearby smooth fiber. This situation resembles the local situation we just treated. The present situation is the one Lefschetz had in mind in the classical monograph [138] and this is why the restriction  $F_{n,d}$  to the line  $\ell$  is called a Lefschetz pencil. The global theory mirrors the local theory exactly. This leads to an associated vanishing lattice, but this time in cohomology, as we shall now explain.

Choose a base point  $* \in \ell \cap U_{n,d}$ . The fundamental group  $\pi_1(U_{n,d}, *)$  acts on  $H_n(X_*, \mathbb{Z})$  through the group generated by so-called Picard–Lefschetz reflections with respect to the vanishing cycles  $\delta_P$ . This is the monodromy representation with image the monodromy group

$$\text{Mon}(\Lambda_{n,d}) \subset \text{O}(\Lambda_{n,d}).$$

The monodromy representation on the vector space  $H_n(X_*, \mathbb{Q})$  turns out to be semi-simple and is a direct sum of two irreducible submodules, the trivial module, also called the fixed homology  $\mathbb{Q} \cdot h$ ,  $h$  the class of a linear section of dimension  $n/2$ , and the so-called variable homology. This direct sum splitting is orthogonal with respect to the intersection pairing, because the monodromy preserves the homeomorphism type of the hypersurface. Of course we can do the same for the middle cohomology and we get a direct sum splitting which is orthogonal with respect to the cup-product pairing. The two are related by the Poincaré duality isomorphism  $H^n(X_*, \mathbb{Z}) \xrightarrow{\sim} H_n(X_*, \mathbb{Z})$ .

We shall be interested in the monodromy action on the Poincaré-dual of the variable cohomology which in this setting coincides with the *primitive cohomology*

$$H_{\text{prim}}^n(X_*) = [h]^\perp \subset H^n(X_*, \mathbb{Z}).$$

**Theorem 18.3.1** ([134, §7]). *Let  $F_{n,d}$  be the universal family of degree  $d$  hypersurfaces in  $\mathbb{P}^{n+1}$  with discriminant  $D_d$ ,  $\ell \subset \mathbb{P}_{n,d}$  a line transversally intersecting  $D_d$  so that  $F_{n,d}|_\ell$  is a Lefschetz pencil. Choose a base point  $*$   $\in \ell \cap U_{n,d}$ . Then*

1. *Under Poincaré duality the set  $\Delta_{d,n}$  of vanishing cocycles obtained by taking the Poincaré duals of the vanishing cycles  $\delta_P$ ,  $P \in D_d \cap \ell$  (transported to  $*$ ), generate the primitive homology  $H_{\text{prim}}^n(X_*)$ .*
2. *All vanishing cocycles are in the same orbit under the monodromy group, and  $(H_{\text{prim}}^n(X_*), \Delta_{d,n})$  is a vanishing lattice.*

*About the proof.* Assertion 1 is a form of Theorem [134, 7.2] and assertion 2 is a consequence of assertion 1, just as in the local situation.  $\square$

To establish the relation with the monodromy group of the tautological family of hypersurfaces we use the global version of (18.4):

$$i_* : \pi_1(\ell \cap U_{n,d}, *) \rightarrow \pi_1(U_{n,d}, *).$$

This version is the result of first restricting to a general planar section on which the discriminant locus appears as a curve  $C$ . By O. Zariski's result [254] this does not change the fundamental groups of the complements, and then we use E. van Kampen's theorem [232] to see that further restricting to a general line  $\ell$  gives a surjection  $\pi_1(\ell - C \cap \ell) \rightarrow \pi_1(\mathbb{P}^2 - \ell)$ .

We now make the essential observation which relates the monodromy group  $\text{Mon}(\Lambda_{n,d})$  of the universal family to the monodromy group  $\text{Mon}(\Lambda_{X,x})$  of an isolated hypersurface singularity  $x \in X$ ,  $X$  a degree  $d$  hypersurface in  $\mathbb{P}^{n+1}$ . Its Milnor fiber  $M$  is the intersection of a smooth hypersurface  $X'$  near  $X$  with a small ball around  $x$ . The injection  $i : M \hookrightarrow X'$  induces a homomorphism  $i' : H_n(M, \mathbb{Z}) \rightarrow H^n(X, \mathbb{Z})$  which is the composition of the induced map  $i_*$  in homology, (the inverse of) Poincaré-duality and an identification of  $H^n(X', \mathbb{Z})$  with  $H^n(X, \mathbb{Z})$  (which depends on the choice of a path to the base point). These homomorphisms all preserve the intersection forms. If the intersection form on  $H_n(M, \mathbb{Z})$  is non-degenerate, the homomorphism  $i'$  is injective and so the vanishing lattice  $(\Lambda_{X,x}, \Delta_{X,x})$  becomes a sublattice of the vanishing lattice  $(H_{\text{prim}}^n(X), \Delta_{d,n})$ . This observation explains why one prefers to work with complete vanishing lattices.

Before we pass to the main result of this section, we first note that the monodromy action on the full middle cohomology group fixes the class  $h$  so it lands in  $O_h(H^n(X_*, \mathbb{Z}))$ , the stabilizer of  $h$  in  $O(H^n(X_*, \mathbb{Z}))$ . The monodromy group is generated by reflections and by Lemma 16.1.1 these induce the identity on the discriminant group. Hence by Theorem 15.1.7 these extend to isometries of the full cohomology group  $H^n(X_*, \mathbb{Z})$ . Consequently one has an embedding

$$\text{Mon}(\Lambda_{n,d}) \hookrightarrow O_h(H^n(X_*, \mathbb{Z})). \quad (18.5)$$

Using this, we can show:

**Theorem 18.3.2** ([18]). *The monodromy group  $\text{Mon}(\Lambda_{n,d})$  of the universal family of degree  $d$  smooth hypersurfaces in  $\mathbb{P}^{n+1}$ ,  $n$  even, equals  $\mathcal{O}^{\varepsilon, \#}(\Lambda_{d,n})$ . Under the embedding (18.5) the group  $\text{Mon}(\Lambda_{n,d})$  has index 2 in  $\mathcal{O}_h(H^n(X_*, \mathbb{Z}))$  if  $d \geq 4$  or  $d = 3, n \neq 2$ . In the remaining cases these groups are equal.*

*Proof.* We treat the various cases. For brevity we set  $G' = \text{Mon}(\Lambda_{n,d})$  and  $G = \mathcal{O}_h(H^n(X_*, \mathbb{Z}))$ .

- If  $d = 2$  we have a quadric with  $H_{\text{prim}}^2(X_*, \mathbb{Z}) = \langle \varepsilon \cdot 2 \rangle$  and then  $G = G' = \{\pm \text{id}\}$ .
- If  $d = 3, n = 2$ , we have a cubic surface. The full cohomology lattice is the Lorentzian lattice  $\mathbb{Z}^{1,6}$  with primitive cohomology isometric to  $E_6(-1)$  since  $E_6(-1)$  is the orthogonal complement of the hyperplane section  $h$  (cf. Eqn. (4.5)). Since the vanishing cycles form a collection of roots which span  $E_6(-1)$ , the monodromy group is the Weyl group of  $E_6(-1)$ .
- $d \geq 4$  or  $d = 3, n \neq 2$ . We show that the vanishing lattice is complete by following the ideas that were presented preceding the statement of the theorem. If  $d \geq 4, n \geq 2$ , we take now for  $F_t$  the hypersurface whose affine equation is  $x_1^3 + x_2^3 + x_3^4 + x_3^d + \sum_{j \geq 4} x_j^2 = 0$ . This is an exceptional singularity of type  $U_{12}$  (cf. Table 18.2.3). To see this, note firstly that  $1 + x_3^{d-4}$  is a unit in  $\mathbb{C}[[x_3]]$  and so may be replaced by 1 in that ring, and, secondly, that adding  $\sum_{j \geq 4} x_j^2$  does not change the type of a singular point ("stably equivalence" equals "equivalence", cf. [5, §1.3]).

For  $d = 3, n \geq 4$ , there is a cubic surface with affine equation  $f(x_1, x_2, x_3) = 0$  with a singularity of type  $E_6$ , namely  $f = x_1^2 + x_1 x_2^2 + x_2^3$  (cf. [52, §9.2.2]). Then the hypersurface with affine equation  $f + x_4^3 + \sum_{j \geq 5} x_j^2$  has a  $U_{12}$ -singularity.

In all of the above cases  $G' = \mathcal{O}^{\varepsilon, \#}(\Lambda_{d,n})$  and we have equality for quadratic hypersurfaces and cubic surfaces. In the other cases  $\Lambda_{d,n}$  contains the lattice  $U = \mathbb{Z}e + \mathbb{Z}f$  since, as a complete lattice, it contains  $L_{\text{min}} := U \oplus U' \oplus A_2(-1)$ . Observe that  $e - \varepsilon f$  is a  $(-2\varepsilon)$ -root with  $\varepsilon$ -spinor norm  $-1$  (cf. Example 17.1.2.2). Hence it does not belong to the group  $G'$ , but it extends to an element of  $G$ . Since the index  $[G : G']$  is at most 2, it is exactly 2.  $\square$

The group of orientation preserving diffeomorphisms  $\text{Diff}^+(X_*)$  has a natural representation in  $H^n(X_*, \mathbb{Z})$ . The preceding result implies:

**Corollary 18.3.3.** *Let  $n$  be even and  $\geq 4$  and let  $\ell \in H^n(X_*, \mathbb{Z})$  be the class of a linear section. Then*

$$\text{Im} [\text{Diff}^+(X_*) \longrightarrow \mathcal{O}(H^n(X_*, \mathbb{Z}))] = \begin{cases} \mathcal{O}_\ell(H^n(X_*, \mathbb{Z})) & \text{if } n \equiv 0 \pmod{4}. \\ \mathcal{O}_\ell(H^n(X_*, \mathbb{Z})) \times \{\pm 1\} & \text{if } n \equiv 2 \pmod{4}. \end{cases}$$

*Proof.* Let  $h$  be the class of a hyperplane section. Then  $H^2(X_*) = \mathbb{Z}h$  and so a diffeomorphism preserves  $h$  up to sign. Since the diffeomorphism induced by complex conjugation reverses the sign on  $h$ , the minus sign actually occurs if  $\frac{1}{2}n$  is odd.

The monodromy operators come from diffeomorphisms and so it suffices to find a diffeomorphism giving an isometry fixing  $\ell$  but of  $\varepsilon$ -spinor norm  $-1$ . We

may suppose  $d \geq 3$ . Then  $\Lambda_{d,n}$  is a complete vanishing lattice and as before it contains a hyperbolic plane  $U$  whence a splitting  $H^n(X, \mathbb{Z}) = U \oplus U^\perp$ . Since  $H^n(S^n \times S^n, \mathbb{Z}) \simeq U$ , this yields a connected sum decomposition

$$X_* = (S^n \times S^n) \# X', \quad H_n(X') \simeq U^\perp.$$

Let  $s$  be the reflection in the equator of the sphere  $S^n$ . Then  $(s, s)$  is an orientation preserving diffeomorphism of  $S^n \times S^n$ . Glue this to the identity on  $X'$ . The resulting diffeomorphism  $f$  by construction induces  $-\text{id}$  on  $U$  and  $\text{id}$  on  $U^\perp$ . Since  $\ell \in U^\perp$ , we have  $f_*(\ell) = \ell$ . On the other hand,  $f_*|_U = -\text{id}$  has  $\epsilon$ -spinor norm  $-1$  as we have observed in the proof of Theorem 18.3.2 above.  $\square$

**Historical and Bibliographical Notes.** The main sources for this chapter are W. Ebeling's articles [60, 59, 61] as well as his book [62]. The results in [62, 63] concerning complete intersection singularities are more delicate since certain degenerate lattices may occur. See also [65] by W. Ebeling and S. Gusein-Zade.

The application to global monodromy groups of tautological families of hypersurfaces is due to A. Beauville [18]. This article also contains results on odd-dimensional hypersurfaces, but here the intersection form is alternating and so the symplectic group replaces the role of the orthogonal group. See [18, Thm. 4]. For  $d$  even, the monodromy group turns out to be the full symplectic group and for  $d$  odd there is a quadratic form  $q : H_n(F_*, \mathbb{Z}) \rightarrow \mathbb{F}_2$  such that  $\text{Mon}(\Lambda_{d,n}) = \{\phi \in \text{Sp}(H_n(F_*, \mathbb{Z})) \mid \phi(q) = q\}$ . See [18, Thm. 4] and W. Janssen's article [110].

A. Beauville further shows (Prop. 5 in loc.cit.) that for  $d$  odd and  $n \neq 1, 3, 7$  the latter monodromy group is realized by orientation preserving diffeomorphisms and that in all other cases the entire symplectic group  $\text{Sp}(H_n(F_*, \mathbb{Z}))$  is realized by orientation preserving diffeomorphisms.

---

## Application to Moduli of K3 Surfaces

### Introduction

We have encountered K3 surfaces on various occasions such as in Section 2.5 where we discussed which unimodular lattices can be represented as the intersection lattice of a topological four-manifold. In this chapter we make a more fundamental use of lattice theoretic considerations to understand the period domain as well as the moduli space of K3 surfaces. The required geometric background on K3 surfaces is summarized in the opening Section 19.1. Next, in Section 19.2 the Torelli theorem and the surjectivity of the period map are briefly discussed. Together these give a "linear algebra" description of the period space of marked K3 surfaces and of marked K3 surfaces with prescribed Néron–Severi lattices. The Torelli theorem in its precise form includes a lattice theoretic description of the automorphism group of a K3 surface. This will be further pursued in Chapter 20. In the rather technical Section 19.3 we describe the relevant moduli spaces. This will be used in a crucial way in Section 20.2 of the next chapter.

In Section 19.5 we turn to characteristic  $p$  where we investigate supersingular K3 surfaces, an arithmetic subject with a completely different flavour, but where lattice theory can be applied equally successfully.

In this chapter  $X$  is a K3 surface and we write  $\Lambda$  instead of  $\Lambda_{K3}$  for the K3 lattice.

### 19.1 Background On K3 Surfaces

A K3 surface is, we recall, a simply connected compact complex surface with trivial canonical bundle. It has a nowhere vanishing holomorphic 2-form, unique up to non-zero multiples. We collect some basic material, mostly without proofs and refer for details to [106, Ch. 8] and [15, Ch. VIII.3]. Consult also Appendix B.3 where some examples are given, notably the Kummer surfaces. Recall that the intersection lattice of a compact oriented four-manifold  $X$ , such as the K3 surface, is the free  $\mathbb{Z}$ -module  $H^2(X, \mathbb{Z})/(\text{torsion})$  equipped with the intersection pairing. Since a K3 surface  $X$  is simply connected,  $H^2(X, \mathbb{Z})$  is free and underlies the intersection lattice.

**Proposition 19.1.1.** *All K3 surfaces  $X$  are Kähler and are mutually diffeomorphic. The Betti numbers are  $b_1(X) = b_3(X) = 0$ ,  $b_2(X) = 22$ , and the Hodge*

numbers are  $h^{1,0}(X) = h^{0,1}(X) = 0$ ,  $h^{2,0}(X) = 1$  and  $h^{1,1}(X) = 20$ . The intersection lattice  $H^2(X, \mathbb{Z})$  is isometric to the K3-lattice

$$\Lambda := U^{\oplus 3} \oplus E_8(-1)^{\oplus 2}.$$

Divisors on a K3 surface enjoy special properties which can be read off from their intersection behaviour:

**Proposition 19.1.2.** *Let  $D$  be a divisor on  $X$ .*

1. *If  $D \cdot D \geq -2$  either  $D$  or  $-D$  is effective.*
2. *If  $D$  is irreducible, then  $D \cdot D \geq -2$  and if equality holds  $D$  is a **nodal curve**, that is, a smooth rational curve.*
3.  *$D$  is ample if and only if  $D \cdot D > 0$  and  $D \cdot D' > 0$  for all nodal curves  $D'$ .*

For brevity, the classes of effective, respectively ample divisors in the Néron–Severi lattice  $\text{NS}(X)$  are called effective, respectively ample classes. Likewise, the class of a nodal curve is called a **nodal class**. Observe that nodal classes are roots in  $\text{NS}(X)$ , but not conversely. In fact,  $(-2)$ -roots in the Néron–Severi lattice are classes of divisors  $D$  with  $D \cdot D = -2$  which are not necessarily effective or irreducible. Reflections in  $(-2)$ -roots in  $\text{NS}(X)$  generate its Weyl group. Since the corresponding hyperplane reflections extend to  $H^2(X, \mathbb{Z})$ , this group can be considered as a subgroup of  $O(H^2(X, \mathbb{Z}))$ . We call it the **Weyl group of  $X$** :

$$W^-(X) := W^-(\text{NS}(X)) \subset O(H^2(X, \mathbb{Z})). \tag{19.1}$$

This group is even a normal subgroup of  $O(H^2(X, \mathbb{Z}))$ .

If  $d \in \text{NS}(X)$  is a root, by the preceding proposition, either  $d$  or  $-d$  is effective, which leads to a canonical partition of the set  $\Delta(\text{NS}(X))$  of roots in the Néron–Severi lattice given by

$$\Delta(\text{NS}(X)) = \Delta_X^+ \cup -\Delta_X^+, \quad \Delta_X^+ = \{\text{effective roots}\}. \tag{19.2}$$

The Hodge index theorem B.2.3 states that the intersection product on  $H_{\mathbb{R}}^{1,1}(X) = H^{1,1}(X) \cap H^2(X, \mathbb{R})$  has signature  $(1, h^{1,1}(X) - 1)$ , and so it gives  $H_{\mathbb{R}}^{1,1}(X)$  the structure of a hyperbolic vector space containing  $\text{NS}(X)$ . As explained in Appendix B.2, there is a preferred component  $C_X$  of the “light cone”  $\{x \in H_{\mathbb{R}}^{1,1}(X) \mid x \cdot x > 0\}$ , namely the one that contains the Kähler classes and which is called the **positive cone**. The group  $W^-(X)$  acts on  $H_{\mathbb{R}}^{1,1}(X)$  and by (16.3) it preserves the positive cone.

The Kähler classes in fact belong to the subcone

$$C_X^{\text{Käh}} = \{x \in C_X \mid x \cdot r > 0 \text{ for all nodal classes } r\}. \tag{19.3}$$

This follows since if  $\kappa$  is a Kähler form and  $D$  a nodal curve, its classes  $[\kappa], [D]$  pair to  $[\kappa] \cdot [D] = \int_D \kappa$ , which, because of the inequality (B.1), is positive. The

converse is also true but lies much deeper. See [106, Ch. 8.5]. This motivates naming  $C_X^{\text{Käh}}$  the **Kähler cone** of  $X$ .

If  $X$  is projective, the ample classes belong to the Kähler cone. Conversely, Proposition 19.1.2 implies that a divisor class in the Kähler cone is an ample class. Consequently, the cone in  $H^2(X, \mathbb{R})$  spanned by the ample classes is

$$C_X^{\text{amp}} = C_X^{\text{Käh}} \cap (\text{NS}(X) \otimes \mathbb{R}). \quad (19.4)$$

This cone is called the **ample cone** of  $X$ . The ample classes are precisely the integral classes of the ample cone.

**Proposition 19.1.3.** 1. *The closure of the Kähler cone is a fundamental domain for the action of the Weyl group  $W^-(X)$  (cf. (19.1)) on  $C_X$ .*

2. *If  $X$  is projective, the closure of the ample cone is a fundamental domain for the action of the Weyl group  $W^-(X)$  on the intersection of the positive cone with  $\text{NS}(X) \otimes \mathbb{R}$ .*

3. *The set of nodal classes determines the Kähler cone and if  $X$  is projective, these nodal classes determine the ample cone.*

4. *The choice of a Kähler class determines the entire Kähler cone and in the projective case, the choice of an ample class determines the entire ample cone.*

*Proof.* 1. This follows from Proposition 17.2.6 and characterization (19.3).

2. This follows directly from (19.4).

3. This is a consequence of Proposition 17.2.6.

4. A Kähler class  $\kappa$  belongs to the Kähler cone. The latter is the unique Weyl chamber containing  $\kappa$ . The second assertion follows from this. The last assertion is a consequence of (19.3).  $\square$

## 19.2 K3 Surfaces: Period Domains, Néron–Severi lattices and Transcendental Lattices

**19.2.A Torelli Theorems.** We refer to Appendix B.4 for the definition of the period domain associated to the polarized Hodge structure on the second cohomology group. In the present situation the period domain is given by

$$D(\Lambda) = \{[u] \in \mathbb{P}(\Lambda \otimes \mathbb{C}) \mid u \cdot u = 0, \text{ and } u \cdot \bar{u} > 0\}.$$

Given a **marking**, i.e., a choice of an isometry  $\varphi : H^2(X, \mathbb{Z}) \xrightarrow{\sim} \Lambda$ , the Hodge structure on  $H^2(X, \mathbb{Z})$  defines a period point in  $D(\Lambda)$ . Indeed  $H^{2,0}(X) \subset H^2(X, \mathbb{C})$  is a line and  $\varphi$  sends the corresponding point of the projective space  $\mathbb{P}(H^2(X, \mathbb{C}))$  to a point in the period domain. Two different markings give period points that

are in the same  $O(\Lambda)$ -orbit. Note also that two markings  $\varphi, \varphi'$  give the same period point in case the markings are opposite, i.e.,  $\varphi' = -\varphi$ .

If one has a family  $\mathcal{X} \rightarrow S$  of K3 surfaces over a smooth complex manifold  $S$  together with a global marking (this is always possible if  $S$  is simply connected), then there is an obvious map  $S \rightarrow D(\Lambda)$ , called the **period map**. Work of Griffiths [87, Part II, §2] implies that the period map is holomorphic. The following – far from trivial<sup>1</sup> – results are crucial for our applications:

**Theorem 19.2.1.** *1. Two K3-surfaces are isomorphic if and only if there are markings such that the corresponding period points are the same ("injectivity of the period map" – or – "Torelli theorem").*

*2. All points of the period domain are period points ("surjectivity of the period map").*

Since the group  $O(\Lambda)$  permutes the choices of a marking, the set of isomorphism classes of K3 surfaces corresponds to the orbit space  $O(\Lambda) \backslash D(\Lambda)$ , which is not a nice topological space since the action of the group  $O(\Lambda)$  is not proper. There are various ways to remedy this. In the non-algebraic situation, instead of taking the quotient of the period domain by  $O(\Lambda)$ , one constructs a covering which takes into account the marking and the Kähler cone. This approach will be sketched in Section 19.3. For other approaches we refer to the discussion in [106, Ch. 6].

There is a more precise version of the Torelli theorem (cf. [15, Ch. VIII. 11]) which can be phrased as follows:

**Theorem 19.2.2.** *Let  $X$  be a K3 surface and  $\gamma$  an isometry of  $H^2(X, \mathbb{Z})$ . Then there exists a unique automorphism of  $X$  inducing  $\gamma$  if and only if the following conditions hold simultaneously:*

- *the complexification  $\gamma_{\mathbb{C}}$  of  $\gamma$  preserves the Hodge decomposition, or, equivalently,  $\gamma_{\mathbb{C}}$  preserves the line spanned by the holomorphic 2-form.*
- *$\gamma_{\mathbb{R}}$  preserves the Kähler cone, or equivalently (by Proposition 19.1.3), sends some Kähler class to a Kähler class.*

**Corollary 19.2.3.** *An isometry of  $H^2(X, \mathbb{Z})$  preserving the Hodge decomposition is, up to sign and (left or right) multiplication with an element of  $W^-(X)$ , induced by a unique automorphism of  $X$ .*

*Proof.* Let  $\gamma$  be an isometry of  $H^2(X, \mathbb{Z})$  preserving the Hodge decomposition and let  $\kappa \in C_X^{\text{Kähler}}$ . Then for a unique element  $w \in W^-(X)$ ,  $\pm w \cdot \gamma(\kappa) \in C_X^{\text{Kähler}}$ , and by Proposition 19.1.3  $\pm w \cdot \gamma$  preserves the Kähler cone and so is induced by a unique automorphism of  $X$ . Since  $W^-(X)$  is a normal subgroup of  $O(H^2(X, \mathbb{Z}))$ , we can also write  $w \cdot \gamma = \gamma \circ (\gamma^{-1} w \gamma) = \gamma \circ w'$  for a unique  $w' \in W^-(X)$ . □

The uniqueness statement in Theorem 19.2.2 is implied by the faithfulness of the action of automorphisms on cohomology:

---

<sup>1</sup>We refer the reader to the bibliographic and historical remarks at the end of this chapter.



**Lemma 19.2.4.** *For a K3 surface  $X$  there is an injection*

$$\mathrm{Aut}(X) \hookrightarrow \mathrm{O}(H^2(X, \mathbb{Z})), \quad g \mapsto g^*.$$

In terms of this representation, the above can be restated as

$$\begin{aligned} \mathrm{Aut}(X) &\simeq \{\gamma \in \mathrm{O}(H^2(X, \mathbb{Z})) \mid \gamma_{\mathbb{C}}(H^{2,0}(X)) = H^{2,0}(X) \text{ and } \gamma_{\mathbb{R}} C_X^{\mathrm{K\ddot{a}h}} = C_X^{\mathrm{K\ddot{a}h}}\}, \\ &\simeq \{\gamma \in \mathrm{O}(H^2(X, \mathbb{Z})) \mid \gamma_{\mathbb{C}}(H^{2,0}(X)) = H^{2,0}(X)\} / \{\pm \mathrm{id}\} \times W^-(X). \end{aligned}$$

Observe also:

**Lemma 19.2.5.** *The marked K3-surfaces  $(X, \varphi)$ ,  $(X, \pm \varphi \cdot w)$ ,  $w \in W^-(X)$  and  $(X, \varphi \cdot g^*)$ ,  $g \in \mathrm{Aut}(X)$ , all have the same period point. In particular, if two marked K3 surfaces have the same period point they need not be isomorphic.*

*Remark 19.2.6.* By Proposition 19.1.3, the Kähler cone is preserved by an isometry  $\gamma$  if and only if  $\gamma_{\mathbb{C}}$  preserves the Hodge decomposition and maps some Kähler class to a Kähler class. This is equivalent to "  $\gamma_{\mathbb{C}}$  preserves the Hodge decomposition and the effective roots".

Let us draw a further consequence of Theorem 19.2.1 which addresses **general behaviour**. We say that a property holds generally on some complex variety if it holds on the complement of countably many proper subvarieties. In this sense the general K3 surface is not algebraic, for instance the Kummer surface constructed from a non-algebraic complex two-torus is not algebraic. Theorem 19.2.1 implies that more is true:

**Corollary 19.2.7.** *The general K3 surface does not have any curves on it, in other words, its Picard number, i.e., the rank of its Néron–Severi lattice, is zero.*

*Proof.* Suppose that  $C \subset X$  is a curve. Its class  $[C]$  is of Hodge type  $(1, 1)$  and hence perpendicular to the class of a non-zero 2-form. In geometric terms this means that the corresponding period point belongs to the hyperplane orthogonal to the image of  $[C]$  in  $\Lambda$ . If we delete from  $D(\Lambda)$  the (countably many) hyperplanes orthogonal to primitive elements in  $\Lambda$ , the resulting set  $D(\Lambda)^{\mathrm{gen}}$  then parametrizes K3 surfaces without curves.  $\square$

**19.2.B Algebraic K3 Surfaces and Their Moduli.** One of the peculiar properties of surfaces is that the mere existence of a divisor  $D$  with  $D \cdot D > 0$  implies already that the surface is algebraic. See e.g. [15, Ch. IV. Th. 6.2]. So a marked K3 surface  $(X, \varphi)$  is algebraic if and only if  $\varphi$  sends some divisor class to a lattice element with positive self intersection. In other words, algebraic K3 surfaces correspond to marked surfaces  $(X, \varphi)$  such that  $\ell \in \Lambda$  exists perpendicular to the period point with  $\ell \cdot \ell > 0$ . Just as in the proof of Corollary 19.2.7, this is equivalent to demanding that some period point of  $X$  lies on the hyperplane  $\ell^{\perp} \subset D(\Lambda)$ . There are infinitely many of those since the intersection number  $\ell \cdot \ell$  takes infinitely many values. However, for fixed  $k$  and primitive  $\ell$  with  $\ell \cdot \ell = 2k$  these form one  $\mathrm{O}(\Lambda)$ -orbit. This is a particular case of Example 15.2.8.1. If  $\ell$  corresponds to the

ample divisor  $D$  on  $X$  with  $D \cdot D = 2k$ , we call the divisor class  $[D]$  a **degree  $2k$  polarization**. The corresponding Hodge structure on  $\Lambda$  will then be such that  $\ell$  has type  $(1, 1)$ . In other words, the period point belongs to

$$D(\ell^\perp) = \{[u] \in D(\Lambda) \mid u \cdot \ell = 0\}.$$

By [15, Ch. VIII, Theorem 22.3] the isometry group  $O(\ell^\perp)$  acts properly and discontinuously on this new domain. The quotient does not yet give the moduli space of algebraic K3 surfaces with a polarization of degree  $2k$ . Indeed, also the hyperplanes orthogonal to  $(-2)$ -roots in  $\ell^\perp \subset \Lambda$  need to be deleted (see [15, Ch. VIII, 22]). This leads to

$$\mathring{D}(\ell^\perp) = D(\ell^\perp) - \bigcup_{r \in \ell^\perp, r \cdot r = -2} r^\perp \cap D(\ell^\perp).$$

The group  $O(\ell^\perp)$  also acts on this domain in a properly discontinuous fashion. By [14] the quotient is a quasi-projective algebraic variety. This is the variety whose points correspond to the isometry classes of K3 surfaces admitting a degree  $2k$  polarization. Such a variety is also called a **moduli space**.<sup>2</sup> Summarizing, we have:

**Theorem 19.2.8** (cf. [15, Ch. VIII, Thm 22.2]). *Fix  $\ell \in \Lambda$  with  $\ell \cdot \ell = 2k$ . The moduli space of K3 surfaces admitting a degree  $2k$  polarization is the quasi-projective variety*

$$O(\ell^\perp) \backslash \mathring{D}(\ell^\perp).$$

**19.2.C Period domains for  $S$ -marked K3 surfaces.** Analogously to Corollary 19.2.7, the rank of the Néron–Severi lattice of the general algebraic K3 surface is 1. Those that have a larger Picard number can be retrieved replacing  $\ell$  with a suitable lattice  $S$  leading to  $S$ -markings.

**Definition 19.2.9.** Suppose that  $S$  is a non-degenerate lattice which is either negative definite or has signature  $(1, r_-)$ ,  $r_- \geq 0$ , and which is primitively embedded in  $\Lambda$ . A marking  $\varphi : H^2(X, \mathbb{Z}) \xrightarrow{\sim} \Lambda$  such that  $S \subset \varphi(\text{NS}(X))$  is called an  **$S$ -marking**. The pair  $(X, \varphi)$  with  $\varphi$  an  $S$ -marking is called an  **$S$ -marked K3 surface**.<sup>3</sup>

The domain

$$D(S^\perp) = \{[u] \in D(\Lambda) \mid u \cdot S = 0\}$$

parametrizes  $S$ -marked K3 surfaces  $(X, \varphi)$ . It has dimension  $20 - \text{rank}(S)$  and (according to Appendix B.4) if  $r_- < 19$  it is connected since  $T = S^\perp$  has signature  $(2, 19 - r_-)$ . Deleting, as before, countably many hyperplanes leaves us with K3 surfaces with Néron–Severi lattice exactly  $\varphi^{-1}S$ .

<sup>2</sup>This is a pedestrian approach. The formal definition of a moduli space is more involved. Nowadays one prefers instead the concept of moduli stack since the latter is better behaved with respect to automorphisms of varieties. See e.g. [106, Chapter 5] for a concise introduction.

<sup>3</sup>Some authors speak of an  $S$ -polarization. Note that  $X$  is projective if and only if  $S$  has one positive eigenvalue and so the terminology  $S$ -marking is more appropriate.

Natural questions are: 1) Which  $S$  occur as the Néron–Severi lattice of a K3 surface? 2) Which  $T$  as the transcendental lattice of a K3 surface? This is in general quite involved, but one can definitely say more about small ranks making use of Example 15.2.8.1:

**Proposition 19.2.10** ([158, §2]). *1. Every non-degenerate negative definite quadratic lattice  $S$  of rank  $\rho \leq 11$  or of signature  $(1, \rho - 1)$ ,  $1 \leq \rho \leq 10$ , occurs as the Néron–Severi lattice of a general  $S$ -marked K3 surface and embeds uniquely in the K3 lattice.*

*2. Every non-degenerate quadratic lattice  $T$  of signature  $(2, 20 - \rho)$ ,  $12 \leq \rho \leq 20$ , occurs as the transcendental lattice of a general  $T^\perp$ -marked K3 surface<sup>4</sup> and embeds uniquely in the K3 lattice.*

As for uniqueness of the isometry class of the Néron–Severi lattice or the transcendental lattice, the situation is in some sense dual:

**Proposition 19.2.11** ([158, Cor. 2.9, Cor. 2.10]). *Let  $X$  be a K3 surface.*

*1. If  $12 \leq \rho(X) \leq 20$ , then the Néron–Severi lattice of  $X$  is unique in its genus.*

*2. If  $\rho(X) \leq 10$ , then the transcendental lattice of  $X$  is unique in its genus.*

*Proof.* Let  $S = \text{NS}(X)$  and  $G$  its discriminant group. Since  $T = S^\perp \subset H^2(X, \mathbb{Z})$  has the same discriminant group, we have  $\ell(G) \leq \text{rank}(T) = 22 - \rho(X) \leq 10$ . The condition of Corollary 14.4.3 is  $\ell(G) \leq \text{rank}(S) - 2 = \rho(X) - 2$ . This is the case since  $10 \leq \rho(X) - 2$ . The proof of the assertion for small Picard numbers is analogous.  $\square$

*Remark 19.2.12. 1.* In the non-algebraic situation  $\text{NS}(X)$  can indeed be negative definite or have a one-dimensional null-space. The last two cases occur if and only if the function field of  $X$  has transcendence degree  $a(X) = 0$ , respectively  $a(X) = 1$ . Indeed, if an isotropic  $f \in \text{NS}(X)$  exists, then  $\pm f$  is effective and one can show (cf. [124, Thm. 4.1, 4.2]) that a suitable multiple defines an elliptic fibration. This implies that  $a(X) \geq 1$ . If  $a(X) = 2$  the surface  $X$  is algebraic (cf. [15, Ch. IV. Corollary 6.5]) and its Néron–Severi lattice is not negative semi-definite. If  $\text{NS}(X)$  is negative definite,  $X$  cannot be elliptic or algebraic, and hence  $a(X) = 0$ .

*2.* By Theorem 15.2.6 any unimodular lattice  $S$  of rank  $\leq 20$  embeds uniquely in the K3 lattice provided  $T = S^\perp$  is indefinite. This ceases to be true if  $T$  is definite which may only occur in the non-algebraic situation. The simplest example is presented by the sublattice  $S = \mathbb{Q}^3 U$ . In the standard embedding its orthogonal complement is  $\mathbb{Q}^2 E_8(-1)$ . However, as we have seen (Example 1.5.1.2), there is another even unimodular rank 16 lattice which is negative definite and indecomposable,  $\Gamma_{16}(-1)$ . By Theorem 2.4.1, which gives the classification of indefinite even unimodular lattices,  $\mathbb{Q}^3 U \oplus \mathbb{Q}^2 E_8(-1) \simeq \mathbb{Q}^3 U \oplus \Gamma_{16}(-1)$ . So two possible period domains then occur for (non-algebraic) K3 surfaces having the same Néron–Severi lattice, but with different transcendental lattices.

<sup>4</sup>Such a K3 surface is projective since  $T^\perp$  has signature  $(1, \rho - 1)$ .

### 19.3 The Moduli Space of Marked K3 Surfaces

The main result from [33] is as follows:

**Theorem 19.3.1.** *There exists a smooth (non-Hausdorff) analytic space  $\mathcal{M}$  of dimension 20 together with a universal family of marked K3 surfaces.*

1. *The induced period map  $\rho : \mathcal{M} \rightarrow D(\Lambda)$  is surjective;*
2. *The fiber over each point  $[u] \in D(\Lambda)$  is discrete (but might be infinite);*
3. *The period map  $\rho$  is étale in the sense that every  $[u] \in D(\Lambda)$  has an open neighbourhood  $U$  so that  $\rho$  maps every connected component of  $\rho^{-1}U$  biholomorphically to  $U$ .*

**19.3.A Construction of the moduli space.** By the results of Appendix B.4, the period domain  $D(\Lambda)$  consisting of period points of marked K3 surfaces is a connected complex manifold of dimension 20. Denote the Hodge decomposition corresponding to  $[u] \in D(\Lambda)$  by<sup>5</sup>

$$\Lambda_{\mathbb{C}} = \Lambda_u^{2,0} \oplus \Lambda_u^{1,1} \oplus \Lambda_u^{0,2}.$$

The above Hodge structures for varying  $[u] \in D(\Lambda)$  define a variation of Hodge structure over  $D(\Lambda)$  in the technical sense of [89] which is also called the tautological variation of Hodge structure. There does not exist a family of marked K3 surfaces  $(X_u, \varphi_u)$ ,  $u \in D(\Lambda)$ , with the property that the Hodge decompositions of  $H^2(X_u)$  under the marking  $\varphi_u$  give the tautological variation, but we can achieve this locally as follows. Let  $X_0$  be a K3-surface. There is a locally universal deformation  $p : \mathcal{X}_U \rightarrow U$  of  $X_0 = p^{-1}(0)$  consisting of K3 surfaces, the so-called **Kuranishi family** for  $X_0$ . One may take for  $U$  a disc centered at 0 and then there is a constant marking  $\varphi_s : H^2(X_s, \mathbb{Z}) \xrightarrow{\sim} \Lambda$  over  $U$ , i.e., a trivialization of the local system  $R^2p_*\mathbb{Z}$ . There are no two isomorphic (marked) fibres in the Kuranishi family. If this would be the case, there is an isomorphism  $g : (X_1, \varphi_1) \rightarrow (X_2, \varphi_2)$ , and then  $\varphi_1 g^* \varphi_2^{-1} = \text{id}_{\Lambda}$  since  $X_1, X_2$  are in a single trivialized family with discrete fibres in the local system  $R^2p_*\mathbb{Z}$ . This implies  $\varphi_1 g^* = \varphi_2$  so that we would get identical period points by (a variation of) Lemma 19.2.5, which contradicts that the period map is an embedding (cf. [87, Part II, §2]).

Consequently, via constant markings one can glue the Kuranishi deformations for the various K3 surfaces and obtain in this way a smooth analytic space  $\mathcal{M}$  over which one has a universal marked family of K3 surfaces with, again by [87, Part II, §2], a holomorphic map

$$\rho : \mathcal{M} \rightarrow D(\Lambda), \tag{19.5}$$

the period map for this family. It is a surjective map (cf. Theorem 19.2.1) but  $\rho$  clearly cannot be injective: by Lemma 19.2.5 two marked K3 surfaces with the same period point need not be isomorphic (as *marked* K3's; Torelli's theorem states

<sup>5</sup>To ease notation we will occasionally write  $u$  instead of  $[u]$  if no confusion is likely to arise.

that they are isomorphic if one allows changing the marking). Indeed, the period point determines the Weyl chambers up to signs through the roots perpendicular to it, and so it does not "see" the Kähler cone. This suggests to add the Weyl chamber data to this marking, yielding a strong marking.

**19.3.B Description of  $\mathcal{M}$  in terms of strong markings.** We give another description (without proofs) of  $\mathcal{M}$  which explains the assertion in Theorem 19.3.1 that the period map is étale. A priori this description gives a different space  $\widetilde{D(\Lambda)}$  which by construction lies étale over the period domain  $D(\Lambda)$ . We refer to loc. cit. that this space is biholomorphic to  $\mathcal{M}$  and that the projection map corresponds to the period map  $\rho$ .

In this alternative description, the fiber of  $\rho$  over a period point  $[u]$  of  $(X, \varphi)$  is constructed in such a way that it indeed parametrizes the supplementary data of Weyl chambers over  $[u]$  which together with  $\varphi$  define a **strongly marked K3 surface**. Recall first (cf. Section B.4) that the intersection form induces a non-degenerate quadratic form of signature  $(1, 19)$  on  $\Lambda_{u, \mathbb{R}}^{1,1}$ , and that the light cone has two components  $\pm C_u$ . The cone  $C_u$  is the union of Weyl chambers  $C_u^P$  parametrized by partitions labeled by  $P$

$$\Delta_u := \Delta_u^P \cup -\Delta_u^P \quad (19.6)$$

of the set  $\Delta_u$  of all roots orthogonal to  $u$ . If the latter set is empty, by convention  $C_u^P = C_u$ . Of course the same partition also determines a Weyl chamber in the opposite cone  $-C_u$ . It turns out that  $\rho^{-1}[u]$  consists of the collection of points  $\{u^{+,P}, u^{-,P}\}_P$ , where  $P$  runs through the partitions of  $\Delta_u$  and where for each  $P$  a pair  $u^{\pm,P} \in \pm C_u^P$  is chosen. The union of the  $\rho^{-1}[u]$  defines  $\widetilde{D(\Lambda)}$  as a set.

Note that  $\#(\rho^{-1}[u])$  may vary wildly with  $u$  and so it seems counter-intuitive that the period map  $\rho$  is a local homeomorphism as indeed it is. On the level of the K3 surfaces the variation of  $\#(\rho^{-1}[u])$  is due to the fact that for varying period points the corresponding K3 surface can acquire wildly varying numbers of nodal curves giving rise to varying numbers of possible markings. This causes the non-Hausdorff nature of the topology of  $\widetilde{D(\Lambda)}$ . Let us illustrate how this can happen. Consider a point  $u \in D(\Lambda)$  such that  $C_u$  is divided in two Weyl chambers parametrized by  $P_1, P_2$ , while  $\Delta_{u'} = \emptyset$  for all points  $u'$  in a punctured neighbourhood  $U$  of  $u$ . Then  $\rho^{-1}U = U^{+,P_1} \cup U^{-,P_1} \cup U^{+,P_2} \cup U^{-,P_2}$  where  $U^{\pm,P_1}$  is glued to  $U^{\pm,P_2}$  over the complement of  $u^{\pm,P_1} \cup u^{\pm,P_2}$ , creating an isolated "double point".

This phenomenon happens indeed as a consequence of the topology of  $\widetilde{D(\Lambda)}$  which we shall describe now. Over a general point  $u$  the fiber of  $\rho$  consists of two points  $u^\pm$  in the two connected components  $\pm C_u$  of the light cone which can be considered as belonging to the two connected components  $D^\pm(\Lambda)$  of  $\mathrm{SO}(3, 19)/\mathrm{SO}(2) \times \mathrm{SO}^+(1, 19)$ . This space has indeed two components since it is a disconnected two-sheeted cover of  $D(\Lambda) = \mathrm{SO}(3, 19)/\mathrm{SO}(2) \times \mathrm{SO}(1, 19)$  which itself is connected by Proposition 13.3.7.

Next, we need a continuity property (cf. [33, Proposition 2.3]) which states that every point  $(u, c) \in D(\Lambda) \times \Lambda_{\mathbb{R}}$  such that  $c \in C_u$  has an open neighbourhood  $U_{u,c} \times K_{u,c}$  with the property that the only reflection hyperplanes in any  $u' \times \Lambda_{\mathbb{R}}$ ,

$u' \in U_{u,c}$ , for roots orthogonal to  $u'$  that meet  $u' \times K_{u,c}$  are ones orthogonal to  $u$ . In particular,  $c$  (considered in the fixed vector space  $\Lambda_{\mathbb{R}}$ ) belongs to a Weyl chamber relative to *all* points in  $U_{u,c}$ .

Now form the topological space  $\widetilde{D(\Lambda)}$  by taking the disjoint union  $\coprod U_{u,c}$  for all  $u \in D(\Lambda)$  and all  $c \in \pm C_u$ , and then glue  $u' \in U_{u_1,c_1}$  to  $u'' \in U_{u_2,c_2}$  if and only if  $\rho(u') = \rho(u'')$  and  $c_1$  and  $c_2$  belong to the same Weyl chamber relative  $\rho(u')$ . By [33, Cor. 2.4] the continuity property implies that in this way  $U_1$  glues to  $U_2$  along a common open set. This makes  $\widetilde{D(\Lambda)}$  an analytic space and  $\rho$  a local homeomorphism. Moreover, the fibers  $\rho^{-1}[u]$  are indeed parametrized by  $\pm P$ , where  $P$  is a partition of the roots  $\Delta_u$ .

To give an idea what this space looks like, recall that a general K3 surface does not have curves and so the positive cone is the only Weyl chamber. If  $u$  is its period point, an open neighbourhood  $U \subset D(\Lambda)$  is covered by two open subsets  $U^\pm \subset \widetilde{D(\Lambda)}$ . For non-general points  $u' \in U$  the cone  $C_{u'}$  has more Weyl chambers  $C_{u'}^P$ , which are present along a subvariety, say  $W$ . Over  $u'$  as well as over the general point of  $W \cap U$  the fiber  $\rho^{-1}u'$  contains the supplementary points  $u'^{\pm P}$ . There are neighbourhoods  $U'^{\pm P} \subset \widetilde{D(\Lambda)}$  for each of these points  $u'^{\pm P}$  which under  $\rho$  map biholomorphically to open subsets in  $D(\Lambda)$ . These are glued to  $U^\pm$  so that the supplementary points  $u'^{\pm P}$  form a non-separated subset each belonging to a distinct open subset of  $\widetilde{D(\Lambda)}$ . This holds for all points in  $\rho^{-1}(W \cap U) \subset \widetilde{D(\Lambda)}$ .

We shall from now on identify  $\widetilde{D(\Lambda)}$  and the moduli space  $\mathcal{M}$  of strongly marked K3-surfaces.

**19.3.C Moduli of S-marked K3 surfaces.** Recall that the period domain of S-marked surfaces is the subdomain  $D(S^\perp) = \{[u] \in D(\Lambda) \mid u \cdot S = 0\}$ , where the lattice  $S \subset \Lambda$  is as in Definition 19.2.9. Consider

$$\mathcal{M}_S := \rho^{-1}D(S^\perp) \subset \mathcal{M}.$$

If  $[u] \in D(S^\perp)$ , the "Néron–Severi lattice"  $NS(u) := \{x \in \Lambda \mid x \cdot u = 0\}$  contains  $S$  and is generally equal to it. As we explained in the previous subsection, this implies that the fiber of  $\rho$  of a general point  $[u] \in D(S^\perp)$  consists of a number of disjoint points parametrized by  $(\pm, P)$ , where  $P$  is a partition of the roots in  $S$ . Since  $\rho$  is a local homeomorphism, one expects that the connected components of  $\mathcal{M}_S$  are also parametrized by  $(\pm, P)$ . This is indeed the case as shown by V. Nikulin ([169, Proposition 2.9]). Even more is true:

**Proposition 19.3.2.** *There is an open dense subset  $\mathring{D}(S^\perp) \subset D(S^\perp)$  so that the roots in  $\Delta_u$ ,  $[u] \in \mathcal{M}_S$ , are irreducible, i.e., for some marking all roots correspond to nodal classes. Let  $P$  be a partition of the roots of  $S$ . The connected components of  $\mathcal{M}_S$  consist of the non-Hausdorff smooth analytic spaces  $\mathcal{M}_S^{\pm, P}$  of dimension  $20 - \text{rank}(S)$ .*

## 19.4 Lattices and Compactifications of Moduli Spaces

This section describes how the lattice theory developed in the earlier chapters plays a role in the construction of compactifications of the moduli spaces of algebraic K3 surfaces.

Recall that in § 19.2.B lattices were used to describe the moduli space of polarized K3 surfaces of degree  $2k$  in arithmetic terms through the period map. Our setting is an elaboration of a special case of the theory described e.g. by W. Baily and A. Borel in [14]. We limit ourselves to an outline of a typical base case, that of the so-called *Satake–Baily–Borel (SBB) compactification* of the moduli space of polarized K3 surfaces of degree 2, but note that lattices also play a role for other degrees and other surfaces, and in more refined (partial) compactifications, with toroidal compactifications as another extreme. For example, E. Looijenga in [143] described an intermediate compactification in the case of K3 surfaces of degree 2 which provides an arithmetic counterpart to J. Shah’s geometric invariant theory approach in [206], and is based on the representation of degree 2 K3 surfaces as double covers of the projective plane branched along sextics.

It turns out that isotropic sublattices play a central role in the construction of the SBB compactification of the moduli space. As stated above, we illustrate this for polarized K3 surfaces of degree 2. So, if - as before -  $\Lambda = E_8(-1) \oplus E_8(-1) \oplus U \oplus U \oplus U$  is the K3 lattice, we aim to represent the polarization by a vector  $h \in \Lambda$  with  $h \cdot h = 2$ . Up to  $O(\Lambda)$ -equivalence  $h$  is unique by Theorem 15.2.6. If  $[D]$  is a degree 2 (almost)<sup>6</sup> polarization, there indeed exists a marking identifying  $[D]$  with  $h \in L$ . We use the standard bases  $\{e, f\}$ ,  $\{e', f'\}$ ,  $\{e'', f''\}$  of the first, second and third copy  $U$  in  $\Lambda$  (so  $e \cdot e = f \cdot f = e \cdot f - 1 = 0$ , etc.). We choose  $h = e'' + f'' \in \Lambda$ . Below we will make use of the standard root bases  $\alpha_1, \dots, \alpha_8$  and  $\alpha'_1, \dots, \alpha'_8$  of the two copies of  $E_8(-1)$ .

The orthogonal complement  $\Lambda_2 = h^\perp = E_8(-1) \oplus E_8(-1) \oplus U \oplus U \oplus \langle e'' - f'' \rangle$  in  $\Lambda$  is a rank 21 lattice of signature  $(2, 19)$ . We view the period point of an almost polarized K3 surface as an element in

$$D(\Lambda_2) = \{\omega \in \mathbb{P}(\Lambda_2)_{\mathbb{C}} \mid \omega \cdot \omega = 0, \omega \cdot \bar{\omega} > 0\}.$$

Since  $\Lambda_2^*/\Lambda_2$  and  $\langle h \rangle^*/\langle h \rangle$  are isomorphic and of order 2, every isometry of  $\Lambda_2$  to itself induces the identity on  $\Lambda_2^*/\Lambda_2$  and hence can be extended to an isometry of  $\Lambda$  fixing  $h$  by Theorem 15.1.7. The image  $\Gamma_2$  of the natural map  $O(\Lambda)_h \rightarrow O(h^\perp)$  is therefore  $O(h^\perp)$  itself, and, similarly to what was discussed in Section 19.2.B,  $D(\Lambda_2)/\Gamma_2$  is quasi-projective, and is a moduli space of almost polarized K3 surfaces of degree 2.

**19.4.A Boundary components.** To obtain the SBB compactification, first ‘boundary components’ are added to  $D(\Lambda_2)$  in such a way that the resulting union  $\hat{D}(\Lambda_2)$

<sup>6</sup>If we allow our surfaces to have rational double point singularities, then in the minimal desingularizations, which are also K3 surfaces, these give rise to curve configurations perpendicular to the pull-back of  $[D]$ . This set-up has various advantages we won’t go into here. In particular, it eliminates the need to exclude the hyperplanes as discussed in Section 19.2.B.

can be provided with a topology leading to a quotient space  $\hat{D}(\Lambda_2)/\Gamma_2$  with the structure of a *compact* complex analytic (even algebraic) space. The boundary components are 0- and 1-dimensional and turn out to correspond to  $\Gamma_2$  orbits of primitive isotropic sublattices of ranks 1 and 2, respectively. Since any element  $\omega \in \Lambda_2 \otimes \mathbb{C}$  satisfying  $\omega \cdot \omega = 0$  and  $\omega \cdot \bar{\omega} > 0$  corresponds to a positive definite plane in  $\Lambda_2 \otimes \mathbb{R}$  spanned by  $\text{Re}(\omega), \text{Im}(\omega)$ , one can imagine that boundary components are related to ‘limits’ of such planes, i.e., an isotropic line or plane. On the geometric side boundary components are related to degenerations of K3 surfaces of degree 2, i.e., double covers of certain singular plane sextics. The isotropic sublattices are also an ingredient in more sophisticated geometrically relevant compactifications.

Let  $I$  be an isotropic subspace of  $\Lambda_2 \otimes \mathbb{R}$ . It corresponds to a boundary component  $F_I \subset \hat{D}(\Lambda_2)$  of  $D(\Lambda_2)$  whose closure is of the form  $\overline{F_I} = \mathbb{P}(I_{\mathbb{C}}) \cap \overline{D(\Lambda_2)}$  (in the case the dimension of  $I$  is 1 this is just a point). For the SBB compactification in our setting, only the so-called rational boundary components play a role. These are the boundary components that correspond to isotropic subspaces defined over the rationals, so that we can restrict our attention to primitive isotropic sublattices  $I$  of  $\Lambda_2$ . Since the signature of  $\Lambda_2$  is  $(2, 19)$ , such isotropic sublattices can only have rank 1 or 2. In the first case the boundary component is a single point, in the second case  $F_I$  is isomorphic to a half-plane in  $\mathbb{P}(I_{\mathbb{C}})$ . If  $I \subset J$ , where  $I$  is a rank 1 isotropic sublattice and  $J$  a rank 2 isotropic sublattice, then  $F_I$  is contained in the closure of  $F_J$ .

**19.4.B Isotropic sublattices of rank 1.**

**Lemma 19.4.1.** *There is only one rank 1 primitive isotropic sublattice of  $\Lambda_2$  up to  $\Gamma_2$ -equivalence.*

*Proof.* We use Corollary 17.3.10 to prove this. Let  $x \in \Lambda_2 = E_8(-1) \oplus E_8(-1) \oplus U \oplus U \oplus \langle v \rangle$  be a primitive isotropic vector, where  $b(v, v) = -2$ . We first show that  $b(x, \Lambda_2) = \mathbb{Z}$ . Suppose  $b(x, \Lambda_2) = m\mathbb{Z}$ , with  $m$  a positive integer. Then  $x/m \in \Lambda_2^* = E_8(-1) \oplus E_8(-1) \oplus U \oplus U \oplus \langle \frac{1}{2}v \rangle$ . So  $x/m = w + \frac{1}{2}\gamma v$ , with  $w \in E_8(-1) \oplus E_8(-1) \oplus U \oplus U$  and  $\gamma \in \mathbb{Z}$ . From  $0 = b(w + \frac{1}{2}\gamma v, w + \frac{1}{2}\gamma v) = b(w, w) - \frac{1}{2}\gamma^2$  we obtain that  $\frac{1}{2}\gamma^2$  is even and hence that  $\gamma$  is even. But then  $x/m \in \Lambda_2$  and  $m = 1$  by primitivity of  $x$ .

By Corollary 17.3.10-2 the vector  $x$  is equivalent to a vector of the form  $ae + f$  for some  $a \in \mathbb{Z}$ , where  $e, f$  are the standard basis vectors of the first copy of  $U$ . Since  $x$  is isotropic,  $a = 0$ , and  $x$  is equivalent to  $f$  (and of course also to  $e'$  in the second copy of  $U$ , etc.) □

**19.4.C Isotropic sublattices of rank 2.** If  $J$  is a rank 2 primitive isotropic sublattice of  $\Lambda_2 = E_8 \oplus E_8 \oplus U \oplus U \oplus \langle e'' - f'' \rangle$ , we may assume by the above lemma that  $J$  contains  $I = \langle e' \rangle$  (in the second copy of  $U$ ), so that we can reduce our search for rank 2 primitive isotropic sublattices in  $\Lambda_2$  to determining rank 1 isotropic sublattices in  $I^\perp/I = E_8(-1) \oplus E_8(-1) \oplus U \oplus \langle e'' - f'' \rangle$  (the second copy of  $U$  taken out) up to  $O(I^\perp/I)$ -equivalence. We first establish that the natural maps  $O^-(\Lambda)_h \rightarrow O(\Lambda_2)$  and  $O(\Lambda_2)_{e'} \rightarrow O(I^\perp/I)$  are surjective.



**Lemma 19.4.2.** *Let  $h = e'' + f'' \in \Lambda$  and  $e'$  be as above. The natural maps  $O^-(\Lambda)_h \rightarrow O(\Lambda_2)$  and  $O(\Lambda_2)_{e'} \rightarrow O(I^\perp/I)$  are surjective.*

*Proof.* Let  $S = \langle h \rangle$  and  $T = \langle h \rangle^\perp = \Lambda_2$ , both non-degenerate primitive sublattices of  $\Lambda$ . Then  $S^*/S$  and  $T^*/T$  are of order 2 so that isometries of  $S$  and  $T$ , respectively, induce the identity on  $S^*/S$  and  $T^*/T$ , respectively. Proposition 15.1.6 implies that every element  $O(\Lambda_2) = O(T)$  extends to an isometry of  $\Lambda$  preserving  $h$ , i.e., an element in  $O^-(\Lambda)_h$ . So the map  $O^-(\Lambda)_h \rightarrow O(\Lambda_2)$  is surjective.

The second claim is easy since every isometry of  $I^\perp/I = E_8(-1) \oplus E_8(-1) \oplus U \oplus \langle e'' - f'' \rangle$  can simply be extended with the identity on the second copy of  $U$  in  $E_8(-1) \oplus E_8(-1) \oplus U \oplus U \oplus \langle e'' - f'' \rangle$ .  $\square$

As before,  $\Lambda_2 = E_8(-1) \oplus E_8(-1) \oplus U \oplus U \oplus \langle v \rangle$ , with  $v = e'' - f''$  and  $v \cdot v = -2$ . If  $J$  is a rank 2 primitive isotropic sublattice of  $\Lambda_2$  containing  $e'$ , then  $J/I$  determines a primitive isotropic rank 1 sublattice in  $I^\perp/I \cong E_8(-1) \oplus E_8(-1) \oplus U \oplus \langle v \rangle$ , an even lattice of hyperbolic signature  $(1, 18)$ . We continue by searching for primitive isotropic rank 1 lattices in  $E_8(-1) \oplus E_8(-1) \oplus U \oplus \langle v \rangle$ , with  $v \cdot v = -2$ . Here we use È. Vinberg's work [236] in which he describes a procedure which, under favourable circumstances, may be used to determine the set of equivalence classes (with respect to lattice isometries) of primitive isotropic rank 1 sublattices in a lattice of hyperbolic signature, a procedure which we briefly discuss. Let  $(M, b)$  be a non-degenerate lattice of signature  $(1, n)$  and let  $C_M$  be one of the two connected components of  $\{x \in M_{\mathbb{R}} \mid b(x, x) > 0\}$ . Let  $O^-(M)$  be the subgroup of index 2 of  $O(M)$  fixing  $C_M$  (see Section 16.1). If the subgroup generated by reflections  $s_v$  with  $b(v, v) < 0$  is of finite index, it has a polyhedral fundamental domain  $P$  of finite volume (viewed in the associated Lobachevskii space  $C_M/\mathbb{R}_+$ ) whose bounding reflection hyperplanes and their relative position can be determined by Vinberg's procedure. A Dynkin diagram is used to represent and visualize this information. From these results one then finds the vertices 'at infinity' of this polyhedron, i.e., the isotropic rank 1 sublattices up to reflection subgroup equivalence. The step from reflection subgroup equivalence to isometry group equivalence is made by using the symmetries of the Dynkin diagram.

The polyhedron  $P$  is described by inequalities of the form  $b(x, v) \geq 0$ , where the vectors  $v$  correspond to the vertices of the diagram. By exploiting a close relative of the distance function in Lobachevskii space, Vinberg's algorithm provides a way to successively compute the bounding hyperplanes of a fundamental domain and to determine when to stop.

According to Vinberg, the vertices in the diagram can be found as follows. Take a vector  $x \in C_M \cap M$ . The idea behind the procedure is to successively look for a bounding hyperplane that is closest to  $x$  (in the Lobachevskii space) given a certain intersection behaviour with hyperplanes found thus far. In practice this means: look for vectors  $v_1, v_2, \dots \in M$  corresponding to reflections (and determining bounding hyperplanes) such that the expression

$$\frac{b(x, z)^2}{|b(z, z)|}, \tag{19.7}$$

which is closely related to the distance function in Lobachevskii space, is minimal for  $z = v_1$  (this means that the hyperplane  $H_1 = v_1^\perp$  is ‘closest’ to  $x$  in the Lobachevskii space), and such that  $v_2$  satisfies  $b(v_2, v_1) \geq 0$  and the expression 19.7 is minimal for  $z = v_2$  given this inequality, and so on. Vinberg furthermore states a test when to stop, namely as soon as the following conditions are satisfied: if, in a given stage, the diagram contains no so-called Lannér diagrams, if every parabolic subdiagram can be extended to a parabolic subdiagram of rank  $n - 1$  (the rank of a parabolic subdiagram is its number of vertices minus its number of connected components), and if a condition is satisfied for pairs of bounding hyperplanes not meeting in the cone (they correspond to dashed rank 2 subdiagrams).

In our situation, the lattice is  $I^+/I \cong E_8(-1) \oplus E_8(-1) \oplus U \oplus \langle v \rangle$ , has rank 19 and is of signature (1, 18). We apply Vinberg’s algorithm, where we start by taking  $x = e + f \in U$  in the positive cone. As for notation, we let  $\omega_1, \dots, \omega_8$  be the dual basis of  $\alpha_1, \dots, \alpha_8$  and  $\omega'_1, \dots, \omega'_8$  the dual basis of  $\alpha'_1, \dots, \alpha'_8$ . Vinberg’s procedure leads to the following vectors (see also the Dynkin diagram for an overview):

- Roots corresponding to hyperplanes with distance 0 to the class of  $e + f$  in Lobachevskii space, i.e., roots that are perpendicular to  $e + f$ : the roots  $\alpha_1, \dots, \alpha_8$  in the first copy of  $E_8(-1)$  and the roots  $\alpha'_1, \dots, \alpha'_8$  of the second copy of  $E_8(-1)$ ; the root  $f - e \in U$  and  $v$  in the last summand.
- Next we take the  $(-2)$ -roots  $\omega_8 + e$  and  $\omega'_8 + e, -v + e$ . These are mutually perpendicular and perpendicular to  $\alpha_1, \dots, \alpha_7, \alpha'_1, \dots, \alpha'_7$ , have inner product  $+1$  with  $f - e$ . The root  $-v + e$  satisfies  $b(-v + e, v) = 2$ . The distance expression is  $1/2$  for these roots.
- Then take  $\omega_1 + \omega'_1 + 2e + 2f - v$ . This root is perpendicular to most of the roots found so far, in particular to  $\omega_8 + e, \omega'_8 + e$ , and  $-v + e$ ; it has inner product  $1$  with  $\alpha_1$  and  $\alpha'_1$ , and inner product  $2$  with  $v$ . The distance expression is  $4^2/2 = 8$  for these roots.
- Finally, we take the  $(-2)$ -roots  $\beta = 2\omega_2 + 2\omega'_7 + 6e + 6f - 3v$  and, symmetrically,  $\beta' = 2\omega'_2 + 2\omega_7 + 6e + 6f - 3v$ . Note that

$$b(\beta, \beta') = b(\beta, v) = b(\beta', v) = 6;$$

the corresponding vertices in the Dynkin diagram are connected by a dashed edge. The distance expression is  $12^2/2 = 72$ .

The resulting Dynkin diagram is shown below.

We briefly verify Vinberg’s conditions (see [235], especially pages 22, and 33–34, or see Ch. 5 in G. Heckman’s more recent notes [95]).

- a) The maximal rank parabolic subdiagrams are all of rank 17:  $\tilde{A}_{17}, \tilde{E}_8 + \tilde{E}_8 + \tilde{A}_1, \tilde{D}_{16} + \tilde{A}_1, \tilde{D}_{10} + \tilde{E}_7$ . Some occur multiple times because of symmetry.
- b) Take two vertices of a dashed line in the diagram; the corresponding roots span a hyperbolic lattice of rank 2. The roots corresponding to the vertices in the diagram not connected to these two span a negative definite lattice  $A_{11} \oplus E_6$  of rank 17. Together the  $17 + 2$  roots span a rank 19 sublattice which is of finite index and hence its orthogonal complement consists of  $\{0\}$  only.

Since the roots represented in the diagram span the lattice, we also see that the symmetries of the graph come from isometries of the lattice  $I^\perp/I$  so that  $O^-(I^\perp/I) = W \rtimes S_3$ . Hence every isotropic vector is equivalent to one of the four types mentioned above.

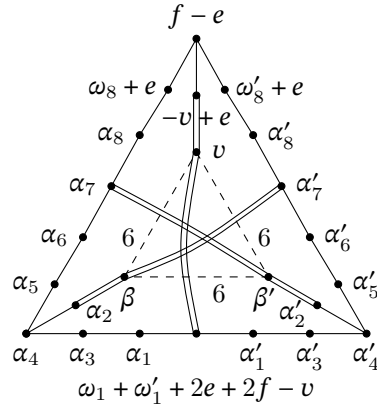


Figure 19.4.1: *Vinberg-Dynkin diagram.*

We conclude that, up to  $O(I^\perp/I)$ -equivalence, we find four distinct isotropic rank 1 sublattices  $\tilde{J}_i$ ,  $i = 1, \dots, 4$ . They are inequivalent since the corresponding root systems in the lattices  $\tilde{J}_i^\perp/\tilde{J}_i$ ,  $i = 1, \dots, 4$  are distinct and hence these lattices are not isometric. The four lifts  $J_i$  of  $\tilde{J}_i$  under  $I^\perp \rightarrow I^\perp/I$  are then inequivalent rank 2 isotropic lattices in  $\Lambda_2$  for a similar reason.

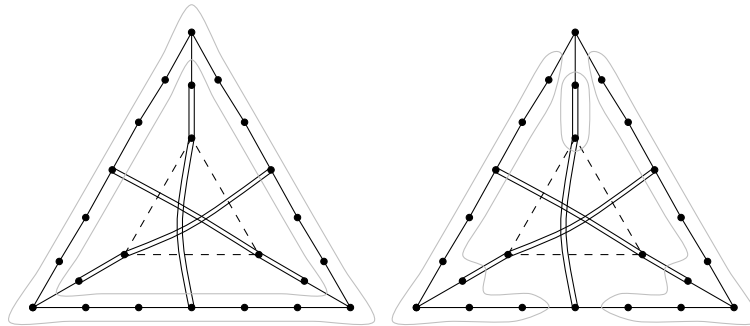


Figure 19.4.2: *Isotropic vector of types  $A_{17}$  and  $E_8+E_8+A_1$  up to diagram symmetry.*

### 19.5 Supersingular K3 Surfaces

In this section we consider projective K3 surfaces over an algebraically closed field of characteristic  $p > 0$ . The main objective of this section is to classify the possible

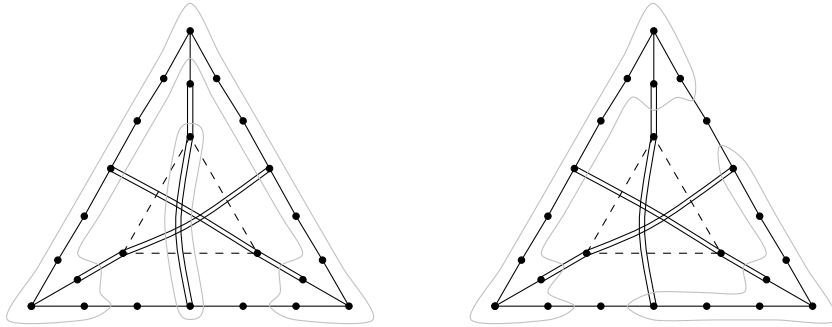


Figure 19.4.3: *Isotropic vectors of types  $D_{16} + A_1$  and  $D_{10} + E_7$  up to diagram symmetry.*

Néron–Severi lattices of supersingular K3 surfaces using the techniques developed so far.

**19.5.A Some characteristic  $p$  tools.** A projective K3 surface can also be defined as a projective 2-dimensional non-singular variety  $X$  with trivial canonical bundle and with  $q(X) = \dim H^1(\mathcal{O}_X) = 0$ . This definition is commonly used when dealing with surfaces in arbitrary characteristics. This agrees with our previous definition for complex projective K3 surfaces. We see this as follows. If  $K_X$  is trivial,  $\kappa(X) = 0$ ,  $p_g(X) = 1$  and  $c_1^2(X) = 0$ . If also  $q(X) = 0$ , then  $\chi(\mathcal{O}_X) = 1 - q(X) + p_g(X) = 2 = \frac{1}{12}c_2(X)$  and hence  $c_2(X) = 24$ . From Theorem B.5.4 we then deduce that  $X$  is indeed a K3 surface.

We shall use some facts from the classification of surfaces in positive characteristics as explained in [23]. Apart from algebraic invariants such as  $p_g$ ,  $q$  and  $\chi(\mathcal{O})$ , which are defined as in the complex case, topological invariants such as the Betti numbers are used. In the complex situation these are defined via singular cohomology which makes use of the complex topology. It turns out that the “classical” Zariski topology does not lead to meaningful invariants, but instead one should resort to étale topology as introduced by A. Grothendieck. Roughly speaking, the usual approach to topology using open subsets is to be replaced by varieties lying in some sense in an unbranched way over Zariski open sets. See [10, 11, 12, 148] for more details. Indeed, using this topology, for any scheme over a field of characteristic  $p$  one can define  $\mathbb{Q}_\ell$ -adic cohomology groups  $H^k(X, \mathbb{Q}_\ell)$ ,  $k = 0, 1, \dots$ , where  $\ell$  is a prime different from  $p$ . If these  $\mathbb{Q}_\ell$ -spaces are finite-dimensional (e.g. if  $X$  is projective) their dimensions  $b_k(X) = \dim H^k(X, \mathbb{Q}_\ell)$  are called the Betti numbers, and these are independent of the choice of the prime  $\ell$ . The cohomology groups  $H^k(X, \mathbb{Q}_\ell)$  assemble to form a ring as in the complex situation, and if  $X$  is non-singular and projective, there is an intersection pairing on  $H^d(X, \mathbb{Q}_\ell)$ ,  $d = \dim X$ .

Assuming from now on that  $d = 2$ , there is an intersection pairing on the Néron–Severi group  $\text{NS}(X)$  coming from intersecting two curves and which is integral

valued. This gives  $\text{NS}(X)$  the structure of an integral lattice which turns out to be non-degenerate. There is a natural "cycle class map"  $\text{NS}(X) \rightarrow H^2(X, \mathbb{Q}_\ell)$  and, after tensoring with  $\mathbb{Q}_\ell$ , the intersection product is compatible with the  $\mathbb{Q}_\ell$ -valued product on the target space.

As demonstrated in [23], the Betti numbers of a K3 surface turn out to be the same as in the complex case:  $b_1(X) = 0$  and  $b_2(X) = 22$ . However, the Néron–Severi group can have rank  $\rho(X)$  up to 22. We concentrate on the maximal value. A K3-surface with  $\rho(X) = 22$  is called a **supersingular K3 surface**. So for those surfaces  $\text{NS}(X)$  is an integral lattice of rank 22. It has signature  $(1, 21)$  but it turns out to be non-unimodular.

**19.5.B Supersingular K3-lattices.** The Néron–Severi lattices for supersingular K3 surfaces all belong to the class of the so-called supersingular K3-lattices defined below (cf. Definition 19.5.1).<sup>7</sup> We explain how these can be classified using the theory we have developed. We also give their construction as given in loc. cit.

**Definition 19.5.1.** Let  $p$  be a prime number. A non-degenerate quadratic lattice  $N$  of rank  $n$  is called a **supersingular K3-lattice** with **Artin invariant**  $\sigma$  if

1.  $n \equiv 6 \pmod{8}$ ,
2.  $N$  is Lorentzian, that is, its signature is  $(1, n - 1)$ ,
3.  $N$  is  $p$ -elementary, i.e.,  $pN^* \subset N \subset N^*$ ,
4.  $N^*/N$  is an  $\mathbb{F}_p$ -vector space of even dimension  $2\sigma$ .

Observe that conditions 1 and 2 ensure that  $\tau(N) \equiv 4 \pmod{8}$ , that is, the index mod 8 equals 4. This turns out to be crucial for the next result to be true. To explain the statement, recall from Section 1.7.B that 2-elementary lattices come in two flavours distinguished by their type. Type I lattices have  $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ -valued discriminant quadratic forms while the discriminant quadratic form of a type II lattice assumes at least one of the values  $\pm\frac{1}{4}$  modulo  $\mathbb{Z}$ .

**Proposition 19.5.2.** *For any odd prime  $p$  a supersingular K3-lattice  $N$  is uniquely determined by  $n$  and  $\sigma$  with  $n, \sigma$  as in Definition 19.5.1. Such lattices only exist if  $0 < \sigma < \frac{1}{2}n$ .*

*If  $p = 2$  we have  $0 < \sigma \leq \frac{1}{2}n$ . There are two types of discriminant forms:*

$$q^\# = \bigoplus^{\sigma-1} \langle u_1 \rangle \oplus \langle v_1 \rangle, \quad 1 \leq \sigma < \frac{1}{2}n, \quad (\text{Type I}),$$

$$q^\# = \langle 2^{-1} \rangle \oplus \langle 3 \cdot 2^{-1} \rangle \oplus \bigoplus^{\sigma-2} \langle u_1 \rangle \oplus \langle v_1 \rangle, \quad \sigma \geq 2, \quad (\text{Type II}).$$

*If  $\sigma = 1$  one has  $q^\# = \langle v_1 \rangle$  and if  $\sigma = \frac{1}{2}n$ ,  $q^\#$  is of type II. In all these cases there exists an up to isometry unique 2-elementary supersingular K3-lattice with discriminant form  $q^\#$ .*

*Proof.* Since  $\tau \equiv 4 \pmod{8}$  the lattice  $N$  cannot be unimodular (see Theorem 2.4.2) and so we must have  $\sigma > 0$ .

<sup>7</sup>These are also called Rudakov–Šafarevič lattices.

Next we investigate existence and uniqueness according to which discriminant forms are possible. This depends on whether  $p$  is odd or even.

**1.  $p$  odd.** Since  $N^*/N$  has even dimension  $2\sigma$ , Table 14.6.1 shows that the value of  $\tau_8$  only depends on  $p \pmod 4$  (take  $w = 2\sigma$ ) and that there is a unique candidate discriminant quadratic form. If  $\sigma < \frac{1}{2}n$  it follows from Theorem 14.6.4 that there exists a supersingular K3-lattice with given torsion quadratic form and from Corollary 14.6.2 that it is unique up to isometry.

Since  $w = 2\sigma$  is even, by Lemma 14.6.1 the discriminant of  $N$  is  $\pm 1$  up to squares, but over the reals the discriminant is  $-1$  as  $n - 1$  is odd. In case  $\sigma = \frac{1}{2}n$ , we thus need to exclude that the reduced discriminant of  $q_N^\#$  equals  $-1$ . To do so, we first consider the case that the discriminant group is isomorphic to  $n = 2\sigma$  copies of  $\mathbb{Z}/p\mathbb{Z}$  with form  $\bigoplus^{2\sigma-1} \langle p^{-1} \rangle \oplus \varepsilon \langle p^{-1} \rangle$ . Note that in this case  $\sigma$  must be odd since  $2\sigma \equiv 6 \pmod 8$ . Now  $\varepsilon = -1$  is a square mod  $p$  if and only if  $p \equiv 1 \pmod 4$ . In this case  $q_N^\# \simeq \bigoplus^{2\sigma} \langle p^{-1} \rangle$ . According to the same table as before, this form has  $\tau_8 \equiv 0 \pmod 8$ . If  $p \equiv 3 \pmod 4$  the other class occurs and so by loc. cit., since  $\sigma$  is odd, we also get  $\tau_8 \equiv 0 \pmod 8$ . So such a lattice is not possible. This excludes  $\sigma = \frac{1}{2}n$ .

**2.  $p = 2$ .** Here the result follows from Theorem 14.6.4 for existence and Corollary 14.6.2 for uniqueness up to isometry.  $\square$

We give a direct **construction of supersingular K3-lattices** following [199, §2]):

**For  $p$  odd:** Here one uses the technique of neighbouring lattices as explained in § 1.7.A. For a vector  $\mathbf{a} = (a_1, \dots, a_k)$  of odd integers we introduce the symmetric lattice

$$E(\mathbf{a}) = \langle a_1 \rangle \oplus \dots \oplus \langle a_k \rangle.$$

As for Example 3 in Section 1.4, introducing

$$E^{(0)}(\mathbf{a}) = \{(x_1, \dots, x_k) \in E(\mathbf{a}) \mid \sum x_j \equiv 0 \pmod 2\},$$

the lattice

$$E'(\mathbf{a}) = \mathbb{Z} \left( \frac{1}{2}, \dots, \frac{1}{2} \right) + E^{(0)}(\mathbf{a}), \left( \frac{1}{2}, \dots, \frac{1}{2} \right) \in E(\mathbf{a}) \otimes \mathbb{Q},$$

is a neighbouring lattice of  $E(\mathbf{a})$ . It is indeed a lattice provided  $\sum a_j \equiv 0 \pmod 4$  and it is even precisely if  $\sum a_j \equiv 0 \pmod 8$ .

We also need the existence of an even positive definite  $p$ -elementary rank 4 lattice  $H_p$  with discriminant  $p^2$ . This can be done using quaternion algebras. See Proposition 5.4.8. As in Example 5.4.9 the associated ternary form is isometric to  $\langle 1 \rangle \oplus \bigoplus^2 \langle p \rangle$  and so  $H_p$  is a  $p$ -elementary lattice.

The construction of  $N$  depends on whether  $\sigma$  is odd or even. Write  $\sigma = 2s + 1$  respectively  $\sigma = 2s + 2$ , and let  $n = 8m + 6$ . Then take

$$\mathbf{a} = (\underbrace{p, \dots, p}_{4s \text{ copies}}, 1, \dots, 1) \in \mathbb{Z}^{8m}.$$

Note that  $\text{disc}(E(\mathbf{a})) = p^{4s}$  is odd and then by Lemma 1.7.1, the discriminant groups of  $E'(\mathbf{a})$  and its neighbour  $E(\mathbf{a})$  are isomorphic to  $\oplus^{4s} \mathbb{Z}/p\mathbb{Z}$  and so these lattices are  $p$ -elementary. Now set

$$N = \begin{cases} U \oplus H_p(-1) \oplus E'(-\mathbf{a}) & \text{if } \sigma \text{ is odd} \\ U(p) \oplus H_p(-1) \oplus E'(-\mathbf{a}) & \text{if } \sigma \text{ is even.} \end{cases}$$

**For  $p = 2$ :** The following table gives supersingular K3-lattices for all types and Artin invariants.

$\sigma$	type	lattice
$\frac{1}{2}n$	II	$\mathbb{Z}^{1,n-1}(2) = \oplus^{n-1} \langle -2 \rangle \oplus \langle 2 \rangle$
$\frac{1}{2}n - 1$	I	$U(-2) \oplus D_4(-1) \oplus \oplus^{\frac{1}{8}(n-6)} E_8(-2)$
	II	$U \oplus \oplus^{n-2} \langle -2 \rangle$
$2 \leq \sigma \leq \frac{1}{2}n - 2$	II	$U \oplus \oplus^{2\sigma-2} \langle -2 \rangle \oplus D_{(n-2)-(2\sigma-2)}(-1)$
$1 \leq \sigma \leq \frac{1}{4}(n-2)$	I	$U \oplus \oplus^{\sigma-1} D_4(-1) \oplus D_{(n-2)-4(\sigma-1)}(-1)$
$\frac{1}{4}(n-2) \leq \sigma \leq \frac{1}{2}n - 3$		
$\sigma \equiv 0 \pmod{4}$	I	$U(2) \oplus \oplus^{\frac{1}{4}(\sigma-4)} E_8(-2) \oplus^3 D_4(-1) \oplus \oplus^{\frac{1}{8}(n+2-2\sigma)} E_8(-1)$
$\sigma \equiv 2 \pmod{4}$	I	$U \oplus \Gamma_{2\sigma-4}(-2) \oplus D_{(n-2)-2\sigma}(-1) \oplus D_4(-1)$
$\frac{1}{4}(n-2) \leq \sigma \leq \frac{1}{2}n - 2$		
$\sigma \equiv 3 \pmod{4}$	I	$U(2) \oplus \oplus^{\frac{1}{4}(\sigma-3)} E_8(-2) \oplus^2 D_4(-1) \oplus \oplus^{\frac{1}{8}(n-2\sigma)} E_8(-1)$
$\sigma \equiv 1 \pmod{4}$	I	$U \oplus \Gamma_{2\sigma-2}(-2) \oplus D_{(n-2)-(2\sigma-2)}(-1)$

Here we use the unimodular lattices  $\Gamma_k$ ,  $k \equiv 0 \pmod{4}$ , from Section 1.4. We saw that  $\Gamma_k$  is positive definite and integral if  $k$  is divisible by 4. The lattice  $\Gamma_k(-2)$  then is even and integral. Example 1.6.8.2 shows that  $\Gamma_k(-2)$  is 2-elementary. To obtain type I lattices one needs to impose that  $k$  is divisible by 8 which explains the difference for the choice of the lattice in the last 4 entries according to the value of  $\sigma \pmod{4}$ . We also note that Table 4.1.1 shows that the root lattices  $D_k$  for even  $k$  are 2-elementary as well.

*Remark 19.5.3.* The above table shows that the unique supersingular lattice of rank  $n = 22$  and with  $\sigma = 1$  is isometric to  $U \oplus N'$  where  $N' = D_{20}(-1)$  and so this is isometric to the Borcherds lattice from Example 17.2.10.5.

**19.5.C Application to supersingular K3 surfaces.** Proposition 19.5.2 implies:

**Corollary 19.5.4.** *Let  $k$  be an algebraically closed field of odd characteristic  $p$  and let  $X$  be a supersingular K3 surface. Then  $\text{NS}(X)$  is a  $p$ -elementary K3-lattice of rank 22 and so it is uniquely determined by the Artin invariant.*

Uniqueness is also true in characteristic 2. We state the result from [199, §2, 3] and we refer to loc. cit. for a proof:

**Theorem 19.5.5.** *Let  $k$  have characteristic 2 and let  $X$  be a supersingular K3 surface over  $k$ . Then  $\text{NS}(X)$  is a supersingular K3-lattice of rank 22 of type I and so it is uniquely determined by the Artin invariant.*

The reader will find in loc. cit. also a precise classification result:

**Theorem** ([199, §3,4]). *Supersingular K3 surfaces in characteristic 2 with Artin invariant  $\sigma$  have a moduli variety  $M_\sigma$  of dimension  $\sigma - 1$ . In other words, the points of  $M_\sigma$  are in one to one correspondence with isomorphism classes of supersingular K3 surfaces with Artin invariant  $\sigma$ .*

As an example, the universal family of K3 surfaces with Artin invariant 10 is given by an equation of the form

$$y^2 = a_2(t)x^4 + a_3(t)x^3 + a_4(t)x^2 + a_5(t)x + a_6(t), \quad (19.8)$$

where the  $a_j(t)$  are polynomials of degree  $j$  in  $t$ . Taking into account the peculiarities of characteristic 2, one writes  $a_{2k}(t) = b_k(t)^2 + a'_{2k}(t)$ , where the prime denotes formal differentiation with respect to  $t$ . Since an equation of the same form of (19.8) arises under the substitution  $y \mapsto y + b_1(t)x^2 + b_2(t)x + b_3(t)$ , one deduces that the coefficients of the polynomials  $a'_2(t)$ ,  $a_3(t)$ ,  $a'_4(t)$ ,  $a_5(t)$ ,  $a'_6(t)$  are “true” parameters. There are  $1 + 4 + 2 + 6 + 3 = 16$  of these. However, it turns out that certain other transformations also give isomorphic surfaces:  $x \mapsto \alpha \cdot x + \beta \cdot t + \gamma$ , where  $\alpha, \beta, \gamma \in k$ ; next  $y \mapsto \delta \cdot y$ ,  $\delta \in k$ , and, finally, every projective linear map of the  $t$ -line. So the number of effective parameters is indeed  $16 - (4 + 3) = 9 = \sigma - 1$ .

Since in odd characteristic there is not a general geometric construction of families of supersingular K3 surfaces, Ogus used an indirect construction to describe their moduli spaces using a “period map”, very much analogous to what we did in Section 19.2. The main result of [176], stated here in a slightly imprecise and simplified form is as follows:

**Theorem** ([176]). *Let  $p \neq 2, 3$  be a prime and  $k$  an algebraically closed field of characteristic  $p$ . Supersingular K3 surfaces with Artin invariant  $\sigma$  have a “moduli space” of dimension  $\sigma - 1$ .*

**Historical and Bibliographical Notes.** A proof for the Torelli theorem for K3 surfaces in the projective case is due to I. Pjateckiĭ-Šapiro and I. Šafarevič [189], and in the Kähler case to D. Burns and M. Rapoport [33]. The surjectivity statements are due to V. Kulikov [130, 131], H. Pinkham–U. Persson [182] in the projective case, and A. Todorov [226], Y. Namikawa [165] in the Kähler setting. Comprehensive proofs can be found in [106] and [15, Ch. VIII]. These results make it possible to describe various moduli spaces for K3 surfaces such as for “lattice polarized K3 surfaces” as in Section 19.2. This is due to D. Morrison [158].

Geometrical meaningful (partial) compactifications of moduli spaces were studied by many people and in various settings. For the setting of locally symmetric varieties, relevant for our work, we refer to [13] and its extensive list of references. The example we discuss in Section 19.4 is based on an outline of a lattice oriented approach for the moduli space of K3 surfaces of degree 2 as described by E. Looijenga in [143]. The diagram occurs in a letter by Looijenga to J. Shah and was also used by F. Scattone in [200].

In Section 19.5 we have used the notion of supersingular surface as in T. Shioda’s article [209]. “Supersingular” might also refer to an a priori different notion introduced by M. Artin in [9]. Only recently it has been shown that his notion coincides with Shioda’s, at



least for  $p \neq 2$ . See the discussion in [106, Ch. 17.2-3]. Our treatment of supersingular K3 surfaces is based on the approach of A. Rudakov and I. Šafarevič in [199]. Using still another "Grothendieck topology" leading to crystalline cohomology, Ogus [175, 176] developed a theory of period maps for supersingular K3 surfaces in characteristics  $p \neq 2, 3$ . See also the lecture notes [139] by C. Liedtke where many of the required techniques are explained. We should however warn the reader that despite the claim in these lecture notes, according to D. Bragg and M. Lieblich [27] the "Artin conjecture" (Conjecture 7.4 in [139]), stating that all supersingular K3 surfaces are unirational, is still open at the moment of writing.

There are now two monographs available devoted to K3 surfaces, [106] by D. Huybrechts and [129] by S. Kondō. Both give extensive background on several of the topics treated in this chapter. While [129] can be viewed as an introduction to K3 surfaces and the related geometry, in [106] the reader finds a vast area of subjects ranging from the complex geometry aspects to arithmetic fineries.

## Automorphism Groups of K3 Surfaces

### Introduction

In Section 20.1 we describe the automorphism group of a K3 surface through the action on cohomology, making use of the Torelli theorem 19.2.1. By definition, the subgroup of symplectic automorphisms is the subgroup fixing a holomorphic 2-form. For algebraic K3 surfaces this group is of finite index in the full group and the quotient group is well understood. This gives a finiteness criterion for automorphisms in terms of the Néron–Severi lattice.

Shifting gears, we may ask which finite groups can occur as a group of symplectic automorphisms of a K3 surface. This is the subject of Section 20.2. In § 20.3 we prove a remarkable result due to S. Mukai on finite groups of symplectic automorphisms, abelian or not. Next, restricting to abelian such groups in Section 20.4, we recall Nikulin’s list of finite abelian groups acting symplectically. Subsequently we show that these act in an essentially unique way on the K3 lattice. The latter proof is technical and depends on the precise description of the moduli space of marked K3 surfaces as given in Section 19.3 of the preceding chapter. It also uses a delicate result concerning the relation between the intersection lattice of a K3 surface and that of the minimal resolution of its quotient by a finite abelian group. The latter result has been placed in Appendix 20.9.

As we have seen, involutions and their quotients come up in many contexts. In Section 20.5 we describe how these act on the intersection lattice. By definition, a Kummer surface is the minimal resolution of a quotient of a torus by its natural involution. In Section 20.6 we give a lattice theoretic characterization of Kummer surfaces. An involution acting on a K3 surface may or may not be symplectic. If it is, it is also called a Nikulin involution; in Section 20.7 we devote a deeper study to these. As to non-symplectic involutions, we only consider the lattice aspects of fixed point free involutions on K3 surfaces whose quotients, by definition, are Enriques surfaces. We return to Enriques surfaces in the next chapter.

Finally, in Section 20.8 we investigate those Nikulin involutions which give a so-called Shioda–Inose structure.

## 20.1 The Automorphism Group of a Projective K3 Surface

In this section  $S$ , respectively  $T = S^\perp$  denotes the Néron–Severi lattice, resp. the transcendental lattice of a K3 surface  $X$  (Compare Lemma B.2.7).

**20.1.A The role of symplectic automorphisms.** The automorphism group of a projective K3 surface  $X$  can be investigated through its natural representation on cohomology, since Theorem 19.2.2 implies that this representation is faithful. The description in terms of the K3 lattice is however rather unwieldy but simplifies for the subgroup  $\text{Aut}_s(X)$  which fix every holomorphic 2-form on  $X$ , the so-called *symplectic automorphisms*. Such automorphisms act as the identity on  $H^{2,0}(X)$ , and hence on the transcendental lattice and consequently induce the identity on  $S^*/S \simeq T^*/T$ . We use the exact sequence of Proposition 15.2.9 in this situation, where now  $L = H^2(X, \mathbb{Z})$ :

$$1 \rightarrow \mathcal{O}^\#(S) \xrightarrow{e_S} \mathcal{O}^\#(L)_S \xrightarrow{\rho_T} \mathcal{O}(T),$$

where  $e_S(\sigma)$  is the extension of  $\sigma \oplus \text{id}_T$ ,  $\sigma \in \mathcal{O}^\#(S)$  and  $\rho_T$  is the restriction. This extension is called the *symplectic extension* of  $\sigma$  which is unique since  $S \oplus T$  generates  $L$ .

To express the group of symplectic automorphisms of  $X$  in terms of the group  $\mathcal{O}^\#(S)$ , we identify the latter with the subgroup of  $\mathcal{O}(L)$  of the symplectic extensions. Note that a symplectic automorphism of  $X$  induces an isometry in  $\mathcal{O}^\#(S)$  preserving the ample cone in  $S_\mathbb{R}$ . Recall (see (17.2)) that the subgroup  $\mathcal{O}^{-\#}(S)$  of  $\mathcal{O}(S)$  is formed by those isometries of  $S$  that preserve the positive light cone intersected with  $S_\mathbb{R}$  and induce the identity on the discriminant group. So it follows from Corollary 19.2.3 that

$$\text{Aut}_s(X) \simeq \mathcal{O}^{-\#}(S)/W^-(S),$$

and fits in the exact sequence

$$1 \rightarrow \text{Aut}_s(X) \rightarrow \text{Aut}(X) \xrightarrow{\rho_T} \mathcal{O}(T).$$

Using these remarks, we state and prove:

**Theorem 20.1.1.** *Let  $X$  be a projective K3 surface. There exists a positive integer  $m$  (depending on  $X$ ) such that there is an exact sequence*

$$1 \rightarrow \text{Aut}_s(X) \rightarrow \text{Aut}(X) \xrightarrow{\rho_T} \mu_m \rightarrow 1,$$

where  $\mu_m$  is the group of  $m$ -th roots of unity in  $\mathbb{C}$ .

The group  $\text{Aut}_s(X)$  is isomorphic to the subgroup of  $\mathcal{O}(H^2(X, \mathbb{Z}))$  consisting of those symplectic extensions of isometries in  $\mathcal{O}^{-\#}(S)$  which preserve the ample cone. This group is isomorphic to the quotient group  $\mathcal{O}^{-\#}(S)/W^-(S)$ .

*Proof.* It remains to show that the image of  $\rho_T$  is a finite group of roots of unity. Since  $X$  is projective,  $T$  has signature  $(2, 20 - \text{rank}(S))$ . Suppose that  $g$  is an automorphism of  $X$ . The induced action  $\gamma = g^*$  on cohomology preserves the complex line  $H^{2,0}(X) \subset T_{\mathbb{C}}$  as well as the complex conjugate line. Consequently,  $\gamma_{\mathbb{R}} \in \text{Aut}(T_{\mathbb{R}})$  belongs to the compact group which preserves the decomposition  $T_{\mathbb{R}} = T' \oplus T''$ ,  $T' = T^{1,1} \cap T_{\mathbb{R}}$  (negative definite),  $T'' = (T^{2,0} \oplus T^{0,2}) \cap T_{\mathbb{R}}$  (positive definite). This implies that such  $\gamma$  form a finite set. Hence each of them acts on the line  $H^{2,0}(X)$  as multiplication by some fixed root of unity. The image of  $\rho_T$  is thus some group of  $m$ -th roots of unity.  $\square$

*Remark 20.1.2.* If  $X$  is a non-projective K3 surface, there can be automorphisms that do not act by multiplication with a root of unity and then  $[\text{Aut}(X) : \text{Aut}_s(X)] = \infty$ . See [106, Ch 15, Example 1.11].

As an immediate consequence of this result one obtains a finiteness criterion for the automorphism group in terms of the Néron–Severi lattice.

**Criterion 20.1.3** ([189, §7, Theorem 1]). *The automorphism group of a complex projective K3 surface  $X$  is finite if and only if  $\mathcal{O}^-(S)/W^-(S)$  is finite. In other words,  $\text{Aut}(X)$  is finite if and only if the Weyl group of  $X$  (cf. 19.1) embeds as a finite index subgroup in the isometry group of the Néron–Severi lattice  $S$ .*

*Proof.* By Theorem 20.1.1 the group  $\text{Aut}(X)$  is finite if and only if this is the case for the group  $\text{Aut}_s(X)$ . Moreover, the theorem states that the image of  $\text{Aut}_s(X)$  has finite index in the group of all isometries of  $S$  preserving the ample cone. Since the latter group is isomorphic to  $\mathcal{O}^-(S)/W^-(S)$ , the result follows.  $\square$

**Examples 20.1.4. 1.** If  $\rho(X) = 1$  the group  $\mathcal{O}^-(S)$  is the identity and so  $\text{Aut}(X)$  is finite. In fact, if  $X$  is a double cover of  $\mathbb{P}^2$  branched along a general sextic curve,  $\text{Aut}(X)$  is generated by the covering involution and in all other cases  $\text{Aut}(X)$  is trivial. See e.g. [106, Ch. 15. Cor. 2.12]. So for all  $k \geq 2$ , the general K3 admitting a degree  $2k$ -polarization has trivial automorphism group.

**2.** Suppose  $\rho(X) = 2$ . Here finiteness occurs if and only if  $S$  has either an isotropic vector or a root. This happens for infinitely many non-isometric lattices. The only possible infinite groups are  $\mathbb{Z}$  and  $\mathbb{Z} * \mathbb{Z}$ . See [75].

**3.** More generally, let  $\mathcal{F}^{\rho}$  be the set of isometry classes of even lattices  $S$  of signature  $(1, \rho - 1)$  for which  $\mathcal{O}^-(S)/W^-(S)$  finite. Then the previous examples show that the sets  $\mathcal{F}^1$  and  $\mathcal{F}^2$  have infinitely many elements. By [170, 172] the set  $\mathcal{F}^{20}$  is empty while for  $\rho = 3, \dots, 19$  there are finitely many isometry classes in  $\mathcal{F}^{\rho}$  and each of these occur as the Néron–Severi lattice of some K3 surface. For geometric constructions (and much more) see [198].

As announced, the arithmetic nature of the description of  $\text{Aut}_s(X)$  has an important consequence. Continuing with the notation as above, introduce the following auxiliary groups:

$$G = \{\gamma \in \mathcal{O}(\Lambda_{K3} \otimes \mathbb{R}) \mid \gamma(S_{\mathbb{R}}) = S_{\mathbb{R}}, \gamma(C_X^{\text{amp}}) = C_X^{\text{amp}}\},$$

$$G_{\mathbb{Z}} = G \cap \mathcal{O}(\Lambda_{K3}), \quad G_{\mathbb{Z}}^- = \{g \in G \cap \mathcal{O}^-(\Lambda_{K3}) \mid g \text{ induces id on } S^*/S\}.$$

Before stating the result we are after, recall that an algebraic matrix group  $G$  defined over a field  $k$  is an affine subvariety of  $M_{n \times n}(k)$ , the affine space of the  $n$  by  $n$  matrices with coefficients in the field  $k$  with group action inherited by matrix multiplication. In particular,  $G$  is given as the zero locus of polynomials from the ring  $k[X_{1,1}, \dots, X_{n,n}]$ .

**Proposition 20.1.5** ([220]). *Suppose  $X$  is a projective K3 surface. Then the group  $G$  is an algebraic group defined over  $\mathbb{Q}$  and hence  $G_{\mathbb{Z}}$  is finitely generated. A marking induces an isomorphism  $\text{Aut}_s(X) \simeq G_{\mathbb{Z}}^-$ . The latter has finite index in  $G_{\mathbb{Z}}$  and hence  $\text{Aut}_s(X)$  as well as  $\text{Aut}(X)$  are finitely generated.*

*Proof.* The isometry group of  $\Lambda_{K3} \otimes \mathbb{R}$  is an algebraic group. Since the coefficients of its defining equations belong to  $\mathbb{Q}$ , this algebraic group is defined over  $\mathbb{Q}$ . The subgroup  $G \subset O(\Lambda_{K3} \otimes \mathbb{R})$  is also an algebraic group defined over  $\mathbb{Q}$  since  $S_{\mathbb{R}}$  comes from a lattice and since the ample cone is determined by a choice of a partition of the roots in  $S$  into positive roots (the effective ones) and negative roots. Then  $G_{\mathbb{Z}}$  is by definition an arithmetic subgroup of  $G$  and by [25, §3] such groups are finitely generated.

Theorem 20.1.1 shows that  $\text{Aut}_s(X) \simeq G_{\mathbb{Z}}^-$ . Since the latter has finite index in  $G_{\mathbb{Z}}$ , the subgroup  $G_{\mathbb{Z}}^-$  is also finitely generated. Again by Theorem 20.1.1, the group  $\text{Aut}_s(X)$  has finite index in  $\text{Aut}(X)$ , and so the latter is finitely generated as well.  $\square$

**20.1.B General behaviour of automorphisms.** In this subsection we show that, up to a possible sign, an automorphism of a projective K3 surface is generally symplectic, in other words we show that generally the values of  $m$  that occur in Theorem 20.1.1 are 1 and 2. We first present an estimate for the values of  $m$  which may occur. So, let  $\varphi$  be an isometry of the transcendental lattice  $T$  of a projective K3 surface  $X$  which preserves the Hodge decomposition and assume that some  $m$ -th root of unity appears as an eigenvalue of  $\varphi$  (Note that if  $\varphi$  comes from an automorphism of  $X$  of finite order there is such an eigenvalue). As usual, let  $\phi$  be the Euler totient function. Since  $\phi(m)$  is at most the degree of the characteristic polynomial of  $\varphi$ , the rank of the lattice  $T$  is at least  $\phi(m)$ . This leads to the algebraic field

$$K_{\rho} = \mathbb{Q} \left( \bigcup_m \exp(2\pi i/m) \right), \quad \phi(m) \leq \text{rank}(T) = 22 - \rho, \quad \rho = \text{rank}(S), \quad (20.1)$$

i.e., the field obtained by adjoining to  $\mathbb{Q}$  all primitive  $m$ -th roots of unity for which  $\phi(m) \leq 22 - \rho$ . The  $m$  that satisfy this inequality for a given  $\rho$  are collected in the following table.

$\rho$	$m$ with $\phi(m) \leq 22 - \rho$
20, 19	1, 2, 3, 4, 6
18, 17	additional $m$ : 5, 8, 10, 12
16, 15	additional $m$ : 7, 9, 14, 18
14, 13	additional $m$ : 15, 16, 20, 24, 30
12, 11	additional $m$ : 11, 22
10, 9, 8, 7	additional $m$ : 13, 21, 26, 28, 36, 42
6, 5	additional $m$ : 17, 32, 34, 40, 48, 60
4, 3	additional $m$ : 19, 27, 38, 54
2, 1	additional $m$ : 25, 33, 44, 50, 66

*Remark 20.1.6.* 1. One can show that all integers

$$m \in \{1, \dots, 22, 24, 26, 27, 28, 30, 32, 34, 36, 38, 40, 42, 44, 48, 50, 54, 66\}$$

occur, in some cases for a unique K3 surface. See [127, 146, 253, 255]. However, it turns out that the numbers 33 and 60 from the above table do not occur.

2. If  $\zeta_m \in \mathbb{C}$  is an  $m$ -th root occurring as an eigenvalue for some  $m$  in the table, then the corresponding eigenspace is defined over  $\mathbb{Q}(\zeta_m)$ .

From the proof of Theorem 20.1.1 one sees that the group of isometries of  $T$  preserving the Hodge decomposition is finite if  $T$  has signature  $(2, *)$ , whence the following result.

**Lemma 20.1.7.** *Suppose  $T$  is the transcendental lattice of a projective K3 surface (so that its signature is of the form  $(2, *)$ ). If no one-dimensional non-zero subspace of  $T_{\mathbb{C}}$  can be defined over the field  $K_{\rho}$  we just introduced, then  $\pm 1$  are the only roots of unity that occur as eigenvalues of an isometry of  $T$  preserving the Hodge decomposition.*

It leads to the notion of  $K_{\rho}$ -genericity:

**Definition 20.1.8.** Let  $\text{rank}(S) = \rho$ . A point  $[u] \in D(S^{\perp})$  is called  $K_{\rho}$ -**generic** or **generic over  $K_{\rho}$**  if the following two conditions hold:

- With  $T = S^{\perp}$ , there is no proper sublattice  $T'$  of  $T$  for which  $\mathbb{C}u \subset T'_{\mathbb{C}}$ . In particular, the Picard number of any corresponding K3 surface  $X$  equals  $\rho = 22 - \text{rank}(T)$ ;
- No one-dimensional subspace of  $T_{\mathbb{C}}$  is defined over  $K_{\rho}$  and so, using the notation of Theorem 20.1.1, either  $\text{Im}(\rho_T)$  is the identity or the order two group  $\{\pm \text{id}\}$ .

Shifting gears, we now let  $S$  be an abstract lattice of signature  $(1, \rho - 1)$  and consider  $S$ -marked K3 surfaces, that is K3 surfaces  $(X, \varphi)$  such that  $S \subset \text{NS}(X)$ . Such surfaces are parametrized by the domain  $D(S^{\perp})$  (cf. Definition 19.2.9). By its very definition,  $K_{\rho}$ -generic period points in  $D(S^{\perp})$  come from  $S$ -marked K3 surfaces with transcendental lattice exactly  $T = S^{\perp}$ . Invoking Lemma 20.1.7, this proves:

**Lemma 20.1.9.** *Let  $K_{\rho}$  be defined by equation (20.1). If  $[u] \in D(S^{\perp})$  is a  $K_{\rho}$ -generic period point of a projective K3 surface, then the only automorphisms of  $T = S^{\perp}$  extending to  $\Lambda_{K3}$  are  $\pm \text{id}$ .*

Since for a K3 surface without nodal curves the Weyl group is trivial, this fact and Theorem 20.1.1 imply:

**Corollary 20.1.10.** *Let  $\rho = \text{rank}(S)$  and  $K_\rho$  defined by equation (20.1). For  $K_\rho$ -generic  $S$ -marked projective K3 surfaces  $X$  without nodal curves one has*

- $\text{Aut}(X) = \text{Aut}_s(X) \times \{\pm 1\} \simeq \text{O}^{-\#}(S) \times \{\pm 1\}$  if and only if  $X$  admits an involution acting as  $-\text{id}$  on  $T$ ;
- $\text{Aut}(X) = \text{Aut}_s(X) \simeq \text{O}^{-\#}(S)$  otherwise.

The first alternative does occur. Indeed any K3 surface  $X$  without nodal curves and whose holomorphic 2-forms are anti-invariant under an involution, such as the universal cover of a general Enriques surface, has this property. Consult Section 21.1 for more details.

## 20.2 Finite Groups Acting On a K3 Surface

From now on the K3 lattice will be denoted as  $\Lambda$  instead of  $\Lambda_{K3}$ .  $G$  denotes a finite subgroup of  $\text{O}(\Lambda)$ .

Recall the notation  $\Lambda^G$  for the  $G$ -invariant sublattice, and  $\Lambda_G$  for its orthogonal complement. Note that  $\Lambda^G$  and  $\Lambda_G$  are non-degenerate if  $G$  is non-trivial. See Example 1.7.3.

**Criterion 20.2.1.** *Let  $X$  be a K3 surface. Then, up to conjugation under the action of  $W^-(X)$ , a finite subgroup  $G$  of  $\text{O}(H^2(X, \mathbb{Z}))$  is induced by automorphisms of  $X$  if and only if the following three conditions hold simultaneously:*

1.  $G$  preserves  $H^{2,0}(X)$ ;
2. There is a  $G$ -invariant element in the positive cone;
3.  $H^2(X, \mathbb{Z})_G \cap \text{NS}(X)$  contains no roots.

*Proof.* If  $G \subset \text{Aut}(X)$ , then item 1 holds trivially. Roots  $r$  belonging to  $\text{NS}(X)$  are orthogonal to  $H^{2,0}(X)$  and so  $\sigma_r$  preserves the latter. Hence item 1 holds also for  $wGw^{-1}$ ,  $w \in W^-(X)$ .

Since  $G \subset \text{Aut}(X)$  is finite and preserves the set of Kähler classes, given a Kähler class  $\ell$ , then so is the non-zero invariant class  $\sum g^*(\ell)$ . In case  $G \subset \text{Aut}(X)$  this proves item 2. Since by the observation in § 17.2.B,  $W^-(X)$  preserves the positive light cone,  $w(\sum g^*(\ell))w^{-1} = \sum g^*(w(\ell))$  is a  $G$ -invariant element in the positive cone for all  $w \in W^-(X)$ , completing the proof of item 2.

Next, assume that  $\Lambda_G \cap \text{NS}(X)$  contains a root  $r$ . Replacing  $r$  with  $-r$  if necessary, we may assume that the root is effective and then, again assuming  $G \subset \text{Aut}(X)$ , also  $\sum g^*(r) \in \Lambda_G \cap \Lambda^G$  is effective, a contradiction since  $\Lambda_G \cap \Lambda^G = 0$ .

This argument is not affected by conjugation with an element from  $W^-(X)$ , proving 3.

For the converse, let  $X$  be a K3 surface and  $G \subset O(H^2(X))$  a finite subgroup satisfying conditions 1–3. Item 1 implies that  $G$  preserves  $H^{1,1}(X)$ . We identify  $H^2(X, \mathbb{Z})$  with the K3 lattice  $\Lambda$  through a marking and so  $G$  preserves  $\Lambda_{\mathbb{R}}^{1,1}$ . Let us consider the  $G$ -invariant subcone  $K = (\Lambda^{1,1})_{\mathbb{R}}^G \cap C_X$  of the positive  $C_X$ . It is non-empty by assumption 2, say  $\kappa \in K$ . The cone cannot be contained in any hyperplane  $H_r$  orthogonal to a root  $r \in \text{NS}(X)$ . Otherwise  $(\Lambda^{1,1})^G \subset r^\perp$  since the open subset  $K$  of  $(\Lambda^{1,1})_{\mathbb{R}}^G$  spans the latter vector space, and then  $r$  would be contained in  $(\Lambda^{1,1})^G$  which contradicts item 3. The Kähler cone is a fundamental domain for the action of  $W^-(X)$ , and so some  $w \in W^-(X)$  sends the element  $\kappa \in K$  to a Kähler class  $w(\kappa)$  and  $g^w := w \circ g \circ w^{-1}$  preserves this Kähler class for every  $g \in G$ . By Theorem 19.2.2,  $g^w$  is induced by a unique automorphism of  $X$ . So  $wGw^{-1} \subset \text{Aut}(X)$ , completing the proof.  $\square$

**Symplectic actions.** There is a related result which gives a criterion for a finite group  $G$  of  $O(\Lambda)$  to act *symplectically* on some K3 surface. Recall that for a sublattice  $S$  of  $\Lambda$  in Section 19.2 we defined the period domain  $D(S^\perp) = \{[u] \in D(\Lambda) \mid u \cdot S = 0\}$ . This is the period domain parametrizing K3 surfaces whose Néron–Severi group contains (a copy of)  $S$ , or, equivalently, whose transcendental lattice is contained in  $T = S^\perp$ . We shall be interested in  $S = \Lambda_G$ , that is, in period points in  $D(\Lambda^G)$ .

**Proposition 20.2.2.** *Let  $G$  be a finite group acting symplectically on a marked K3 surface  $X$ . Then, via the marking,  $\Lambda_G$  does not contain roots and the period point of  $X$  belongs to  $D(\Lambda^G)$ .*

*Let  $G$  be a finite subgroup of  $O(\Lambda)$ . Suppose  $\text{rank}(\Lambda_G) \leq 18$  and that  $\Lambda_G$  does not have roots. If the period point of  $X$  belongs to  $D(\Lambda^G)$ , then, up to conjugation with some  $w \in W^-(X)$ , every  $g \in G$  acts symplectically on  $X$  via the marking. Moreover, on the connected subset corresponding to K3-surfaces with Néron–Severi group equal to  $\Lambda_G$ ,*

$$\mathring{D}(\Lambda^G) = \{[u] \in D(\Lambda^G) \mid \varphi \text{NS}(X) = \Lambda_G, [u] \text{ period point of } (X, \varphi)\}, \quad (20.2)$$

one can take  $w = \text{id}$ .

*Proof.* First assume that  $G$  acts symplectically on  $X$ . A marking sends the transcendental lattice of  $X$  into  $\Lambda^G$  and so, by definition, the period point of  $X$  belongs to  $D(\Lambda)$ . But also  $\Lambda_G \subset S$ ,  $S$  the image of the Néron–Severi lattice under the marking and so, by Criterion 20.2.1  $\Lambda_G$  does not contain roots.

Conversely, since by assumption on the period point the transcendental lattice is contained in  $\Lambda^G$ ,  $G$  acts trivially on the transcendental lattice and hence also on  $H^{2,0}(X)$ . In particular,  $G$  acts symplectically in cohomology and the  $G$ -action on  $H^2(X)$  preserves the Hodge decomposition. To show that the  $G$ -action on cohomology is induced from a  $G$ -action on  $X$  it suffices to verify the conditions of Criterion 20.2.1. First of all, the  $G$ -action preserves each of the cones  $\pm C_X$ .



This can be seen as follows. Since  $\text{rank}(\Lambda^G) \geq 4$  and the signature of  $\Lambda$  is  $(3, 19)$ , the non-degenerate lattice  $\Lambda^G$  cannot be positive definite and since the period point belongs to  $\Lambda^G \otimes \mathbb{C}$ , the lattice  $\Lambda^G$  cannot be negative definite either, hence is indefinite and so meets the positive cone. Since  $G$  fixes its intersection with the positive cone pointwise,  $G$  must preserve  $C_X$  as well as  $-C_X$ . As  $G$  is finite, it follows that there is a  $G$ -invariant element in each of the cones. Secondly, we just recalled that, by definition,  $\Lambda_G \subset \text{NS}(X)$ , and since  $\Lambda_G$  does not contain roots, all conditions of Criterion 20.2.1 are fulfilled and so up to conjugation with an element of the Weyl group of the Néron–Severi group the cohomological  $G$ -action comes from a  $G$ -action on the K3 surface. If the Néron–Severi group coincides with  $\Lambda_G$  this Weyl group is trivial. This happens for period points outside the countably many hyperplane orthogonal to roots in  $\Lambda$ . This set is connected since hyperplanes are of real codimension 2.  $\square$

A marked K3 surface  $(X, \varphi)$  with a symplectic  $G$ -action determines a  $G$ -action on  $\Lambda$ . If  $\iota : G \hookrightarrow \text{O}(H^2(X))$  is the action on cohomology, the one on  $\Lambda$  is given by

$$\iota_\varphi : G \hookrightarrow \text{O}(\Lambda), \quad g \mapsto \varphi \iota(g^{-1}). \quad (20.3)$$

A different marking for  $X$  gives a conjugate embedding so that the conjugation class of  $\iota_\varphi(G)$  in  $\text{O}(\Lambda)$  only depends on  $\iota$ . So also the isometry class of the lattice fixed under  $\iota_\varphi(G)$  only depends on  $\iota$ , or, more precisely on the image  $\iota(G)$ , we shall denote any representing lattice by  $\Lambda^{\iota(G)}$  and its orthogonal complement by  $\Lambda_{\iota(G)}$ . This leads to:

**Definition 20.2.3.** A marked K3-surface  $(X, \varphi)$  with symplectic  $G$ -action and induced embedding  $\iota : G \hookrightarrow \text{O}(\Lambda)$  is called a  $(\iota, G)$ -**marked K3 surface**.

We can then rephrase the above proposition as follows:

**Corollary 20.2.4.** *Suppose that  $\Lambda_{\iota(G)}$  has rank  $\leq 18$  and does not contain roots. Then  $\mathring{D}(\Lambda^{\iota(G)})$  is the period domain of  $(\iota, G)$ -marked K3 surfaces.*

Recalling the period map (19.5) for the universal family of marked K3 surfaces, the smooth analytic space

$$\mathcal{M}_{\iota(G)} = \mathcal{M} \cap \rho^{-1}(\mathring{D}(\Lambda^{\iota(G)})) \quad (20.4)$$

is the moduli-space of  $(\iota, G)$ -marked K3-surfaces. For the corresponding period points the associated light cone has two components and since the Néron–Severi lattice has no roots, there are two choices for the Kähler cone. Replacing a marking by its negative exchanges these two cones and hence we have:

**Proposition 20.2.5.** *Let  $G$  be a finite group. The moduli space of  $(\iota, G)$ -marked K3 surfaces  $\mathcal{M}_{\iota(G)}$  has two connected components  $\mathcal{M}_{\iota(G)}^\pm$  corresponding to two opposite markings.*

Next, we consider how the image of  $G$  in  $O(\Lambda)$  varies in a family of  $(\iota, G)$ -marked K3 surfaces. We have seen that two markings for a given K3 surface lead to conjugate copies of the group  $G$  in  $O(\Lambda)$ . For a family  $f : \mathcal{X} \rightarrow S$  of K3 surfaces over a contractible base  $S$  with  $G$ -action a similar result is true: a trivialization of the local system  $R^2 f_* \mathbb{Z}$  leads to a fixed copy of  $G$  in  $O(\Lambda)$ ; changing the trivialization leads to a conjugate copy. A patching argument deals with a general base. In particular we have:

**Corollary 20.2.6.** *The images of  $G$  in  $O(\Lambda)$  for the members of the universal family of  $(\iota, G)$ -marked K3 surfaces over a connected component of  $\mathcal{M}_{\iota(G)}$  belong to the same conjugacy class in  $O(\Lambda)$ .*

**Classification of quotient surfaces.** To determine the place of the quotient surfaces  $X/G$  in the classification, we first consider the fixed points of the  $G$ -action on a K3 surface  $X$ . As we have remarked previously, by [35] the action of a non-trivial  $g \in G$  at a fixed point can be linearized. This implies that the fixed locus of  $g$  in  $X$  is either empty or a disjoint union of smooth curves and isolated points. Suppose  $x \in X$  is a fixed point of  $g$  and that  $g$  acts symplectically. With  $T_x X$  the tangent space at  $x$ ,  $g$  acting symplectically translates as  $\det(g|_{T_x X}) = 1$ . This implies that  $x$  is an isolated fixed point since no direction in  $T_x X$  can be fixed (a curve of fixed points would give an eigenvalue 1). So its image in  $Y$  is a quotient singularity, hence, by Proposition 4.5.2, it is a du Val singularity.

**Proposition 20.2.7.** *Let  $G$  be a finite group of automorphisms of a K3 surface  $X$ , then:*

1. *If  $G$  acts symplectically,  $X/G$  has at most du Val singularities and its minimal resolution is a K3 surface;*
2. *If  $G$  does not act symplectically,  $X/G$  is either rational or birational to an Enriques surface. It is isomorphic to an Enriques surface if  $G$  has order 2 and acts freely on  $X$ .*

*Proof.* 1. We have just noted that  $Y = X/G$  has at most isolated du Val singularities. Denote its minimal resolution by  $\tilde{Y}$ . The non-zero holomorphic 2-form on  $X$  is  $G$ -invariant and therefore descends to a non-zero holomorphic 2-form on  $X/G$  outside the singular points. This non-zero holomorphic 2-form on the complement of the singularities on  $Y$  pulls back to the complement of the exceptional curves of  $\tilde{Y}$  and extends to  $\tilde{Y}$  (residues along exceptional curves vanish). So  $\tilde{Y}$  has trivial canonical bundle. Since  $b_1(X) = 0$ , also  $b_1(\tilde{Y}) = 0$  and so, by the classification of surfaces B.5.4,  $\tilde{Y}$  is a K3 surface.

2. In this case  $p_g(\tilde{Y}) = 0$  and  $b_1(\tilde{Y}) = 0$ . Again, the classification theorem of surfaces shows that in this case  $\tilde{Y}$  is either rational or birational to an Enriques surface. An involution acting freely produces by definition an Enriques surface.  $\square$

### 20.3 Finite Groups Acting Symplectically: Universality of the Mathieu Group $M_{23}$

Here  $X$  is a K3 projective surface,  $H^2(X, \mathbb{Z})$  will be identified with the K3 lattice  $\Lambda$ ,  $G$  is a finite subgroup of  $O(\Lambda)$  acting symplectically. Finally  $S = \text{NS}(X)$  and  $T = S^\perp$ .

The Mathieu group  $M_{24}$  has been introduced in Section 5.1. We recall that it is the subgroup of the symmetric group  $\mathfrak{S}_{24}$  preserving the Golay code. This group acts transitively on the set  $\Omega = \{1, \dots, 24\}$  and  $M_{23}$  is the stabilizer of one of the elements of  $\Omega$  for which we may and do take 24.

**Theorem 20.3.1** (Mukai, [159]). *A finite group  $G$  arises as a subgroup of  $\text{Aut}_s(X)$  for some projective K3 surface  $X$  if and only if  $G$  is isomorphic to a subgroup of the Mathieu group  $M_{23}$  for which the induced action on  $\Omega$  has at least 5 orbits.*

*Sketch of the proof of the only if part.* The proof is subdivided in the following steps:

**Step 1. Proof that there exists some Niemeier lattice  $N^1$  and a primitive embedding**

$$j : M := \Lambda_G \oplus A_1(-1) \hookrightarrow N(-1). \quad (20.5)$$

First of all we establish that  $\Lambda_G$  is negative definite. To prove this, first note that  $T \subset \Lambda^G$  since  $G$  consists of symplectic automorphisms, and so  $\Lambda_G \subset S$  with  $S$  of signature  $(1, \rho - 1)$ . Since  $X$  is projective and  $G$  is finite there exists an ample invariant class, say  $y \in \Lambda^G \cap S$ , and  $\Lambda_G \subset S$  is orthogonal to  $y$  and hence  $\Lambda_G$  is negative definite.

By the third condition of Proposition 15.2.1, the desired embedding exists if a positive definite lattice of rank  $24 - \text{rank}(M) = 23 - \text{rank}(\Lambda_G)$  and with discriminant quadratic form  $q_M^\#$  exists. We show this by verifying the conditions of Theorem 12.4.4. The first condition is automatic since  $M$  is an integral lattice, and condition 2 on the length of the discriminant group is satisfied since

$$\begin{aligned} \ell(M) &= \ell(\text{dg}_{\Lambda_G}) + 1 = \ell(\text{dg}_{\Lambda^G}) + 1 \\ &\leq \text{rank}(\Lambda^G) + 1 \\ &= 22 - \text{rank}(\Lambda_G) + 1 \\ &= 24 - (\text{rank}(\Lambda_G) + 1). \end{aligned}$$

Finally, condition 3 on the 2-primary discriminant group holds since  $\langle 2^{-1} \rangle$  splits off due to the orthogonal summand  $A(-1)$ . This also implies that  $\ell(\text{dg}_{M_p}) < \text{rank}(M)$  so that condition 3 for  $p \neq 2$  is vacuous.

**Step 2. The case where  $N$  is the Niemeier lattice with root lattice  $R = \bigoplus_{i=1}^{24} \mathbb{Z}e_i$ ,  $e_i \cdot e_i = 2$ .**

In Section 5.1 we have seen that  $N$  is associated to the Golay code  $C_{\text{Gol}} \subset \mathbb{F}_2^{24}$ . We claim that  $O(N) = (\mathbb{Z}/2\mathbb{Z})^{24} \rtimes M_{24}$ . Indeed,  $(\mathbb{Z}/2\mathbb{Z})^{24} \rtimes \mathfrak{S}_{24}$  acts on  $R$  by

<sup>1</sup>Recall that a Niemeier lattice is a positive definite even unimodular lattice of rank 24.

permuting the basis vectors and sign changes. Since  $\text{rank}(N) = 24$ , an isometry is completely determined by the action on a spanning set such as  $\{e_1, \dots, e_{24}\}$  and preserves this set up to signs, whence an inclusion  $O(N) \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^{24} \rtimes \mathfrak{S}_{24}$ . However,  $N$  is associated to the Golay code and  $M_{24}$  is the stabilizer of this code and so  $O(N) \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^{24} \rtimes M_{24}$ . Since every element of the right-hand side actually gives an isometry of  $N$ , we have equality.

The action of  $G$  extends to an action on the Niemeier lattice by letting it act as the identity on the orthogonal complement of the image of  $j(\Lambda_G) \subset N$  under the embedding  $j$  from (20.5). This is possible by Theorem 15.1.7 since  $G$  acts as the identity on  $\Lambda^G$  and consequently it also acts as the identity on the discriminant group of  $\Lambda_G$ . Hence we get an inclusion  $G \hookrightarrow O(N)$  and, since  $W(N) = (\mathbb{Z}/2\mathbb{Z})^{24}$ , we obtain an induced homomorphism

$$\varphi : G \rightarrow O(N)/W(N) \simeq M_{24}.$$

We claim that  $\varphi$  is an injection. Note first that the action of  $G$  on  $N$  is constructed in such a way that  $N_G \subset \Lambda_G$ . Moreover, since  $G$  acts symplectically,  $T \subset \Lambda^G$  and hence  $N_G \subset \Lambda_G \subset S$ , that is,  $N_G$  consists of algebraic classes. Next observe that  $O(N)/W(N)$  can be identified with the subgroup of  $O(N)$  which leaves a Weyl chamber of  $W(N)$  invariant and so  $\varphi$  is an injection if its image leaves each Weyl chamber invariant. To prove this, it suffices to show that  $N^G$  meets a Weyl chamber in its interior. Suppose that this is not the case. Then the linear subspace  $N_{\mathbb{R}}^G \subset N_{\mathbb{R}}$  is contained in some reflection hyperplane  $e_i^\perp$ . But then  $e_i \in N_G$  and hence  $e_i$  is a root in  $\Lambda_G$  contradicting Criterion 20.2.1. Finally, since the root corresponding to the  $A_1(-1)$ -summand embedded in  $N$  is fixed by all  $\sigma \in G$ , letting it correspond to  $e_{24}$ , we get an embedding  $G \hookrightarrow M_{23}$ .

It remains to show that  $G$  has at least 5 orbits in  $\Omega$ . To see this, first remark that  $\text{rank}(N^G) \geq 3$  since  $G$  acts trivially on  $T$  which has rank  $\geq 3$ , and hence  $\text{rank}(N_G) \leq 19$  so that the  $G$ -invariant sublattice  $N^G$  of  $N$  has rank  $\geq 24 - 19 = 5$ . Let  $f_1, \dots, f_5 \in N^G$  be independent elements, say  $f_i = \sum_{j=1}^{24} f_{ij}e_j$ . The matrix  $F = (f_{ij})$  thus has rank 5. From  $\sigma(f_i) = f_i$ ,  $\sigma \in G \subset \mathfrak{S}_{24}$ , one sees that  $f_{ij} = f_{i\sigma^{-1}(j)}$ . So if  $k$  and  $\ell$  are in the same  $G$ -orbit, then the  $k$ -th and  $\ell$ -th columns are equal. Since  $\text{rank}(F) \geq 5$ , we must then have at least 5 orbits in  $\Omega$ .

The argument for the other Niemeier lattices is simpler. See S. Kondō's paper [128] for details.

We refer to *loc. cit.* for a proof of the converse statement which uses Criterion 20.2.1. □

## 20.4 Finite Abelian Groups Acting Symplectically

In this section we discuss which finite abelian groups act symplectically on K3 surfaces. The main goal is to show that each of these groups act in an essentially unique way in cohomology.

**20.4.A An inventory.** Suppose  $G$  acts symplectically on a K3 surface  $X$ . By Proposition 20.2.7,  $Y = X/G$  has at most du Val singularities and its minimal resolution  $\tilde{Y}$  is a K3 surface. The classes of the components in the minimal resolution  $\tilde{Y}$  generate a sublattice of  $H^2(\tilde{Y}, \mathbb{Z})$  which is denoted  $M'_Y$ . Its primitive closure,  $M_Y$ , is called the *resolution lattice of the quotient K3 surface*.

**Lemma 20.4.1.** *The possible finite abelian groups  $G$  acting effectively and symplectically (and their invariants) are those which are given in Table 20.4.1,*

Table 20.4.1: Groups  $G$

$G$	exceptional divisor	rank $M_Y$	signature $\Lambda^G$	$\text{dg}_{M_Y}$
$\mathbb{Z}/2\mathbb{Z}$	$8A_1$	8	(3, 11)	$\oplus^6 \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z}$	$6A_2$	12	(3, 7)	$\oplus^4 \mathbb{Z}/3\mathbb{Z}$
$\mathbb{Z}/5\mathbb{Z}$	$4A_4$	16	(3, 3)	$\oplus^2 \mathbb{Z}/5\mathbb{Z}$
$\mathbb{Z}/7\mathbb{Z}$	$3A_6$	18	(3, 1)	$\mathbb{Z}/7\mathbb{Z}$
$\mathbb{Z}/4\mathbb{Z}$	$2A_1 + 4A_3$	14	(3, 7)	$\oplus^2 \mathbb{Z}/2\mathbb{Z} \oplus^2 \mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/6\mathbb{Z}$	$2(A_1 + A_2 + A_5)$	16	(3, 3)	$\oplus^2 \mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/8\mathbb{Z}$	$A_1 + A_3 + 2A_7$	18	(3, 1)	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
$\oplus^2 \mathbb{Z}/2\mathbb{Z}$	$12A_1$	12	(3, 7)	$\oplus^8 \mathbb{Z}/2\mathbb{Z}$
$\oplus^3 \mathbb{Z}/2\mathbb{Z}$	$14A_1$	14	(3, 5)	$\oplus^8 \mathbb{Z}/2\mathbb{Z}$
$\oplus^4 \mathbb{Z}/2\mathbb{Z}$	$15A_1$	15	(3, 4)	$\oplus^7 \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$4(A_1 + A_3)$	16	(3, 3)	$\oplus^2 \mathbb{Z}/2\mathbb{Z} \oplus^2 \mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$3(A_1 + A_5)$	18	(3, 1)	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
$\oplus^2 \mathbb{Z}/3\mathbb{Z}$	$8A_2$	16	(3, 3)	$\oplus^4 \mathbb{Z}/3\mathbb{Z}$
$\oplus^2 \mathbb{Z}/4\mathbb{Z}$	$6A_3$	18	(3, 1)	$\oplus^2 \mathbb{Z}/4\mathbb{Z}$

*Proof for  $G$  cyclic of prime order  $p$ .* We have seen in § 4.5.A that the fixed points of a generator  $g$  all give  $A_{p-1}$  singularities. Their number,  $n_p$ , can be found by calculating the Euler number  $e(Y)$  in two ways. The first is by comparing it with the Euler number of the K3 surface  $\tilde{Y}$  which equals  $e(\tilde{Y}) = 24$ . Each of the  $n_p$  singularities on  $Y$  resolves into an  $A_{p-1}$ -configuration. Each of these has Euler number  $p$ . Hence  $e(Y) = e(\tilde{Y}) - n_p p + n_p = 24 + n_p(1 - p)$ . On the other hand  $X \rightarrow Y$  is a  $p$ -fold cover which is unbranched in the complement of the  $n_p$  fixed points, while each fixed point gives a single (singular) point on  $Y$ . We find  $e(Y) = (e(X) - n_p)/p + n_p = 24/p + n_p(p - 1)/p$ . Comparison gives  $(p + 1)n_p = 24$  and so  $(p + 1)|24$ . Since  $n_p$  configurations of type  $A_{p-1}$  produce a negative definite lattice of rank  $n_p(p - 1) \leq 19$ , we obtain  $p \leq 7$ . This gives the first block of the first and second column.

Next, to calculate  $\text{rank}(H^2(X, \mathbb{Z})^G)$ , we apply the ordinary Lefschetz fixed point formula [88, Ch 3.4] to the action of  $g \neq \text{id}$  on  $H^2(X, \mathbb{Q})$ . In our case it reads

$$2 + \text{Tr}(H^2(X, \mathbb{Q})) = \text{number of fixed points} = n_p,$$

where  $\text{Tr}$  denotes the trace. The irreducible representations of  $G$  correspond to the subrepresentations of the regular representation  $R(G)$  of  $G$  that have rational trace. For  $G$  cyclic of prime order  $p$  there are exactly two such representations: the trivial representation and a rank  $p - 1$  representation with trace  $-1$ . See e.g. [205, Exercise 13.1]. So, if  $\dim H^2(X, \mathbb{Q})^G = d$ , one has  $2 + d - (22 - d)/(p - 1) = n_p$  which gives the penultimate column in the table.

Since  $M'_Y = \bigoplus^{n_p} A_{p-1}(-1)$ , we find  $\text{disc}(M'_Y) = \pm p^{n_p}$  by Lemma 4.1.7. Theorem 20.9.6.1 in the appendix to this chapter, tells us that  $[M_Y : M'_Y] = |G|$ , and so, applying Lemma 1.2.2, we get  $\text{disc}(M_Y) = \pm p^{n_p-2}$ . Next, from the inclusions  $M'_Y \subset M_Y \subset M_Y^* \subset M_G^*$  it follows that  $M_Y^*/M'_Y \subset M_G^*/M'_Y$ . So, since by Table 4.1.1 the discriminant group of  $A_{p-1}(-1)$  is the cyclic group  $\mathbb{Z}/p\mathbb{Z}$ , the group  $M_Y^*/M'_Y$  is a direct sum of cyclic groups of order  $p$ , and hence its quotient  $M_Y^*/M_Y$  as well. Combining with  $\text{disc}(M_Y) = \pm p^{n_p-2}$ , we find  $d_{\mathfrak{g}_{M_Y}} = \bigoplus^{n_p-2} \mathbb{Z}/p\mathbb{Z}$ . This gives the last column.

*Proof of the remaining cases.* See [169, §6]. □

**Example 20.4.2.** The first example in the above list is the Nikulin involution. The table shows that it has eight fixed points which upon resolving gives eight  $-2$  curves whose classes  $e_1, \dots, e_8$  span  $\bigoplus^8 A_1(-1)$ . The primitive closure in  $H^2$  has an extra element  $\frac{1}{2} \sum_j e_j$ . So the resolution lattice is the Nikulin lattice (see Definition 5.2.9) with discriminant group  $\bigoplus^6 \mathbb{Z}/2\mathbb{Z}$ .

Table 20.4.2

$G$	cyclic subgroup	occurring types $\mu$ and $n(\mu)$	$m(\mu)$
$\bigoplus^2 \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	all 3 types, 2	4
$\bigoplus^3 \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	all 7 types, 2	2
$\bigoplus^4 \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	all 15 types, 2	1
$\bigoplus^2 \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	all 4 types, 3	2
$\bigoplus^2 \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	none	0
	$\mathbb{Z}/4\mathbb{Z}$	all 6 types, 4	1
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$(1, 2), (1, 0), 2$	2
	$\mathbb{Z}/4\mathbb{Z}$ ,	all 2 types, 4	2
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	all 3 types, 2	1
	$\mathbb{Z}/3\mathbb{Z}$	none	0
	$\mathbb{Z}/6\mathbb{Z}$	all 3 types, 6	1

**20.4.B Isometry class of the resolution lattice.** We shall give a lattice theoretical description of the resolution lattice  $M_Y$  in terms of the group  $G$ . To begin, a non-trivial stabilizer of a point  $p \in X$  is cyclic (analyse its action on  $T_p(X)$ ). A finite group has an invariant factor decomposition isomorphic to  $\bigoplus_{j=1}^s \mathbb{Z}/d_j\mathbb{Z}$ ,  $d_1|d_2|\dots$  and a cyclic subgroup of  $G$  is then determined by an  $s$ -tuple of integers (modulo  $d_j$  in the  $j$ -th summand), its *type*, for which we use the letter  $\mu$ . The

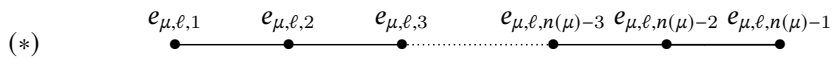
order of the group will be denoted  $n(\mu)$ . In case  $G = \oplus^k \mathbb{Z}/2\mathbb{Z}$ ,  $k = 2, 3, 4$ , we also identify the type with a non-zero vector in  $\mathbb{F}_2^k$ . Cyclic groups  $G$  have types consisting of a sole number, which is a divisor of  $|G|$ .

Not every possible type occurs for K3 surfaces in this way, and there may be multiple occurrences, say  $m(\mu)$  of type  $\mu$ , each corresponding to an  $A_n$ -type singularity with  $n = n(\mu) - 1$ . For cyclic groups the numbers  $m(\mu)$  of subgroups with type  $\mu$  can be read off from the table (second column) we gave in Lemma 20.4.1. For the non-cyclic groups the complete list (with proofs) can be found in [169, §6], copied as Table 20.4.2.

The aimed for description of the lattices  $M_Y$  in terms of  $G$  can now be given. We first introduce  $M'_G$  which as a free  $\mathbb{Z}$ -module is generated by  $e_{\mu,\ell,k}$  where  $\mu$  runs over the types for  $G$  which actually occur according to Tables 20.4.1 and 20.4.2, the integer  $\ell$  runs from 1 to  $m(\mu)$ , and  $k$  from 1 to  $n(\mu) - 1$ . The lattice structure is given by declaring

$$M'_G := \bigoplus_{\mu} \bigoplus_{\ell=1}^{m(\mu)} A_{n(\mu)-1}(-1),$$

where the  $\ell$ -th copy is generated by the set of roots  $\{e_{\mu,\ell,1}, \dots, e_{\mu,\ell,n(\mu)-1}\}$  as in the graph (\*) below.



We furthermore put

$$E_G := \bigcup_{\mu,\ell} \{e_{\mu,\ell,1}, \dots, e_{\mu,\ell,n(\mu)-1}\} \tag{20.6}$$

$$M_G := \text{smallest sublattice of } M'_G \otimes \mathbb{Q} \text{ containing } M'_G \text{ and } \{x \in J_G\} \tag{20.7}$$

where  $J_G$  is the set of  $\ell(G)$  supplementary (representatives of) generators from the last column in Table 20.4.3. From this table we see that the choice of the supplementary generators is such that the torsion group  $M_G/M'_G$  is isomorphic to  $G$ . On the geometric side,  $M_Y$  and  $M_G$  are indeed isometric and this gives the searched for abstract description of  $M_Y$ . See Lemma 20.4.3 below for details.

**Lemma 20.4.3.** *Let  $X$  be a K3 surface and  $G$  a finite abelian group acting symplectically on  $X$  with quotient  $Y = X/G$ . Let  $E_Y$  be the collection of classes of the exceptional curves of the minimal resolution  $\tilde{Y}$  of  $Y$ ,  $M'_Y$  the lattice they span and  $M_Y$  its resolution lattice, i.e., the primitive closure of  $M'_Y$  in  $H^2(\tilde{Y})$ .*

1. *There exists an isometry  $\varphi : M_Y \xrightarrow{\sim} M_G$  such that  $\varphi(E_Y) = E_G$ ; hence  $\varphi$  sends  $M'_Y$  to  $M'_G$  inducing a group isomorphism  $\bar{\varphi} : M_Y/M'_Y \xrightarrow{\sim} M_G/M'_G$ .*
2. *The embedding  $M_Y \xrightarrow{\varphi} M_G \hookrightarrow \Lambda$  extends to an  $M_G$ -marking  $H^2(\tilde{Y}) \xrightarrow{\sim} \Lambda$ . Any two embeddings of  $M_Y \hookrightarrow \Lambda$  are conjugate under  $O(\Lambda)$ .*

*Proof.* 1. This follows from a straightforward calculation for which we refer to [169, §6]. The last assertion can be seen from the shape of the supplementary generators in Table 20.4.3.

2. Extension follows from Witt's extension theorem 15.1.7 and the uniqueness of

Table 20.4.3

$G$	$\ell(G)$	set $J_G$ of generators for $M_G/M'_G$
$\mathbb{Z}/2\mathbb{Z}$	1	$f$
$\mathbb{Z}/3\mathbb{Z}$	1	$f$
$\mathbb{Z}/5\mathbb{Z}$	1	$f_{(1),1} + f_{(1),2} + 2f_{(1),3} + 2f_{(1),4}$
$\mathbb{Z}/7\mathbb{Z}$	1	$f_{(1),1} + 2f_{(1),2} + 3f_{(1),3}$
$\mathbb{Z}/4\mathbb{Z}$	1	$f$
$\mathbb{Z}/6\mathbb{Z}$	1	$f$
$\mathbb{Z}/8\mathbb{Z}$	1	$f_{(4)} + f_{(2)} + f_{(1),1} + f_{(1),2}$
$\oplus^2 \mathbb{Z}/2\mathbb{Z}$	2	$f'_1, f'_2$
$\oplus^3 \mathbb{Z}/2\mathbb{Z}$	3	$f'_1, f'_2, f'_3$
$\oplus^4 \mathbb{Z}/2\mathbb{Z}$	4	$f'_1, f'_2, f'_3, f'_4$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	2	$f_{(1,2)} + f_{(1,0)} + 2f_{(1,1)}$ $f_{(1,2)} + f_{(0,1)} + f_{(1,1)}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	2	$f_{(1,0)} + f_{(1,3)} + 3f_{(1,2)} + 3f_{(1,1)}$ $f_{(0,1)} + f_{(1,0)} + f_{(1,2)} + f_{(1,3)} + 2f_{(1,1)}$
$\oplus^2 \mathbb{Z}/3\mathbb{Z}$	2	$f_{(1,0)} + f_{(1,1)} + f_{(0,1)}$ $f_{(1,1)} + f_{(0,1)} + f_{(1,2)}$
$\oplus^2 \mathbb{Z}/4\mathbb{Z}$	2	$f_{(1,0)} + f_{(1,2)} + f_{(1,1)} + f_{(1,3)} + 2f_{(2,1)}$ $2f_{(1,2)} + f_{(1,3)} + f_{(0,1)} + f_{(2,1)} + f_{(1,1)}$

In the table we make use of some auxiliary vectors in  $M'_G \otimes \mathbb{Q}$ , namely the vectors  $f_{\mu,\ell} = \frac{1}{n_\mu} \sum_{k=1}^{n(\mu)-1} k e_{\mu,\ell,k}$ ,  $f = \sum_{\mu,\ell} f_{\mu,\ell}$ , and  $f'_q = \frac{1}{2} \sum_{\mu \in H_q} e_{\mu,1,1}$ , where  $H_q = \{\mu = (\mu_1, \dots, \mu_k) \in \mathbb{F}_2^k \mid \mu_q = 1\}$ ,  $q = 2, 3, 4$ .

the embedding up to conjugation follows from Theorem 15.2.6. The conditions in the statements are indeed satisfied, since first of all  $M_Y^\perp$  is indefinite because  $M_Y$  is negative definite of rank  $\leq 18$ . Secondly,  $\text{rank}(M_G) \leq 18 \leq \text{rank}(\Lambda) - 3$ . Thirdly, by Lemma 20.4.1, in all cases the table (last column) we gave in Lemma 20.4.1 shows that the number of generators of the discriminant group of  $M_G \simeq M_Y$  is at most  $\text{rank}(M_G^\perp) - 2$ .  $\square$

**Example 20.4.4.** Continuing with  $G = \mathbb{Z}/2\mathbb{Z}$ , i.e., the Nikulin involution (cf. Example 20.4.2), we see that the 8 types  $\mu$  are given by the 8 basisvectors of  $\mathbb{F}_2^8$ , and  $n(\mu) = 2$ ,  $m(\mu) = 1$ . The extra generator is  $f = \frac{1}{2} \sum e_j$ . Then  $M'_G = \oplus^8 A_1(-1)$ ,  $M_G = \Lambda_{\text{Nik}}$  and  $M_G/M'_G \simeq \mathbb{Z}/2\mathbb{Z}$ .

**20.4.C K3 surfaces with symplectic  $G$ -action and their quotients.** In the previous subsection we showed that the K3 surface  $\tilde{Y} = \tilde{X}/G$  admits an  $M_G$ -marking and so belongs to the period domain  $D(M_G^\perp)$ . In fact for these surfaces the roots in  $E_G$  correspond to nodal classes. This justifies the concept of an  $(M_G, E_G)$ -*marking*, where  $E_G$  corresponds to nodal classes under the marking. In particular,



the roots in  $E_G$  are irreducible. We set

$$\mathring{D}(M_G^\perp) := \{[u] \in D(M_G^\perp) \mid [u] \text{ is } (M_G, E_G)\text{-marked}\}. \tag{20.8}$$

Surprisingly, conversely an  $(M_G, E_G)$ -marked K3 surface  $\tilde{Y}$  determines in a canonical way a K3 surface  $X$  with symplectic  $G$ -action such that  $\widetilde{X/G} = \tilde{Y}$ . More precisely:

**Proposition 20.4.5.** 1) *Let  $\tilde{Y}$  be a K3 surface admitting an  $(M_G, E_G)$ -marking.*

- *The  $(M_G, E_G)$ -marking gives a canonical identification*

$$\iota^* : \text{Ext}^1(G) \xrightarrow{\sim} M_Y/M'_Y. \tag{20.9}$$

- *There exists a K3-surface  $X$  and an embedding  $\iota : G \hookrightarrow \text{Aut}_s(X)$  such that the minimal resolution of singularities of  $X/\iota(G)$  is isomorphic to  $\tilde{Y}$ . Moreover,  $\tilde{Y}$  has an  $(M_G, E_G)$ -marking inducing  $\iota^*$ .*

2) *Conversely, every K3-surface  $X$  with symplectic  $G$ -action comes in this way from some  $(M_G, E_G)$ -marked K3 surface. Two such marked K3-surfaces come from (possibly different) embeddings  $\iota, \iota' : G \hookrightarrow \text{Aut}_s(X)$  if and only if  $\iota' = \iota\alpha$  where  $\alpha$  is an automorphism of the group  $G$ .*

*Proof.* 1) By definition, there is a set of nodal curves  $\{E_{\mu,\ell,k}\}$  on  $\tilde{Y}$  whose classes under the marking correspond to those in  $E_G$ . Let  $Y' = \tilde{Y} - \bigcup_{\mu,\ell,k} E_{\mu,\ell,k}$ . Observe that one can apply formulas (20.22) and (20.25) in the Appendix to this chapter even if one does not know that a group acts. Since in our situation  $H_1(\tilde{Y}) = 0$ , the argument which we give there then yields a canonical identification  $\text{Tors } H^2(Y') = M_Y/M'_Y = \text{Ext}^1(G)$ . This proves the first assertion.

By the universal coefficient theorem this implies  $\text{Tors } H_1(Y') = G$ . Hence, there is an unramified cover  $\pi' : X' \rightarrow Y'$  with covering group  $G$ . Let  $T \subset \tilde{Y}$  be a small enough tubular neighborhood of an  $A_{n(\mu)-1}$ -configuration. The inverse image  $(\pi')^{-1}T'$ ,  $T' = T \cap Y'$  consists of  $|G|/n(\mu)$  disjoint isomorphic copies of the universal cover  $B'$  of  $T'$ . This follows since the fundamental group of  $T' = T \cap Y'$  is cyclic of order  $n(\mu)$  because the  $A_{n(\mu)-1}$ -configuration can be blown down to a cyclic quotient singularity  $y$  of type  $A_{n(\mu)-1}$ . Moreover,  $B' = B - x$  for some ball  $B$  with center  $x$ . We can now glue  $X'$  to the disjoint union of these balls  $B$  along the  $B'$ , obtaining a compact complex manifold  $X$ . The action of the covering group  $G$  of  $X' \rightarrow Y'$  extends to  $X$  such that each of the points  $x$  becomes a fixed point (Hartog's theorem). In particular, we get an embedding  $\iota : G \hookrightarrow \text{Aut}_s(X)$ . Then  $Y := X/\iota(G)$  has  $\tilde{Y}$  as its minimal desingularization and  $x$  maps to the corresponding point  $y \in Y$ . We claim that  $X$  is a K3 surface. To show this, remark that  $e(X) = 24$ , as can be seen by reversing the argument in the proof of Lemma 20.4.1. Next, a non-zero holomorphic 2-form  $\eta$  on  $\tilde{Y}$  restricts to a holomorphic 2-form on  $Y'$  which lifts to a non-zero 2-form on  $X'$  extending to  $X$  as a  $G$ -invariant non-zero 2-form (a priori its zero locus is either empty or a divisor – the last possibility is excluded). But then  $X$  is a K3 surface, by the classification theorem B.5.4. By

construction  $Y = X/\iota(G)$ . The construction of  $Y$  gives an  $(M_G, E_G)$ -marking for  $\tilde{Y}$  and an isomorphism  $\iota^*$ .

2) Suppose  $\iota : G \hookrightarrow \text{Aut}_s(X)$ . Then the minimal resolution of  $Y = X/\iota(G)$  is a K3-surface admitting an  $(M_G, E_G)$ -marking, and one has an induced isomorphism  $\iota^* : \text{Ext}^1(G) \xrightarrow{\sim} M_Y/M'_Y$  which encodes the  $G$ -action. Precomposing the embedding with an automorphism  $\alpha$  of  $G$  gives the isomorphism  $\iota^* \circ \text{Ext}(\alpha)$ . The minimal resolutions of  $X/\iota(G)$  and  $X/\iota\alpha(G)$  are isomorphic. On the other hand isomorphic minimal resolutions of quotients of two symplectic  $G$  actions on  $X$  can only arise if the  $G$ -action on  $X$  preserves the set of fixed points of each given type. Such a permutation comes from a lattice isometry of  $M_Y$  preserving the set  $E_Y$ , i.e., from some isometry in  $A(M_Y) = \{\gamma \in \text{O}(M_Y) \mid \gamma(E_Y) = E_Y\}$ . For any  $\gamma \in A(M_Y)$  consider the commutative diagram

$$\begin{array}{ccc}
 M_Y & \xrightarrow{\gamma} & M_Y \\
 \downarrow & & \downarrow \\
 M_Y/M'_Y & \xrightarrow{\bar{\gamma}} & M_Y/M'_Y \\
 \uparrow \iota^* & & \uparrow \iota^* \\
 \text{Ext}^1 G & \xrightarrow{\text{Ext}(\alpha)} & \text{Ext}^1 G,
 \end{array}$$

where  $\bar{\gamma}$  is induced from the natural map  $\rho_Y : A(M_Y) \rightarrow A(M_Y/M'_Y)$ . Since  $\text{Ext}$  is functorial,  $\alpha$  is defined by the commutativity of the diagram. The above argument shows that  $\rho_Y$  is surjective. Hence every K3-surface with symplectic  $G$ -action comes in this way from some  $(M_G, E_G)$ -marked K3 surface.  $\square$

**20.4.D Uniqueness of the  $G$ -action on cohomology.** Let  $G$  be any of the possible abelian groups of Table 20.4.1. Recall that a marked K3-surface  $(X, \varphi)$  with symplectic  $G$ -action and induced embedding  $\iota : G \hookrightarrow \text{O}(\Lambda)$  is called a  $(\iota, G)$ -marked K3 surface. Proposition 20.2.5 states that the moduli space  $\mathcal{M}_{(\iota, G)}$  of  $(\iota, G)$ -marked surfaces consists of two components.

The main result in this section, due to V. Nikulin, states that there is in fact only one conjugacy class (irrespective of the  $G$ -action):

**Theorem 20.4.6** ([169, Thm. 4.7]). *Let  $G$  be a finite abelian group acting symplectically (and effectively) on some K3 surface  $X$ . Then the  $G$ -action on the K3 lattice induced by some marking of  $X$  is up to conjugacy uniquely determined by  $G$ .*

To achieve our goal, first recall that by Corollary 20.2.6 over connected components of the moduli space  $\mathcal{M}_{(\iota, G)}$  incorporating the action of the group  $G$ , we stay within the same conjugacy class. So there are at most two classes. To compare K3 surfaces whose moduli points are in different connected components we will use the moduli space  $\mathcal{M}_{M_G}$  related to the quotients  $Y = X/G$ . This comparison makes essential use of the fact that  $\mathcal{M}_{M_G}$  does not depend on the embedding of  $G$  in the orthogonal group of the K3 lattice.

We divide the proof accordingly into several steps.

*Proof. Step 1: on the moduli space of  $M_G$ -marked K3 surfaces.* Recall (cf. (20.8)) that the domain  $\mathring{D}(M_G^\perp)$  is the period domain of  $(M_G, E_G)$ -marked K3 surfaces. The sublattice  $M'_G \subset M_G$  is a root lattice and the set of roots  $P(M'_G)$  that are non-negative linear combinations of the standard root basis for  $M'_G$  define a partition  $P(M_G) \cup -P(M_G)$ . By Proposition 19.3.2 this partition determines two preferred connected components of  $\mathcal{M}_{M_G}$  corresponding to markings for which  $\pm E_G$  is a set of nodal curves, say

$$\mathcal{M}_{M_G}^{+,P(M_G)} \sqcup \mathcal{M}_{M_G}^{-,P(M_G)} \subset \overline{\mathring{D}(M_G^\perp)}. \tag{20.10}$$

These correspond to opposite markings permuted by  $-\text{id} \in \text{O}(\Lambda)$ .

**Step 2: relating  $\mathcal{M}_{M_G}$  and  $\mathcal{M}_{\iota(G)}$ .** By Proposition 20.4.5 we can assign to the moduli point of an  $(M_G, E_G)$ -marked surface  $(\tilde{Y}, \varphi)$ , say  $m = m(\tilde{Y}, \varphi) \in \mathcal{M}_{M_G}^{\pm, P(M_G)}$  a unique K3 surface  $X_m$  equipped with symplectic  $G$ -action.

A marking  $\psi : H^2(X_m) \xrightarrow{\sim} \Lambda$  induces a  $G$ -action on  $\Lambda$  given by formula (20.3) and hence a  $(\iota, G)$ -marked K3 surface (see Definition 20.2.3)  $(X_m, \iota_m, \psi)$ , where  $\iota_m$  is the action on cohomology. Different markings  $\psi$  give conjugate embeddings  $G \hookrightarrow \text{O}(\Lambda)$  and so we are free to choose a marking  $\psi = \psi_m$ . A choice of the positive light cone then gives a moduli point in  $\mathcal{M}_{\iota(G)}$  and hence an assignment

$$m = m(\tilde{Y}, \pm\varphi) \in \mathcal{M}_{M_G}^{\pm, P(M_G)} \mapsto (X_m, \iota_m, \psi_m, \pm) \in \mathcal{M}_{\iota(G)}^\pm.$$

By Proposition 20.4.5.(4), every  $(X, \iota, \psi, \pm) \in \mathcal{M}_{\iota(G)}^\pm$  comes in this way from a moduli point of  $\mathcal{M}_{M_G}$ .

Hence it suffices to show that for  $m, m' \in \mathcal{M}_{M_G}^{\pm, P(M_G)}$  the  $G$ -actions  $\iota_m$  and  $\iota_{m'}$  on  $\Lambda$  give conjugate subgroups  $\iota_m(G), \iota_{m'}(G)$  of  $\text{O}(\Lambda)$ . For brevity we shall say that in this case  **$m$  and  $m'$  give conjugate  $G$ -actions.**

To show that this is the case, it suffices to

1. construct an open neighborhood of a given moduli point of  $\mathcal{M}_{M_G}$  so that the points in this neighborhood give conjugate  $G$ -actions;
2. show that  $G$ -actions coming from the two connected components  $\mathcal{M}_{M_G}^{\pm, P(M_G)}$  are conjugate within  $\text{O}(\Lambda)$ .

**Step 3: local comparison of  $\mathcal{M}_{M_G}$  and  $\mathcal{M}_{\iota(G)}$ .** We fix a moduli point  $m \in \mathcal{M}_{M_G}^+$  whose period point is that of the marked K3 surface  $(\tilde{Y}_m, \varphi_m)$ . Let  $(X_m, \iota_m, \psi_m)$  be the corresponding K3 surface with  $G$ -action. Let  $V \subset \mathcal{M}_{\iota(G)}^+$  be a disc centered at  $m$  and let  $\mathcal{X}|_V$  be the restriction of the universal  $\Lambda_G$ -marked family to  $V$ . By local universality, the group  $G$  acts on  $\mathcal{X}$ . The fibers  $X_v/G = Y_v$  of the quotient  $\mathcal{Y} = \mathcal{X}/G$  have the same type and number of quotient singularities along the (disconnected) submanifold of  $\mathcal{Y}$  which is the image of the union  $\Sigma \subset \mathcal{X}$  of fixed point manifolds

of  $G$ . Let  $v_o \in V$  and  $s \in \Sigma \cap X_{v_o}$ . Locally around  $s$  the total space of the family  $\mathcal{Y}$  is isomorphic to  $(U_s/G_s) \times V$ , where  $G_s$  is the stabilizer subgroup of  $s$  in  $G$  and  $U_s$  is a  $G_s$ -invariant open subset of the fiber  $X_{v_o}$ . The minimal resolution  $\widetilde{U}_s/G_s$  of  $U_s/G_s$  gives an open subset in  $\widetilde{Y}_{v_o}$ . A patching argument shows that there is a global resolution  $\widetilde{\mathcal{Y}}$  of  $\mathcal{Y}$ , which locally is isomorphic to  $\widetilde{U}_s/G_s \times V$ . There results a commutative diagram

$$\begin{array}{ccccc} \mathcal{X}|_V & \longrightarrow & \mathcal{Y}|_V & \longleftarrow & \widetilde{\mathcal{Y}}|_V \\ & \searrow u & \downarrow & \swarrow v & \\ & & V & & \end{array}$$

and  $u^{-1}m = (X_m, \iota_m, \psi_m)$ ,  $v^{-1}m = (\widetilde{Y}_m, \varphi_m)$ .

The next step consists of comparing the period maps  $p_u$  and  $p_v$  for the two families  $\mathcal{X}|_V$ , respectively  $\widetilde{\mathcal{Y}}|_V$ . To do this, we first link the two period points over  $m \in V$ . We use the natural map  $\theta_m : H^2(\widetilde{Y}_m) \rightarrow H^2(X_m)$  of Theorem 20.9.6.1 together with the two markings  $\varphi_m$  and  $\psi_m$  to transform the sequence (20.24) into an exact sequence of abstractly given lattices,

$$0 \rightarrow M_G/M'_G \rightarrow \Lambda/M'_G \xrightarrow{\theta'} \Lambda^G, \quad \theta' = \psi_m \circ \theta \circ \varphi_m^{-1}, \quad \Lambda^G/\text{Im}(\theta') \simeq H^3(G). \quad (20.11)$$

Theorem 20.9.6 also implies that  $\theta'$  restricts to  $M_G^\perp \subset \Lambda/M'_G$  and then induces an embedding  $M_G^\perp \hookrightarrow \Lambda^G$  of free  $\mathbb{Z}$ -modules of the same rank (but which multiplies the intersection form by  $|G|$ ). Consequently, one obtains an isomorphism

$$\begin{aligned} \theta'_{m,\mathbb{C}} : [M_G^\perp]_{\mathbb{C}} &\xrightarrow{\simeq} [\Lambda^G]_{\mathbb{C}}, \\ [\varphi_m(H^{2,0}(\widetilde{Y}_m))] &\mapsto [\psi_m(H^{2,0}(X_m))] \end{aligned}$$

relating the period points of  $(\widetilde{Y}_m, \varphi_m)$  and  $(X_m, \psi_m)$ .

Next, we extend the preceding isomorphisms  $\theta'_{m,\mathbb{C}}$  over  $V$ . To start, note that the exact sequence (20.24) extends over  $V$  as an exact sequence of sheaves of  $\mathbb{Z}$ -modules. Now choose trivializing markings for the local systems  $R^2u_*\mathbb{Z}$  and  $R^2v_*\mathbb{Z}$  which coincide at  $m \in V$  with  $\varphi_m$ , respectively  $\psi_m$ . So the exact sequence (20.11) holds at every point  $m' \in V$  and  $\theta'_{m',\mathbb{C}}$  sends the period of  $(\widetilde{Y}_{m'}, \varphi_{m'})$  to the period point of  $(X_{m'}, \psi_{m'})$  for all  $m' \in V$ . In other words, the period map  $p_u : V \rightarrow D(\Lambda^{\iota(G)})$  and  $p_v : V \rightarrow D(M_G^\perp)$  fit in a commutative diagram

$$\begin{array}{ccc} & & p_u(V) \subset D(\Lambda^{\iota(G)}), \\ & \nearrow p_u & \uparrow \simeq \theta' \\ V & & \\ & \searrow p_v & p_v(V) \subset D(M_G^\perp), \end{array}$$

where  $\theta'$  is an injective (but a priori only continuous) map onto the image of the period map  $p_u$ . Because  $\mathcal{X}|_V$  is a locally universal family,  $p_u$  is injective, and so  $p_v$  must be injective. To finish, we make a crucial

**Observation.** *The period domains  $D(\Lambda^G)$  and  $D(M_G^\perp)$  associated to finite abelian groups acting symplectically on K3 surfaces have the same dimension.*

This follows from Table 20.4.1 and the existence of the isometry  $M_Y \simeq M_G$ . The observation implies that  $p_\nu$  is an open immersion and so the image is the desired open neighborhood of the period point of  $(\tilde{Y}, \varphi_m)$ , identified with an open neighborhood of its moduli point  $m$ . This finishes the first step in our strategy.

**Step 4: finishing the proof: relating different components.** We come to the second point of our strategy: comparing the  $G$ -actions coming from the two connected components  $\mathcal{M}_{M_G}^{\pm, P(M_G)}$ .

The two preferred partitions  $\pm P(M_G)$  from opposite cones are related by an isometry of the root lattice  $M'_G$ . To see this, note that by [26, VI.1.6, Cor. 3] there is an involution  $w'_0$  belonging to the Weyl group of the root system which sends the all roots of a lattice isometric to a direct sum of type  $A$  lattices to their negatives. So it does not preserve  $P(M_G)$  but  $-w'_0$  does. It extends to an isometry  $-w_0$  of  $\Lambda$ , which sends the positive light cone to its opposite (since by Observation 17.2.B  $w_0$  preserves the positive light cone). Hence we have shown:

**Lemma 20.4.7.** *If  $(\tilde{Y}, \varphi_o)$  has moduli point  $m = [\tilde{u}_1] \in \mathcal{M}_{M_G}^{+, P(M_G)}$ , then the moduli point  $-w_0(m)$  of  $(\tilde{Y}, -w_0 \circ \varphi_o)$  belongs to  $\mathcal{M}_{M_G}^{-, P(M_G)}$ .*

So we now have two moduli points  $m, -w_0(m)$ , on the two components for the same surface  $\tilde{Y}$ ,  $Y = X/G$ , equipped with two markings that are related by the lattice isometry  $-w_0$ . We next find out how the  $G$ -actions on the corresponding surfaces  $X_m$  and  $X_{-w_0(m)}$  are related. We start by recalling that there is a canonical isomorphism  $\iota^* : \text{Ext}^1(G) \xrightarrow{\sim} M_Y/M'_Y$  (see Eqn. (20.9)) which prescribes how  $G$  acts on  $X$ . The two markings  $\varphi_o$  and  $-w_0 \circ \varphi_o$  then induce  $\overline{\varphi_o} \circ \iota^* : \text{Ext}^1(G) \xrightarrow{\sim} M_G/M'_G$ , and respectively  $-\overline{w_0} \circ \overline{\varphi_o} \circ \iota^*$ , where  $\overline{w_0}$  is the automorphism of  $M_G/M'_G$  induced by  $w_0$  and  $\overline{\varphi_o}$  is induced by the marking. So the two actions of  $G$  on the K3 lattice differ by composition with the automorphism  $-\overline{w_0}$  of  $G$ .

**Lemma.** *One has  $\overline{w_0} = \text{id}$  on  $M_G/M'_G$  and so composing the marking with  $-w_0$  results in the opposite  $G$ -action.*

*Proof.* The assertion being clear for  $G = \oplus^k \mathbb{Z}/2\mathbb{Z}$ , we turn to the extra generators for  $M_G$  which are all  $\mathbb{Z}$ -linear combinations of the  $f_{\mu, \ell}$  and we have

$$\begin{aligned} w_0(f_{\mu, \ell}) &= \frac{1}{n(\mu)} \sum_{k=1}^{n(\mu)-1} k e_{\mu, \ell, k} = \frac{1}{n(\mu)} \sum_{k'=1}^{n(\mu)-1} (-n(\mu) + k') e_{\mu, \ell, k'} \\ &\equiv \frac{1}{n(\mu)} \sum_{k'=1}^{n(\mu)-1} k' e_{\mu, \ell, k'} \pmod{M'_G}. \end{aligned}$$

Hence  $\overline{w_0} = \text{id}$  as claimed. □

We can now finish the proof.

**Case 1.** In case  $G \simeq \oplus \mathbb{Z}/2\mathbb{Z}$  the automorphism  $-\bar{w}_0$  is the identity and so  $G$  acts up to conjugation with  $-w_0$  in the same way on  $G$ -marked K3 surfaces with moduli points in either one of the two components and this proves the theorem for these cases.

**Case 2.** For the other groups  $G$  we replace the extension of  $-w'_0$  by a different extension which leads to a second moduli point on the same connected component while the two  $G$ -actions still are opposite. We first show how to construct such an extension.

*Claim.*  $-w'_0$  also extends to an isometry  $w$  of the entire K3 lattice such that  $w$  preserves the positive light cone in  $\Lambda^{1,1}$  of  $(\tilde{Y}, \varphi_o)$ .

*Proof of the Claim.* For simplicity of notation we set  $L := M_G^\perp$ . We first search an isometry  $w''$  of  $L$  that induces on  $\text{dg}_L$  the same isometry as the one induced by  $-w'_0$  but which at the same time preserves the positive light cone of  $L_{\mathbb{R}}^{1,1}$ . Then the extension criterion Proposition 15.1.6 provides an extension  $w$  of  $w''$  to all of  $\Lambda$  preserving the light cone of  $\Lambda^{1,1} \otimes \mathbb{R}$ .

To proceed, we first observe that the map  $w_0$  is a product of reflections and so, by Lemma 16.1.1, induces the identity on the discriminant group. Hence  $w = -w_0$  induces  $-\text{id}$  on the discriminant group of  $M_G$ . Since the discriminant group of  $L$  is the same as for  $M_G$ , we could take  $w'' = -\text{id}$ . We seek however a lift  $w''$  of  $r_L(w)$  to  $L$  which has signed spinor norm 1 since by the arguments in Section 16.1 such an isometry will preserve the positive light cone of  $\Lambda^{1,1} \otimes \mathbb{R}$ , as desired. Theorem 14.5.5 gives us a criterion for the existence of a rotation with real spinor norm 1. Such an element has also signed spinor norm 1 since it is a product of an even number of reflections. We verify the conditions: Lemma 20.4.1 tells us that  $L$  is indefinite of rank  $\geq 3$  (indeed it is of signature  $(3, 19 - \text{rank}(L))$ ), and secondly, the number of generators of the discriminant group of  $M_G$  and hence of  $\text{dg}_L = \text{dg}_{M_G^\perp}$  is at most its length minus 2. This finishes the construction of the searched for  $w''$ .

We can now finish the proof in this case. Recall that  $(\tilde{Y}, \varphi_o)$  has moduli point  $m \in \mathcal{M}_{M_G}^{+,P(M_G)}$ . Because  $w$  preserves the positive light cone for the marked K3 surface  $\tilde{Y}$ , the moduli point  $w(m)$  also belongs to  $\mathcal{M}_{M_G}^{+,P(M_G)}$ .

So  $-w_0(m)$  and  $w(m)$  belong to different components, but, by construction, the corresponding  $G$ -actions on the K3 lattice are the same up to conjugation. Hence both components lead to the same conjugacy class. This finishes the proof in this case. □

To indicate that from a geometric perspective this theorem is quite unexpected we exhibit some examples of K3-surfaces which admit actions of small groups acting symplectically on totally different K3 surfaces.

**Examples 20.4.8. 1.** Examples from [79] with  $\mathbb{Z}/3\mathbb{Z}$ -action.

- The total space of the elliptic surface  $y^2 = x^3 + (t^3 - s^3)^4$  in Weierstraß form (with  $s$  a parameter) can be shown to be a K3-surface which admits a torsion section of order 3 given by  $t \mapsto (x, y) = (0, (t^3 - s^3)^2)$  and so admits an order 3 symplectic

transformation (by translation). If we vary  $s$  we get a 1-dimensional family of such surfaces.

- The action of a generator of  $\mathbb{Z}/3\mathbb{Z}$  on  $\mathbb{P}^2$  given by  $\sigma(x : y : z) = (x : \rho_3 y : \rho_3^2 z)$ ,  $\rho_3 = \exp(2\pi i/3)$  leaves invariant the 10 monomials  $x^6, x^4 y z, x^3 y^3, x^3 z^3, x^2 y^2 z^2, xy^4 z, xyz^4, y^6, y^3 z^3, z^6$  and a general linear combination  $f(x, y, z)$  of such monomials gives a smooth  $\mathbb{Z}/3\mathbb{Z}$ -invariant sextic plane curve. The double cover of  $\mathbb{P}^2$  branched in this sextic is a K3 surface with equation  $w^2 = f(x, y, z)$  and  $\sigma$  lifts to an automorphism. It preserves the non-zero holomorphic 2-form  $\Omega/w$ , where  $\Omega = xdy \wedge dz + ydz \wedge dx + zdx \wedge dy$ . The family depends on  $10 - 3 = 7$  effective parameters since the projective transformations commuting with  $\sigma$  are the diagonal transformations.

- Similarly, one has an action of  $\mathbb{Z}/3\mathbb{Z}$  on  $\mathbb{P}^3$  given by  $\sigma(x : y : z : t) = (x : y : \rho_3 z : \rho_3^2 t)$  and the general  $\sigma$ -invariant quartic  $g$  is a smooth K3-surface and  $\sigma$  restricts to it symplectically since a non-zero holomorphic 2-form is given by the residue of  $\Omega_3/f$  where  $\Omega_3 = x dy \wedge dz \wedge dt + y dz \wedge dt \wedge dx + z dt \wedge dx \wedge dy + t dx \wedge dy \wedge dz$ . A dimension count shows that this gives a family depending on 7 effective parameters.

2. Examples from [174]. A very general Kummer surface of product type is the Kummer surface of a product of non-isogeneous elliptic curves. Such a surface has 4 different elliptic fibrations with a 2-torsion section and 3 different elliptic fibrations with  $(\mathbb{Z}/2\mathbb{Z})^2$ -torsion. Hence these have 4 different symplectic  $\mathbb{Z}/2\mathbb{Z}$ -actions and 3 different symplectic  $(\mathbb{Z}/2\mathbb{Z})^2$ -actions. Such surfaces depend on 2 effective parameters.

## 20.5 Involutions on K3 Surfaces

In this section we shall write  $H^2(X), H^2(Y), \dots$  to mean integral cohomology. We continue to write  $\Lambda$  for the K3 lattice.

Our aim is to investigate involutions  $g$  on a K3 surface and characterize several of these lattice theoretically, such as the Enriques involution.

**20.5.A Group Theoretical Invariants.** A result [192] due to I. Reiner describes the representations of a cyclic group acting on a free  $\mathbb{Z}$ -module  $L$  of finite rank. For a cyclic group  $G = \{1, g\}$  of order 2 this result states that the module  $L$  is the direct sum of three types of irreducible  $G$ -submodules, the trivial rank 1 representation, the rank 1 representation  $-\mathbf{1}$  on which  $g = -\text{id}$ , and, finally, the 2-dimensional representation  $U$  on which  $g$  acts by permuting the two basis vectors. Hence one has a direct sum decomposition  $L = L_+ \oplus L_- \oplus L_{\text{sw}}$ , where  $L_{\pm} = \{x \in L \mid g(x) = \pm \text{id}\}$  and  $L_{\text{sw}} = \oplus^c U$  (the symbol "sw" stands for "swapping"). The three integers

$$a := \text{rank}(L_+), b := \text{rank}(L_-), c := \frac{1}{2} \text{rank}(L_{\text{sw}})$$

combined give  $t(g) = (a, b, c)$ , which we shall call the *type of the involution*. Since  $g$  acts with trace 0 on  $U$  we see:

$$\text{Tr}(g) = a - b. \tag{20.12}$$

Note that if  $L$  is a non-degenerate lattice and  $g$  an isometry of  $L$ , the above direct sum decomposition is *not* in general an orthogonal decomposition. However, as we have seen in Example 1.7.3, in the case  $g$  is an isometry the sublattice  $L^G \oplus L_G$  spans a finite index sublattice of  $L$ , where, we recall,  $L^G = \{x \in L \mid g(x) = x\}$  and  $L_G = (L^G)^\perp$ . Since  $L_{\text{sw}}$  has a basis  $\{e_1, f_1, \dots, e_c, f_c\}$  such that  $g(e_j) = f_j, g(f_j) = e_j, j = 1, \dots, c$ , the lattice  $L^G$  is spanned by  $L_+ \oplus \bigoplus_{j=1}^c \mathbb{Z}(e_j + f_j)$ . The lattice spanned by  $L_- \oplus \bigoplus_{j=1}^c \mathbb{Z}(e_j - f_j)$  is primitive, is contained in  $L_G$  and, since it has the same rank, is equal to  $L_G$ . We deduce:

**Lemma 20.5.1.** *If  $L$  is a unimodular lattice, and  $G$  acts as isometries, one has*

$$\begin{aligned} \text{rank}(L^G) &= a + c, \text{rank}(L_G) = b + c, \\ [L : (L^G \oplus L_G)] &= 2^c, \\ |\text{disc}(L^G)| &= |\text{disc}(L_G)| = 2^c. \end{aligned} \tag{20.13}$$

**20.5.B Implications of the Lefschetz Fixed Point Formula.**

**Lemma 20.5.2.** *Suppose  $X$  is a K3 surface with an involution  $g : X \rightarrow X$ . If  $g$  is symplectic, it has 8 isolated fixed points and the quotient is a surface with 8 ordinary double points with a K3 surface as its minimal resolution. In that case,  $\text{Tr}(g^*|_{H^2(X)}) = 6$  and the invariant lattice has rank 14, i.e.,  $a+c = 14$ , where  $(a, b, c)$  is the type of  $g^*$ .*

*If  $g$  is not symplectic, there are at most disjoint fixed point curves and  $Y = X/G$  is smooth. If  $\text{Tr}(g^*|_{H^2(X)}) = -2$ , then  $a + c = 10$ .*

*Proof.* Symplectic involutions have been dealt with in Lemma 20.4.1. We showed that there are 8 isolated fixed points and that the quotient has a K3 surface as its minimal resolution. We also showed that the invariant lattice  $H^2(X)^G$  has rank 14.

Since at a fixed point the action can be locally linearized (cf. [35]), in the non-symplectic case there can at most be fixed point curves (consisting of disjoint smooth components). A generalization of the Lefschetz fixed point formula (cf. for example [228, Lemma 1.6]) reads:

$$2 + \text{Tr}(g^*|_{H^2(X)}) = \# \text{ isolated fixed points} + \sum_{F \text{ fixed curve}} e(F),$$

and then simplifies to  $2 + \text{Tr}(g^*|_{H^2(X)}) = \sum_F e(F)$ , where we sum over fixed point curves  $F$ . Hence, if  $\text{Tr}(g^*|_{H^2(X)}) = -2$ , then  $\sum_F e(F) = 0$ . Finally, from  $a+b+2c = 22$  and  $a - b = \text{Tr } g^* = -2$  we obtain  $a + c = 10$ . □



*Remark 20.5.3.* If the second case of the above lemma occurs and no fixed curves are present,  $Y$  is an Enriques surface. We give two examples where  $Y$  is a rational surface. First, consider an elliptic pencil  $\lambda C + \mu C' = 0$ ,  $(\lambda : \mu) \in \mathbb{P}^1$ , on  $\mathbb{P}^2$  where  $C, C'$  are smooth elliptic curves intersecting transversally (in 9 points), and let  $Y$  be the blow-up of  $\mathbb{P}^2$  in the nine base points of the pencil. Let  $X$  be the double cover of  $Y$  branched in the strict transform of  $C + C'$ . Note that  $e(Y) = 3 + 9 = 12$  and  $e(X) = 24$  as it should. Classical algebraic geometry teaches us that coordinates can be fixed so that a pencil of cubics passes through 4 fixed points in general position and the pencil is determined by the choice of 4 further points, giving 8 moduli. The resulting surface  $X$  is a K3 surface admitting an involution which produces  $Y$ .

The second example starts from a pencil of elliptic curves on  $\mathbb{P}^1 \times \mathbb{P}^1$  defined by a pair of smooth curves of bidegree  $(2, 2)$  meeting transversally (in 8 points). So here we have to blow up the 8 intersection points which gives a smooth rational surface with  $e = 4 + 8 = 12$  as well.

**Proposition 20.5.4.** *Let  $X$  be a K3 surface with an involution  $g$  inducing  $g^*$  on  $H^2(X)$  and set  $G = \langle g^* \rangle$ .*

*If  $g$  is an Enriques involution, i.e., a fixed point free involution, then  $H^2(X)^G \simeq U(2) \oplus E_8(-2)$  of signature  $(1, 9)$ . The invariants  $(a(g^*), b(g^*), c(g^*))$  are  $(0, 2, 10)$ .*

*If  $g$  is a Nikulin involution (i.e., a symplectic involution), the discriminant group of  $H^2(X)^G$  is isomorphic to  $\oplus^8 \mathbb{Z}/2\mathbb{Z}$ . The invariants of  $g^*$  are  $(6, 0, 8)$  and the signature of  $H^2(X)^G$  equals  $(3, 11)$ .*

*Proof.* Let  $g$  be an Enriques involution and let  $Y = X/\langle g \rangle$ . We first claim that  $H_Y$ , the intersection lattice of  $Y$ , is isometric to  $U \oplus E_8(-1)$ . Note that this lattice is unimodular, and of rank 10 by Lemma 20.5.2. Since  $c_1^2(Y) = 0$  and  $e(Y) = 24/2 = 12$ , the index of  $H_Y$  equals  $-8$ . Then apply the classification of even unimodular lattices given in Section 2.4.

Since the induced quotient map  $\pi : X \rightarrow Y$  is unramified of degree 2, there is an isometric embedding  $\pi^* H_Y(2) \hookrightarrow H^2(X)$ . By Proposition A.6.2 the image is  $H^2(X)^G$ . Since  $H_Y(2) \simeq U(2) \oplus E_8(-2)$ , we see that the signature of  $H^2(X)^G$  equals  $(1, 9)$ . The discriminant being equal to  $2^{10}$ , formula (20.13) shows that  $c = 10$ . It then follows that  $a = 0$  and hence  $b = 2$ .

The case of a symplectic involution is slightly more involved. As for Kummer surfaces (see Appendix B.3), the involution on  $X$  extends to the blow-up in the 8 fixed points with quotient a K3 surface  $\tilde{Y}$ . The primitive closure of the lattice spanned by the 8 nodal curves on  $\tilde{Y}$  is a Nikulin lattice  $\Lambda_{\text{Nik}}$ . Hence for  $Y = X/G$  we have  $b_2(Y) = 22 - \text{rank}(\Lambda_{\text{Nik}}) = 22 - 8 = 14$ . By Proposition 5.2.10 the discriminant group of the Nikulin lattice is isomorphic to  $\oplus^6 \mathbb{Z}/2\mathbb{Z}$ . Hence, by Example 20.9.7 the discriminant group of  $H^2(X)^G$  is isomorphic to  $\oplus^8 \mathbb{Z}/2\mathbb{Z}$  and so  $c = 8$ . By Lemma 20.5.2 it then follows that  $a = 6$  and hence  $b = 0$ . Let  $\tilde{X}$  be the blow-up of  $X$  in the 8 fixed points of  $g$ . The signature of  $H^2(\tilde{X})^G$  equals  $(3, 19)$ , the same as that of  $H^2(\tilde{Y})$ . Indeed, over  $\mathbb{Q}$  these have the same intersection forms. By Lemma B.5.2,  $H^2(\tilde{X}) \simeq H^2(X) \oplus \oplus^8 \langle -1 \rangle$ . The exceptional curves are  $G$ -stable and so the signature of  $H^2(X)^G$  is indeed equal to  $(3, 11)$ .  $\square$

**20.5.C On Involutions and Transcendental Lattices.** In this subsection we consider Hodge-theoretic aspects of the action of an involution on a Kähler surface  $X$ . This involves  $\text{Trs}(X)$ , the transcendental lattice of  $X$ , which, we recall (cf. Appendix B.2), is the smallest primitive sublattice  $T'$  of the intersection lattice of  $X$  such that  $H^{2,0}(X) \subset T' \otimes \mathbb{C}$ . Indeed, the main result is Proposition 20.5.5. It plays a central role in subsequent sections, e.g., in the study of Kummer surfaces in Section 20.6 and of Inose–Shioda structures in Section 20.8. For this reason, we broaden our view and let  $X$  be any Kähler surface admitting an involution  $g$  with finite (possibly empty) fixed point set  $\Sigma$ . As before, we set

$$\begin{aligned} \pi & : X \rightarrow Y = X/G, \quad G = \{1, g\}, \\ \tilde{X} & = \text{the blow-up of } X \text{ at } \Sigma. \end{aligned}$$

The fixed points of  $g$  give ordinary double points on  $Y$  and  $g$  extends to  $\tilde{X}$  with quotient  $\tilde{Y}$ , a resolution of the singularities of  $Y$ . The exceptional curves on  $\tilde{X}$  map to  $(-2)$ -curves under the canonical morphism

$$\tilde{\pi} : \tilde{X} \rightarrow \tilde{Y} = \tilde{X}/G.$$

The Gysin map  $\tilde{\pi}_! : H^2(\tilde{X}) \rightarrow H^2(\tilde{Y})$  is the map Poincaré dual to the induced map in 2-homology<sup>2</sup> and preserves the Hodge decomposition (see e.g. [186, Lemma 1.19]). By Lemma B.5.2,  $H^2(X)$  is a direct summand of  $H^2(\tilde{X})$  and so  $\tilde{\pi}_!|_{H^2(X)}$  also preserves the Hodge decomposition. The main result now reads as follows:

**Proposition 20.5.5.** *Let  $X$  be a Kähler surface admitting an involution  $g$ , and let  $G = \{1, g\}$  and  $\tilde{\pi} : \tilde{X} \rightarrow \tilde{Y}$  as above.*

1. *If all holomorphic 2-forms are invariant under  $g$ , then  $\text{Trs}(X) \subset H^2(X)^G$ .*
2. *If, moreover,  $L$  is a primitive sublattice of  $H^2(X)^G$  such that  $\text{Trs}(X) \subset L$  and such that  $\tilde{\pi}_!L$  is primitive in  $H^2(\tilde{Y})$ , then  $\tilde{\pi}_! : \text{Trs}(X)(2) \xrightarrow{\sim} \text{Trs}(\tilde{Y}) = \text{Trs}(Y)$  is an isometry.*

*Proof.* The assumption on holomorphic 2-forms means  $H^{2,0}(X) \subset H^2(X, \mathbb{C})^G$ . Since  $\text{Trs}(X)$  is the smallest primitive sublattice of  $H^2(X)$  such that  $H^{2,0}(X) \subset \text{Trs}(X) \otimes \mathbb{C}$ , also  $\text{Trs}(X) \subset H^2(X)^G$ , proving the first assertion.

To show the second assertion, we first claim that the assumption that  $\tilde{\pi}_!L$  is primitive in  $H^2(\tilde{Y})$  implies that  $\tilde{\pi}_! \text{Trs}(X)$  is also primitive in  $H^2(\tilde{Y})$ . To prove this, suppose that for some  $x \in H^2(\tilde{Y})$  and some positive integer  $k$  one has  $kx = \tilde{\pi}_!t \in \tilde{\pi}_!L$  for some  $t \in \text{Trs}(X)$ . Then  $x = \tilde{\pi}_!x'$  for some  $x' \in H^2(\tilde{Y})$  and some positive integer  $k$  one has  $kx = \tilde{\pi}_!t \in$ , and so, since  $\tilde{\pi}_!$  is injective,  $t = kx'$ . But by primitivity of  $\text{Trs}(X)$ , we then have  $x' \in \text{Trs}(X)$  and so  $kx = k\tilde{\pi}_!x'$ . Since  $H^2(X)$  has no torsion,  $x = \tilde{\pi}_!x'$  and so we have shown primitivity.

As a consequence,  $\tilde{\pi}_! \text{Trs}(X) \subset \text{Trs}(\tilde{Y})$  is an inclusion of primitive sublattices of  $H^2(\tilde{Y})$  of the same rank and so  $\tilde{\pi}_! \text{Trs}(X) = \text{Trs}(\tilde{Y})$ . On the other hand, making use of item 1, by Lemma 20.9.3 in the Appendix to this chapter, we have an isometry  $\tilde{\pi}_! : L(2) \xrightarrow{\sim} \tilde{\pi}_!L$ . Hence  $\tilde{\pi}_!$  sends  $\text{Trs}(X)(2)$  isometrically to  $\tilde{\pi}_! \text{Trs}(X) = \text{Trs}(\tilde{Y})$ .  $\square$

<sup>2</sup>See page 399 in the appendix to this chapter.

### 20.6 Kummer Surfaces Revisited

**20.6.A The Kummer Involution.** We recall (cf. Appendix B.3) that a K3 surface  $Y$  is a Kummer surface if it is the minimal resolution of the quotient of a complex 2-torus  $X$  under the standard involution. We have used coding theory in Subsection 5.2 to show that  $Y$  is Kummer if and only if it contains a set  $\mathcal{C}$  of 16 disjoint nodal curves (cf. Proposition 5.2.7). Then the primitive closure  $N_{\mathcal{C}}$  of their span in  $H^2(Y, \mathbb{Z})$  is isometric to the Kummer lattice  $\Lambda_{\text{Kum}}$  associated to the code  $D_5 = E^1(\mathbb{F}_2^4)$  of affine linear functions on a four-dimensional  $\mathbb{F}_2$ -vector space. Hence we obtain a primitive embedding  $\Lambda_{\text{Kum}} \subset \text{NS}(Y)$  fitting in the commutative diagram

$$\begin{CD} N_{\mathcal{C}} @>>> H^2(Y, \mathbb{Z}) \\ @V \simeq VV @VV \varphi \simeq V \\ \Lambda_{\text{Kum}} @>>> \Lambda_{\text{K3}} \end{CD}$$

The essential information about the Kummer lattice is summarized as follows.

- Proposition 20.6.1.** *1. The discriminant quadratic form of the Kummer lattice is isometric to  $((\mathbb{Z}/2\mathbb{Z})^6, \oplus^3 u_1)$ .*
- 2. The orthogonal complement of  $\Lambda_{\text{Kum}}$  in the K3-lattice is isometric to  $\oplus^3 U(2)$ .*
- 3. The embedding  $\Lambda_{\text{Kum}} \hookrightarrow \Lambda_{\text{K3}}$  is unique up to an isometry of the K3 lattice.*

*Proof.* 1. By Lemma 5.2.6 the Kummer lattice  $\Lambda_{\text{Kum}}$  is a 2-elementary lattice of type I with discriminant group  $\oplus^6 \mathbb{Z}/2\mathbb{Z}$ . Its signature mod 8 is 0. Since the discriminant quadratic form is  $\mathbb{Z}/2\mathbb{Z}$ -valued, applying Proposition 14.6.3.2 to the indefinite lattice  $\Lambda_{\text{Kum}} \oplus U$  with the same discriminant quadratic form, one deduces the isometry  $q_{\Lambda_{\text{Kum}}}^{\#} \simeq \oplus^3 u_1$ .

2. The orthogonal complement of the Kummer lattice has index 0 and rank 6 and by Proposition 15.1.3 the discriminant form is  $-q_{\Lambda_{\text{Kum}}}^{\#} \simeq \oplus^3 u_1$ . The lattice  $\oplus^3 U(2)$  has the same signature and discriminant form as  $\Lambda_{\text{Kum}}^{\perp}$  and hence belongs to the same genus. By Theorem 14.4.2 (and case 2 of Theorem 14.2.5) this genus contains only one isometry class. The result then follows. <sup>3</sup>

3. Since the discriminant form of the Kummer lattice splits off  $u_1$  and no rank 1 quadratic torsion form does, we can apply Witt’s extension theorem 15.1.7 together with Theorem 14.5.5 with  $S = \Lambda_{\text{Kum}}$  and  $T = S^{\perp} \simeq \oplus^3 U(2)$ . The conditions on  $T$  required to apply the last theorem are satisfied as we just saw in the proof of item 2. □

This has a surprising consequence:<sup>4</sup>

**Corollary 20.6.2** ([168]). *A K3 surface cannot have more than 16 disjoint nodal curves. A singular K3 surface embedded as a degree  $d$  surface in projective space*

<sup>3</sup>There is also a geometric argument (cf. [15, Ch. VIII.5]) to prove that  $\Lambda_{\text{Kum}}^{\perp} \simeq \oplus^3 U(2)$ .

<sup>4</sup>For a proof using coding theory, see [185].

with  $d \not\equiv 0 \pmod{4}$  and whose singularities are at most ordinary double points can have at most 15 of these.

*Proof.* Suppose  $X$  is a K3 surface with  $> 16$  disjoint nodal curves. As we recalled, by Proposition 5.2.7 any 16 among these curves arise from the nodes of a Kummer surface and the primitive sublattice of  $\text{NS}(X)$  they span is isometric to the Kummer lattice  $\Lambda_{\text{Kum}}$ . By Proposition 20.6.1 the orthogonal complement is isometric to  $\oplus^3 U(2)$ . Classes of remaining nodal curves belong to this lattice. This is a contradiction since the self-intersection of any element of  $\oplus^3 U(2)$  is divisible by 4.

If  $X \rightarrow \bar{X} \subset \mathbb{P}^n$  acquires double points, any hyperplane section not passing through them corresponds to a class  $h \in H^2(X, \mathbb{Z})$  orthogonal to the corresponding nodal classes. Hence, if  $\bar{X}$  would have 16 double points, then  $h \in \Lambda_{\text{Kum}}^\perp$  and  $d = h \cdot h \equiv 0 \pmod{4}$ , from which the last assertion follows.  $\square$

**20.6.B Characterizing Kummer surfaces.** If  $X$  is a complex two-torus, we denote by  $Y = \text{Km}(X)$  the associated (smooth) Kummer surface and by  $\pi' : X \dashrightarrow Y$  the canonical rational 2-to-1 map. In this section we establish a characterization of Kummer surfaces in terms of the Néron–Severi lattice and the transcendental lattice. We need an auxiliary Hodge-theoretic result.

**Lemma 20.6.3.** *Suppose that  $L = \oplus^3 U$  has a rank 2 Hodge structure of K3 type.<sup>5</sup> Then there is a complex 2-torus  $X$  and an isometry  $H^2(X, \mathbb{Z}) \xrightarrow{\sim} L$  preserving the Hodge structure.*

*Proof.* Let  $\{e_i, f_i\}$  be the standard basis of the  $i$ -th copy of  $U$  in  $L = \oplus^3 U$ ,  $i = 1, 2, 3$ . Suppose the Hodge structure is given by the non-zero  $(2, 0)$ -class  $\omega = \sum_{i=1}^3 a_i e_i + b_i f_i \in L_{\mathbb{C}}$ . It satisfies the two conditions  $\omega \cdot \omega = 0$  and  $\omega \cdot \bar{\omega} > 0$ , which translate as

$$a_1 b_1 + a_2 b_2 + a_3 b_3 = 0, \quad \text{Re}(a_1 \bar{b}_1 + a_2 \bar{b}_2 + a_3 \bar{b}_3) > 0. \quad (20.14)$$

Without loss of generality we may assume that  $a_1 \neq 0$  and so, by scaling  $\omega$ , we can also choose  $a_1 = 1$ . Let  $\{\epsilon_1, \epsilon_2\}$  be the standard basis of  $\mathbb{C}^2$ . We claim that for the 2-torus  $X$  we can take  $\mathbb{C}^2/\Gamma$ , where  $\Gamma = \mathbb{Z}\epsilon_1 + \mathbb{Z}\epsilon_2 + \mathbb{Z}(-b_3\epsilon_1 + a_2\epsilon_2) + \mathbb{Z}(b_2\epsilon_1 + a_3\epsilon_2)$ .

First we show that the four generators  $\gamma_1, \gamma_2, \gamma_3, \gamma_4$  of the lattice are linearly independent over  $\mathbb{R}$ . Writing  $a_k = t_k + iu_k$ ,  $b_k = v_k + iw_k$ ,  $k = 1, 2, 3$ , with real  $t_k, u_k, v_k, w_k$ , The four generators in the basis  $\epsilon_1, i\epsilon_1, \epsilon_2, i\epsilon_2$  give the columns of the matrix

$$\begin{pmatrix} 1 & 0 & -v_3 & v_2 \\ 0 & 0 & -w_3 & w_2 \\ 0 & 1 & t_2 & t_3 \\ 0 & 0 & u_2 & u_3 \end{pmatrix}$$

and so linear independence over  $\mathbb{R}$  comes down to  $u_2 w_2 + u_3 w_3 \neq 0$ . This is a consequence of (20.14):

$$\begin{aligned} 0 &= \text{Re}(b_1 + a_2 b_2 + a_3 b_3) = v_1 + t_2 v_2 - u_2 w_2 + t_3 v_3 - u_3 w_3 \\ 0 &< \text{Re}(\bar{b}_1 + a_2 \bar{b}_2 + a_3 \bar{b}_3) = v_1 + t_2 v_2 + u_2 w_2 + t_3 v_3 + u_3 w_3. \end{aligned}$$

<sup>5</sup>See Definition B.4.1.3.

Next, we turn to the Hodge structure which is induced from the non-zero holomorphic 2-form  $dz_1 \wedge dz_2$  on  $\mathbb{C}^2$  and on  $X$  (here,  $z_1, z_2$  are coordinates on  $\mathbb{C}^2$ ). Note first that in general, if  $\Gamma$  is generated by the vectors  $v_1, v_2, v_3, v_4$ , with dual basis  $u^i$ , then

$$dz_1 \wedge dz_2 = \sum_{i < j} \det(v_i v_j) u^i \wedge u^j,$$

where  $\det(v_i v_j)$  is shorthand for the 2 by 2 matrix containing the coefficients of  $v_i$  (resp.  $v_j$ ) with respect to the standard basis of  $\mathbb{C}^2$  in the first (resp. second) column. In our case, using the shorthand  $\gamma_{ij} = \gamma_i \wedge \gamma_j$ , and  $\gamma_{ij}^*$  for their duals, the ordered basis

$$\gamma_{12}^*, \gamma_{34}^*, \gamma_{13}^*, \gamma_{42}^*, \gamma_{14}^*, \gamma_{23}^*$$

gives an identification with  $\oplus^3 U$ , since the intersection product is essentially the wedge product. For instance  $\gamma_{12}^* \cdot \gamma_{34}^* = \gamma_1^* \wedge \gamma_2^* \wedge \gamma_3^* \wedge \gamma_4^*$  corresponds to 1.

We next have to express the cohomology class of  $dz_1 \wedge dz_2$  in terms of the (complexified) basis of  $\wedge^2 \Gamma^*$ :

$$\begin{aligned} dz_1 \wedge dz_2(\gamma_{12}) &= 1 & dz_1 \wedge dz_2(\gamma_{13}) &= a_2 & dz_1 \wedge dz_2(\gamma_{14}) &= a_3 \\ dz_1 \wedge dz_2(\gamma_{23}) &= b_3 & dz_1 \wedge dz_2(\gamma_{24}) &= -b_2 & dz_1 \wedge dz_2(\gamma_{34}) &= -a_3 b_3 - a_2 b_2 = b_1. \end{aligned}$$

Then  $dz_1 \wedge dz_2 = \gamma_1^* \wedge \gamma_2^* + b_1 \gamma_3^* \wedge \gamma_4^* + a_2 \gamma_{13}^* + b_2 \gamma_{24}^* + a_3 \gamma_{14}^* + b_3 \gamma_{23}^*$ . So the isometry  $\oplus^3 U \rightarrow H^2(X, \mathbb{Z})$  sending  $e_1$  to  $\gamma_{12}^*$ , etc., is a Hodge isometry, sending  $\omega$  to  $dz_1 \wedge dz_2$ .  $\square$

**Proposition 20.6.4.** 1. A K3 surface  $Y$  is a Kummer surface if and only if the following conditions hold simultaneously <sup>6</sup>:

- (a)  $\text{Trs}(Y)$  embeds primitively in  $\oplus^3 U(2)$ ;
- (b) the abstract Kummer lattice  $\Lambda_{\text{Kum}}$  embeds primitively in  $\text{NS}(Y)$ .

If this is the case, say  $Y = \text{Km}(X)$ , then there is an isometry  $\text{Trs}(Y) \simeq \text{Trs}(X)(2)$ .

- 2.  $Y = \text{Km}(X)$  is an algebraic Kummer surface if and only if there exists an even lattice  $T'$  such that  $\text{Trs}(Y) \simeq \oplus^e U(2) \oplus T'(2)$ , where  $e = \max(0, k-1)$ , and  $(2, k)$  is the signature of  $\text{Trs}(Y)$ .

*Proof.* 1. First we discuss the "only if" part. If  $X$  is a two-torus,  $H^2(X, \mathbb{Z})$  can be identified with the lattice  $L = \oplus^3 U$  and  $\text{Trs}(X) \subset L$ . Let  $Y = \text{Km}(X)$  and let  $X \dashrightarrow Y$  be the rational double cover as in diagram (20.19). The Gysin homomorphism  $H^2(\tilde{X}, \mathbb{Z}) \rightarrow H^2(Y, \mathbb{Z})$  induces a homomorphism  $\pi_1 : H^2(X, \mathbb{Z}) \rightarrow H^2(Y, \mathbb{Z})$  since the cohomology of the blow-up  $\tilde{X}$  splits off  $H^2(X, \mathbb{Z})$  as a direct orthogonal summand. The Kummer involution acts on  $H^2(X, \mathbb{Z})$  as the identity and so Lemma 20.9.3 implies that  $\pi_1 H^2(X, \mathbb{Z}) \simeq L(2)$ . Since the Kummer involution also acts as the identity on the transcendental lattice,  $\pi_1 \text{Trs}(X)(2) = \text{Trs}(Y)$ . Hence  $\text{Trs}(Y) \subset L(2)$ . Clearly (b) holds since the Kummer lattice embeds in  $H^2(Y, \mathbb{Z})$ .

<sup>6</sup>In the algebraic case, or if the Néron-Severi lattice is negative definite, these two conditions are equivalent.

For the converse observe that the above argument shows that assumption (a) implies that the lattice  $L(2)$  inherits a K3-type Hodge structure whose transcendental lattice is the image of  $\text{Trs}(Y)$  in  $L(2)$ . This Hodge structure induces one on  $L$  with transcendental lattice  $\text{Trs}(Y)(\frac{1}{2})$ . By Lemma 20.6.3 there is a complex torus  $X$  with  $\text{Trs}(X) = \text{Trs}(Y)(\frac{1}{2})$ . We shall show that the Kummer surface  $Y' = \text{Km}(X)$  is isomorphic to  $Y$  by constructing a Hodge isometry  $\lambda : H^2(Y', \mathbb{Z}) \xrightarrow{\sim} H^2(Y, \mathbb{Z})$  and applying the global Torelli theorem 19.2.1.

As before, there is a rational map  $\pi' : X \dashrightarrow Y'$  inducing a homomorphism  $\pi'_* : H^2(X, \mathbb{Z}) \rightarrow H^2(Y', \mathbb{Z})$  with image a sublattice of  $H^2(Y', \mathbb{Z})$  isometric to  $L(2)$ . By Proposition 5.2.7 the Kummer lattice is isometric to  $\Lambda_{\text{Kum}}$ . It is orthogonal to  $\text{Im}(\pi'_*)$ . Since  $\text{disc}(\Lambda_{\text{Kum}}) = 2^6 = \text{disc}(L(2)) = \text{disc}(\text{Im}(\pi'_*))$ , the orthogonal complement of the Kummer lattice coincides with  $\text{Im}(\pi'_*)$  and so is primitively embedded in  $H^2(Y', \mathbb{Z})$ .

Now pass to the  $Y$ -side. By assumption (b)  $\Lambda_{\text{Kum}}$  embeds primitively in  $\text{NS}(Y)$  and  $\text{NS}(Y)$  embeds primitively in  $H^2(Y, \mathbb{Z})$ ,  $\Lambda_{\text{Kum}}$  embeds primitively in the K3-lattice. Its orthogonal complement is isometric to  $L(2)$ . This follows since by Corollary 14.4.4  $L(2)$  is the unique lattice in its genus up to isometry (because  $6 < \frac{1}{2}(6^2 + 1)$ ). We now can define primitive embeddings  $\sigma : \Lambda_{\text{Kum}} \hookrightarrow H^2(Y, \mathbb{Z})$  by sending the Kummer lattice of  $Y'$  to its image in  $\text{NS}(Y)$  under the given embedding, and  $\tau : L(2) \hookrightarrow H^2(Y, \mathbb{Z})$  by identifying  $\sigma(\Lambda_{\text{Kum}})^\perp$  with  $\pi'_*H^2(X, \mathbb{Z})$ , the copy of  $L(2)$  which contains  $\text{Trs}(Y)$ . By Proposition 14.5.1 the reduction morphism  $r_T : \mathcal{O}(T) \rightarrow \mathcal{O}(\text{dg}_T)$ ,  $T = \Lambda_{\text{Kum}}$ , is surjective and so, after possibly changing  $\sigma$  by an isometry of  $\Lambda_{\text{Kum}}$  (so that we still have  $\Lambda_{\text{Kum}} \subset \text{NS}(Y)$ ), the embedding  $\sigma \oplus \tau$  extends to an isometry  $\lambda : H^2(Y', \mathbb{Z}) \xrightarrow{\sim} H^2(Y, \mathbb{Z})$ . By construction,  $\lambda$  sends  $\text{Trs}(Y') \subset H^2(Y', \mathbb{Z})$  to  $\text{Trs}(Y) \subset H^2(Y, \mathbb{Z})$  and hence  $\lambda$  is a Hodge isometry which finishes the proof that  $Y \simeq Y'$ .

To show the final assertion that  $\text{Trs}(X)(2) \simeq \text{Trs}(Y)$ , observe that by Proposition 20.5.5  $\pi'_*\text{Trs}(X)(2) \simeq \text{Trs}(Y')$  and that  $\lambda(\text{Trs}(Y')) = \text{Trs}(Y)$ .

2. In the algebraic situation the signature of  $\text{Trs}(Y)$  is  $(2, k)$  for some  $k \in \mathbb{Z}_{\geq 0}$ . Also  $\text{Trs}(Y) \simeq \text{Trs}(X)(2)$ , and so we may apply Example 15.2.5 to  $\text{Trs}(X)$  which implies the desired result for  $\text{Trs}(Y)$ . □

## 20.7 Nikulin Involutions Revisited

In this section  $H^2(-)$  is integral cohomology and  $\Lambda$  stands for the K3 lattice.

Recall that a Nikulin involution is the same as a symplectic involution. Our first goal is to show that its induced action in cohomology (after an appropriate choice of marking) corresponds to the *lattice Nikulin involution*  $\iota_{\text{Nik}}$  defined as

$$\begin{aligned}
 V \oplus E_8(-1) \oplus E_8(-1) &\xrightarrow{\iota_{\text{Nik}}} V \oplus E_8(-1) \oplus E_8(-1), & V &:= \bigoplus^3 U, \\
 (v, e, e') &\mapsto (v, e', e).
 \end{aligned}
 \tag{20.15}$$

The invariant part is isometric to  $V \oplus E_8(-2)$  and the anti-invariant part is isometric to  $E_8(-2)$ .

We can now make our first goal precise:

**Proposition 20.7.1.** *Let  $X$  be a K3 surface admitting a Nikulin involution  $\iota$  and let  $G$  be the cyclic group generated by this involution. Then there is a commutative diagram*

$$\begin{array}{ccc}
 H^2(X) & \xrightarrow[\lambda]{\sim} & \Lambda \\
 \downarrow \iota & & \downarrow \iota_{\text{Nik}} \\
 H^2(X) & \xrightarrow[\lambda]{\sim} & \Lambda.
 \end{array} \tag{20.16}$$

*In other words, a K3 surface with a Nikulin involution admits a marking which turns this involution into a lattice Nikulin involution. Its period point belongs to  $D(\Lambda^G)$ , and<sup>7</sup>  $H^2(X)^G \simeq \Lambda^G = \mathbb{Q}^3 U \oplus E_8(-2)$ .*

*A K3 surface  $X$  with period point in  $D(\Lambda^G)$  admits a Nikulin involution which is, up to conjugation by an element of  $W^-(X)$ , induced by the lattice Nikulin involution  $\iota_{\text{Nik}}$  as in (20.16). If the period point is general,  $\text{NS}(X) \simeq \Lambda_G \simeq E_8(-2)$ .*

*Proof.* Let  $X$  be a K3 surface with a Nikulin involution  $\iota$ . Proposition 20.5.4 states that  $H^2(X, \mathbb{Z})^G$  has signature  $(3, 11)$  and discriminant group  $\mathbb{Q}^8 \mathbb{Z} / 2\mathbb{Z}$ . Then its orthogonal complement, the anti-invariant sublattice of  $H^2(X, \mathbb{Z})$ , say  $M$ , has signature  $(0, 8)$  and discriminant group  $M^*/M = \mathbb{Q}^8 \mathbb{Z} / 2\mathbb{Z}$ .

We first show that  $M$  is isometric to  $E_8(-2)$ , the anti-invariant lattice for the lattice Nikulin involution. To start, since  $M$  is 2-elementary, Lemma 14.6.1 shows that its 2-adic localization is of the form  $M_2 = M^{(1)}(2)$  with  $M^{(1)}$  unimodular. Then  $M_2 = 2M_2^*$  and so (since  $M$  is 2-elementary) also  $M = 2M^*$ . This implies that  $M = M'(-2)$  with  $M'$  unimodular. By the classification of rank 8 positive definite unimodular lattices given in [119] either  $M' \simeq \mathbb{Q}^8 \langle 1 \rangle$  or  $M' \simeq E_8$ . In the first case  $M \simeq \mathbb{Q}^8 \langle -2 \rangle$  which contradicts Proposition 20.2.2 (the anti-invariant lattice under a symplectic isometry does not contain roots). Having shown this,  $H^2(X, \mathbb{Z})^G$ , the orthogonal complement of  $M$ , has discriminant form isometric to that of  $V \oplus E_8(-2) = \mathbb{Q}^3 U \oplus E_8(-2)$ , the invariant lattice of  $\iota_{\text{Nik}}$ . Since  $H^2(X, \mathbb{Z})^G$  and  $\Lambda^G$  have the same rank, index and discriminant form, they are in the same genus, and so they are isometric by Corollary 14.4.3.

Next, observe that by Lemma 17.2.2 the group  $\text{O}(E_8(-2)) = \text{O}(E_8)$  is generated by reflections. By Lemma 16.1.1 these induce the identity on the discriminant group. So by Proposition 15.1.6 one has a commutative diagram (20.16), as asserted.

For the second part of the proof, we show the existence of a Nikulin involution on a K3 surface  $X$  with period point  $[\eta] \in D(\Lambda^G)$ . Via the marking  $\text{NS}(X)$  contains a lattice isometric to  $\Lambda_G$ , and the induced lattice involution  $\iota$  on cohomology preserves  $H^{2,0}(X)$ . To see that  $\iota$  comes from a surface involution, we apply Criterion 20.2.1. Since the invariant part of  $H^2(X, \mathbb{R})$  has signature  $(3, 11)$ , it contains the light cone and there exists a Kähler class invariant under the involution.

<sup>7</sup>This also confirms the first entry in Table 20.9.1.

Lastly, the anti-invariant sublattice of  $H^2(X, \mathbb{Z})$  does not contain roots, since it is isometric to  $E_8(-2)$ . The criterion then implies that  $\iota$  is conjugate (under  $W^-(X)$ ) to a linear map on cohomology induced by an involution on  $X$  which is necessarily symplectic, that is, a Nikulin involution.  $\square$

Observe that the corresponding period domain  $D(\Lambda^G)$  as an open subset of a quadric in  $\mathbb{P}(\Lambda^G)$  has dimension 12. The Néron–Severi group of a K3 surface with period point in this period domain contains  $E_8(-2)$  and generally one has  $\text{NS}(X) \simeq E_8(-2)$  so that such surfaces are generally non-algebraic. The algebraic ones belong to countably many irreducible families of dimension 11 as we shall show now. First we determine the candidate Néron–Severi lattices.

**Proposition 20.7.2** ([83, §2]). *Fix a positive integer  $k$  and let  $N_k = E_8(-2) \oplus \langle 2k \rangle$ . For even  $k$  it has an up to isometry unique index 2 even overlattice, say  $N'_k$ , which contains  $E_8(-2)$  and  $\langle 2k \rangle$  primitively. For  $k$  odd there are no such overlattices.*

*Proof.* We shall employ the technique of overlattices as explained in Sections 1.7.C and 15.1. We set  $N = E_8(-2) \oplus \mathbb{Z} \cdot f$  with  $f \cdot f = 2k$ . An order 2 isotropic subgroup  $I$  of  $N^*/N$  (with respect to the discriminant bilinear form) corresponds to an overlattice  $L$  with  $N$  as index 2 sublattice and vice versa. Given  $I$ , the corresponding overlattice admits both  $E_8(-2)$  and  $\mathbb{Z} \cdot f$  as primitive sublattices provided the intersections of  $I$  with  $\text{dg}_{E_8(-2)}$  and  $\text{dg}_{\mathbb{Z} \cdot f}$  are zero. Since  $\text{dg}_{E_8(-2)} \simeq \oplus^8 \mathbb{Z}/2\mathbb{Z}$  is 2-torsion,  $I$  is then generated by an element of the form  $\frac{1}{2}e + \frac{1}{2}f + N$ , where  $e \in E_8(-2)$  is such that  $\frac{1}{2}e \notin N$ .

For an overlattice to be even, we use the discriminant quadratic form  $q^\#$  on  $I$ . Observe that  $q^\#(\frac{1}{2}f + N) \equiv \frac{k}{4} \pmod{\mathbb{Z}}$  and that  $q^\#(\frac{1}{2}e + N) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ . So  $I$  is isotropic with respect to  $q^\#$  if and only if  $q^\#(\frac{1}{2}e + N) + \frac{k}{4} \equiv 0 \pmod{\mathbb{Z}}$ . Since  $q^\#(\frac{1}{2}e + N)$  is either  $0 \pmod{\mathbb{Z}}$  or  $\frac{1}{2} \pmod{\mathbb{Z}}$ ,  $k$  must be even. Moreover, if  $k \equiv 0 \pmod{4}$ , then  $q^\#(\frac{1}{2}e + N) \equiv 0 \pmod{\mathbb{Z}}$ , i.e.,  $e \cdot e \equiv 0 \pmod{8}$ , and if  $k \equiv 2 \pmod{4}$ , then  $q^\#(\frac{1}{2}e + N) \equiv \frac{1}{2} \pmod{\mathbb{Z}}$ , that is,  $e \cdot e \equiv 4 \pmod{8}$ . If  $k$  is odd, there are no even index 2 overlattices.

In the case where  $k \equiv 0 \pmod{4}$  and  $q^\#(\frac{1}{2}e + N) \equiv 0 \pmod{\mathbb{Z}}$ , we show that all such vectors  $\frac{1}{2}e + N$  are in the same  $\text{O}(\text{dg}_N)$ -orbit. It suffices to observe that the vectors  $\frac{1}{2}e + E_8(-2)$  are in the same  $\text{O}(\text{dg}_{E_8(-2)})$ -orbit, and this follows from an extension of the Witt extension theorem mentioned in Remark 7.2.9 (or from detailed knowledge of the inner product space  $E_8(-2)/2E_8(-2)$ ). The case where  $k \equiv 2 \pmod{4}$  and  $q^\#(\frac{1}{2}e + N) \equiv \frac{1}{2} \pmod{\mathbb{Z}}$  is handled in a similar way. It then follows that elements of the form  $\frac{1}{2}e + \frac{1}{2}f + N$  are in the same orbit as well in each of the two cases.

Finally, we prove that in each of the two cases the resulting overlattices are isometric. Here we use that the natural homomorphism  $\text{O}(N) \rightarrow \text{O}(\text{dg}_N)$  is surjective by Theorem 14.5.5 14.5.5 and Proposition 10.2.2 10.2.2, so that for each isometry in  $\text{O}(\text{dg}_N)$  taking an isotropic subgroup to another one, there exists a lift in  $\text{O}(N)$  relating the corresponding overlattices.  $\square$

We shall now show, following [83], that the algebraic K3 surfaces admitting a Nikulin involution have a moduli space of dimension  $20 - 9 = 11$ , where 9 is the rank of the Néron–Severi group of the general such K3 surface. The nature of the



moduli space depends on  $k$ . For each odd number  $k$  the period space is irreducible, for  $k$  even there are two components. The proof uses that by Proposition 19.2.10 each of the lattices  $S = N_k$  or  $S' = N'_k$  can be embedded primitively in the K3 lattice so that we can speak of  $S$ -marked or  $S'$ -marked K3 surfaces. Indeed, the corresponding period domains parametrize the K3 surfaces we are after:

**Proposition 20.7.3.** *Let  $N_k$  (respectively  $N'_k$ ) be primitively embedded in the K3 lattice. The period-domain for  $N_k$ -marked or  $N'_k$ -marked K3 surfaces has dimension 11. With  $G$  the group generated by  $\iota_{\text{Nik}}$ , any of these period domains are cut out in  $D(\Lambda^G)$  by a hyperplane.*

*The general point of  $D(N_k^\perp)$  corresponds to a K3 surface  $X$  with  $\text{NS}(X) \simeq N_k$  and likewise for  $N'_k$ . Any such marked K3 surface admits a Nikulin involution induced by the lattice Nikulin involution  $\iota_{\text{Nik}}$ .*

*Proof.* Let  $\ell$  be a generator of the second summand of  $N_k = E_8(-2) \oplus \langle 2k \rangle$ . Its orthogonal complement in  $N_k$  as well as in  $N'_k$  is the sublattice  $E_8(-2)$  which does not contain  $-2$ -roots. Hence  $\ell \cdot r \neq 0$  for all roots  $r$  in either one of these lattices, i.e.,  $\ell$  belongs to the interior of some Weyl chamber. So, if  $X$  is an  $N_k$ -marked K3 surface or an  $N'_k$ -marked K3 surface, we can adapt the marking in such a way that  $\ell$  is an ample class.

Assume for simplicity that we are in the  $N_k$ -marked case. Then, since the period point of  $X$  is assumed to be general, we may henceforth assume that  $\text{NS}(X)$  corresponds to  $N_k$ . If one defines  $\iota = -\text{id}$  on the first summand  $E_8(-2)$  of  $N_k$  and  $\iota = \text{id}$  on the orthogonal complement of this summand in  $\Lambda_{\text{K3}}$ , it extends to an involution  $\iota$  on  $\Lambda_{\text{K3}}$  by the extension criterion from Theorem 15.1.7 (use that the discriminant group of  $E_8(-2)$  is 2-torsion). Let  $G$  be the order two group generated by  $\iota$ . Under the marking  $\text{Trs}(X) \subset \Lambda^G$ , so that  $G$  preserves the Hodge decomposition. Moreover,  $G$  preserves the ample class  $\ell$ . So by Theorem 19.2.2 the involution  $\iota$  is induced by a unique (symplectic) involution on  $X$ . By Proposition 20.7.1 this implies that  $\iota = \iota_{\text{Nik}}$ , the lattice Nikulin involution. Hence  $D(N_k^\perp) \subset D(\Lambda^G)$ .

The above argument is essentially the same for  $N'_k$ . □

### 20.8 Shioda–Inose structures

In Corollary 5.2.8 we showed that every Kummer surface  $\text{Km}(A)$  (the minimal resolution of the quotient of a complex 2-torus  $A$  by the involution  $j$  sending  $x \in A$  to  $-x$ ) admits a double cover  $\tilde{X}$  with 8 exceptional curves which is the blow-up of a K3 surface  $X$ . Moreover, the covering involution  $\iota$  on  $X$  is a Nikulin involution and  $\tilde{Y} = \text{Km}(A)$  is the minimal resolution of  $X/\iota$ . The resulting diagram

$$\begin{array}{ccccc}
 \begin{array}{c} \curvearrowright \\ X \end{array} & \longleftarrow & \tilde{X} & & A \\
 \downarrow & \dashrightarrow & \downarrow \pi & \dashrightarrow & \downarrow \\
 Y = X/\iota & \longleftarrow & \tilde{Y} = \text{Km}(A) & \longrightarrow & A/j
 \end{array} \tag{20.17}$$

is called a *Shioda–Inose structure*.<sup>8</sup>

Next we abstract from this specific situation to the one described in the appendix to this chapter. By (20.20) the manifold  $X' = X - \Sigma$ , ( $\Sigma$  is the fixed point set of  $\iota$ ), is shown to have the same 2-cohomology as  $X$ . Since  $\pi : X' \rightarrow Y'$ ,  $Y' = Y - \iota(\Sigma)$  is a topological double covering, the transfer homomorphism  $t^* : H^2(X') \rightarrow H^2(Y')$  is well defined. Moreover, the inclusion  $X' \hookrightarrow X$  induces an isomorphism  $H^2(X) \simeq H^2(X')$  and so the transfer homomorphism extends to  $H^2(X)$  and can be identified with the Gysin homomorphism  $\pi_!$ . By Lemma 20.9.3.1 in the appendix to this chapter one has

$$\pi^* \circ \pi_!(x) = x + t^*(x), \quad x \in H^2(X, \mathbb{Z}). \quad (20.18)$$

Let us consider the following lattice theoretic situation involving the abstract Nikulin lattice  $\Lambda_{\text{Nik}}$ , a rank 8 positive definite even lattice of discriminant  $2^6$  (see § 5.2.B). It leads to the left-hand half of the above diagram (20.17), without the condition  $\tilde{Y}$  is a Kummer surface:

**Theorem 20.8.1** ([158, Th. 5.7]). *Let  $(X, \varphi)$  be a marked K3 surface such that  $\varphi^{-1}(\oplus^2 E_8(-1))$  embeds into  $\text{NS}(X)$ . Then with the notation as above*

1. *there is a Nikulin involution  $\iota$  on  $X$  with  $\pi : \tilde{X} \rightarrow \tilde{Y}$ ;*
2. *there exists a primitive embedding  $\Lambda_{\text{Nik}} \oplus E_8(-1) \hookrightarrow \text{NS}(\tilde{Y})$ ;*
3. *The Gysin morphism  $\pi_!$  induces an isometry  $\text{Trs}(X)(2) \xrightarrow{\cong} \text{Trs}(\tilde{Y})$ .*

*Proof.* **1.** The lattice Nikulin involution  $\iota_{\text{Nik}}$  on  $\Lambda_{\text{K3}}$  (see (20.15)) gives an involution on  $H^2(X, \mathbb{Z})$  as follows. Since  $\iota_{\text{Nik}}$  switches the two copies of  $E_8(-1)$  inside  $\Lambda_{\text{K3}}$  and is the identity on its orthogonal complement, via the marking this gives an involution  $\iota'$  on the embedded copy of  $\oplus^2 E_8(-1)$ . We let  $G$  be the group generated by  $\iota'$ . Then the anti-invariant lattice  $(H^2(X))_G = (H^2(X)^G)^\perp$  is isometric to  $E_8(-2)$  and thus does not contain roots. So  $H^2(X)_G \cap \text{NS}(X)$  does not contain roots, that is, condition 3 of Criterion 20.2.1 is fulfilled. Condition 1 holds since  $H^2(X)_G \subset \text{NS}(X)$  and so  $\text{Trs}(X) \subset \text{NS}(X)^\perp \subset H^2(X)^G$ . Condition 2 holds since  $H^2(X)^G$  has signature  $(3, 11)$  and therefore intersects the positive cone. It follows that for some  $w \in W^-(X)$ ,  $w'w^{-1}$  is induced by an involution  $\iota$  on  $X$  which by construction is a Nikulin involution. This shows item 1. Note also that upon replacing the embedding  $\varphi^{-1}$  by  $w \circ \varphi^{-1} : E_8(-1)^{\oplus 2} \hookrightarrow H^2(X, \mathbb{Z})$ , the induced involution  $t^*$  on cohomology acts in a similar way as  $\iota'$ .

**2.** The Nikulin involution on  $X$  has eight isolated fixed points, which on  $\tilde{Y}$  give eight  $(-2)$ -curves and the primitive closure of the span of their classes is a copy of  $\Lambda_{\text{Nik}}$ , the Nikulin lattice, in  $\text{NS}(\tilde{Y})$ . The second summand comes from the two copies of  $E_8(-1)$  in the K3 lattice under the Gysin morphism  $\pi_! : H^2(X, \mathbb{Z}) \rightarrow H^2(\tilde{Y}, \mathbb{Z})$ , as we now show. By construction,  $t^*$  interchanges the two copies of

<sup>8</sup>So named after [211, §3] where this structure has been introduced and studied.

$E_8(-1)$  in  $H^2(X, \mathbb{Z})$ . So if  $x, x'$  belong to the same copy, and hence  $\iota^*(x) \cdot x' = 0$ , then

$$(x + \iota^*(x)) \cdot (x' + \iota^*(x')) = x \cdot x' + \iota^*x \cdot \iota^*x' = 2x \cdot x'.$$

If  $\tau : \tilde{X} \rightarrow X$  is the blowing up in the fixed-point set  $\Sigma$ , then  $\tau^* : H^2(X, \mathbb{Z}) \hookrightarrow H^2(\tilde{X}, \mathbb{Z})$  by Lemma B.5.2. So we may identify  $x$  and  $x'$  with their counterparts in  $H^2(\tilde{X}, \mathbb{Z})$ . By (20.18) one has

$$y = x + \iota(x) = \pi^* \pi_1(x), \quad y' = x' + \iota(x') = \pi^* \pi_1(x'),$$

an equality of  $G$ -invariant elements. Then Lemma 20.9.3.2 implies

$$\pi_1(\pi^* \pi_1 x) \cdot \pi_1(\pi^* \pi_1 x') = \pi_1 y \cdot \pi_1 y' = 2y \cdot y' = 4x \cdot x'.$$

Since  $\pi$  has degree 2,  $\pi_1 \pi^*$  is multiplication by 2 and the left-hand side equals  $4\pi_1 x \cdot \pi_1 x'$ . In other words,  $\pi_1$  is an isometry on each of the two copies of  $E_8(-1)$  in  $H^2(X, \mathbb{Z})$  and maps these to the same sublattice of  $H^2(\tilde{Y}, \mathbb{Z})$ . These map into  $\text{NS}(\tilde{Y})$  since  $\pi_1$  preserves the Hodge structure (see e.g. [186, Lemma 1.19]). Summarizing,  $\text{NS}(\tilde{Y})$  contains a copy of  $\Lambda_{\text{Nik}} \oplus E_8(-1)$ . Since the first summand, the Nikulin lattice, is primitively embedded and the second summand is unimodular, their direct sum is also primitively embedded as claimed, finishing the proof of 2.

**3.** We aim to apply Proposition 20.5.5 in the present situation where

$$\text{Trs}(X) \subset L, \quad L = (\oplus^2 E_8(-1))^\perp \subset H^2(X, \mathbb{Z})^G.$$

Then  $L \simeq V$ . To be able to apply the proposition, we show first that  $\tilde{\pi}_1 L$  is a primitive sublattice of  $H^2(\tilde{Y}, \mathbb{Z})$ . So we introduce

$$M := (\tilde{\pi}_1 L)^\perp.$$

Then  $M^\perp$  is the smallest primitive sublattice of  $H^2(\tilde{Y}, \mathbb{Z})$  containing  $\tilde{\pi}_1 L$ . We wish to show that  $M^\perp = \tilde{\pi}_1 L$ . By the same argument as before,  $\pi_1$  multiplies the intersection form on the invariant part by 2 and so  $\tilde{\pi}_1 L$  is isometric to  $V(2)$  and so has discriminant  $2^6$ . On the other hand, by Lemma 1.2.2 we have

$$\begin{aligned} \text{disc}(\tilde{\pi}_1 L) &= [M^\perp : \tilde{\pi}_1 L]^2 \cdot \text{disc}(M^\perp) \\ &= [M^\perp : \tilde{\pi}_1 L]^2 \cdot \text{disc}(M). \end{aligned}$$

But  $\text{disc}(M) = \text{disc}(\tilde{\pi}_1 L) = 2^6$  and so  $M^\perp = \tilde{\pi}_1 L$ , as asserted. By construction  $\text{Trs}(\tilde{Y}) \subset \tilde{\pi}_1 L$  and so we can indeed apply Proposition 20.5.5 and conclude that  $\pi_1 : \text{Trs}(X)(2) \xrightarrow{\sim} \text{Trs}(\tilde{Y})$ .  $\square$

Using the previous result, one can characterize the Shioda–Inose structures as follows.

**Theorem 20.8.2** ([158, Thm. 6.3]). *Let  $X$  be a K3 surface. Consider the following properties.*

1.  $X$  admits a Shioda–Inose structure;

- 2. there is a complex 2-torus  $A$  with  $\text{Trs}(X) \simeq \text{Trs}(A)$ ;
- 3. there is a primitive embedding  $\text{Trs}(X) \subset \oplus^3 U$ ;
- 4. there is an embedding  $\oplus^2 E_8(-1) \subset \text{NS}(X)$ .

One has the implications  $1 \implies 2 \implies 3$ . If, moreover,  $X$  is algebraic, then  $3 \implies 4 \implies 1$ , and hence in this case all of the above properties are equivalent.

*Proof.*  $1 \implies 2$ : By Theorem 20.8.1,  $\text{Trs}(Y) \simeq \text{Trs}(X)(2)$ , where  $Y$  is the Kummer surface of  $A$  as in the definition of a Shioda–Inose structure. Since also  $\text{Trs}(Y) \simeq \text{Trs}(A)(2)$  we conclude that  $\text{Trs}(X) \simeq \text{Trs}(A)$ .

$2 \implies 3$ : Take  $A$  as in 2. Then, by 2, the natural embedding  $\text{Trs}(A) \subset H^2(A, \mathbb{Z}) \simeq U^{\oplus 3}$  induces  $\text{Trs}(X) \hookrightarrow U^{\oplus 3}$ .

Now assume that  $X$  is algebraic.

$3 \implies 4$ : The given embedding, say  $\varphi$ , extends as  $\varphi \oplus 0 : \text{Trs}(X) \hookrightarrow \Lambda_{K3}$ . Now  $\text{Trs}(X)$  has signature  $(2, k)$ ,  $k \leq 3$ , and thus, by Proposition 19.2.10, it embeds uniquely in  $\Lambda_{K3}$ . This shows that  $\varphi \oplus 0$  gives the canonical embedding  $\text{Trs}(X) \subset H^2(X, \mathbb{Z}) = \oplus^3 U \oplus \oplus^2 E_8(-1)$ , which implies that  $\text{NS}(X)$  contains  $\oplus^2 E_8(-1)$ .

$4 \implies 1$ . By Theorem 20.8.1 there is a Nikulin involution  $\iota : X \rightarrow X$  such that for the rational quotient map  $\pi : X \dashrightarrow Y$  we have  $\pi_! : \text{Trs}(X)(2) \xrightarrow{\simeq} \text{Trs}(Y)$ . Moreover,  $\Lambda_{\text{Nik}} \oplus E_8(-1) \subset \text{NS}(Y)$ . The crucial remarks now are:

- $M = \Lambda_{\text{Nik}} \oplus E_8(-1)$  as well as the Kummer lattice  $\Lambda_{\text{Kum}}$  are negative definite and have the same discriminant form  $u_1^{\oplus 3}$  and so belong to the same genus.
- $\text{NS}(Y)$  has rank  $\geq 16 \geq \frac{1}{2} \text{rank}(L) = 11$  and so, by Corollary 15.2.7, the isometry class of the lattice  $\text{NS}(Y)$  is unique in its genus.

The lattice  $M$  embeds primitively in  $\text{NS}(Y)$  and hence by Corollary 15.1.4 also  $\Lambda_{\text{Kum}}$  embeds primitively in  $\text{NS}(Y)$ . But then  $Y = \text{Km}(A)$ , proving 1. □

We come back to the article [211] by T. Shioda and H. Inose where the structure named after them was introduced. In loc. cit. they applied it to the smallest possible transcendental lattices, those of rank 2. These correspond to positive definite integral quadratic forms. Two such forms are isometric if they are equivalent under conjugation by  $\text{SL}_2(\mathbb{Z})$ . Any K3 surface with a transcendental lattice  $T$  of rank 2 has no moduli and Theorem 20.8.2 implies that these are obtained from an algebraic torus  $A$  via a Shioda–Inose structure. It is shown in [211] that in fact  $A$  is a product of two elliptic curves. Summarizing:

**Corollary 20.8.3.** *A K3-surface  $X$  whose transcendental lattice  $T$  has rank 2 is obtained from a product of two elliptic curves by means of a Shioda–Inose structure. Such surfaces have no moduli and correspond one-to-one to points of the set of isometry classes of positive definite even lattices of rank 2.*

**Example 20.8.4** (Non-Kummer Nikulin quotients and non-algebraic K3 surfaces with a Shioda–Inose structure). By Theorem 19.2.1, there is a K3-surface  $X$  with a marking  $\varphi : H^2(X, \mathbb{Z}) \xrightarrow{\simeq} \Lambda_{K3}$  such that  $\varphi(\text{Trs}(X)) = \oplus^3 U \subset \oplus^3 U \oplus \oplus^2 E_8(-1)$ .

Since  $\text{NS}(X)$  is then negative definite, such K3 surfaces (and all of its quotients by an involution) are not algebraic. We next observe that, since  $\text{NS}(X) \simeq \mathbb{Q}^2 E_8(-1)$ , Theorem 20.8.1 implies that, first of all,  $X$  admits a Nikulin involution with quotient  $Y$  and with  $\text{Trs}(Y) \simeq \mathbb{Q}^3 U(2)$  (so  $Y$  is not algebraic), and, secondly, that  $\text{NS}(Y)$  contains  $\Lambda_{\text{Nik}} \oplus E_8(-1)$ . Note also that  $\text{rank}(\text{NS}(Y)) = \text{rank}(\text{NS}(X)) = 16$  so that the index  $[\text{NS}(Y) : \Lambda_{\text{Nik}} \oplus E_8(-1)]$  is finite. Suppose that there exists a torus  $A$  with  $Y = \text{Km}(A)$ . Since the two-forms are preserved in a Shioda–Inose structure, we would have a Hodge isometry  $H^2(A) \simeq U^{\oplus 3} \simeq \text{Trs}(X)$ . Hence for the Kummer quotient  $Y$ , by Theorem 20.6.4 one would have  $\text{Trs}(Y) = \mathbb{Q}^3 U$  and a primitive embedding  $\Lambda_{\text{Kum}} \subset \text{NS}(Y)$ , which must be an equality since  $\text{disc}(\text{NS}(Y)) = \text{disc}(\text{Trs}(Y)) = 2^6 = \text{disc}(\Lambda_{\text{Kum}})$ . Similarly, since  $\text{disc}(\Lambda_{\text{Kum}}) = 2^6 = \text{disc}(\Lambda_{\text{Nik}})$ , the inclusion  $\Lambda_{\text{Nik}} \oplus E_8(-1) \subset \text{NS}(Y)$  becomes an equality. Since  $\Lambda_{\text{Kum}}$  is clearly indecomposable, it cannot be isometric to  $E_8(-1) \oplus \Lambda_{\text{Nik}}$  and there is no Shioda–Inose structure involving  $Y$ .

On the other hand, there are non-algebraic surfaces admitting a Shioda–Inose structure: just start with a non-algebraic 2-torus. By Corollary 5.2.8 the corresponding Kummer surface is a Nikulin quotient, say of a (necessarily non-algebraic) K3 surface  $X$  and so here is no Shioda–Inose structure involving  $X$ .

We already observed (see Remark 19.2.12.2) that  $T = \mathbb{Q}^3 U$  embeds in two ways into the K3 lattice: the standard embedding with  $T^\perp = \mathbb{Q}^2 E_8(-1)$  and another embedding with  $T^\perp = \Gamma_{16}(-1)$ . The above argument shows that in order for  $X$  to have a Shioda–Inose structure, the first embedding is impossible. This implies that  $D(\mathbb{Q}^3 U) \subset D(\Lambda)$  is the period domain of K3 surfaces admitting a Shioda–Inose structure, where  $T = \mathbb{Q}^3 U \subset \Lambda$  is *not* the standard embedding. The general point represents non-algebraic surfaces, while the algebraic ones are given by countably many hyperplanes in this 4-dimensional period domain.

## 20.9 Appendix: On Surfaces Admitting an Action of a Finite Group

In this section  $X$  is any compact (smooth) complex surface with a faithful action of a finite group  $G$ , and  $\tilde{Y}$  denotes the minimal resolution of  $Y = X/G$ . We write  $H^2(X), H^2(Y), \dots$  to mean integral cohomology while  $H_1(X), H_2(Y), \dots$  stands for integral homology. We relate the intersection lattices of  $X$  and  $\tilde{Y}$ . The main result, Theorem 20.9.6, is quite technical, but it is of crucial importance for applications to K3 surfaces in Section 20.2.

**20.9.A The set-up.** By [35], the action of  $g \in G$  on the tangent space at a fixed point can be linearized which implies that the fixed locus of  $g$  in  $X$  is either empty or a disjoint union of smooth curves and points. The image in  $Y$  of an isolated fixed point of  $g$  acting on  $X$  by definition is a quotient singularity, hence by Proposition 4.5.2, a du Val singularity. We assume that there are only (finitely many) isolated fixed points and we employ the following notation:

- $\sigma : \tilde{Y} \rightarrow Y$ : the minimal resolution of  $Y$ ;

- $\Sigma \subset X$ : the finite set of fixed points of the  $G$ -action;
- $\bar{p} \in Y$ : the image of  $p \in \Sigma \subset X$ , under  $\pi : X \rightarrow Y$ ;
- $\tau : \tilde{X} \rightarrow X$ : a minimal the blow-up of  $X$  in the points of  $\Sigma$  so that  $\pi$  extends as  $\tilde{\pi} : \tilde{X} \rightarrow \tilde{Y}$ ;
- $E_p \subset \tilde{Y}$ : the exceptional divisor over  $\bar{p}$ ;

We gather the information in the following commutative diagram:

$$\begin{array}{ccccc}
 & & \tau & & \\
 & & \curvearrowright & & \\
 X & \xleftarrow{j'} & X' = X - \Sigma & \xlongequal{\quad} & \tilde{X} - \tilde{\pi}^{-1}E \hookrightarrow \tilde{X} \\
 \pi \downarrow & & \downarrow & & \downarrow \tilde{\pi} \\
 Y & \xleftarrow{j} & Y' = X/G - \pi(\Sigma) & \xlongequal{\quad} & \tilde{Y} - E \hookrightarrow \tilde{Y} \\
 & & \sigma & & \\
 & & \curvearrowleft & & 
 \end{array} \tag{20.19}$$

Using the Mayer–Vietoris sequence applied to the open sets  $X - \Sigma$  and a union of balls around the points of  $\Sigma$ , one gets isomorphisms

$$j'^* : H^q(X) \xrightarrow{\sim} H^q(X'), \quad j'^* : H^q(X)^G \xrightarrow{\sim} H^q(X')^G, \quad q = 0, 1, 2. \tag{20.20}$$

Since by Lemma B.5.2 the induced map  $\tau^*$  makes  $H^2(X)$  into a direct summand of  $H^2(\tilde{X})$ , we may and shall consider  $H^2(X)$  as a subgroup of  $H^2(\tilde{X})$ .

Recall that for continuous maps  $f : X \rightarrow Y$  between connected oriented manifolds  $X, Y$  of dimensions  $d, d'$  respectively, the induced maps  $f_* : H_q(X) \rightarrow H_q(Y)$ ,  $q = 0, \dots, d$ , in homology can be combined with the two Poincaré duality isomorphisms  $H_c^q(X) \xrightarrow{\cong} H_{d-q}(X)$  and  $H_c^{d'-(d-q)}(Y) \xrightarrow{\cong} H_{d-q}(Y)$  to give the **Gysin homomorphisms** in (compactly supported) cohomology <sup>9</sup>  $f_! = (D')^{-1} \circ f_* \circ D : H_c^q(X) \rightarrow H_c^{d'-d+q}(Y)$ . See e.g. [50, Ch. VIII §10].

We shall also make use of extensions of the Gysin homomorphisms in the case of regular topological coverings, such as  $\pi : X' \rightarrow Y'$ , the so-called **transfer homomorphisms**  $t^* : H^k(X') \rightarrow H^k(Y')$  and  $t_* : H_k(Y') \rightarrow H_k(X')$ ,  $k \in \mathbb{Z}$ . See e.g. [94, §3.2]. If we compose these with the usual induced maps  $\pi^*$  and  $\pi_*$ , one obtains similar rather obvious identities which we shall state only for cohomology:

**Lemma 20.9.1.** *Let  $\pi : X' \rightarrow Y' = X'/G$  be as above. Then*

1.  $t^* \pi^* : H^k(Y') \rightarrow H^k(X')$  is multiplication by  $n = |G|$ .  
 $\pi_* t_* : H^k(X') \rightarrow H^k(Y')$  is induced by the action of  $\sum_{g \in G} g \in \mathbb{Z}[G]$ .
2.  $\pi^* : H^k(Y') \rightarrow H^k(X')$  has its image in  $H^k(X')^G$ . The kernel of  $\pi^*$  as well as the kernel of  $t^* : H^k(X')^G \rightarrow H^k(Y')$  is  $n$ -torsion.
3. If  $H^k(X')$  is a free  $\mathbb{Z}$ -module, then  $H^k(X')^G$  is the primitive closure of  $\text{Im}(\pi^*)$ .

<sup>9</sup>also called Umkehr homomorphisms.

*Proof.* For the proofs of item 1 we refer to [94, §3.2].

2. Since  $\pi \circ g = \pi$  for every  $g \in G$ , one has  $g^*(\pi^*(y)) = \pi^*(y)$ ,  $y \in H^*(Y')$ , and so  $\pi^*(y)$  is  $G$ -invariant. Item 1 shows that  $\pi^*$  and  $t^*|H^k(X')^G$  are injective modulo  $n$ -torsion.

3. By item 2,  $\text{Im}(\pi^*)$  has the same rank as  $H^k(X')^G$ . So it suffices to show that  $H^k(X')^G$  is a primitive sublattice of  $H^k(X')$ . To see this, observe that if a  $G$ -module  $M$  is without torsion,  $M^G$  is a primitive sublattice of  $M$  since, if for some  $x \in M$  and  $g \in G$  one has  $mx = mg(x) \in M^G$ , then  $x = g(x)$ .  $\square$

*Remark 20.9.2.* If  $X'$  (and hence  $Y'$ ) are oriented compact connected manifolds, the transfer homomorphisms are the same as the Gysin homomorphisms. If  $X'$  and  $Y'$  are oriented but not necessarily compact, the Gysin maps  $\pi_! : H_c^k(X') \rightarrow H_c^k(Y')$  extend the transfer maps, i.e., there is a commutative diagram

$$\begin{array}{ccc} & \xleftarrow{\pi^*} & \\ H^k(X') & \xrightarrow{t^*} & H^k(Y') \\ \uparrow & & \uparrow \\ H_c^k(X') & \xrightarrow{\pi_!} & H_c^k(Y'). \end{array} \quad (20.21)$$

Returning to our setting we have:

**Lemma 20.9.3.** 1. One has  $\tilde{\pi}^* \tilde{\pi}_!(u) = \sum_{g \in G} g^*(u)$ ,  $u \in H^2(X)$ .

2. The Gysin morphism  $\tilde{\pi}_! : H^2(\tilde{X}) \rightarrow H^2(\tilde{Y})$  restricted to  $H^2(X)^G$  is injective and multiplies the intersection form by  $|G|$ .

*Proof.* 1. Let  $u \in H^2(X)$ . Using diagram (20.21) in case  $k = 2$  where  $H_c^2(X') \simeq H^2(X') \simeq H^2(X)$ , Lemma 20.9.1.2 implies 1. Indeed, in this case the diagram extends as follows

$$\begin{array}{ccc} H_c^k(X') & \xrightarrow{\pi_!} & H_c^k(Y') \\ \parallel & & \downarrow \\ H^2(X) & \xleftarrow{\pi^*} & H^2(Y) \\ \tau^* \downarrow & & \downarrow \sigma^* \\ H^2(\tilde{X}) & \xrightarrow{\tilde{\pi}_!} & H^2(\tilde{Y}). \\ & \xleftarrow{\tilde{\pi}^*} & \end{array}$$

2. If  $u, u' \in H^2(X)$ , setting  $y = \tilde{\pi}_!(\tau^*u)$ ,  $y' = \tilde{\pi}_!(\tau^*u')$ , one finds  $\tilde{\pi}^*y \cdot \tilde{\pi}^*y' = |G|y \cdot y'$ , since  $\tilde{\pi}$  has degree  $|G|$ . Assume now that  $u, u' \in H^2(X)^G$ . Using item 1 and the (cup-product preserving) injectivity of  $\tau^*$  which allows to drop  $\tau^*$ , we have:

$$|G|(\tilde{\pi}_!u, \tilde{\pi}_!u') = \tilde{\pi}^* \tilde{\pi}_!u \cdot \tilde{\pi}^* \tilde{\pi}_!u' = |G|^2 u \cdot u'.$$

This implies that  $\tilde{\pi}_!$  restricts injectively to  $H^2(X)^G$  (since this lattice is non-degenerate), and so 2 follows.  $\square$

Next, we relate the cohomology groups of  $X'$  and its compactification  $X$ , as well as those of  $Y'$  and its compactification  $\tilde{Y}$ . To do this, we shall make use of a variant of the so-called **Gysin exact sequence** which relates the cohomology of an oriented differentiable manifold  $M$  and the cohomology of the complement of a smooth submanifold  $N \subset M$ :

$$\cdots \rightarrow H^q(N) \rightarrow H^{q+e}(M) \rightarrow H^{q+e}(M-N) \rightarrow H^{q+1}(N) \rightarrow \cdots \quad e = \text{codim}_{\mathbb{R}} N.$$

This is a slightly less known sequence and hence we explain how it arises. One starts with the long exact sequence in cohomology for the pair  $(M, M-N)$ . By the excision property, the terms  $H^q(M, M-N)$  can be replaced with  $H^q(T, T-N)$ , where  $T$  is a suitably small neighborhood of  $N$  in  $M$ . The so-called tubular neighborhood theorem (cf. [135, Chapter 4.5]) gives a nice choice for  $T$  which ensures that  $T$  is diffeomorphic to the total space of a 2-disc bundle over  $N$ , where we identify  $N$  with the zero section  $s_0$  of this 2-disc bundle of  $N$  in  $M$ . Finally, by Thom's theorem (cf. [219, Ch. 5.7, Thm 10]) we have a natural identification  $H^q(T, T-s_0) = H^{q-e}(N)$ . In our case,  $N$  is not a submanifold but an *A-D-E* configuration in a complex surface. However, we explained in § 4.4.C that a neighborhood of such a configuration is obtained by plumbing the tubular neighborhoods of the components of the configuration. This comes down to identifying the two 2-discs over an intersection point  $p$  of two intersecting components. Since  $H^q(E) = \bigoplus_{p \in \Sigma} H^q(E_p)$  and  $H^1(E_p) = 0$  (the curves  $E_p$  are unions of smooth rational curves), the Gysin sequence for the pair  $(\tilde{Y}, E)$  leads to

$$0 \rightarrow \bigoplus_{p \in \Sigma} H^0(E_p) \xrightarrow{i_*} H^2(\tilde{Y}) \xrightarrow{\tilde{j}^*} H^2(\tilde{Y} - E) = H^2(Y') \rightarrow H^1(E) = 0. \quad (20.22)$$

**20.9.B The case where  $G$  is abelian.** In this subsection  $G$  is an abelian group acting on  $X$  with quotient  $Y$ . The goal is to relate  $H^2(X)^G$  to  $H^2(Y)$ . Over  $\mathbb{Q}$  the groups are isomorphic, but the possible torsion in the integral cohomology groups complicates matters. It is easy to impose a condition which implies that the related groups  $H^2(X)$  and  $H^2(\tilde{Y})$  are free of torsion, since the universal coefficient theorem implies that this is equivalent to  $H_1(X)$  and  $H_1(\tilde{Y})$  being free of torsion. The stronger assumption that  $X$  be simply connected and that  $H_1(\tilde{Y}) = 0$  would ensure this. A property of the group action, which holds in the cases of interest to us, makes the last condition superfluous:

**Lemma 20.9.4.** *With  $X, G, \Sigma, Y, \tilde{Y}$  as in § 20.9.A (with  $G$  abelian), let  $G_p, p \in \Sigma$ , be the stabilizer of  $p$  in  $G$ . Suppose that  $X$  is simply connected and that the homomorphism  $\bigoplus_{p \in \Sigma} G_p \rightarrow G$  induced by inclusion is surjective. Then  $H_1(\tilde{Y}) = 0$ .*

*Proof.* Let  $U = \tilde{Y} - E = Y - \pi(\Sigma)$ , and  $V = \bigcup_{p \in \Sigma} T(E_p)$ , the union of tubular neighbourhoods  $T(E_p)$  of the exceptional sets  $E_p, p \in \Sigma$ . Then  $U \cap V = \bigcup_{p \in \Sigma} T^0(E_p)$ , where  $T^0(E_p)$  can be identified with the quotient of a punctured ball by  $G_p$ . This quotient has fundamental group  $G_p$  since in real dimensions  $\geq 3$  a once punctured



ball is simply connected. Part of the Mayer–Vietoris sequence for the open cover  $\{U, V\}$  of  $\tilde{Y}$  in homology (cf. [94, §2.2]) reads

$$H_1(U \cap V) \rightarrow H_1(U) \oplus H_1(V) \rightarrow H_1(\tilde{Y}) \rightarrow H_0(U \cap V) \rightarrow \dots$$

Since  $X' = X - \Sigma$  is simply connected and  $X' \rightarrow Y' = Y - \pi(\Sigma) = U$  is a Galois cover,  $\pi_1(Y') = H_1(Y') = G$  and so, by what we just said, the Mayer–Vietoris sequence reads as follows

$$\bigoplus_{p \in \Sigma} G_p \rightarrow G \rightarrow H_1(\tilde{Y}) \xrightarrow{\delta} \bigoplus_{p \in \Sigma} \mathbb{Z} \rightarrow \mathbb{Z} \oplus \bigoplus_{p \in \Sigma} \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow 0.$$

Hence the assumption that  $\bigoplus_{p \in \Sigma} G_p \rightarrow G$  is surjective implies  $H_1(\tilde{Y}) = 0$ . □

**Example 20.9.5.** If  $G$  is a finite abelian group acting symplectically on a K3 surface  $X$ , Tables 20.4.1 and 20.4.2 show that the assumption on the stabilizers is satisfied in this case. However, the conclusion that  $H_1(\tilde{Y}) = 0$  in this case follows also directly since  $\tilde{Y}$  is a K3 surface.

To arrive at the desired comparison stated as Theorem 20.9.6 below, we make use of Proposition A.6.2 which provides an exact sequence

$$0 \rightarrow \text{Ext}^1(G) \rightarrow H^2(Y') \xrightarrow{\pi^*} \mathbb{H} \rightarrow 0, \quad \mathbb{H} := \ker(H^2(X')^G \xrightarrow{\delta} H^3(G)), \quad (20.23)$$

describing what happens in cohomology under  $\pi : X' \rightarrow Y'$ , the induced unramified  $G$ -cover over the smooth part  $Y'$  of  $Y$ . Observing that by (20.20) the inclusion  $X' \hookrightarrow X$  induces an isomorphism  $H^2(X) \simeq H^2(X')$ , we see that in particular the image of  $\pi^*$  in  $H^2(X')^G$  can be considered as a subgroup of  $H^2(X)^G$  of finite index  $\leq |H^3(G)|$ . Note also that  $\mathbb{H}$ , as a subgroup of the torsion free group  $H^2(X)$  inherits a lattice structure from the intersection product on  $H^2(X)$ . Introducing the following additional lattices:

$$M'_Y = \text{sublattice of } \mathbb{H}_{\tilde{Y}} = H^2(\tilde{Y})/\text{Tors} \text{ spanned by} \\ \text{the classes of the components of the } E_i.$$

$$M_Y = \text{primitive closure of } M'_Y \text{ in } \mathbb{H}_{\tilde{Y}},$$

we can now state the central result of this section:

**Theorem 20.9.6.** *Let  $X$  be a compact complex surface admitting an action by a finite abelian group  $G$  of order  $n$ , let  $\pi : X \rightarrow Y = X/G$  be the quotient map,  $\tilde{Y}$  the minimal resolution of singularities of  $Y$ ,  $X'$  the complement of the fixed points of  $G$ ,  $Y' = X'/G$ , and  $j' : X' \hookrightarrow X$ ,  $\tilde{j} : Y' \hookrightarrow \tilde{Y}$  the inclusions.*

*Assume that  $Y := X/G$  has at most cyclic quotient singularities, that  $X$  is simply connected and that  $H_1(\tilde{Y}) = 0$ . Then the following assertions hold:*

1. *Setting  $\theta := (j'^*)^{-1} \circ \pi^* \circ \tilde{j}^* : H^2(\tilde{Y}) \rightarrow H^2(X)^G$ , the image of  $\theta$  belongs to  $\mathbb{H}$  (cf. (20.23)) and there is an exact sequence*

$$0 \rightarrow M_Y/M'_Y \rightarrow H^2(\tilde{Y})/M'_Y \xrightarrow{\theta} \mathbb{H} \rightarrow 0. \quad (20.24)$$

*The factor group  $M_Y/M'_Y$  is canonically isomorphic to  $\text{Ext}^1(G)$ .*

2.  $\theta$  induces an isomorphism  $H^2(\tilde{Y})/M_Y \xrightarrow{\cong} H$  and an injection  $M_Y^\perp \hookrightarrow H$ . This is an injection of free  $\mathbb{Z}$ -modules of the same rank, but  $\theta|_{M_Y^\perp}$  multiplies the intersection form with  $|G|$ . In case  $G$  is cyclic,  $H = H^2(X)^G$ .
3. The elementary divisors  $e_1|e_2|\cdots|e_r$  of the discriminant group of  $M_Y$  all divide  $n = |G|$ .
4. The length of the discriminant group of the sublattice  $H \subset H^2(X)$  is at least equal to  $\text{rank}(H^2(X)^G) - r$ . Its elementary divisors are obtained by omitting the integers equal to 1 from the list  $(n/e_1, \dots, n/e_r, n, \dots, n)$  (the size of this list equals  $\text{rank}(H) = \text{rank}(H^2(X)^G) = b_2(\tilde{Y}) - \text{rank}(M_Y)$ ).

The discriminant bilinear form of  $H$  assumes values in  $n^{-1}\mathbb{Z}/\mathbb{Z}$ . If the intersection form on  $X$  is even, the discriminant quadratic form takes values in  $(2n)^{-1}\mathbb{Z}/\mathbb{Z}$ .

*Proof.* **1.** We first show that

- $\tilde{j}$  induces an isomorphism  $\tilde{j}^* : H^2(\tilde{Y})/M'_Y \xrightarrow{\cong} H^2(Y')$ ;
- there is a canonical identification  $\text{Tors } H^2(Y') = M_Y/M'_Y = \text{Ext}^1(G)$ .

To start, remark that since  $H_1(\tilde{Y}) = 0$ , by the universal coefficient theorem  $H^2(\tilde{Y})$  has no torsion. Next, we invoke the exact sequence (20.22). Note that the image of the map  $i_*$  in this sequence is precisely the lattice  $M'_Y$ . Since  $M_Y$  is its primitive closure,  $H^2(\tilde{Y})/M_Y$  is without torsion and under  $\tilde{j}^*$  it is isomorphic to  $H^2(Y')$  modulo torsion. Consequently, the sequence implies

$$H^2(\tilde{Y})/M'_Y = H^2(Y'), \quad \text{Tors } H^2(Y') = M_Y/M'_Y. \tag{20.25}$$

On the other hand,  $\pi$  restricted to  $X'$  gives an unramified Galois cover  $\pi : X' \rightarrow Y'$  and so, since  $X'$  is simply connected, one has  $\pi_1(Y') = G$  and so  $H_1(Y') = \text{Tors } H_1(Y') = G$  since  $G$  is abelian. By the universal coefficient theorem ([94, Thm. 3.2]),  $\text{Tors } H^2(Y') = \text{Ext}^1(G)$ . Using (20.23), the exact sequence (20.24) is then a direct consequence of (20.20) and (20.22).

**Proof of 2.** The exact sequence (20.24) shows that  $\theta$  induces an isomorphism between  $H^2(\tilde{Y})/M_Y$  and  $H$ . Since  $M'_Y$  is non-degenerate,  $M_Y^\perp \cap M'_Y = \{0\}$ , so the homomorphism  $\theta$  restricts injectively to  $M_Y^\perp$ . The morphism  $\tilde{\pi} : \tilde{X} \rightarrow \tilde{Y}$  induced by  $\pi$  is finite of degree  $|G|$  and so, using the cup product,  $\tilde{\pi}^*(y) \cup \tilde{\pi}^*(y') = \tilde{\pi}^*(y \cup y') = |G|y \cup y'$  for all  $y, y' \in H^2(\tilde{Y})$ . In particular, the restriction of the intersection form on  $H^2(\tilde{Y})$  to  $M_Y^\perp$  gets multiplied by  $|G|$  under  $\theta$ . For the last statement one makes use of the vanishing of  $H^3(G)$  in case  $G$  is cyclic.

**Proof of 3 and 4.** We are now in the following abstract setting: one has

- a primitive non-degenerate sublattice  $T := M_Y$  of a unimodular lattice  $(L, b) := H_{\tilde{Y}}$  with orthogonal complement  $S := T^\perp$  (and so  $T = S^\perp$ );
- a lattice  $H$  of rank  $N$ ;
- an isomorphism  $\theta : L/T \xrightarrow{\cong} H$  of  $\mathbb{Z}$ -modules such that for  $x, y \in S$  one has

$b'(\theta(x), \theta(y)) = n \cdot b(x, y)$ , where  $b'$  is the bilinear form on  $H$ .

Next, recall that by Lemma 1.6.2 the correlation map induces an isomorphism  $\bar{\beta}_S : L/T \xrightarrow{\sim} S^*$  of free  $\mathbb{Z}$ -modules. By what we have said before, on the finite index sublattice  $\theta(S) \subset H$  the form  $b'$  coincides with  $b(n)$ . But then  $\theta \cdot (\bar{\beta}_S)^{-1}$  identifies  $(S^*, b_{\mathbb{Q}}(n))$  with the (integral) lattice  $H$ . Note that since  $L$  is unimodular, by Lemma 1.7.6 the sublattices  $S$  and  $T$  have isomorphic discriminant groups, hence the same length and the same elementary divisors. So we continue with  $S$  instead of  $T$ . Now apply Remark 1.6.10 to the lattice  $S$  and its dual and with  $\rho = n$ . The discriminant group of  $H = S^*(n)$  has elementary divisors obtained from  $(e_1^*, \dots, e_N^*) = (n/e_1, \dots, n/e_r, n, \dots, n)$  by omitting the  $e_j^*$  with  $e_j^* = 1$  (recall that  $\text{rank}(H) = N$ ) and putting them in the right order. This shows in particular that  $e_j | n$ ,  $j = 1, \dots, r$ , and so, if  $y \in S^*$ , then  $n \cdot y \in S$ . From the description of the discriminant form of  $S^*(n)^*/S^*(n)$  in Remark 1.6.10 it follows that the discriminant bilinear form  $(b')^\#$  assumes values in  $n^{-1}\mathbb{Z}/\mathbb{Z}$ . A similar reasoning holds for the discriminant quadratic form in case  $b'$  is even. Finally, since  $\text{dg}_H$  has at least  $N - r$  elementary divisors equal to  $n \neq 1$ , its length is at least  $N - r$ .  $\square$

**Example 20.9.7.** For an involution one has  $n = 2$ , and all elementary divisors of the discriminant group of  $M_Y$  are equal to 2. Hence, in this case the discriminant group of the invariant lattice is isomorphic to  $\oplus^\ell \mathbb{Z}/2\mathbb{Z}$ ,  $\ell = b_2(\bar{Y}) - \ell(M_Y)$ , and if the intersection form on  $X$  is even, then the discriminant quadratic form can be of type I, or of type II (cf. Definition 1.7.2).

*Remark 20.9.8.* Contrary to the claim in [169, §8.5], the homomorphism  $\pi^{* *} : H^2(Y') \rightarrow H^2(X')^G$  is not in general surjective, for instance if  $b_1(X') \neq 0$ .

Table 20.9.1: The lattices  $\Lambda^G$  for symplectic  $G$ -actions on K3 surfaces

$G$	$\text{dg}_{\Lambda^G}$	$\text{disc}(\Lambda^G)$	$\Lambda^G$
$\mathbb{Z}/2\mathbb{Z}$	$\oplus^8 \mathbb{Z}/2\mathbb{Z}$	$2^8$	$E_8(-2) \oplus \oplus^3 U$
$\mathbb{Z}/3\mathbb{Z}$	$\oplus^6 \mathbb{Z}/3\mathbb{Z}$	$3^6$	$U \oplus \oplus^2 U(3) \oplus \oplus^2 A_2$
$\mathbb{Z}/5\mathbb{Z}$	$\oplus^4 \mathbb{Z}/5\mathbb{Z}$	$5^4$	$U \oplus \oplus^2 U(5)$
$\mathbb{Z}/7\mathbb{Z}$	$\oplus^3 \mathbb{Z}/7\mathbb{Z}$	$7^3$	$U(7) \oplus \begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix}$
$\mathbb{Z}/4\mathbb{Z}$	$\oplus^2 \mathbb{Z}/2\mathbb{Z} \oplus \oplus^4 \mathbb{Z}/4\mathbb{Z}$	$2^{10}$	$Q_4$
$\mathbb{Z}/6\mathbb{Z}$	$\oplus^4 \mathbb{Z}/6\mathbb{Z}$	$6^4$	$U \oplus \oplus^2 U(6)$
$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \oplus^2 \mathbb{Z}/8\mathbb{Z}$	$8^3$	$U(8) \oplus \langle 2 \rangle \oplus \langle 4 \rangle$
$\oplus^2 \mathbb{Z}/2\mathbb{Z}$	$\oplus^6 \mathbb{Z}/2\mathbb{Z} \oplus \oplus^2 \mathbb{Z}/4\mathbb{Z}$	$2^{10}$	$\oplus^2 U(2) \oplus Q_{2,2}$
$\oplus^3 \mathbb{Z}/2\mathbb{Z}$	$\oplus^6 \mathbb{Z}/2\mathbb{Z} \oplus \oplus^2 \mathbb{Z}/4\mathbb{Z}$	$2^{10}$	$\oplus^3 U(2) \oplus \oplus^2 \langle -4 \rangle$
$\oplus^4 \mathbb{Z}/2\mathbb{Z}$	$\oplus^6 \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$-2^9$	$\langle -8 \rangle \oplus \oplus^3 U(2)$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\oplus^2 \mathbb{Z}/2\mathbb{Z} \oplus \oplus^4 \mathbb{Z}/4\mathbb{Z}$	$2^{10}$	$Q_{2,4}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z} \oplus \oplus^2 \mathbb{Z}/12\mathbb{Z}$	$2^4 3^3$	$R_4$
$\oplus^2 \mathbb{Z}/3\mathbb{Z}$	$\oplus^4 \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$	$3^6$	$\oplus^2 U(3) \oplus \begin{pmatrix} 2 & 3 \\ 3 & 0 \end{pmatrix}$
$\oplus^2 \mathbb{Z}/4\mathbb{Z}$	$\oplus^2 \mathbb{Z}/2\mathbb{Z} \oplus \oplus^2 \mathbb{Z}/8\mathbb{Z}$	$2^8$	$S_4$

In the present situation, where  $b_1(X) = 0$ , Proposition A.6.2 asserts surjectivity up to a group of finite index in  $H^3(G)$ . Since the latter group is non-zero if  $G$  is not cyclic, this affects the results of [169, §10], e.g. the list of the discriminant groups of loc. cit. p. 133. This has been observed by A. Garbagnati in her thesis [76]. See also [81] where one finds a corrected list as well as a lattice-type description of the  $G$ -invariant lattices reproduced as Table 20.9.1. In this table, one has used the following abbreviations:

$$\begin{aligned}
 Q_4 &= \begin{pmatrix} 0 & 4 & 0 & 2 & 0 & -1 & 0 & 0 \\ 4 & 0 & 4 & 4 & -4 & 0 & 0 & -4 \\ 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 4 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & -4 & 0 & 0 & -2 & -1 & 0 & -2 \\ -1 & 0 & 0 & -1 & -1 & -2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 \\ 0 & -4 & 0 & 0 & -2 & 1 & 0 & -2 \end{pmatrix}, & Q_{2,2} &= \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & -2 & 2 & 0 & 0 & 0 \\ 0 & 2 & -4 & 2 & 0 & 0 \\ 0 & 0 & 2 & -4 & 2 & 0 \\ 0 & 0 & 0 & 2 & -4 & 4 \\ 0 & 0 & 0 & 0 & 4 & -8 \end{pmatrix}, \\
 Q_{2,4} &= \begin{pmatrix} 4 & -2 & 0 & 0 & 0 & 0 \\ -2 & 0 & -2 & 0 & 0 & 0 \\ 0 & -2 & -64 & -4 & 0 & 0 \\ 0 & 0 & -4 & 0 & -4 & 0 \\ 0 & 0 & 0 & -4 & -80 & 4 \\ 0 & 0 & 0 & 0 & 4 & 0 \end{pmatrix}, & R_4 &= \begin{pmatrix} 0 & 6 & 0 & 0 \\ 6 & 0 & -3 & 0 \\ 0 & -3 & 6 & 6 \\ 0 & 0 & 6 & 8 \end{pmatrix}, & S_4 &= \begin{pmatrix} 4 & 6 & 0 & 0 \\ 6 & 4 & 6 & 4 \\ 0 & 6 & 4 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix}.
 \end{aligned}$$

**Historical and Bibliographical Notes.** Proposition 20.1.3, the application to automorphism groups, is due to Pjateckiĭ–Šapiro and Šafarevič and expanded in great detail by V. Nikulin in [172]. Proposition 20.1.5 describing the algebraic nature of the automorphism group is due to H. Sterk [220].

S. Mukai [159] discovered that all finite symplectic groups of automorphisms of a K3 surface appear as certain subgroups of  $M_{23}$ , one of the sporadic simple groups. The sketch of the proof we give of this result (based on Niemeier lattices) is due to S. Kondō, c.f. [128]. For other results on special automorphisms on K3 surfaces using lattice theory, see also [6, 7, 76, 77, 80, 82]. That finite abelian groups acting symplectically on a K3 surface have an essentially unique action in cohomology is due to V. Nikulin [169] whose proof we have followed in Section 20.2. The uniqueness of a symplectic action in cohomology for (not necessarily abelian) finite groups acting on a K3 surface has been discussed by K. Hashimoto in [93] making use of the embeddings of  $G$  in  $M_{23}$ . He shows that except for four groups one also has uniqueness (up to conjugation).

Our treatment in Section 20.6 is based on Nikulin’s article [168]. We also made use of Lemma 20.6.3 which is inspired by Ch. 3.2.4 in D. Huybrechts’s book [106]. The lattice theoretic study of the polarized K3 surfaces admitting a Nikulin involution is due to B. van Geemen and A. Sarti [83]. For geometrically constructed K3 surfaces with a Nikulin involution see Section 3 in loc. cit. The lattice theoretic arguments used for Nikulin involutions and for the Shioda–Inose structures are largely due to D. Morrison [158]. The term “Shioda–Inose structure” refers to the article [211] by T. Shioda and H. Inose.

We finish by mentioning some related developments concerning so-called generalized Kummer surfaces, that is, K3 surfaces which by definition are the minimal resolutions of a quotient of two-dimensional complex tori by some finite group  $G$ . If  $G$  fixes the origin, apart from the cyclic group  $\mathbb{Z}/2\mathbb{Z}$  which gives the Kummer surface, only cyclic groups of order 3, 4, 6, binary dihedral groups  $\tilde{D}_4, \tilde{D}_6$  and the binary tetrahedral groups are possible. See [74]. The analog of the Kummer lattice for the cyclic case has been studied by J. Bertin in [22], and for the remaining groups by K. Wendland [249] and A. Garbagnati

[78]. There are also groups  $G$  acting in such a way that not all  $g \in G$  have the same fixed points. This is only possible if  $G$  is the quaternion group or the binary dihedral group  $\tilde{D}_{12}$ , and these have been studied by X. Roulleau in [197].

The generalized Kummer surfaces also appear in the construction of generalized Shioda–Inose structures  $(X, A, G)$ , where  $X$  is a K3 surface,  $A$  an abelian surface, and the finite group  $G$  acts on  $A$  and it acts symplectically on  $X$  such that  $X/G = A/G$  is a generalized Kummer surface. These have been classified in [178] by H. Önsiper and S. Sertöz.

## Applications to Enriques Surfaces

### Introduction

Since an Enriques surface is the quotient of a K3 surface by a fixed point free involution, the moduli space of Enriques surfaces should be a "subspace" of the moduli space of K3 surfaces. We make this precise in Section 21.1. We also consider moduli for those Enriques surfaces that have at least one nodal curve. Like we did for K3 surfaces, once we have a description of the moduli space, we can make use of this to investigate the automorphism groups of Enriques surfaces. This is taken up in Section 21.2. Surprisingly, the automorphism group is generally infinite – for instance for Enriques surfaces without nodal curves. In this case, as well as for the case of a general nodal Enriques surface, the automorphism groups can be described explicitly.

### 21.1 Enriques Surfaces: Moduli

In this chapter  $(X, j)$  is a pair of a K3 surface together with a fixed point free involution  $j$ . As before, the cyclic group of order 2 generated by  $j$  is denoted  $G$ . The quotient  $X/G = Y$  is an Enriques surface. We continue to denote the K3 lattice by  $\Lambda$ .

The basic invariants of an Enriques surface  $Y$  are as follows (see e.g. Appendix B.3)

$$b_1(Y) = 0, \quad p_g(Y) = 0, \quad H^2(Y)/\text{torsion} \simeq \Lambda_{\text{Enr}},$$

where  $\Lambda_{\text{Enr}} := U \oplus E_8(-1)$  is the *Enriques lattice*. Below we shall also encounter  $\Lambda_{\text{Enr}}(2)$  and its discriminant quadratic form given by (see Example 11.2.5.3)

$$q_{\Lambda_{\text{Enr}}(2)}^{\#} \simeq \oplus^5 u_1. \quad (21.1)$$

**21.1.A Moduli for Enriques surfaces.** The fixed point free involution  $j$  on the K3 surface  $X$  induces an involution  $j^*$  on  $H^2(X, \mathbb{Z})$  which can be described abstractly, using a properly chosen isometry  $H^2(X, \mathbb{Z}) \simeq \Lambda$ . To explain this, we rewrite the K3 lattice as  $\Lambda = U \oplus W \oplus W'$ , where  $W, W'$  are copies of the Enriques lattice. This last decomposition can be used to define the *lattice Enriques involution*

$$t_{\text{Enr}}(u, v, v') = (-u, v', v), \quad (u, v, v') \in U \oplus W \oplus W'.$$

The invariant lattice  $\Lambda^G$  consists of the vectors  $(0, v, v)$ , and so it is isometric to  $\Lambda_{\text{Enr}}(2)$ . Proposition 15.2.10 then implies that there is a marking  $\varphi : H^2(X, \mathbb{Z}) \rightarrow \Lambda$  fitting in a commutative diagram<sup>1</sup>

$$\begin{array}{ccc} H^2(X, \mathbb{Z}) & \xrightarrow{\sim \varphi} & \Lambda \\ j^* \downarrow & & \downarrow \iota_{\text{Enr}} \\ H^2(X, \mathbb{Z}) & \xrightarrow{\sim \varphi} & \Lambda. \end{array} \quad (21.2)$$

Such a marking  $\varphi$  is called a **marking for**  $(X, j)$ . Since  $Y = X/G = X/\langle j \rangle$  has no non-zero holomorphic 2-forms, the involution  $j^*$  acts as  $-\text{id}$  on  $H^{2,0}(X)$  and hence also on the corresponding period point  $[\omega] = \varphi[H^{2,0}(X)]$ . So  $[\omega]$  belongs to  $D(\Lambda) \cap \mathbb{P}(\Lambda_G) = D(\Lambda_G)$  where  $\Lambda_G$  is the anti-invariant lattice. For later reference, we observe

$$\Lambda_G = \{(u, w, -w) \in U \oplus W \oplus W'\} \simeq U \oplus \Lambda_{\text{Enr}}(2). \quad (21.3)$$

We claim that a period point  $[\omega] \in D(\Lambda_G)$  such that  $[\omega]$  is not orthogonal to any root of  $\Lambda_G$  corresponds to a K3 surface admitting an Enriques involution. To show this, observe that by Criterion 20.2.1 it suffices to show that a) there is a  $G$ -invariant element in the positive cone, and b)  $\Lambda_G \cap \text{NS}(X)$  contains no roots. As to a), by the surjectivity of the period map (Theorem 19.2.1.2), there exists a marked K3 surface  $X$  with period point  $[\omega]$ . We now identify  $H^2(X, \mathbb{Z})$  with  $\Lambda$  through this marking. By assumption  $\iota_{\text{Enr}}(\omega) = -\omega$ , and so the involution preserves  $H^{2,0}(X)$ . Moreover,  $\iota_{\text{Enr}}$  acts as  $-\text{id}$  on the transcendental lattice and so this lattice is contained in  $\Lambda_G$ . Hence  $\text{NS}(X)$  and a fortiori  $H^{1,1}(X)$  contain  $\Lambda^G$ , a lattice of signature  $(1, 9)$ , and so condition a) holds. A root  $r \in \Lambda_G$  cannot be the class of a divisor since by assumption  $r \cdot \omega \neq 0$  and so b) holds as well. Consequently,  $X$  admits an involution  $j$  which under the marking corresponds to  $\iota_{\text{Enr}}$ . Such an involution  $j$  is fixed point free by Lemma 20.5.2, since  $\text{Tr}(j^*) = \text{Tr}(\iota_{\text{Enr}}) = -2$ . So  $X/G$  is an Enriques surface and the marking is a marking for  $(X, j)$ .

We shall indicate how this implies that Enriques surfaces depend on 10 moduli. We just showed that markings for  $(X, j)$  give period points in

$$D_{\text{Enr}} = D(\Lambda_G) - \bigcup_{r \in \Lambda_G, r \cdot r = -2} H_r \cap D(\Lambda_G), \quad H_r = r^\perp, \quad (21.4)$$

and that, conversely, such points correspond to period points for Enriques surfaces coming from marked pairs  $(X, j)$  of a K3 surface equipped with an Enriques involution. Such period points will be called **period points of Enriques surfaces**. The group

$$\Gamma_{\text{Enr}} := \{\gamma \in \text{O}(\Lambda) \mid \gamma \circ \iota_{\text{Enr}} = \iota_{\text{Enr}} \circ \gamma\} \quad (21.5)$$

acts on  $D_{\text{Enr}}$  in a discrete and proper fashion. If  $\varphi$  is a marking for  $(X, j)$ , then  $\gamma \circ \varphi$ ,  $\gamma \in \Gamma_{\text{Enr}}$ , is a marking for a pair  $(X', j')$  with  $X'/j'$  isomorphic to  $X/j$ . The converse holds also and so the (10-dimensional) quotient  $\Gamma_{\text{Enr}} \backslash D_{\text{Enr}}$  classifies isomorphism classes of Enriques surfaces.

<sup>1</sup>See also [15, Lemma VIII.19.1].

**21.1.B Nodal types and the ample cone for Enriques surfaces.** In what follows we shall identify  $H^2(X, \mathbb{Z})$  with the K3 lattice  $\Lambda$  through a fixed  $(X, j)$ -marking and we let  $[\omega]$  be the corresponding period point. The sublattice corresponding to the Néron–Severi lattice of  $X$  will be denoted by  $S$ . Let  $\pi^* : \Lambda_{\text{Enr}} \rightarrow \Lambda^G$  be the injective map induced by  $\pi : X \rightarrow Y = X/G$ . This identifies the Enriques lattice with  $\Lambda^G(\frac{1}{2})$ .

As is the case for a K3 surface, the ample cone in the Enriques lattice can be described by means of roots. In the present case we need an adapted version which uses pairs of roots on the covering K3 surface.

**Definition 21.1.1.** For any subset  $R$  of a lattice, we let  $\langle R \rangle$  be the smallest primitive sublattice containing  $R$ .

1. An ordered pair of  $(-2)$ -roots  $\{r, t_{\text{Enr}}(r)\}$ ,  $r \in \Lambda$ , which satisfy  $r \cdot t_{\text{Enr}}(r) = 0$  is called an  $t_{\text{Enr}}$ -**adapted root pair**. The collection of all  $t_{\text{Enr}}$ -adapted root pairs of  $\Lambda$  is denoted by  $\Delta(\Lambda, t_{\text{Enr}})$ . If  $\{r, t_{\text{Enr}}(r)\} \in \Delta(\Lambda, t_{\text{Enr}})$ , we set  $r^\pm := r \pm t_{\text{Enr}}(r)$ . The corresponding root  $\mathbf{r} \in \Lambda_{\text{Enr}}$  in the Enriques lattice is given by  $\pi^* \mathbf{r} = r^+$ . In particular  $\Delta^\pm(X) \subset \text{NS}(X)$ .
2. Two sets  $R, R'$  of roots in  $\Lambda$  are said to be equivalent if the sublattices  $\langle R \rangle$  and  $\langle R' \rangle$  of  $\Lambda$  are isometric under  $O(\Lambda)$ .
3. Geometry enters by passing to roots that are nodal classes, that is, classes of smooth  $(-2)$ -curves:

$$\begin{aligned} \Delta(X) &:= \{ \{r, t_{\text{Enr}}(r)\} \in \Delta(\Lambda, t_{\text{Enr}}) \mid r \text{ is a nodal class} \}, \\ \Delta^\pm(X) &:= \{ r^\pm \mid \{r, t_{\text{Enr}}(r)\} \in \Delta(X) \}, \\ \Delta(Y) &:= \{ \mathbf{r} \mid \{r, t_{\text{Enr}}(r)\} \in \Delta(X) \} \subset \Lambda_{\text{Enr}}. \end{aligned}$$

Note that  $r$  is a nodal class if and only if  $t_{\text{Enr}}(r)$  is a nodal class because of the commutative diagram (21.2).

In this situation we say that  $(X, j)$  is of **nodal type**  $\Delta(X)$ .

There is a useful transitivity property:

**Proposition 21.1.2.** *If  $\{r, t_{\text{Enr}}(r)\}$  and  $\{s, t_{\text{Enr}}(s)\}$  are two  $t_{\text{Enr}}$ -adapted root pairs, there exists  $\gamma \in \Gamma_{\text{Enr}}$  for which  $\gamma(r^-) = s^-$ .*

*Proof.* Note that  $r^+ \in S := \Lambda^G$  and  $r^- \in T := \Lambda_G$  are  $(-4)$ -roots. Observe that since  $T = U \oplus U(2) \oplus E_8(-2)$ , Example 15.3.5.2 applies and shows that either the orbit of  $r^-$  under  $O(T)$  contains a vector contained in the  $U$ -component or its orbit contains a vector in  $U(2) \oplus E_8(-2)$ . The first alternative cannot occur as we show now. Assume  $r^-$  is such a vector which itself is contained in the  $U$ -component. Write  $r \in \Lambda \simeq U \oplus W \oplus W'$  in components as  $r = (u, w, t_{\text{Enr}}(w'))$ . Then  $r^- = (2u, w - w', w' - w)$  and so, if  $r^-$  would belong to the  $U$ -component, then  $W = w'$  and its self-intersection would be  $4u \cdot u \equiv 0 \pmod{8}$  which contradicts  $r^- \cdot r^- = -4$ . Hence the second alternative holds, and so some  $\gamma^- \in O(T)$  sends  $r^-$  to a  $(-4)$ -root in  $U(2) \oplus E_8(-2)$  (note that this lattice contains many  $(-4)$ -roots). A similar argument shows that an isometry of  $T$  sends  $s^-$  to a  $(-4)$ -root in  $U(2) \oplus E_8(-2)$ . All  $(-4)$ -roots in  $U(2) \oplus E_8(-2)$  are equivalent under isometries



of this sublattices, and can be extended to  $T$ . Therefore we may assume that  $\gamma^-(r^-) = s^-$ .

With  $r_T : \mathcal{O}(T) \rightarrow \mathcal{O}(\text{dg}_T)$  the reduction homomorphism, the isometry  $r_T(\gamma^-)$  yields an isometry of  $\text{dg}_S$  since  $q_T^\# = -q_S^\#$  for the respective discriminant forms. On the other hand, upon applying Theorem 14.5.5, we see that the reduction homomorphism  $r_S$  is surjective. Hence there exists  $\gamma^+ \in \mathcal{O}(S)$  with  $r_S(\gamma^+) = r_T(\gamma^-)$  and so, by Proposition 15.1.6,  $\gamma^+ \oplus \gamma^-$  extends to an isometry  $\gamma$  of  $\Lambda$ . By construction  $\gamma \in \Gamma_{\text{Enr}}$ .  $\square$

*Remark.* The above result implies that after a possible change of marking, we may assume that for any given  $\iota_{\text{Enr}}$ -adapted root pair  $\{r, \iota_{\text{Enr}}(r)\}$ , the associated root  $r^-$  is of the form  $\rho - \iota_{\text{Enr}}(\rho)$  where  $\rho$  is any root contained in the  $W$ -summand. Indeed, for such a choice,  $\{\rho, \iota_{\text{Enr}}(\rho)\}$  is an  $\iota_{\text{Enr}}$ -adapted root pair such that  $\rho^-$  is in the  $\mathcal{O}(\Lambda_G)$ -orbit of  $r^-$ .

**Proposition 21.1.3.** *Let  $(X, j)$  be a pair of a K3 surface equipped with an Enriques involution and let  $Y = X/G$  be the quotient Enriques surface. Use a marking for  $(X, j)$  to identify  $H^2(X)$  with  $\Lambda$  and  $H^2(Y)/\text{Tors}$  with  $\Lambda_{\text{Enr}} = \Lambda^G(\frac{1}{2})$ . Let  $\Delta(X)$  be the nodal type of  $X$  and set*

$$\begin{aligned} \mathcal{C}_{X,j}^{\text{amp}} &:= \{x \in \Lambda^G \otimes \mathbb{R} \mid x \in \mathcal{C}_X, x \cdot r^+ > 0 \text{ for all } \{r, \iota_{\text{Enr}}(r)\} \in \Delta(X)\} \\ &= \{y \in \Lambda_{\text{Enr}} \otimes \mathbb{R} \mid y \in \mathcal{C}_Y, y \cdot r > 0 \text{ for all } r \in \Delta(Y)\}. \end{aligned}$$

Then  $\mathcal{C}_{X,j}^{\text{amp}} = \mathcal{C}_X^{\text{amp}} \cap \Lambda^G \otimes \mathbb{R}$  corresponds to the ample cone of  $Y$ . Its closure is a fundamental domain for the action of

$$W^-(\Delta^+(X)) := \text{subgroup of } \mathcal{O}(\Lambda^G) \text{ generated by } \sigma_{r \circ \iota_{\text{Enr}}(r)} = \sigma_{r^+}, \quad \{r, \iota_{\text{Enr}}(r)\} \in \Delta(X),$$

on the positive cone of  $\Lambda^G \otimes \mathbb{R}$ . The latter Weyl group depends only on the set of nodal classes on  $Y$ , more precisely, on  $\Delta(Y)$ .

*Proof.* If  $x \in \Lambda^G \otimes \mathbb{R}$ , we have  $x = \pi^*y$  for some  $y \in \Lambda_{\text{Enr}} \otimes \mathbb{R}$  and if  $x \in \mathcal{C}_X$ , then  $y \in \mathcal{C}_Y$ . Since  $x \cdot r^+ = \pi^*y \cdot \pi^*r = 2y \cdot r$ , the definition of  $\Delta(X)$  and  $\Delta(Y)$  implies that  $x \cdot r^+ > 0$  for all  $\{r, \iota_{\text{Enr}}(r)\} \in \Delta(X)$  if and only if  $y \cdot r > 0$  for all  $r \in \Delta(Y)$ . Assume now that  $x \in \mathcal{C}_{X,j}^{\text{amp}}$ . We show that  $x \cdot r > 0$  for all nodal classes  $r$  on  $X$ , not only for the  $\iota_{\text{Enr}}$ -adapted ones. So, assume that  $r \cdot \iota_{\text{Enr}}r \neq 0$ . Since  $r$  and  $\iota_{\text{Enr}}(r)$  are nodal classes, then  $r \cdot \iota_{\text{Enr}}r > 0$ . Then also the self-intersection of  $r + \iota_{\text{Enr}}(r)$  is non-negative, since it is equal to  $-4 + 2r \cdot \iota_{\text{Enr}}(r)$  and it is divisible by 4. Consequently,  $r + \iota_{\text{Enr}}(r)$  is in the closure of the positive cone, while  $x$  belongs to the interior. Hence  $2x \cdot r = x \cdot (r + \iota_{\text{Enr}}(r))$  which is positive by Lemma 16.1.3. It follows that  $\mathcal{C}_{X,j}^{\text{amp}} = \mathcal{C}_X^{\text{amp}} \cap \Lambda^G = \mathcal{C}_Y^{\text{amp}}$ .

With respect to the action of  $W^-(\Delta^+(X))$  on the positive cone of  $\Lambda^G \otimes \mathbb{R}$ , the partitioning of  $\Delta^+(X)$  into effective  $(-4)$ -roots and their negatives, corresponds to the fundamental domain  $\overline{\mathcal{C}_{X,j}^{\text{amp}}}$ , i.e. the closure of  $\mathcal{C}_{X,j}^{\text{amp}}$  in the positive cone. The last assertion follows by the very definition of  $\Delta(Y)$ .  $\square$

We have seen that the group  $\Gamma_{\text{Enr}}$  preserves the period domain for Enriques surfaces. More precisely, if  $\gamma \in \Gamma_{\text{Enr}}$  and  $\varphi : H^2(X, \mathbb{Z}) \xrightarrow{\sim} \Lambda$  is a marking for  $(X, j)$ , then  $\gamma \circ \varphi$  is a marking for an isomorphic pair  $(X', j')$ . In case  $X = X'$  this means that  $\gamma$  preserves the period point, i.e., identifying  $H^2(X)$  with  $\Lambda$  through  $\varphi$ , the isometry  $\gamma$  is a Hodge isometry. In this situation  $\gamma$  is induced by an automorphism of  $X$  and so:

**Corollary 21.1.4.** *As in the preceding paragraph, assume that  $\gamma \in \Gamma_{\text{Enr}}$  preserves the period point of an Enriques surface  $X/\langle j \rangle$  (and hence induces a Hodge isometry on  $H^2(X, \mathbb{Z})$ ). Then for some  $w \in W^-(\Delta^+(X))$  the isometry  $w \circ \gamma$  is induced by a unique automorphism of  $X$  commuting with  $j$ .*

*Proof.* Let  $\kappa \in C_{X,j}^{\text{amp}}$ . Then  $\gamma(\kappa)$  belongs to the positive cone of  $\Lambda^G \otimes \mathbb{R}$  and Proposition 21.1.3 tells us that for some  $w \in W^-(\Delta^+(X))$  the element  $w \circ \gamma(\kappa)$  belongs to  $C_{X,j}^{\text{amp}} \subset C_X^{\text{amp}}$ . Then, by Theorem 19.2.2,  $w \circ \gamma$  is induced by a unique automorphism  $g$  of  $X$ . Since  $g^* \circ j^* = w \circ \gamma \circ j^* = j^* \circ w \circ \gamma = j^* \circ g^*$ , the automorphism  $g$  commutes with  $j$  (by unicity).  $\square$

The above considerations shed light on the nodal type  $\Delta(X)$  of  $(X, j)$ . First of all, note that

$$\Delta_\omega := \{ \{r, \iota_{\text{Enr}} r\} \in \Delta(\Lambda, \iota_{\text{Enr}}) \mid r \cdot \omega = 0 \}, \quad [\omega] \text{ period point of } (X, j), \quad (21.6)$$

is the subset of  $\iota_{\text{Enr}}$ -adapted roots in  $\Lambda$  belonging to  $\text{NS}(X)$ . Next, observe that the action of  $\sigma_r \circ \sigma_{\iota_{\text{Enr}}(r)} \in W^-(\Delta^+(X))$  extends to the entire K3 lattice  $H^2(X, \mathbb{Z})$  and preserves  $C_X$ . The ample cone of  $X$  is a fundamental domain for the action of  $W^-(\Delta^+(X))$  on the positive cone and in this way determines  $\Delta(X)$  as the set of indecomposable roots  $r$  with  $r \cdot x > 0$  for all  $x$  in the ample cone. By Proposition 17.2.6 there is a partition  $\Delta_\omega = \Delta_\omega^+ \cup -\Delta_\omega^+$  which is closed under taking sums, and  $\Delta(X)$  is exactly the subset of the indecomposable roots in  $\Delta_\omega^+$ . The isometry class of the lattice spanned by roots of  $\Delta_\omega^+$  does not depend on the chosen partition. Hence we have shown:

**Lemma 21.1.5.** *Let  $\omega$  be the period point of a marked pair  $(X, j)$ ,  $X$  a K3 surface  $X$  equipped with an Enriques involution  $j$ , and let the nodal set  $\Delta_\omega$  be given by equation (21.6). Then any partition  $\Delta_\omega = \Delta_\omega^+ \cup -\Delta_\omega^+$  closed under taking sums determines  $\Delta(X)$  up to equivalence. In other words, the nodal type of  $X$  is completely determined by  $\Delta_\omega$ .*

*Remark 21.1.6.* Let  $\omega$  be the period point of a  $j$ -marked K3 surface  $(X, \varphi)$  and let  $\gamma \in \Gamma_{\text{Enr}}$ . Then  $\omega' = \gamma(\omega)$  is the period point of an isomorphic  $j'$ -marked K3-surface  $(X', \gamma \circ \varphi)$ . Under  $\gamma$  the sets  $\Delta_\omega$  and  $\Delta_{\omega'}$  correspond and the same holds for their Weyl chambers. If  $r \in \Delta(X)$  is indecomposable, also  $\gamma(r)$  is indecomposable. Hence isomorphic Enriques surfaces have the same nodal type.

**21.1.C Nodal types for Enriques surfaces.** The goal of this subsection is to show that there are at most finitely many nodal types. We make use of the (+)-*root invariant*  $\delta^+(X)$  which is defined using the mod 2 reduction map  $r_2 : \Lambda \rightarrow \Lambda \otimes \mathbb{F}_2 \simeq \Lambda/2\Lambda$ :

$$\delta^+(X) = r_2(\Delta^+(X)) \subset \Lambda^G \otimes \mathbb{F}_2 = \Lambda^G/2\Lambda^G.$$

The quadratic form on  $\Lambda^G \otimes \mathbb{F}_2$  is inherited from the quadratic form on  $\Lambda^G$  and is in a natural way isometric to the unique non-degenerate quadratic form  $\oplus^5 u_1$  with Arf invariant 0 (see (21.1)). Root invariants are equivalent if they are related through an isometry of this discriminant quadratic form.

The invariant  $\delta^+(X)$  admits a description in terms of  $\Lambda_G$ , as we explain now. The lattices  $\Lambda^G$  and  $\Lambda_G$  are primitive sublattices of  $\Lambda$ . As in Section 15.1, the maps  $\Lambda \rightarrow \text{dg}_{\Lambda_G}$  and  $\Lambda \rightarrow \text{dg}_{\Lambda^G}$  induce an isometry  $\text{dg}_{\Lambda_G} \xrightarrow{\cong} \text{dg}_{\Lambda^G}$ . For a pair  $\{r, \iota_{\text{Enr}} r\}$  in  $\Delta(X)$  this implies that the class of  $\frac{1}{2}r^- \in \text{dg}_{\Lambda_G}$  is mapped to the class of  $\frac{1}{2}r^+$  in  $\text{dg}_{\Lambda^G}$ . On the span  $\langle \Delta^-(X) \rangle$  of such classes  $r^-$ ,  $\{r, \iota_{\text{Enr}} r\}$  in  $\Delta(X)$ , this can be rephrased as a map of  $\mathbb{F}_2$ -vector spaces

$$\begin{aligned} \xi : \langle \Delta^-(X) \rangle / 2\langle \Delta^-(X) \rangle \simeq \langle \Delta^-(X) \rangle \otimes \mathbb{F}_2 &\longrightarrow \Lambda^G \otimes \mathbb{F}_2 \\ r^- \bmod 2 &\longmapsto r^+ \bmod 2 \end{aligned} \quad (21.7)$$

preserving quadratic forms. However, since the form induced on  $\langle \Delta^-(X) \rangle \otimes \mathbb{F}_2$  need not be non-degenerate, the map  $\xi$  is in general not an embedding. Indeed,  $\ker \xi$  is the null-space of the quadratic form and the image of  $\xi$  in  $\Lambda^G \otimes \mathbb{F}_2$  is precisely  $\delta^+(X)$ , which shows:

**Lemma 21.1.7.** *Let  $H := \ker \xi \subset \langle \Delta^-(X) \rangle \otimes \mathbb{F}_2$ . Then the map  $\xi$  establishes an isomorphism  $[\langle \Delta^-(X) \rangle \otimes \mathbb{F}_2] / H \xrightarrow{\cong} \delta^+(X)$ .*

This lemma replaces the (+)-root invariant  $\delta^+(X)$  with the pair  $(\langle \Delta^-(X) \rangle \otimes \mathbb{F}_2, H)$ , the (-)-*root invariant*. Equivalent (+)-root invariants give equivalent (-)-root invariants, that is root invariants related by an isometry induced by  $\Gamma_{\text{Enr}}$ . By construction of the quadratic forms, the map  $\xi$  preserves equivalent root invariants. There are only finitely many such invariants due to the following crucial observation.

**Lemma 21.1.8.**  *$\langle \Delta^-(X) \rangle (\frac{1}{2})$  is a negative definite root lattice (and hence isometric to an orthogonal direct sum of the negative definite root lattices of types A-D-E). The rank of  $\langle \Delta^-(X) \rangle$  is at most 10 and so  $\langle \Delta^-(X) \rangle$  belongs to finitely many isometry types.*

*Proof.* Since  $\langle \Delta^-(X) \rangle$  is contained in  $\Lambda_G$ , a lattice of signature  $(2, 10)$ , and is perpendicular to the transcendental lattice, a lattice of signature  $(2, 20 - \text{rank}(\text{NS}(X)))$ , the lattice  $\langle \Delta^-(X) \rangle$  is a negative definite sublattice of the Néron-Severi lattice of rank at most 10.  $\square$

Note that  $r_2^{-1}(\Delta^\pm(X) \otimes \mathbb{F}_2) = \Delta^\pm(X)$  and since the (+)- and the (-)-invariants determine each other, the nodal type of  $\Delta(X)$  of  $X$  is completely determined by either one of the root invariants. Hence:

**Corollary 21.1.9.** *There are finitely many possible nodal invariants  $\Delta(X)$  (up to equivalence) and hence an Enriques surface can have at most finitely many nodal types.*

**21.1.D Moduli for nodal Enriques surfaces.**

**Lemma 21.1.10.** *Let  $(X, j)$  be a K3-surface equipped with a fixed point free involution  $j$ , and with nodal type  $\Delta(X)$ . A marking for  $(X, j)$  identifies the transcendental lattice  $T$  of  $X$  with a sublattice of  $\langle \Delta^-(X) \rangle^\perp \cap \Lambda_G$ .*

*Proof.* Recall that we have identified  $\text{NS}(X)$  with  $S \subset \Lambda$  and that  $T = S^\perp$ . Hence  $\Lambda^G \subset S$  since the Néron–Severi group of  $Y = X/G$  is all of  $H^2(Y, \mathbb{Z})$  and so  $T \subset \Lambda_G$ . On the other hand, we have  $\Delta^-(X) \subset S$ , and so  $T \subset \Delta^-(X)^\perp$ .  $\square$

Observe now that for any  $x \in \Lambda$  the linear forms  $b(x, -)$  and  $b(t_{\text{Enr}}(x), -)$  evaluated on  $\Lambda_G$  only differ by a sign and so the hyperplanes  $H_x = \{[\omega] \in D_{\Lambda_G} \mid \omega \cdot x = 0\}$  and  $H_{t_{\text{Enr}}(x)}$  are the same. This applies in particular to  $t_{\text{Enr}}$ -adapted root pairs  $\{r, t_{\text{Enr}}r\}$  so that the hyperplane  $D_{\text{Enr}} \cap H_r$  in fact only depends on  $r^-$ . For a collection  $\Delta$  of  $t_{\text{Enr}}$ -adapted root pairs, the intersection of the hyperplanes orthogonal to the roots thus only depends on  $\Delta^-$  and we denote it by

$$D_{\text{Enr}}^{\Delta^-} = \bigcap_{r \in \Delta} D_{\text{Enr}} \cap H_r = \{[\omega] \in D_{\text{Enr}} \mid \Delta_\omega = \Delta\}, \tag{21.8}$$

where we recall that  $\Delta_\omega$  is given by equation (21.6). Hence Lemma 21.1.5 tells us that this is the period space of **Enriques surfaces of nodal type  $\Delta$** . Its codimension in  $D_{\text{Enr}}$  is the rank of  $\langle \Delta^- \rangle$ . If  $\Delta$  is not empty, the Enriques surface  $X/G$  has nodal curves, and we say then that  $X/G$  is a **nodal Enriques surface**. In case  $\Delta^-$  generates a rank one lattice, we call  $X/G$  a **general nodal Enriques surface**.

If  $\gamma \in \Gamma_{\text{Enr}}$ , then  $\gamma(\Delta)$  is an equivalent nodal type and

$$\mathcal{M}_{\text{Enr}}^{\Delta^-} := \Gamma_{\text{Enr}} \backslash \left[ \bigcup_{\gamma \in \Gamma_{\text{Enr}}} D_{\text{Enr}}^{\gamma(\Delta^-)} \right],$$

is the moduli space of Enriques surfaces of nodal type  $\Delta$ . By Remark 21.1.6 the isomorphism class of such a moduli space indeed only depends on the nodal type.

**Example 21.1.11.** We consider the case of a general nodal Enriques surface  $Y = X/G$ , i.e.  $\Delta^-(X) = \{r^-\}$ . The corresponding moduli space has dimension 9. By construction, the Néron–Severi group of  $X$  contains  $r^-$  as well as the invariant lattice  $\Lambda^G$ . But we can say more using the notion of an  $S$ -marking where  $S$  is the smallest primitive sublattice of  $\Lambda$  containing  $\Lambda^G$  and  $r^-$ . The period domain  $D(S) \cap D_{\text{Enr}}$  is precisely the period space  $D_{\text{Enr}, r^-}$  since both have codimension 1.

Next, we compute the isometry classes of  $S$  and  $T$ . By Proposition 21.1.2, we may assume that  $r^-$  belongs to the  $E_8(-2)$ -copy in  $\Lambda_G = U \oplus U(2) \oplus E_8(-2)$ . Since  $T$  is orthogonal to  $r^-$ , and since the orthogonal complement of any root in  $E_8$  is isometric to  $E_7$  as we already have seen (cf. Lemma 4.1.3), we deduce that

$T \simeq U \oplus U(2) \oplus E_7(-2)$ . By Example 11.2.5.4 the discriminant form of  $T$  is then isometric to  $u_1 \oplus \langle 2^{-2} \rangle \oplus u_1^{\oplus 3}$ . Hence

$$q_S^\# = -q_T^\# \simeq u_1 \oplus \langle -2^{-2} \rangle \oplus u_1^{\oplus 3}.$$

Next, from Examples 11.2.5 and using Corollary 14.4.3, we deduce that  $S$  is isometric to the unique even lattice of signature  $(1, 10)$  with this discriminant form, namely  $U \oplus \langle -4 \rangle \oplus E_8(-2)$ . Here we use that  $\ell(\text{dg}_S) = 9 \leq 11 = \text{rank}(S)$ .

## 21.2 Automorphisms of Enriques Surfaces

**21.2.A General Enriques surfaces.** Automorphisms of Enriques surfaces not always act faithfully on cohomology as is the case for K3 surfaces. There are indeed examples of this phenomenon. See [160] as well as the historical and bibliographical remarks at the end of this chapter. We shall investigate automorphisms indirectly by their effect on the cohomology of the universal cover and thus bypass this problem.

Automorphisms of  $Y = X/G$  lift in two ways to automorphisms of  $X$  commuting with  $j$ . So

$$\text{Aut}(Y) = \text{Aut}(X, j)/G, \quad \text{Aut}(X, j) = \{g \in \text{Aut}(X) \mid g \circ j = j \circ g\}.$$

In order to relate isometries of  $\Lambda_{\text{Enr}}$  to those of the K3 lattice, one identifies  $\Lambda^G$  with the lattice  $\Lambda_{\text{Enr}}(2)$ . By (21.1) its discriminant quadratic form is isometric to  $\oplus^5 u_1$ , the non-degenerate quadratic form on the  $\mathbb{F}_2$ -vector space  $\Lambda_{\text{Enr}}/2\Lambda_{\text{Enr}} = \mathbb{F}_2^{10}$  with Arf invariant 0. Since  $\Lambda^G = \Lambda_{\text{Enr}}(2)$ , the dual of  $\Lambda^G$  is  $\frac{1}{2}\Lambda^G$  and so the discriminant group of  $\Lambda^G$  can be identified with  $\Lambda_{\text{Enr}}/2\Lambda_{\text{Enr}} \simeq \mathbb{F}_2^{10}$ . Hence the reduction map  $\rho_{\Lambda_{\text{Enr}}(2)}$  can be viewed as the mod 2 reduction map

$$\rho_2 : \text{O}(\Lambda^G) \rightarrow \text{O}(\Lambda_{\text{Enr}}/2\Lambda_{\text{Enr}}).$$

The kernel of this reduction map, the mod 2 congruence subgroup which conform (17.3) is denoted  $\text{O}(\Lambda^G)[2]$ , plays a central role:

**Lemma 21.2.1.** *The map  $\rho_2$  is surjective and  $\ker(\rho_2) = \text{O}^\#(\Lambda^G) = \text{O}(\Lambda_{\text{Enr}})[2]$ .*

*Proof.* It suffices to remark that  $\rho_2$  is surjective as explained in Example 14.5.6.  $\square$

The following concept similar to the terminology for K3 surfaces was introduced by S. Mukai and H. Ohashi in [161]:

**Definition 21.2.2.** As before, let  $Y = X/G$  be an Enriques surface. An automorphism  $g \in \text{Aut}(Y)$  is *semi-symplectic* if one of its two lifts to  $X$  is symplectic. The group of semi-symplectic transformations of  $Y$  is denoted  $\text{Aut}_s(Y)$ .

Observe that the Picard number for the K3 cover of a general non-nodal Enriques surface  $Y$  equals the Picard number of  $Y$ , that is, it equals  $\rho = 10$ . This is why  $K_{10}$ -genericity as in Eqn.(20.1) is going to play a role. Recall that Lemma 20.1.9 states that this implies that then all automorphisms of  $Y$  are semi-symplectic. The main result is as follows.

**Theorem 21.2.3** ([16, 172]). *Let  $Y$  be an Enriques surface without nodal curves. Then*

$$\text{Aut}_s(Y) \simeq \text{O}^{\#,-}(\Lambda^G) \simeq \text{O}^-(\Lambda_{\text{Enr}})[2].$$

*In particular, Enriques surfaces without nodal curves have an infinite group of automorphisms. If the period point of  $Y$  in  $D(\Lambda_G)$  is  $K_{10}$ -generic, then all automorphisms of  $Y$  are semi-symplectic.*

*Proof.* Since  $Y$  is non-nodal we can identify the Néron–Severi lattice of  $X$  with  $S = \Lambda^G$  and then  $T = \Lambda_G$  is the transcendental lattice.

Let  $g \in \text{Aut}_s(Y)$  and consider its symplectic lift  $\tilde{g}$  on  $X$ . Being symplectic, it induces the identity on  $T$  and hence also on  $T^*/T \simeq S^*/S$ . Furthermore it preserves the ample cone (which coincides with the positive cone since there are no nodal classes) and so  $\tilde{g}^*|_S \in \text{O}^{\#,-}(S)$ . Conversely, if  $\gamma \in \text{O}^{\#,-}(S)$ , the isometry  $\gamma \oplus \text{id}_T$  of  $S \oplus T$  extends as an isometry to  $\Lambda$ . It preserves the ample cone and respects the Hodge structure and so by Theorem 19.2.2 it is induced by a (symplectic) automorphism of  $X$ .  $\square$

This has several applications as explained e.g. in [16]. As a typical example we show:

**Corollary 21.2.4.** *A non-nodal  $K_{10}$ -generic Enriques surface  $Y$  has 17·31 distinct elliptic fibrations.*

*Proof.* By [15, LemmaVIII. 17.4] a primitive isotropic vector  $e \in C_Y \subset \Lambda_{\text{Enr}}$  corresponds to a pair of half pencils, that is irreducible curves  $E, E'$  with  $E + E' = K_Y$ , and for which the linear system  $|2E| = |2E'|$  is an elliptic pencil<sup>2</sup>

Let  $\Gamma = \text{O}^-(\Lambda_{\text{Enr}})$ , the group of lattice isometries with  $(-)$ -spinor norm 1 (see Section 16.1).The lattice theoretic part of the proof consists of the following steps:  
**Step 1: Transitivity on isotropic vectors.** We claim that the full group  $\text{O}(\Lambda_{\text{Enr}})$  acts transitively on primitive isotropic vectors  $e$  and it then follows that  $\Gamma = \text{O}^-(\Lambda_{\text{Enr}})$  acts transitively on primitive isotropic vectors in the closure of the positive cone. To show the claim, remark that by unimodularity of  $\Lambda_{\text{Enr}}$  there exists a vector  $f \in \Lambda_{\text{Enr}}$  with  $f \cdot e = 1$ . Replacing  $f$  with  $f - q(f)e$ , we may assume that  $f$  is also isotropic. But then  $\{e, f\}$  spans a hyperbolic plane  $U'$  and  $(U')^\perp \simeq E_8(-1)$  since it is unimodular, negative definite and of rank 8. This shows that there is an isometry sending  $U'$  to the copy  $U$  inside  $\Lambda_{\text{Enr}}$  and  $(U')^\perp$  to  $E_8(-1)$ . This isometry sends  $e$  to a basis vector of  $U$  and so  $\text{O}(\Lambda_{\text{Enr}})$  acts transitively on primitive isotropic vectors. For the remainder of the proof we shall identify  $U'$  with  $U$  and  $(U')^\perp$  with  $E_8(-1)$ .

<sup>2</sup>Recall that for an effective divisor  $D$  on  $Y$ , the associated linear system is given by  $|D| = \mathbb{P}(H^0(Y, \mathcal{O}_Y(D)))$ .

**Step 2: Calculation of the stabilizer  $\Gamma_e$  of  $e$  in  $\Gamma$ .** Let  $\gamma \in \Gamma_e$ , then  $\gamma$  induces an isometry  $e^\perp \bmod \mathbb{Z}e \simeq E_8(-1)$ . The resulting map  $\Gamma_e \rightarrow \mathcal{O}(E_8(-1)) = W(E_8)$  (the last equality follow from Corollary 17.2.3) is surjective since any element in  $E_8(-1)$  can be extended to  $\Lambda_{\text{Enr}}$  by defining it as the identity on the  $U$ -summand. As for the kernel of the map, we first note that for any  $y \in E_8(-1)$  the Eichler–Siegel transformation  $\psi_{e,-y}$  given by

$$\psi_{e,-y}(x) = x - (x \cdot y)e + (x \cdot e)y - (x \cdot e)q(y)e, \quad x \in \Lambda_{\text{Enr}},$$

is in  $\Gamma_e$ . Conversely, if  $\gamma \in \ker(\Gamma_e \rightarrow \mathcal{O}(E_8(-1)))$ , then from  $0 = \gamma(e) \cdot \gamma(e) = \gamma(f) \cdot \gamma(f)$ ,  $1 = \gamma(e) \cdot \gamma(f)$  we find  $\gamma(f) = -q(y)e + f + y$  for some  $y \in E_8(-1)$ . Similarly, we find  $\gamma(z) = z - (z \cdot y)e$  for  $z \in E_8(-1)$ . But then  $\gamma = \psi_{e,-y}$ . This shows that  $\Gamma_e \simeq E_8 \rtimes W(E_8)$  with twisted product  $(y, \gamma_1) \cdot (y', \gamma'_1) = (y + \gamma_1(y'), \gamma_1 \circ \gamma'_1)$  induced by the tautological action of  $W(E_8)$  on  $E_8(-1)$ .

**Step 3: Calculation of  $\Gamma[2]_e$ , the stabilizer of  $e$  in  $\Gamma[2]$ .**<sup>3</sup> The 2-congruence subgroup of  $W(E_8)$  is  $\{\pm \text{id}\}$ . See for example [26, Exerc, Chap 6, §4]. Then  $\Gamma[2]_e = 2E_8 \times \{\pm \text{id}\}$ .

**Step 4: The order of the modulo 2 reduction of  $\Lambda_{\text{Enr}}$ .** By Example 8.2.4 the Arf invariant of  $\Lambda_{\text{Enr}}/2\Lambda_{\text{Enr}}$  is 0 and the form is isometric to  $\oplus^5 u_1$ . Then, by the calculations in Section 16.3 we have

$$|\mathcal{O}(\oplus^5 u_1)| = 2 \cdot 2^{5 \cdot 4} \cdot (2^5 - 1)(2^2 - 1)(2^4 - 1)(2^6 - 1)(2^8 - 1) = 2^{21} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot 31.$$

**Step 5: Final argument.** The number of  $\Gamma[2]$ -orbits of  $e$  can be found as follows. The group  $\Gamma[2]$  is normal in  $\Gamma$  and so all  $\Gamma[2]$ -orbits are equivalent under  $\Gamma$  and thus the desired number equals

$$|\mathcal{O}(\Lambda_{\text{Enr}}/2\Lambda_{\text{Enr}})| / |\Gamma_e : \Gamma[2]_e|.$$

Since  $\Gamma_e = E_8 \rtimes W(E_8)$  and  $\Gamma[2]_e = 2E_8 \times \{\pm \text{id}\}$ , the index  $[\Gamma_e : \Gamma[2]_e]$  equals

$$\#(\mathbb{F}_2^8) \cdot \frac{1}{2} |W(E_8)| = 2^8 \cdot 2^{13} \cdot 3^5 \cdot 5^2 \cdot 7 = 2^{21} \cdot 3^5 \cdot 5^2 \cdot 7,$$

and we get the desired number of elliptic fibrations.  $\square$

**21.2.B Automorphisms of Enriques surfaces of fixed nodal type.** Let  $(X, j)$  be a K3 surface endowed with an Enriques involution, and which has nodal type  $\Delta := \Delta(X)$ . For simplicity of notation we also set  $\Delta^\pm := \Delta^\pm(X)$  and we identify  $\Delta(Y)$ ,  $Y = X/G$  with  $\Delta$ .

With  $S = \langle \Lambda, \Delta^- \rangle$ , the smallest primitive sublattice of the K3 lattice  $\Lambda$  generated by  $\Lambda^G$  and  $\Delta^-$ , the moduli point of  $(X, j)$  belongs to the period domain

$$D_{\text{Enr}}(S) := D(S) \cap D_{\text{Enr}} \subset D(S) \cap D(\Lambda_G),$$

the period domain of Enriques surfaces of nodal type  $\Delta$ . The codimension of  $D(S)$  in  $D(\Lambda)$  equals  $\text{rank}(S)$  and so the Néron–Severi lattice of a general Enriques surface  $X$  of nodal type  $\Delta$  is precisely  $S$ .

<sup>3</sup>Recall that  $\Gamma[2]$  is the two-congruence subgroup of  $\Gamma$  (cf. (17.3)).

Theorem 20.1.1 tells us that the group of symplectic automorphisms of  $X$  equals  $\mathcal{O}^{-\#}(S)/W^-(S)$  while for  $Y = X/G$  we need to restrict to the corresponding subgroup of  $\mathcal{O}(S, \iota_{\text{Enr}})$ . By Proposition 21.1.3, the Weyl group of  $S$  is generated by reflections in the  $(-4)$ -roots  $s^+ \in \Delta^+$  and hence

$$\text{Aut}_s(X, j) \simeq \mathcal{O}^{-\#}(S, \iota_{\text{Enr}})/W^-(\Delta^+).$$

Note that for all  $r \in \Delta$  the composition  $s_r \circ s_{\iota_{\text{Enr}} r}$  acts as  $s_{r^+}$  on  $\Lambda$  which gives a natural extension of the action of  $W^-(\Delta^+)$  to  $S$ . Since  $S = \langle \Lambda^G \oplus \Delta^- \rangle$  and  $\mathcal{O}(\langle \Lambda^G \oplus \Delta^- \rangle) = \mathcal{O}(\Lambda^G \oplus \Delta^-)$ , setting

$$G(\Delta^-) := \mathcal{O}^{-\#}(\Lambda^G) \times \mathcal{O}^{-\#}(\langle \Delta^- \rangle) = \mathcal{O}^-(\Lambda_{\text{Enr}}) \times \mathcal{O}^-(\langle \Delta^- \rangle), \quad (21.9)$$

we have shown

**Theorem 21.2.5.** *Let  $Y$  be a general Enriques surface of nodal type  $\Delta$ . Its group of semi-symplectic automorphisms is given by  $\text{Aut}_s(Y) = G(\Delta^-)/W^-(\langle \Delta^+ \rangle)$ .*

*Remark 21.2.6.* The group  $\mathcal{O}^-(\langle \Delta^- \rangle)$  contains  $W^-(\Delta^-)$ . By Lemma 21.1.8  $\Delta^-(-\frac{1}{2})$  is a root lattice and so is an orthogonal sum of (classical) irreducible root lattices of type  $A$ - $D$ - $E$ . This decomposition is unique up to permuting isometric irreducible sublattices (by the unicity of the decomposition of a positive definite lattice stated by Theorem 1.12.3) and so by Corollary 17.2.3,  $\mathcal{O}^{-\#}(\langle \Delta^- \rangle)/W^-(\Delta^-)$  is a product of permutation groups coming from isometric factors of the same type provided  $\Delta^-(-\frac{1}{2})$  does not contain irreducible sublattices of type  $D_4$ . In that case the occurrence of such a factor contributes an extra factor, namely the cyclic group  $C_3$ .

**21.2.C Automorphisms of general nodal Enriques surfaces.** In this section  $Y = X/G$  is a general nodal Enriques surface such that  $X$  has Picard number 11, as considered in Example 21.1.11. In this situation  $\Delta^-$  consists of a single pair  $\{r^-, -r^-\}$ . We first calculate  $\Delta(Y)$ , the set of nodal classes of  $Y$  (up to sign).

**Proposition 21.2.7.** *Let  $N$  be the sublattice of the Enriques lattice generated by the set  $\mathbf{R}$  of roots  $\mathbf{s} \in \Lambda_{\text{Enr}}$  corresponding to  $\iota_{\text{Enr}}$ -adapted root pair such that  $s^- = r^-$ . Then  $N = \mathbb{Z}\mathbf{r} \oplus 2 \cdot \mathbf{r}^\perp$  and the roots of  $N$  are precisely the roots that make up  $\Delta(Y)$ .*

*Proof.* First we consider  $r$  and  $\iota_{\text{Enr}}(r)$ . Write  $r = (u, w, \iota_{\text{Enr}}(w')) \in U \oplus W \oplus W'$ . Then  $\iota_{\text{Enr}}(r) = (-u, w', \iota_{\text{Enr}}(w))$  and  $\rho := w + w' \in \Lambda_{\text{Enr}}$  corresponds to  $r^+$ . Setting  $\tau = w - w'$ , the vector  $2u + \tau \in U \oplus \Lambda_{\text{Enr}}$  corresponds to  $r^-$ . The conditions  $r \cdot r = -2$ ,  $r \cdot \iota_{\text{Enr}} r = 0$ ,  $r^+ \cdot r^- = 0$  are equivalent to the three conditions  $\rho \cdot \rho = -2$ ,  $\tau \cdot \tau = -2 - 2u \cdot u$  and  $\rho \cdot \tau = 0$ . Since  $\rho \pm \tau \in 2\Lambda_{\text{Enr}}$ , we may write  $w = \frac{1}{2}(\rho + \tau)$  and  $w' = \frac{1}{2}(\rho - \tau)$ .

Next we consider the set  $\{s, \iota_{\text{Enr}}(s)\} \in \Delta(X)$  with  $s^- = r^-$ . Then, similarly as above,  $s = (u, \frac{1}{2}(\sigma + \tau), \frac{1}{2}\iota_{\text{Enr}}(\sigma - \tau))$ , where  $\sigma \in \Lambda_{\text{Enr}}$  corresponds to the root  $\mathbf{s}$ . Comparing with  $r = (u, \frac{1}{2}(\rho + \tau), \frac{1}{2}\iota_{\text{Enr}}(\rho - \tau))$  one gets

$$s = r + (0, t, \iota_{\text{Enr}}(t)), \quad 2t = \sigma - \rho.$$



Then  $\mathbf{s} = \mathbf{r} + 2t$  in  $\Lambda_{\text{Enr}}$  and so  $\mathbf{s} \cdot \mathbf{s} = -2 = -2 + 4\mathbf{r} \cdot t + 4t \cdot t$  gives  $(\mathbf{r} + t) \cdot t = 0$ . It follows that  $a\mathbf{r} + t$  is orthogonal to  $\mathbf{r}$  if  $a := -\frac{1}{2}t \cdot t$  and so

$$\mathbf{s} = \mathbf{r} + 2t = (1 - 2a)\mathbf{r} + 2(a\mathbf{r} + t) \in \mathbb{Z}\mathbf{r} + 2\mathbf{r}^\perp$$

and hence  $\Delta(Y) \subset N$ . Conversely, if  $t \in \Lambda_{\text{Enr}}$  satisfies  $(\mathbf{r} + t) \cdot t = 0$ , then  $\mathbf{s} := \mathbf{r} + 2t$  is a root corresponding to  $s^+$ , where  $s = \mathbf{r} + t + t_{\text{Enr}}(t)$ . Since  $s^- = \mathbf{r}^-$ , we have  $s \in \Delta(X)$ .

Now roots in  $\Lambda_{\text{Enr}}$  are all conjugate and so we may assume that  $\mathbf{r}$  is a root in the  $E_8(-1)$  summand. If  $\{e, f\}$  is the standard basis for the copy of  $U$  in  $\Lambda_{\text{Enr}}$ , then setting  $t = e - \mathbf{r}$  or  $t = f - \mathbf{r}$ , we see that  $(\mathbf{r} + t) \cdot t = 0$ . So then  $U \subset U \oplus E_8(-1)$  belongs to  $N$ . Similarly this holds for  $t = e + f - g$ , where  $g \in E_8(-1)$  is a root orthogonal to  $\mathbf{r}$ . So  $\mathbb{Z}\mathbf{r} + 2\mathbf{r}^\perp \subset N$  and hence we have equality.  $\square$

*Remark 21.2.8.* Using a reduction to  $(-4)$ -roots whose  $U$ -component is equal to 0, one can show that  $\Gamma_{\text{Enr}}$  acts transitively on roots  $s \in \Delta(X)$  for which  $s^- = \mathbf{r}^-$ .

**Corollary 21.2.9.** *The group  $O^-(N)/W^-(N) = O(N)/W^-(N)$  contains an infinite abelian free group of rank 7.*

*Proof.* With  $\{e, f\}$  the standard basis for the copy of  $U$  in  $\Lambda_{\text{Enr}}$ , write  $e = \pi^*e$ ,  $e$  in the Enriques lattice, note that  $2e$  is one of the generators of  $N$ . In this lattice  $2e$  is primitive and isotropic and  $(2e)^\perp/2e \simeq \langle -2 \rangle \oplus 2 \cdot E_7(-1)$ . Taking the root lattice  $\langle -2 \rangle$  of rank 1 in the statement of Proposition 17.3.7, the corollary follows.  $\square$

We now describe the automorphism group of a general nodal Enriques surface  $Y$ . At this point, recall that if the period point of the universal cover  $X$  is  $K_{11}$ -generic in the sense of Definition 20.1.8, then Lemma 20.1.9 implies that all automorphisms of the Enriques surface are semi-symplectic as in Definition 21.2.2. In this case the group  $G(\Delta^-)$  defined in formula (21.9) is just  $O(\Lambda_{\text{Enr}})[2] \times \{\text{id}, s_{\mathbf{r}}\}$  and hence:

**Corollary 21.2.10** ([173, 187]). *The group of semi-symplectic automorphisms of the general nodal Enriques surface  $Y = X/\langle j \rangle$  is isomorphic to*

$$O(\Lambda_{\text{Enr}})[2] \times \{\text{id}, s_{\mathbf{r}}\}/W^-(N),$$

where  $N \simeq \langle -2 \rangle \oplus 2 \cdot (U \oplus E_7(-1))$ . If, moreover the period point of  $(X, j)$  is  $K_{11}$ -generic, then all automorphisms of  $Y$  are semi-symplectic.

From Corollary 21.2.9 we then deduce:

**Corollary 21.2.11.** *The automorphism group of a general nodal Enriques surface contains a free abelian group of rank 7 and hence is infinite.*

*Remark 21.2.12.* Recall (cf. Lemma 4.1.5) that  $\tilde{T}_{2,3,6}$  is an isometric copy of the Enriques lattice. Let  $\mathbf{r}$  be the root  $\alpha_9$  in the diagram for Lemma 4.1.5. Then  $\mathbb{Z}\mathbf{r} \oplus \mathbf{r}^\perp \subset \Lambda_{\text{Enr}}$  is isometric to  $\tilde{T}_{2,4,6} \subset \tilde{T}_{2,3,6}$ , the so-called **Reye lattice**. Note that  $N = \mathbb{Z} \cdot \mathbf{r} \oplus 2\mathbf{r}^\perp$  has index 2 in the Reye lattice. Since  $\tilde{T}_{2,4,6}$  has index 2 in  $\Lambda_{\text{Enr}}$ ,

using the mod 2 reduction  $\rho_2 : \Lambda_{\text{Enr}} \rightarrow \Lambda_{\text{Enr}}/2\Lambda_{\text{Enr}}$ , one can characterize the Reye lattice as

$$\tilde{T}_{2,4,6} = \rho_2^{-1}(\rho_2(\mathbf{r})) = \{x \in \Lambda_{\text{Enr}} \mid x \equiv \mathbf{r} \pmod{2\Lambda_{\text{Enr}}}\},$$

while  $N = \ker \rho_2|_{\mathbf{r}^\perp}$ . Using this, D. Allcock [1] and F. Cossec–I. Dolgachev [45] gave an alternative proof of Corollaries 21.2.9 and 21.2.10.

**Historical and Bibliographical Notes.** For the moduli of complex Enriques surfaces there are two approaches. The first is E. Horikawa’s [100, 101] using degeneration methods. The second method, used in Ch. VIII. 21 of the book [15] by W. Barth, K. Hulek, C. Peters and A. van de Ven, is not geometric. In the present approach we use a simpler variant of this which is essentially due to Y. Namikawa (cf. [166]).

The results on the automorphism group of Enriques surfaces without nodal curves are due to W. Barth and C. Peters [16] as well as to I. Dolgachev [51] and V. Nikulin [172]. Those on nodal Enriques surfaces are due to D. Allcock [1] and F. Cossec–I. Dolgachev [45] but we give here an alternative presentation based on [187] which depend on previous results [45] by F. Cossec and I. Dolgachev and [173] by V. Nikulin respectively. The Reye lattice coming up in Dolgachev’s presentation, has been named after Th. Reye who in [193] constructed the Reye congruence, probably the first construction (in 1886!) of an Enriques surface.

It is by no means true that all Enriques surfaces have an infinite isomorphism group. The cited works give many examples of Enriques surface with only finitely many automorphisms. A systematic study thereof has been made by V. Nikulin [173] and S. Kondō [126]. We also want to mention Chapter 9 in S. Kondō’s monograph [129] which contains background on moduli spaces and automorphisms, and contains several instructive examples.

Finally, we want to point out that also in positive characteristic one can use lattice theory to describe moduli and automorphisms of Enriques surfaces. See for instance the forthcoming monograph [46, 53] by I. Dolgachev in cooperation with F. Cossec, C. Liedtke (for part I) and S. Kondō (for part I and II).

# A

## Background in Algebra and Number Theory

### A.1 Modules over Principal Ideal Domains

We collect some standard results about modules over a principal ideal domain  $R$ . For background and proofs of the results see for instance [242, Ch. 12].

Let  $M$  be a finitely generated  $R$ -module. By definition its *torsion submodule* equals

$$\text{Tors}(M) = \{x \in M \mid \exists r \in R, r \neq 0 \text{ such that } rx = 0\}.$$

The quotient  $M/\text{Tors}(M)$  is isomorphic to a direct sum of  $\text{rank}(M)$  copies of  $R$ . Such a module is called a *free  $R$ -module*. Any submodule of a free module is free and a quotient of an  $R$ -module by a submodule of the same rank is torsion:

**Lemma A.1.1.** *Let  $R$  be a principal ideal domain and let  $M$  be a free finitely generated  $R$ -module and  $M' \subset M$  a submodule of the same rank. Then  $M/M'$  is an  $R$ -torsion module and every torsion module is of this form. More precisely,  $M$  admits a basis  $\{e_1, \dots, e_{r+s}\}$  such that  $M' = \bigoplus_{k=1}^r R e_k \oplus \bigoplus_{k=1}^s R \cdot (d_k e_{r+k})$  with  $d_j$  non-units such that  $d_1 | d_2 | \dots | d_s$ , and hence  $M/M' \simeq R/d_1 R \oplus \dots \oplus R/d_s R$ .*

This result leads to:

**Theorem A.1.2** (Elementary divisor theorem). *Let  $R$  be a principal ideal domain and let  $T$  be a finitely generated torsion  $R$ -module. There is an isomorphism  $T \simeq R/d_1 R \oplus \dots \oplus R/d_s R$ , with  $d_j$  non-units such that  $d_1 | d_2 | \dots | d_s$ . The ideals generated by  $d_j$ , the **elementary divisors**, are uniquely determined by  $T$  and the resulting decomposition is the **invariant factor decomposition** of  $T$ .*

There is another canonical decomposition for  $T$ . First some terminology. For  $p \in R$  irreducible, one says that a finitely generated torsion module is  *$p$ -primary* if every element is annihilated by some power of  $p$ . Setting

$$T_p = \{x \in T \mid p^n \cdot x = 0 \text{ for some power } p^n \text{ of } p\},$$

we obtain the maximal  $p$ -primary torsion submodule, the  $p$ -primary part of  $T$ . This leads to the  *$p$ -primary decomposition*, or *Sylow decomposition*:

$$T = \bigoplus_{(p) \text{ prime ideal}} T_p, \quad T_p \simeq \underbrace{\bigoplus_{e \geq 1} R/p^e R \oplus \dots \oplus R/p^e R}_{s_{p,e}}. \quad (\text{A.1})$$

The  $s_{p,e}$  summands of the decomposition of  $T_p$  with fixed  $e$  are called the *homogeneous summands of exponent  $e$* . Note that the above isomorphism for  $T_p$  is *not* canonically determined by  $T$  as demonstrated in Example A.1.4.2 below.

To relate this decomposition to the invariant factor decomposition, one uses that if  $\gcd(r, r') = 1$  in  $R$ , then we obtain  $R/r'r'R \simeq R/rR \oplus R/r'R$ . Write  $d_j = \text{unit} \cdot \prod_{p \text{ irreducible}} p^{a_{jp}}$ ,  $j = 1, \dots, s$ . Then  $R/d_jR \simeq \bigoplus_p R/p^{a_{jp}}R$  and so  $T_p \simeq \bigoplus_{j=1}^s R/p^{a_{jp}}R$ .

We frequently use the concept of length: the **length**  $\ell(G)$  of a finite abelian torsion  $R$ -module  $G$  is equal to the minimal number of generators (by definition). In particular, the length of  $T_p$  is at most  $s$ , and for primes dividing  $d_1$  the length equals  $s$ .

If  $T = T_p$  is homogeneous of degree  $e$ , its length equals the number of summands isomorphic to  $R/p^eR$ . So in (A.1) the length of  $T_p$  equals  $\sum_e s_{p,e}$  and we have:

**Lemma A.1.3.** *The length of a torsion  $R$ -module  $T$  of finite rank with Sylow decomposition  $T = \bigoplus T_p$  equals  $\max(\ell_p) = \#(\text{elementary divisors})$  where  $\ell_p$  is the length of  $T_p$ .*

**Examples A.1.4.** 1. If  $R = \mathbb{Z}$  a torsion module is the same as a finite abelian group, and a  $p$ -primary  $\mathbb{Z}$ -torsion module is the same as a  $p$ -primary group.

2. We assume  $R = \mathbb{Z}$ . Suppose the elementary divisors of  $T$  are  $(4, 12, 48)$ . Then  $T_2 \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ ,  $T_3 \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$  and  $\ell(T) = 3$ . Suppose  $\{e_1, e_2, e_3\}$  is an ordered basis of  $T_2$ , i.e., a basis reflecting the above isomorphism. Then  $\{f_1 = e_1 + 2e_2 + 4e_3, f_2 = e_2 + 4e_3, f_3 = 3e_3\}$  is also an ordered basis of  $T_2$  and so the isomorphism  $T_2 \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$  is not unique.

We finish this section by recalling some modular arithmetic. The multiplicative group of units  $R^\times$  of the ring  $R = \mathbb{Z}/m\mathbb{Z}$  has order  $\varphi(m)$ , the number of elements modulo  $m$  that are coprime with  $m$ . In what follows elements  $r$  of  $R$  are viewed as additive classes of integers modulo  $m$  and we write  $r = \bar{x}$ , where  $x \in \mathbb{Z}$ . If the group  $(\mathbb{Z}/m\mathbb{Z})^\times$  is cyclic and  $r$  is a generator, one says that  $r$  is a *primitive generator modulo  $m$* . We denote the (multiplicative) cyclic group of order  $n$  by  $C_n$  (in contrast to the additive version  $\mathbb{Z}/n\mathbb{Z}$ ).

The next result can be found in elementary textbooks on number theory, e.g. [113].

**Lemma A.1.5.** 1. *The units of the finite cyclic groups have the following structure:*

(a) *For  $p$  odd the groups  $(\mathbb{Z}/p^k\mathbb{Z})^\times$  and  $(\mathbb{Z}/2p^k\mathbb{Z})^\times$  are cyclic of order  $p^k - p^{k-1}$ . For  $p = 2$  we have*

$$(\mathbb{Z}/2^k\mathbb{Z})^\times = \begin{cases} 1 & \text{if } k = 1 \\ C_2 \text{ generated by } \overline{-1} & \text{if } k = 2 \\ C_2 \times C_{2^{k-2}} \text{ generated by } (\overline{-1}, \overline{\pm 3}) & \text{if } k \geq 3. \end{cases}$$

(b) *In general, writing  $m = 2^k \prod_p p^{k_p}$ , where the product is over odd primes  $p$ , we have*

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq (\mathbb{Z}/2^k\mathbb{Z})^\times \times \prod_p (\mathbb{Z}/p^{k_p}\mathbb{Z})^\times.$$

In particular, only for  $m = 2, 4, p^k$  and  $2p^k$  there exist primitive generators modulo  $m$ .

2. The group  $D(\mathbb{Z}/m\mathbb{Z})$  of units of  $\mathbb{Z}/m\mathbb{Z}$  modulo squares has the following structure:

(a) In the cases  $m = p^k$  and  $2p^k$  the group  $D(\mathbb{Z}/m\mathbb{Z})$  is cyclic of order 2 and generated by a non-square modulo  $p^k$ :

$$D(\mathbb{Z}/p^k\mathbb{Z}) = \{1, u \bmod p^k\} \simeq C_2, \quad p \text{ an odd prime and } u \text{ a non-square modulo } p^k.$$

(b) For  $p = 2$  we have:

$$D(\mathbb{Z}/2^k\mathbb{Z}) = \begin{cases} \{\bar{1}\} & \text{for } k = 1, \\ \{\bar{1}, \bar{3}\} \simeq C_2 & \text{for } k = 2, \\ \{\bar{1}, \bar{3}, -\bar{3}, -\bar{1}\} \simeq C_2 \times C_2 & \text{if } k \geq 3. \end{cases}$$

## A.2 The Field $\mathbb{Q}_p$

We collect some basic properties of the  $p$ -adic field  $\mathbb{Q}_p$ . The proofs can be found for instance in [204, Chap. II].

**The  $p$ -adic valuation and  $\mathbb{Q}_p$ .** The field of  $p$ -adic numbers  $\mathbb{Q}_p$  is the completion of  $\mathbb{Q}$  with respect to the  *$p$ -adic valuation*  $v_p$  on  $\mathbb{Q}$  which is defined as follows: first, one sets  $v_p(0) = \infty$ . Next, for a non-zero number  $x = p^k \frac{u}{v}$  with  $\gcd(u, p) = \gcd(v, p) = 1$ , one sets

$$v_p(x) = k, \quad \|x\|_p = p^{-k}. \quad (\text{A.2})$$

Obviously, one has

$$v_p(xy) = v_p(x) + v_p(y). \quad (\text{A.3})$$

Furthermore,  $v_p$  is a non-archimedean valuation in the sense that

$$v_p(x + y) \geq \min(v_p(x), v_p(y)) \text{ with equality if } v_p(x) \neq v_p(y). \quad (\text{A.4})$$

By definition of a completion, we have a natural embedding

$$\iota_p : \mathbb{Q} \hookrightarrow \mathbb{Q}_p. \quad (\text{A.5})$$

We may think of  $\mathbb{Q}_p$  as the field of Laurent series of the form

$$x_{-m}p^{-m} + \cdots + x_{-1}p^{-1} + x_0 + x_1p + \cdots + x_kp^k + \cdots, \quad x_j \in [0, p-1].$$

The series without terms having negative powers of  $p$  form the subring of the integers  $\mathbb{Z}_p$ ; the units therein correspond to the power series starting with a non-zero constant term. The ring  $\mathbb{Z}_p$  is a *principal ideal domain*: an ideal  $I$  is generated by an element  $x \in I$  with minimal valuation  $k$ , for example  $x = p^k$  so that  $I = (p^k)$ .

Laurent series having only a finite number of terms give rational numbers of the form  $x/p^m$  with  $x \in \mathbb{Z}$  and  $\gcd(x, p) = 1$ . The totality of such rational numbers forms a subring  $\mathbb{Q}^{(p)} \subset \mathbb{Q}$ . The integers of course form a subring of  $\mathbb{Q}_p$  as well as of  $\mathbb{Z}_p$ . Since under the inclusions  $\mathbb{Q}^{(p)} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{Q}_p$  the rational number  $y = x/p^m$ ,  $x \in \mathbb{Z}$ , is a  $p$ -adic integer if and only if  $y$  is an integer, one obtains an injection  $\mathbb{Q}^{(p)}/\mathbb{Z} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ , and from the description of  $\mathbb{Q}_p$  as Laurent series in  $p$ , this is a surjection as well. Hence, one obtains an isomorphism

$$\mathbb{Q}^{(p)}/\mathbb{Z} \simeq \mathbb{Q}_p/\mathbb{Z}_p.$$

There are also natural reduction homomorphisms

$$\mathbb{Z}_p \rightarrow \mathbb{Z}/p^{k+1}\mathbb{Z}, \quad u = x_0 + x_1p + \dots + x_kp^k + \dots \mapsto x_0 + x_1p + \dots + x_kp^k = u \pmod{p^{k+1}}.$$

For  $k = 0$  this is a surjection  $\mathbb{Z}_p \rightarrow \mathbb{F}_p$  with kernel the maximal ideal  $(p) \subset \mathbb{Z}_p$ . The groups  $D(\mathbb{Q}_p)$  and  $D(\mathbb{Z}_p)$  are described by the following result.

**Theorem A.2.1.** *1. Suppose  $p$  is an odd prime. Then  $x \in \mathbb{Q}_p^\times$  can be written uniquely as  $x = up^k$  with  $u$  a unit in  $\mathbb{Z}_p$ . It is a square if and only if  $k$  is even and  $u \equiv 1 \pmod{p}$ .*

*The group  $D(\mathbb{Q}_p)$  is isomorphic to the Klein group with representatives  $1, p, u, up$ , where  $u$  is a unit in  $\mathbb{Z}_p$  such that  $u \pmod{p}$  is a non-square.*

*The group  $D(\mathbb{Z}_p)$  is cyclic of order two, generated by a non-square in  $\mathbb{Z}_p^\times$ .*

*2. A dyadic number  $x \in \mathbb{Q}_2$  can be uniquely written as  $x = u \cdot 2^k$ ,  $u$  a unit in  $\mathbb{Z}_2$ . It is a square if and only if  $k$  is even and  $u \equiv 1 \pmod{8}$ . The group  $D(\mathbb{Q}_2)$  is isomorphic to  $C_2 \times C_2 \times C_2$  with generators  $2, 3, 5 \pmod{8}$ .*

*A unit  $u \in \mathbb{Z}_2$  is a square if and only if  $u \pmod{8}$  is a square, and  $D(\mathbb{Z}_2)$  is isomorphic to the Klein group  $(\mathbb{Z}/8\mathbb{Z})^\times = C_2 \times C_2$  with generators  $3, 5 \pmod{8}$ .*

**Topology on  $\mathbb{Q}_p$ .** The  $p$ -adic valuation induces a distance on the field  $\mathbb{Q}_p$  given by  $d(x, y) = \|x - y\|_p$  and hence we get a topology, the  **$p$ -adic topology**. The subring  $\mathbb{Z}_p$ , being the projective limit of the finite groups  $A_n = \mathbb{Z}/p^n\mathbb{Z}$  can be equipped with a topology by demanding that the  $A_n$  have the discrete topology. Hence  $\mathbb{Z}_p$  is compact. It turns out (cf. [204, Ch. II, Prop. 3]) that this topology coincides with the  $p$ -adic topology. One then easily deduces ([204, Ch. II, Prop. 4]):

**Proposition A.2.2.** *The  $p$ -adic topology on  $\mathbb{Q}_p$  has the following properties:*

- 1.  $\mathbb{Q}_p$  is locally compact and contains  $\mathbb{Z}_p$  as an open compact subring.*
- 2. The field  $\mathbb{Q}$  is dense in  $\mathbb{Q}_p$  and the ring  $\mathbb{Z}$  is dense in  $\mathbb{Z}_p$ .*

### A.3 Approximation Theorems Related to Vector Spaces and Lattices

The classical approximation theorems gathered in this section play a role in Chapter 14. We refer to [36, Chapter 9] and [122, §23,24] for more details.

Recall that  $\mathcal{P}$  is the set of places of  $\mathbb{Z}$ , i.e., the set of prime numbers, finite places of  $\mathbb{Z}$ , together with  $\infty$ , the infinite place of  $\mathbb{Z}$ . Given a finite subset  $S \subset \mathcal{P}$ , the embeddings  $\iota_p : \mathbb{Q} \hookrightarrow \mathbb{Q}_p$  (see (A.5)) and the natural embedding  $\iota_\infty : \mathbb{Q} \hookrightarrow \mathbb{R} = \mathbb{Q}_\infty$  induce a diagonal embedding  $\iota_S : \mathbb{Q} \hookrightarrow \prod_{v \in S} \mathbb{Q}_v$ . It enjoys a well-known density property (cf. [204, Ch II.2.2]):

**Proposition A.3.1** (Weak approximation). *If  $S$  is finite, the embedding  $\iota_S$  is a dense embedding with respect to the product topology.*

We derive from this a result which is used in the main text:

**Corollary A.3.2.** *Suppose that for some finite set  $S \subset \mathcal{P}$  and all  $p \in S$  we are given  $c_p \in \mathbb{Q}_p^\times$ . Then there exists  $c \in \mathbb{Q}^\times$  such that the coset of  $c$  in  $D(\mathbb{Q}_p)$  equals the coset of  $c_p$  for all  $p \in S$ .*

*Proof.* The crucial remark here is that any  $c \in \mathbb{Q}^\times$  sufficiently close to a representative of  $c_p \in D(\mathbb{Q}_p)$  still represents the class of  $c_p$ . For  $p = \infty$  this is clear. For a prime  $p$  we can write  $c_p = c - d_p$ , where  $c = \sum_{j \leq k} \gamma_j p^j \in \mathbb{Q}$  and  $d_p = \sum_{j > k} \gamma_j p^j$ , where  $k$  is chosen so that  $c = c_p + d_p$  with  $v_p(d_p) \geq v_p(c_p) + 3$ . Setting  $e_p = c_p^{-1} d_p$ , by (A.3) one has  $v_p(e_p) \geq 3$  and then the  $p$ -adic unit  $1 + e_p$  is a square by Theorem A.2.1, and consequently  $c = c_p(1 + e_p)$  is equal to  $c_p$  up to squares. In other words, if the  $p$ -adic distance of  $c$  to  $c_p$  is less than  $p^{-3}$ , then  $c$  represents  $c_p(\mathbb{Q}_p^\times)^2$ . The weak approximation theorem then gives us a rational number  $c$  this close to  $c_p$  for all  $p \in S$ .  $\square$

Next let  $V$  be a finite dimensional  $\mathbb{Q}$ -vector space and let  $V_v$ ,  $v \in \mathcal{P}$ , be its localization. The latter vector space has a natural  $v$ -adic topology making  $V_v$  homeomorphic to  $\mathbb{Q}_v^n$ ,  $n = \dim V$ . The natural embedding  $V \hookrightarrow V_v$ ,  $v \in \mathcal{P}$ , is continuous for the  $v$ -adic topology and applying Proposition A.3.1, we find that the natural diagonal embedding

$$V \hookrightarrow \prod_{v \in S} V_v, \quad S \subset \mathcal{P} \text{ finite} \quad (\text{A.6})$$

is dense. This embedding induces a natural embedding  $O(V) \hookrightarrow \prod_{v \in S} O(V_v)$ . Since an orthogonal transformation can have determinant  $\pm 1$ , this cannot be a dense embedding, but for the special orthogonal group one has a density result:

**Proposition A.3.3** (Weak approximation for the rotation group). *Let  $(V, q)$  be a (non-degenerate) quadratic  $\mathbb{Q}$ -vector space and let  $S \subset \mathcal{P}$  be a finite set of places. Then the natural diagonal embedding  $SO(V) \hookrightarrow \prod_{v \in S} SO(V_v)$  is dense.*

For proofs see, e.g., [36, Chapter 9, Thm. 7.2], [122, Satz 23.1].

**Corollary A.3.4.** *Let  $(V, q)$  be a (non-degenerate) quadratic  $\mathbb{Q}$ -vector space of dimension  $\geq 2$ . Let  $S \subset \mathcal{P}$  be a finite set of places. Suppose that  $t \in \mathbb{Q}^\times$  is represented by  $q$ . Then for given  $x_v \in V_v$ ,  $v \in S$  with  $q(x_v) = t$ , there exists  $x \in V$  with  $q(x) = t$  which is as close to each of the  $x_v$  as we want.*

*Proof.* Let  $z \in V$  be such that  $q(z) = t$ . Since  $q(z) = q(x_v)$ , within  $V_v$  one can apply Witt's extension theorem 7.2.8 to extend the isometry  $z \mapsto x_v$  to an isometry  $g_v \in \mathbf{O}(V_v)$ . To get a rotation, we might have to replace  $g_v$  by  $g_v \circ \sigma_w$  where  $\sigma_w$  is the reflection in a vector  $w$  orthogonal to  $v$ . This is possible since  $\dim V \geq 2$ . Now approximate the  $g_v$  by  $g \in \mathbf{SO}(V)$ , then  $x = g(z)$  approximates  $g_v(z) = x_v$ .  $\square$

*Remark A.3.5.* As to lattices, since  $\mathbb{Z}_p$  is open and compact in  $\mathbb{Q}_p$ , any lattice  $L_p$  in  $V_p$  is open and compact in  $V_p$ . This is not the case for the place  $\infty$ . Also, the subgroup  $\mathbf{O}(L_p)$  of  $\mathbf{O}(V_p)$  stabilizing a lattice  $L_p \subset V_p$  is an open subgroup.

There are also strong approximation results, valid for *indefinite* quadratic spaces. The following result is a lattice version:

**Theorem A.3.6** (Strong Approximation Theorem [36, Ch. 9, Thm. 1.5]). *Let  $(L, b)$  be a non-degenerate indefinite integral lattice of rank  $\geq 4$  and  $t$  a non-zero integer. Suppose that*

$$b(x_p, x_p) = t \text{ for some } x_p \in L_p \text{ (and all } p \in \mathcal{P}\text{)}.$$

*Then there exists  $x \in L$  such that  $b(x, x) = t$ .*

*Further, given a finite set of places  $S \subset \mathcal{P}$ , we can require  $x \in L$  to be  $p$ -adically arbitrarily close to  $x_p$  for all  $p \in S$ .*

This approximation theorem is at the heart of the proof of the strong approximation theorem for the spin group, Theorem 14.3.1. Let us give another application which is used in the main text.

**Corollary A.3.7.** *Let  $(L, b)$  be an indefinite non-degenerate quadratic lattice of rank  $\geq 4$  and let  $x \in L$  be a vector with  $b(x, x) = t \neq 0$ . Then there are infinitely many  $y \in L$  with  $b(y, y) = t$ .*

*Proof.* Let  $S = \{p\}$  be an odd prime number such that  $L_p$  is unimodular, which is clearly possible (take for  $p$  any odd prime not dividing  $\text{disc}(L)$ ). By Corollary 10.2.4  $L_p$  has an isotropic vector and hence the hyperbolic plane  $U$  splits off from  $L_p$ . Relative to the standard basis  $\{e, f\}$  for  $U$ , a vector  $x = \xi_1 e + \xi_2 f \in L_p$  satisfies  $t = b(x, x)$  if  $2\xi_1\xi_2 = t$ . This equation has infinitely many solutions  $(2u, tu^{-1})$ ,  $u \in \mathbb{Z}_p^\times$ , and so we have infinitely many  $y_p^i \in L_p$ ,  $i = 1, 2, \dots$ , with  $b(y_p^i, y_p^i) = t$ . Taking  $y_p^i \in L_p$  for this fixed prime  $p$ , and the localization  $x_q$  of the vector  $x$  at places  $q \neq p$ , the strong approximation theorem (with  $S = \{p\}$ ) provides a vector  $y^i \in L$  for which  $b(y^i, y^i) = t$  and such that its localization at  $p$  is as close as we want to any of the given  $y_p^i$ . This gives infinitely many vectors  $y^i \in L$  for which  $b(y^i, y^i) = t$ .  $\square$

## A.4 Hilbert Symbols

The reader finds here properties of the Hilbert symbols relevant for this book, as treated in [204, Ch. II and Ch. III].



In this section Legendre symbols are employed whose definition we recall. Let  $p$  be a prime, then for  $x \not\equiv 0 \pmod{p}$

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a square mod } p \\ -1 & \text{else.} \end{cases}$$

The Legendre symbol is multiplicative in the sense that  $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right)$ . This can be used to calculate these symbols effectively. For more information, see e.g. [204, Chap. I].

**Definitions and Properties.** Let  $v \in \mathcal{P}$  and let  $a, b \in \mathbb{Q}_v^\times$ . Define the *Hilbert symbol* (at  $v$ ) as follows:<sup>1</sup>

$$(a, b)_v = \begin{cases} 1 & \text{if } z^2 = ax^2 + by^2 \text{ has a non-trivial solution } (z, x, y) \text{ in } \mathbb{Q}_v^3, \\ -1 & \text{otherwise.} \end{cases}$$

This symbol only depends on the class of  $a$  and  $b$  modulo multiplication by a square. For the place  $v = \infty$  one has

$$(1, 1)_\infty = (1, -1)_\infty = (-1, 1)_\infty = 1, \quad (-1, -1)_\infty = -1.$$

To compute these symbols at primes, Hensel's Lemma (cf. [204, II.2.2, Cor. 1]) is useful:

**Lemma A.4.1** (Hensel's lemma). *Let  $f(X_1, \dots, X_n) \in \mathbb{Z}_p[X_1, \dots, X_n]$  and suppose that  $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_p^n$  is a simple zero of  $f \pmod{p}$ , that is,  $f(\mathbf{a}) \equiv 0 \pmod{p}$  and the gradient  $\nabla f$  at  $\mathbf{a}$  is not identically zero mod  $p$ . Then this zero can be lifted to  $\mathbb{Z}_p^n$ . In other words, there exists  $\mathbf{b} \in \mathbb{Z}_p^n$  with  $f(\mathbf{b}) = 0$  and  $\mathbf{a} \equiv \mathbf{b} \pmod{p}$ .*

**Example A.4.2.** Suppose  $p$  is an odd prime. The equation  $ax^2 + by^2 = c$ ,  $a, b \in \mathbb{F}_p^\times$ , and  $c \in \mathbb{F}_p$  has at least one solution by the "shoe box principle". Indeed, consider  $D = \{0, 1, \dots, \frac{1}{2}(p-1)\}$ ; then the maps

$$D \rightarrow \mathbb{F}_p, \quad x \mapsto ax^2, \quad y \mapsto c - by^2$$

are injective and so their images have at least one element in common. Of course, this could be the trivial solution in case  $c = 0$ , but, if  $a, b, c$  lift to units in  $\mathbb{Z}_p$ , the equation  $ax^2 + by^2 = c$  has a solution in  $\mathbb{Z}_p$  as we see from Hensel's Lemma A.4.1. In particular, taking  $c = 1$ , we see that  $(a, b)_p = 1$  in this case.

We also need a more subtle dyadic version (cf. [204, II.2.2 Cor. 3]):

**Lemma A.4.3** (Hensel's lemma, II). *Let  $q$  be a unimodular dyadic quadratic form of rank  $n$ , and let  $\mathbf{a} \in \mathbb{Z}_2$ . If a primitive dyadic solution for  $q(\mathbf{x}) \equiv \mathbf{a} \pmod{8}$  exists, then there is also a "true" dyadic solution for  $q(\mathbf{x}) = \mathbf{a}$ .*

<sup>1</sup>Also written as  $\left(\frac{a, b}{v}\right)$ .

The Hilbert symbol at  $v$  is a symmetric bilinear function

$$D(\mathbb{Q}_v) \times D(\mathbb{Q}_v) \xrightarrow{(-, -)_v} \{\pm 1\}.$$

To calculate the symbol, it is enough to know it on a set of generators (see e.g. [204, Ch. III, Thm. 1]):

**Theorem A.4.4.** *Let  $a, b \in \mathbb{Q}_p$ ,  $p$  prime. Write  $a = p^\alpha u$ ,  $b = p^\beta v$  with  $u, v \in \mathbb{Z}_p^\times$ . Then, recalling that*

$$\varepsilon(u) = \begin{cases} 0 & \text{if } u \equiv 1 \pmod{4}, \\ 1 & \text{if } u \equiv -1 \pmod{4}, \end{cases} \quad \text{and } \omega(u) = \begin{cases} 0 & \text{if } u \equiv \pm 1 \pmod{8}, \\ 1 & \text{if } u \equiv \pm 3 \pmod{8}, \end{cases}$$

one has:

1. *If  $p$  is odd,  $(a, b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$ . In particular, if  $a$  and  $b$  are units,  $(a, b)_p = 1$ .*
2. *For  $p = 2$ , write  $a = 2^\alpha u$ ,  $b = 2^\beta v$  with  $u, v \in \mathbb{Z}_2^\times$ . Then*

$$(a, b)_2 = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)}.$$

Consult [204, III.1] for a proof. It is a consequence of the following rules. Here  $a, a', b, c \in \mathbb{Q}_v^\times$ .

$$(a, b)_v = (b, a)_v, \tag{A.7}$$

$$(a, c^2)_v = 1, \tag{A.8}$$

$$(a, -a)_v = (a, 1 - a)_v = 1, \tag{A.9}$$

$$(aa', b)_v = (a, b)_v (a', b)_v \tag{A.10}$$

$$(a, b)_v = (a, -ab)_v = (a, (1 - a)b)_v. \tag{A.11}$$

We give an application to solve the question "for how many vectors  $b \in D(\mathbb{Q}_p)$  one has  $(a, b)_p = 1$  or  $(a, b)_p = -1$ ". The answer is needed in Chapter 3. Note that this makes sense since  $(a, b)_p$  only depends on the classes of  $a$  and  $b$  in  $D(\mathbb{Q}_p)$ . Since the formulation of the result uses linear algebra over the field  $\mathbb{F}_2$ , observe that the ring  $D(\mathbb{Q}_p)$  can be considered as a vector space  $V$  over the field  $\mathbb{F}_2$ , and Theorem A.2.1 gives its dimension:

$$r := \dim V = \begin{cases} 2 & \text{if } p \neq 2 \\ 3 & \text{if } p = 2. \end{cases}$$

The result we are after is as follows:

**Lemma A.4.5.** *1. Let  $r = \dim_{\mathbb{F}_2} D(\mathbb{Q}_p)$  and let  $a \in D(\mathbb{Q}_p)$ . For  $a \neq 1$  and  $\varepsilon \in \{1, -1\}$ , the equation  $(a, x)_p = \varepsilon$  has  $2^{r-1}$  solutions. For  $a = 1$  one has  $(a, x)_p = 1$  for all  $x \in D(\mathbb{Q}_p)$  and  $(1, x)_p = -1$  has no solutions.*

2. Let  $\mathbf{a}, \mathbf{a}' \in D(\mathbb{Q}_p)$ . Assume that for some  $\varepsilon, \varepsilon' \in \{1, -1\}$  each of the two equations  $(\mathbf{a}, x)_p = \varepsilon$  and  $(\mathbf{a}', x)_p = \varepsilon'$  has a solution in  $D(\mathbb{Q}_p)$ . Then no common solution exists if and only if one has simultaneously  $\mathbf{a} = \mathbf{a}'$  and  $\varepsilon = -\varepsilon'$ .

*Proof.* 1. This can be seen as follows. The equation  $(\mathbf{a}, x)_p = 1$  gives the kernel of the homomorphism of groups  $x \mapsto (\mathbf{a}, x)_p$  and so defines a hyperplane in  $D(\mathbb{Q}_p)$ . It contains  $2^{r-1}$  elements and its complement  $\{x \in D(\mathbb{Q}_p) \mid (\mathbf{a}, x)_p = -1\}$  is an affine hyperplane, also counting  $2^{r-1}$  elements. The last statement is (A.8).

2. If each of the equations has solutions and the sets of solutions  $H_{\mathbf{a}}^\varepsilon, H_{\mathbf{a}'}^{\varepsilon'}$  are disjoint, both sets must contain  $2^{r-1}$  elements and also  $\varepsilon = -\varepsilon'$ . But then  $H_{\mathbf{a}}^{\pm 1} = H_{\mathbf{a}'}^{\pm 1}$  and so  $(x, \mathbf{a})_p = (x, \mathbf{a}')_p$  for all  $x \in D(\mathbb{Q}_p)$ . This implies that also  $\mathbf{a} = \mathbf{a}'$ .  $\square$

**Global properties** Consult [204, Ch. III.2]) for the following two results.

**Theorem A.4.6** (Hilbert's product formula). *Given  $\mathbf{a}, \mathbf{b} \in \mathbb{Q}^\times$ , then  $(\mathbf{a}, \mathbf{b})_v = 1$  for all but a finite number  $S$  of places and for those  $\prod_{v \in S} (\mathbf{a}, \mathbf{b})_v = 1$ .*

**Theorem A.4.7** (Existence of rational numbers with given Hilbert symbol). *Given a finite set of non-zero rational numbers  $\{\mathbf{a}_j\}_{j \in I}$  and a family of numbers  $\{\varepsilon_{j,v}\}_{j \in I, v \in \mathcal{P}}$ , each equal to  $\pm 1$ . Suppose that the following conditions are verified*

1. *All but a finite number of the  $\varepsilon_{j,v}$  are equal to 1.*
2. *For all  $j \in I$  one has  $\prod_{v \in \mathcal{P}} \varepsilon_{j,v} = 1$ .*
3. *(Local existence) For all  $v \in \mathcal{P}$  there exists  $x_v \in \mathbb{Q}_v$  such that  $(\mathbf{a}_j, x_v)_v = \varepsilon_{j,v}$  for all  $j \in I$ .*

*Then there exists a non-zero rational number  $x$  such that*

$$(\mathbf{a}_j, x)_v = \varepsilon_{j,v} \text{ for all } j \in I \text{ and all } v \in \mathcal{P}.$$

*Conversely, if such  $x$  exists, 1, 2 and 3 must hold.*

## A.5 Symplectic Forms and Symplectic Groups

In this section the reader finds basic material on the symplectic group; see D. Taylor's book [223].

Let  $V$  be a finite dimensional vector space over some field  $k$  which is equipped with an **alternating bilinear form**  $b$ , that is a bilinear form for which

$$b(x, x) = 0, \quad x \in V.$$

Consequently, since  $0 = b(x + y, x + y) = b(y, x) + b(x, y)$ , the form  $b$  is skew-symmetric. If the characteristic of  $k$  is different from 2, then the converse is true.

The pair  $(V, b)$  is called a **symplectic  $k$ -space**. As for symmetric bilinear forms, one can define orthogonality and orthogonal direct sums. A symplectic form  $b$  is non-degenerate if any  $x$  for which  $b(x, V) = 0$  necessarily vanishes.

**Examples A.5.1.** 1. The standard example of a non-degenerate symplectic space is the **symplectic plane**  $J$  with basis  $\{e, f\}$  and symplectic form  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ . The basis  $\{e, f\}$  is called a **symplectic pair**.

2. We get examples in all even dimensions by taking orthogonal direct sums  $J^{\oplus n} = J \oplus \cdots \oplus J$  ( $n$  copies). Reordering basis vectors, we find that  $J^{\oplus n}$  is isometric to the standard symplectic form

$$J_n = \begin{pmatrix} \mathbf{0}_n & \mathbf{1}_n \\ -\mathbf{1}_n & \mathbf{0}_n \end{pmatrix}.$$

In other words, in a suitable basis  $\mathbf{E} = \{e_1, \dots, e_{2n}\}$ , the form becomes

$$b_{\mathbf{E}}(x, y) = \sum_{i=1}^n (x_i y_{n+i} - y_i x_{n+i}), \quad x = \sum_{j=1}^{2n} x_j e_j, \quad y = \sum_{j=1}^{2n} y_j e_j.$$

3. If  $\text{char}(k) = 2$ , the polar form  $b_q$  of a non-degenerate quadratic form  $q$  is a non-degenerate symplectic form. This explains why symplectic forms come up naturally in the study of quadratic forms in characteristic 2.

A  $k$ -linear map between symplectic  $k$ -spaces preserving the symplectic form is called a **symplectic map** and two symplectic spaces are isometric if there exists a symplectic isomorphism between them. Isometries of  $(V, b)$  are called symplectic automorphisms and these form a subgroup  $\text{Sp}(V)$  of  $\text{GL}(V)$ , the **symplectic group** of  $V$ . The classification of non-degenerate symplectic forms up to symplectic isomorphism is very straightforward since any non-degenerate symplectic form is isometric to the standard form:

**Proposition A.5.2.** *A non-degenerate  $k$ -symplectic space  $(V, b)$  is isometric to  $(k^{2n}, J^{\oplus n})$ , and in particular must be even dimensional. In a suitable basis the Gram matrix of  $b$  is  $J_n$ , the standard symplectic form.*

*Proof.* Let  $e$  be any non-zero vector. Since  $b$  is non-degenerate, there is a vector  $f$  with  $b(e, f) \neq 0$ , and by scaling  $f$  if necessary, one may assume that  $b(e, f) = 1$ . Then  $\{e, f\}$  spans a symplectic plane  $J$  and  $V = J \oplus J^\perp$  as for symmetric bilinear forms. One concludes by induction.  $\square$

We next show that the symplectic group of  $V$  is generated by the so-called symplectic transvections. Recall that an ordinary **transvection** of a  $k$ -vector space  $V$  along the hyperplane  $H \subset V$  is a  $k$ -linear transformation  $\tau : V \rightarrow V$  such that  $\ker(\tau - \text{id}) = H$  and  $\text{Im}(\tau - \text{id}) \subset H$ . Phrased in geometric terms, the points fixed by  $\tau$  form a hyperplane  $H$  and  $\tau$  moves points of  $V$  parallel to the hyperplane  $H$ .

Suppose that  $V$  in addition admits a non-degenerate symplectic form  $b$ . Given  $u \in V$  and a non-zero constant  $a \in k$ , the standard example of a transvection preserving the symplectic form is given by

$$\tau_{u,a}(x) = x + a \cdot b(u, x)u.$$

The fixed hyperplane  $H$  is given by the equation  $b(u, x) = 0$  and since  $b(u, u) = 0$ , the point  $u$  belongs to  $H$  and so  $\tau_{u,a}(x) - x \in H$ , i.e.,  $\tau_{u,a}$  is indeed a transvection. These are the only ones as we show now:

**Lemma A.5.3.** *In a non-degenerate symplectic  $k$ -space, a symplectic transvection  $\tau$  is of the form  $\tau = \tau_{u,a}$ .*

*Proof.* Let  $\tau$  be a symplectic transvection along the hyperplane  $H$ . This hyperplane can be written as  $H = u^\perp$  for some  $u \in V$ . In particular,  $\tau(x) = x$  for  $x \in u^\perp$ . Since  $\text{Im}(\tau - \text{id})$  is a one-dimensional subspace of  $H$ , there exists  $w \in H$ ,  $a \in k$ , such that

$$\tau(x) = x + a \cdot b(u, x)w.$$

Consider  $(x, y) = (\tau(x), \tau(y)) = (x, y) + a \cdot b(u, x)b(w, y) + a \cdot b(u, y)b(w, x)$ . Choose  $x$  such that  $b(x, w) = -1$ . Then  $b(u, y) = b(u, x)b(w, y)$  for every  $y$ , and so  $u^\perp = w^\perp$ . But then  $w$  and  $u$  are linearly dependent and so  $\tau$  is of the desired form.  $\square$

**Proposition A.5.4.** *The symplectic group  $\text{Sp}(V)$  is generated by symplectic transvections.*

*Proof.* Let  $G$  be the subgroup of  $\text{Sp}(V)$  generated by symplectic transvections. We show that  $G = \text{Sp}(V)$ .

**Step 1:  $G$  acts transitively on non-zero vectors.** To show this, let  $x, y \in V$  be two non-zero vectors. Distinguish two cases:

(1a):  $b(x, y) \neq 0$  so that we have a transvection  $\tau_{x-y, a}$  with  $a = b(x, y)^{-1}$ . Then

$$\begin{aligned} \tau_{x-y, a}(x) &= x + b(x, y)^{-1} \cdot b(x, x - y)(x - y) \\ &= x - (x - y) = y. \end{aligned}$$

The above formula exhibits transvections that permute non-orthogonal vectors while fixing vectors orthogonal to their difference, an observation which we shall use below:

$$b(x, y) \neq 0, b(z, x - y) = 0 \implies \exists \tau \in G \text{ such that } \tau(x) = y, \tau(z) = z. \quad (\text{A.12})$$

(1b):  $b(x, y) = 0$ . There exists a vector  $z \in V$  in the complement of  $x^\perp \cup y^\perp$ . We then apply the first case to  $(x, z)$  and  $(z, y)$  successively.

**Step 2:  $G$  acts transitively on symplectic pairs.** So let  $\{e, f\}$  and  $\{e', f'\}$  be two symplectic pairs. By Step 1 there exists a  $\gamma \in G$  with  $\gamma(e) = e'$ , and so  $\gamma$  transforms the pair  $\{e, f\}$  in, say,  $\{e', f''\}$ . We search for a  $\tau \in G$  with  $\tau(e') = e'$

but  $\tau(f'') = f'$ . Again we have two cases:

(2a):  $b(f'', f') \neq 0$ . Observe that then

$$\begin{aligned} b(f'' - f', e') &= b(f'', e') + 1 \\ &= b(\gamma(f), \gamma(e)) + 1 = 0, \end{aligned}$$

and so we may apply (A.12) to find the desired element in  $G$ .

(2b):  $b(f'', f') = 0$ . Observe that in this case  $\{e', f''\}, \{e', e' + f''\}, \{e', f'\}$  are symplectic pairs satisfying  $b(f'', e' + f'') \neq 0$  and  $b(e' + f'', f') \neq 0$ . So by the previous case, there exist  $\tau_1 \in G$  with  $\tau_1(e') = e', \tau_1(f'') = e' + f''$ , and  $\tau_2 \in G$  with  $\tau_2(e') = e'$  and  $\tau_2(e' + f'') = f'$ . So  $\tau_2 \tau_1 \in G$  is as required.

**Step 3: Completion of the proof.** The proof for  $\dim V = 2$  follows from Step 2 and for  $\dim V > 2$  one applies induction: pick any symplectic pair  $\{e, f\}$  and let  $P$  be the plane they span. Then  $V = P \oplus P^\perp$ . If  $\sigma \in \text{Sp}(V)$  then  $\{\sigma(e), \sigma(f)\}$  is a symplectic pair and by Step 2 there is an element  $\tau \in G$  such that  $\tau \sigma(e) = e$  and  $\tau \sigma(f) = f$ . By induction on the dimension,  $\tau \sigma$  restricts to  $P^\perp$  as a product of transvections and by extending the latter to transvections of  $V$  by letting them act as the identity on  $P$  we see that  $\tau \sigma \in G$  and so  $\sigma \in G$ .  $\square$

## A.6 Cohomology of Groups and Group Actions

We present a rudimentary introduction to group (co)homology and applications to free group actions on manifolds. For more details we refer to the books [32] by K. Brown, [247] by Ch. Weibel, and [94] by A. Hatcher. In the following  $G$  is a finite group.

A  $G$ -*module* is an abelian group  $M$  equipped with a  $G$ -action, or, equivalently, a  $\mathbb{Z}[G]$ -module. Given a  $G$ -module  $M$ , we set

$$\begin{aligned} M^G &= \{x \in M \mid gx = x, \forall g \in G\}, \\ M_G &= M/IM, \quad I = \langle gx - x, x \in M, g \in G \rangle. \end{aligned}$$

In other words,  $M^G$  is the largest submodule on which  $G$  acts as the identity and  $M_G$  is the largest quotient of  $M$  on which  $G$  acts trivially.

**Group (co)homology** of  $G$  can be defined topologically as the (co)homology of a topological space  $X$  which has fundamental group  $G$  and has no higher homotopy groups. These groups turn out to be independent of the choice of such  $X$ .

As an example, for  $G = \mathbb{Z}$ , one takes for  $X$  the circle and hence  $H_0(G) = H_1(G) = \mathbb{Z}$  and  $H_k(G) = 0$  for  $k \neq 0, 1$ . It is easy to see that  $H_*(G)$  can equivalently be defined in a purely algebraic way as the homology of any free resolution  $F_\bullet$  of  $\mathbb{Z}$  over the group ring  $\mathbb{Z}[G]$ . The definition of  $H^*(G)$  is slightly more elaborate and we give it below for any  $G$ -module  $M$ .

There is also a topological approach to (co)homology of  $G$ -modules, but the algebraic definition is simpler to state: Let  $F_\bullet$  a free  $\mathbb{Z}[G]$ -resolution of  $\mathbb{Z}$ , one defines

$$H_q(G, M) = H_q(F_\bullet \otimes_{\mathbb{Z}[G]} M), \quad H^q(G, M) = H^q(\text{Hom}_G(F_\bullet, M)).$$

If  $M = \mathbb{Z}$  with the trivial group action, these groups give back the ordinary group (co)homology.

We state (without proofs) some facts about group (co)homology that are used below:

**Lemma A.6.1.** 1. Let  $M$  be a  $G$ -module. Then  $H^0(G, M) = M^G$  and  $H_0(G, M) = M_G$ . In particular,  $H^0(G) = H_0(G) = \mathbb{Z}$ .

2. If  $G$  is a finite group of order  $n$ , then the groups  $H^q(G, M)$ ,  $H_q(G, M)$ ,  $q \geq 1$ , are  $n$ -torsion. If  $G$  is a finite abelian group and  $G$  acts trivially on  $M$ , then  $H^1(G, M) \simeq \text{Hom}(G, M)$ ,  $H_1(G, M) \simeq G \otimes M$  and, in particular,  $H^1(G) = 0$  and  $H_1(G) \simeq G$ .

3. If  $G$  is a finite abelian group  $H^2(G) = \text{Ext}^1(G, \mathbb{Z}) \simeq G$ .

4. If  $G$  is cyclic of order  $n$ , then  $H^j(G) = 0$  for  $j$  odd and  $H^j(G) \simeq G$  for  $j > 0$  even, while  $H_j(G) \simeq G$  for  $j$  odd and  $H_j(G) = 0$  for  $j > 0$  even.

We now turn to applications in topology. Assuming that  $X$  is a CW-complex, one has the **Cartan–Leray spectral sequence** ([32, Thm. VII.7.9])

$$E_2^{p,q} = H^p(G, H^q(X)) \implies H^{p+q}(Y).$$

This spectral sequence expresses the (integral) cohomology of the quotient in terms of the group (co)homology of the  $G$ -module  $H^*(X)$  and it implies:

**Proposition A.6.2.** Suppose  $X$  is a connected CW-complex with finite rank cohomology groups and with  $H_1(X) = 0$ . If  $G$  is a finite abelian group acting freely on  $X$  with quotient map  $\pi : X \rightarrow Y = X/G$ , then

1.  $H^2(X)$  has no torsion and  $\text{Tors} H^2(Y) = \text{Ext}^1 G$ .

2. There is a natural map  $\delta : H^2(X)^G \rightarrow H^3(G)$  and an exact sequence

$$0 \rightarrow \text{Ext}^1 G \rightarrow H^2(Y) \xrightarrow{\pi^*} \ker(H^2(X)^G \xrightarrow{\delta} H^3(G)) \rightarrow 0.$$

Moreover, there is an induced isomorphism

$$H^2(Y)/\text{Tors}(H^2(Y)) \xrightarrow{\sim} \ker(\delta).$$

In case  $G$  is cyclic,  $\delta = 0$  and hence  $\pi^*$  surjects onto  $H^2(X)^G$ .

*Proof.* 1. By the universal coefficient theorem,  $\text{Tors} H^2(X) = \text{Ext}^1 H_1(X) = 0$  and  $\text{Tors} H^2(Y) = \text{Ext}^1 H_1(Y)$ . The first equality proves the first assertion. Since  $G$  is an abelian covering group for the covering  $\pi : X \rightarrow Y = X/G$ , it follows that  $H_1(Y) = G$ , proving the second assertion. Indeed, the abelianization of the exact sequence

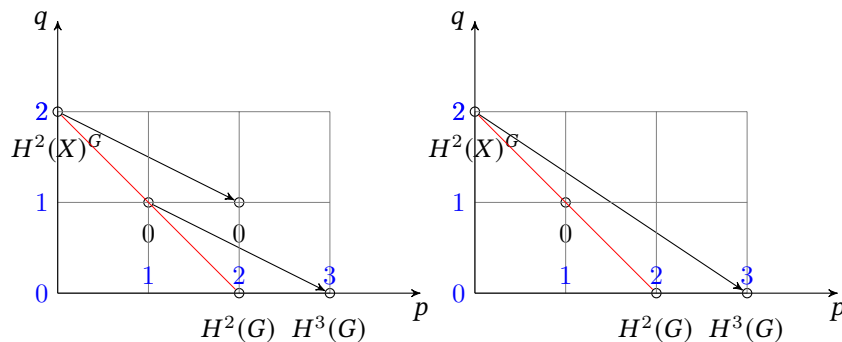
$$1 \rightarrow \pi_1(X, x_0) \xrightarrow{\pi_*} \pi_1(Y, \pi(x_0)) \rightarrow G \rightarrow 1$$

gives the exact sequence  $0 = H_1(X) \xrightarrow{\pi^*} H_1(Y) \rightarrow G \rightarrow 0$ .

2. We invoke the cohomology Cartan–Leray spectral sequence

$$E_2^{p,q} = H^p(G, H^q(X)) \implies H^{p+q}(Y), \quad p + q = 2.$$

The  $E_2$ -page and the  $E_3$ -page are as follows:



By the universal coefficient theorem  $H_1(X, \mathbb{Z}) = 0$  implies  $H^1(X, \mathbb{Z}) = 0$  and so  $E_2^{p,q} = 0$  for  $q = 1$ . It follows that  $E_\infty^{1,1} = 0$ . The spectral sequence gives a filtration  $0 \subset F^2 \subset F^1 \subset F^0 = H^2(Y)$  whose graded groups are  $E_\infty^{p,2-p} = F^p/F^{p+1}$  and so  $F^2 = F^1$ . Equivalently, there is an exact sequence

$$0 \rightarrow E_\infty^{2,0} \rightarrow H^2(Y) \rightarrow E_\infty^{0,2} \rightarrow 0. \tag{A.13}$$

One has  $H^2(G) = E_2^{2,0} = E_\infty^{2,0}$ . Also,  $E_3^{0,2} = E_2^{0,2} = H^2(X)^G$  since  $E_2^{2,1} = 0$ , and  $E_\infty^{0,2} = E_4^{0,2} = \ker(\delta = d_3^{0,2} : H^2(X)^G \rightarrow H^3(G))$ . Since  $H^2(G) = \text{Ext}^1 G$ , the sequence (A.13) becomes

$$0 \rightarrow \text{Ext}^1 G \rightarrow H^2(Y) \xrightarrow{\pi^*} \ker(H^2(X)^G \xrightarrow{\delta=d_3^{0,2}} H^3(G)) \rightarrow 0.$$

Combining this with item 1, we see that  $\pi^*$  induces the stated isomorphism between the resulting free groups. If  $G$  is cyclic,  $H^3(G) = 0$  and then  $\pi^*$  surjects onto  $H^2(Y)^G$ . □



## B

---

### Background on Complex Surfaces

In the present book only Kähler surfaces will play a role. For the notions we use from complex and Kähler geometry one may consult e.g. [88, 105].

#### B.1 Generalities on Kähler Geometry

Let us briefly recall here the basics. A hermitian metric on a complex manifold can be given by its associated metric (1, 1)-form  $\kappa$ . This is a real form which in local coordinates  $(z_1, \dots, z_n)$  is given by the expression

$$\kappa = \sqrt{-1} \sum_{i,j=1}^n h_{ij} dz_i \wedge d\bar{z}_j, \quad h_{ij} = \bar{h}_{ji}.$$

The metric is Kähler if  $\kappa$  is a closed form, which then is called the associated **Kähler form**. So its class is a (real) cohomology class of type (1, 1). A manifold admitting a Kähler metric is called a **Kähler manifold**. Prominent examples are smooth complex projective varieties, and complex tori. Using the Kähler form  $\kappa$ , we shall make use of a general positivity condition related to complex submanifolds  $Y \subset X$ , namely the inequality

$$\int_Y \underbrace{\kappa \wedge \dots \wedge \kappa}_k > 0, \quad k = \dim Y. \quad (\text{B.1})$$

We shall also be using numerical invariants defined for any compact complex manifold  $X$  by way of the sheaf  $\Omega_X^p$  of holomorphic  $p$ -forms on  $X$ :

$$H^{p,q}(X) = H^q(X, \Omega_X^p), \quad h^{p,q}(X) = \dim H^q(X, \Omega_X^p) \text{ (the Hodge numbers).}$$

If  $X$  is Kähler, the groups  $H^{p,q}(X)$  can be viewed as subspaces of the De Rham cohomology (with complex coefficients) and one of the cornerstones of Kähler geometry is the assertion that  $H^{p,q}(X) \subset H^{p+q}(X, \mathbb{C})$  is the subspace of cohomology representable by closed forms of type  $(p, q)$ . As a consequence one obtains the Hodge decomposition:

$$H^k(X, \mathbb{C}) = \bigoplus_{p+q=k} H^{p,q}(X), \quad \overline{H^{p,q}(X)} = H^{q,p}(X).$$

## B.2 Basic Invariants of Surfaces

**Topological invariants.** Since  $X$  is a connected oriented compact four-manifold, the Betti numbers satisfy

$$b_0(X) = b_4(X) = 1, \quad b_1(X) = b_3(X).$$

The cup-product form is a symmetric bilinear unimodular pairing

$$S_X : H_X \times H_X \longrightarrow \mathbb{Z} \quad H_X = H^2(X, \mathbb{Z})/\text{torsion}, \quad (\text{B.2})$$

also called the *intersection form* of  $X$ .<sup>1</sup> Its signature is denoted  $(b^+(X), b^-(X))$  and the *index* is

$$\tau(X) = b^+(X) - b^-(X).$$

There are further invariants, a priori depending on the (almost) complex structure: the Chern classes  $c_1(X) \in H^2(X, \mathbb{Z})$  and  $c_2(X) \in H^4(X, \mathbb{Z})$ . Also  $c_1^2(X) = c_1(X) \cdot c_1(X)$  belongs to  $H^4(X, \mathbb{Z})$ . The classes  $c_1^2(X)$  and  $c_2(X)$  can and will be considered as integers (and called Chern numbers) via the isomorphism  $H^4(X, \mathbb{Z}) \simeq \mathbb{Z}$  given by the canonical orientation of  $X$ . The Chern numbers are (oriented) topological invariants:  $c_2(X)$  can be identified with the Euler number  $e(X)$ ; that  $c_1^2(X)$  is a topological invariant is a consequence of a deep theorem, the index theorem ([98, Thm. 8.2.2]):

**Theorem B.2.1** (Index theorem – special case). *For a compact differentiable 4-manifold  $X$  admitting a complex structure, the index  $\tau(X)$  satisfies*

$$\tau(X) = \frac{1}{3}(c_1^2(X) - 2c_2(X)).$$

*Remark B.2.2.* The Chern class  $c_1(X) \in H^2(X, \mathbb{Z})$  is also represented by the class of the inverse of the canonical line bundle<sup>2</sup>  $K_X$ . In particular, for a compact complex surface  $X$  one has  $c_1^2(X) = K_X \cdot K_X$ .

**Complex Invariants.** From now on we assume that  $X$  is a compact connected Kähler surface. The Hodge decomposition for  $H^1$  and  $H^2$  reads as follows:

$$\left. \begin{aligned} H^1(X, \mathbb{C}) &= H^{1,0}(X) \oplus H^{0,1}(X), & H^{1,0}(X) &= \overline{H^{0,1}(X)} \\ H^2(X, \mathbb{C}) &= H^{2,0}(X) \oplus H^{1,1}(X) \oplus H^{0,2}(X) & H^{2,0}(X) &= \overline{H^{0,2}(X)} \\ & & H^{1,1}(X) &= \overline{H^{1,1}(X)}. \end{aligned} \right\} \quad (\text{B.3})$$

We make frequently use of the Hodge index theorem<sup>3</sup>:

<sup>1</sup>The name comes from the intersection product on homology classes which corresponds to cup product under Poincaré duality.

<sup>2</sup>For the notion of canonical line bundle, see the discussion on page 444 about the Kodaira dimension.

<sup>3</sup>It can also be regarded as a consequence of the Lefschetz decomposition for surfaces (cf. [105, Cor. 3.3.16]).

**Theorem B.2.3** (Hodge Index Theorem). *For a Kähler surface  $X$  the intersection form gives the real vector space  $H^{1,1}(X)_{\mathbb{R}} = H^{1,1}(X) \cap H^2(X, \mathbb{R})$  the structure of a hyperbolic space, i.e., the signature of the restriction of the intersection form on this space is  $(1, h^{1,1}(X) - 1)$ .*

It follows that the considerations of Example 16.1 apply to  $H^{1,1}(X)_{\mathbb{R}}$ : the light cone  $\{x \in H^{1,1}(X)_{\mathbb{R}} \mid x \cdot x > 0\}$  consists of two connected components. In the present situation, the **positive cone** is the one that contains the Kähler classes. The set of Kähler classes is a convex cone and so has to belong to just one connected component of the light cone. We denote it by

$$C_X = \text{component of } \{x \in H^{1,1}(X)_{\mathbb{R}} \mid x \cdot x > 0\} \text{ containing Kähler classes.} \quad (\text{B.4})$$

The Kähler classes span a subcone, the **Kähler cone**.

Another important formula is **Noether's formula** [15, p. 26], a special case of the Riemann–Roch formula:

$$\chi(\mathbb{C}_X) = 1 - q(X) + p_g(X) \quad (\text{the arithmetic genus}) = \frac{1}{12}(c_1^2(X) + c_2(X)). \quad (\text{B.5})$$

Since  $q(X) = \frac{1}{2}b_1(X)$  is a topological invariant, it follows from Noether's formula that the same is true for  $p_g(X)$ . Because of the Hodge decomposition (B.3), this is likewise true for  $h^{1,1}(X) = b_2(X) - 2p_g(X)$ . Hence, for compact Kähler surfaces the Hodge numbers  $h^{p,q}(X)$  are topological invariants. Consequently, the signature (and hence the index) can be expressed in terms of Hodge numbers:

$$b^+(X) = 2p_g(X) + 1, \quad b^-(X) = h^{1,1}(X) - 1 \implies \tau(X) = 2p_g(X) + 2 - h^{1,1}(X). \quad (\text{B.6})$$

This shows that the intersection form  $S_X$  can only be indefinite or positive definite. In the indefinite case, by the main result of Chapter 2, this unimodular form is uniquely determined by its parity and signature. If the form happens to be positive definite, by (B.6) we have  $\tau = 2p_g + 1$ . The index theorem B.2.1 combined with the Noether formula (B.5) then yields the following expressions for  $c_1^2$  and  $c_2$ :

$$\begin{aligned} c_1^2 &= 10p_g - 8q + 9, \\ c_2 &= 2p_g - 4q + 3, \end{aligned}$$

so that  $c_1^2 - 3c_2 = 4(p_g + q)$ . From the table of the classification theorem B.5.4, we see that  $c_1^2 - 3c_2 \leq 0$  except for ruled surfaces and, possibly, for surfaces of general type. The former have indefinite forms as we shall see in Section B.3, and for the latter the inequality is precisely the Bogomolov–Miyaoka–Yau inequality for which we refer to [15, §VII.4]. Hence  $p_g = q = 0$  and then necessarily<sup>4</sup>  $S_X \simeq \langle 1 \rangle$ . So we have shown:

**Lemma B.2.4.** *Let  $X$  be a Kähler surface. If  $S_X$  is definite,  $S_X \simeq \langle 1 \rangle$ .*

Therefore, in all cases the intersection form  $S_X$  is uniquely determined by its parity and signature.

<sup>4</sup>One can show that for simply connected surfaces this only happens for the projective plane. See e.g. [15, Thm. V.1.1].

**Invariants related to divisors.** A divisor  $D$  on a surface  $X$  defines a cohomology class  $[D] \in H^2(X, \mathbb{Z})$ . Divisors with the same class are said to be homologically equivalent and so the group of divisors on  $X$  modulo homological equivalence, by definition the *Néron–Severi group*  $\text{NS}(X)$ , embeds in  $H^2(X, \mathbb{Z})$ . Its rank is the *Picard number*  $\rho(X)$  of  $X$ . We shall identify  $\text{NS}(X)$  with its image in  $H^2(X, \mathbb{Z})$ . The resulting cohomology classes are the algebraic classes. By the Lefschetz (1, 1)-theorem these are precisely the classes of Hodge type (1, 1):

**Proposition B.2.5.** *Let  $X$  be a complex surface. Then  $\text{NS}(X)$  is the subgroup of  $H^2(X, \mathbb{Z})$  consisting of classes of type (1, 1).*

The intersection form  $S_X$  induces the structure of an integral lattice on the free group  $\text{NS}(X)/\text{torsion}$ , the *Néron–Severi lattice* or *Picard lattice*. Usually one uses a dot to denote the intersection product of divisor classes. For non-algebraic surfaces the resulting lattice might be negative definite or it could be totally isotropic (and hence degenerate). However, as soon as there exists a divisor  $D$  for which  $[D] \cdot [D] > 0$ , the surface is projective algebraic (cf. [15, Thm. IV.6.2]) and there is a classical result that states that then the Picard lattice is of Lorentzian type:

**Theorem B.2.6** (Algebraic Index Theorem [15, IV, Cor. 2.16], [19, p. 8]). *Let  $X$  be a smooth complex projective surface. The intersection pairing restricts non-degenerately to the Néron–Severi group  $\text{NS}(X)$  and has signature  $(1, \rho - 1)$ . In particular, if  $D$  is a divisor with  $D \cdot D > 0$ , any class in  $\text{NS}(X)$  orthogonal to  $D$  has negative self-intersection.*

One uses often the so-called *adjunction formula* or *genus formula* for an irreducible curve  $D$  on a surface  $X$  (cf. [15, Ch. II, 11], [19, p. 8]):

$$2p_a(D) - 2 = K_X \cdot D + D \cdot D, \quad p_a(D) = g(\tilde{D}) + \delta, \tag{B.7}$$

where  $p_a(D)$  is called the arithmetic genus of  $D$ ,  $\tilde{D}$  is a smooth model of  $D$ ,  $g(\tilde{D})$  its genus, and  $\delta \geq 0$  its defect, which vanishes precisely when  $D$  is smooth.

**The transcendental lattice.** Recall the Hodge decomposition of  $H^2(X, \mathbb{C})$ ,  $H^2(X, \mathbb{C}) = H^{2,0}(X) \oplus H^{1,1}(X) \oplus H^{0,2}(X)$ . We just saw that the Néron–Severi lattice is the sublattice of  $H_X$  consisting of integral classes of Hodge type (1, 1). In other words,

$$S(X) = \text{NS}(X)/\text{torsion} = H_X \otimes \mathbb{C} \cap H^{1,1}(X),$$

and so it is the largest (primitive) sublattice of  $H_X$  such that  $S(X) \otimes \mathbb{C} \subset H^{1,1}(X)$ . Complementary to it we have the *transcendental lattice* of  $X$ :

$$\text{Trs}(X) = \text{the smallest primitive sublattice } T' \text{ of } H_X \text{ such that } H^{2,0}(X) \subset T' \otimes \mathbb{C}.$$

The transcendental lattice is a sub Hodge structure of  $H^2(X, \mathbb{Z})$ , since being integral one has  $\text{Trs}(X) \otimes \mathbb{C} = H^{2,0}(X) \oplus H^{0,2} \oplus [H^{1,1} \cap \text{Trs}(X)]$ . By type considerations, under cup-product  $H^{2,0}(X) \oplus H^{0,2}(X)$  is orthogonal to  $H^{1,1}(X)$  and so  $\text{Trs}(X)^\perp$  is contained in  $S(X)$  but need not be equal to it, since in the non-projective case

$S(X)$  can be degenerate. From what has been said so far, we clearly have equality otherwise:

**Lemma B.2.7.** *Let  $X$  be a compact Kähler surface such that its Néron–Severi lattice is non-degenerate (e.g. if  $X$  is projective), then  $\text{Trs}(X)$  and  $\text{NS}(X)/\text{torsion}$  are orthogonal complements of each other in  $H_X$ .*

### B.3 Examples

1. The most basic examples of surfaces are  $\mathbb{P}^2$  and  $\mathbb{P}^1 \times \mathbb{P}^1$ . These are birationally equivalent to each other (see e.g. Example B.5.1) and any surface birational to  $\mathbb{P}^2$  is called a **rational surface**. Apart from the just mentioned surfaces also the Hirzebruch surfaces  $F_n, n \in \mathbb{N}$ , belong to this class. The surface  $F_n$  is the total space of the  $\mathbb{P}^1$ -bundle over  $\mathbb{P}^1$  possessing a unique section  $C_n$  with self-intersection  $-n$ . The Hirzebruch surface  $F_0$  is just  $\mathbb{P}^1 \times \mathbb{P}^1$  and only  $F_1$  has an exceptional curve. These surfaces are all simply connected and  $b_2(\mathbb{P}^2) = h^{1,1}(\mathbb{P}^2) = 1$  while  $b_2(F_n) = h^{1,1}(F_n) = 2$ .

Let us describe the intersection lattices.

- The class  $\ell$  of a line generates  $H^2(\mathbb{P}^2, \mathbb{Z})$  and since  $\ell^2 = 1$  we get  $S_{\mathbb{P}^2} \simeq \langle 1 \rangle$ .
- For a quadric, the classes  $\ell$  and  $\ell'$  of the two rulings give a basis for  $H^2(\mathbb{P}^1 \times \mathbb{P}^1, \mathbb{Z})$ , and since  $\ell^2 = (\ell')^2 = 0$  and  $\ell \cdot \ell' = 1$  we find  $S_{\mathbb{P}^1 \times \mathbb{P}^1} \simeq U$ , the hyperbolic plane.
- For  $F_n$  the class of a fiber and the class of  $C_n$  give a basis for  $H_{F_n}$ . The Gram matrix is  $\begin{pmatrix} 0 & 1 \\ 1 & -n \end{pmatrix}$ . Now use Example 1.13.1.(5). We deduce that  $S_{F_n} \simeq U$  if  $n$  is even and  $S_{F_n} \simeq W = \langle 1 \rangle \oplus \langle -1 \rangle$  if  $n$  is odd. Since these two lattices are not isometric, the Freedman result 2.5.2 implies that the Hirzebruch surfaces belong to two distinct topological types.

2. A **ruled surface of genus  $g$**  is a  $\mathbb{P}^1$ -bundle over a curve of genus  $g$ . If  $g > 0$  these are not simply connected; in fact  $b_1 = 2g = 2g$  and  $b_2 = h^{1,1} = 2$  for them. As for Hirzebruch surfaces the intersection lattice has rank 2 and is either isometric to  $U$  or to  $\langle 1 \rangle \oplus \langle -1 \rangle$ . See [19, Prop. III.18].

3. **Smooth surfaces of degree  $d$  in  $\mathbb{P}^3$** . These are simply connected and  $b_2 = d^3 - 4d^2 + 6d - 2$ . See e.g. [15, V. Prop. 2.1]. For  $d = 2$  we get a smooth quadric which is isomorphic to  $\mathbb{P}^1 \times \mathbb{P}^1$  (think of the two rulings on a quadric surface). For  $d = 4$  we get a K3 surface, a class of surfaces we discuss below as the next example.

The canonical class, Chern classes and (some) intersection lattices of the preceding surfaces are given in Table B.3.1. Here,  $h$  is the class of a hyperplane,  $f$  the class of a fiber and  $s$  the class of a section.

4. A **K3 surface** is a simply connected surface with trivial canonical bundle. Such a surface is not necessarily algebraic but always Kähler. All K3 surfaces are

Table B.3.1: Invariants of the surfaces of examples 1, 2 and 3

$X$	$K_X = -c_1(X)$	$c_1^2(X)$	$c_2(X)$	$S_X$
$\mathbb{P}_2$	$-3h$	9	3	$\langle 1 \rangle$
$F_n, n$ even	$-(2+n)f - 2s$	8	4	$U$
$F_n, n$ odd	$-(2+n)f - 2s$	8	4	$W = \langle 1 \rangle \oplus \langle -1 \rangle$
ruled surface	$(2g - 2 + s^2)f - 2s$	$8(1 - g)$	$4(1 - g)$	$U$ or $W$
degree $d$				
surface in $\mathbb{P}^3$	$(d - 4)h$	$d(d - 1)^2$	$d(d^2 - 4d + 6)$	—

known to be diffeomorphic to each other. For proofs of these assertions see for instance [15, Ch. VIII]. Examples are

- Kummer surfaces. These are minimal resolutions of singularities of quotients of 2-dimensional complex tori by the natural involution  $z \mapsto -z$ .
- Smooth degree four surfaces in  $\mathbb{P}^3$ .
- Smooth complete intersections of three quadratics in  $\mathbb{P}^5$ .

Curious how a K3 surface might look like? In Fig. B.3.1 one finds a picture of (the real part of) a K3 surface constructed with the SURFER software. See <https://imaginary.org/program/surfer>.

The invariants of a K3 surface  $X$  are as follows (cf. [15, Ch. VIII]):

$$b_1(X) = 0, \quad b_2(X) = 22.$$

$$S_X = \Lambda_{K3} = U \oplus U \oplus U \oplus E_8(-1) \oplus E_8(-1).$$

We contend ourselves explaining how to determine  $S_X$ , given its rank  $b_2(X)$ . By Proposition 2.5.4 the intersection form is even since the canonical bundle of  $X$  is trivial; indeed the nowhere zero holomorphic two-form gives a trivialization of the canonical bundle. The index formula (Theorem B.2.1) tells us that the index is  $\frac{1}{3}(-24) = -16$ . But then by Corollary 2.4.3 the lattice  $S_X$  is uniquely determined and hence isometric to the K3 lattice.

In the special case of a Kummer surface we shall explain in detail how to calculate the Betti numbers. The surjectivity of the period map (see 19.2.1) implies that all K3 surfaces can be put in one family with a connected base and then these are necessarily all diffeomorphic to one another (Ehresmann’s theorem, cf. [105, Prop. 6.2.2]) and so have the same Betti numbers.

**Kummer surfaces.** In this book Kummer surfaces play a special role and we shall investigate them in some more detail.

To explain their **construction** we start with a complex two-torus  $A = \mathbb{C}^2/\Gamma$ . Here  $\Gamma \simeq \mathbb{Z}^4$  is a lattice inside  $\mathbb{C}^2 \simeq \mathbb{R}^4$ . The quotient of  $A$  by the standard involution  $i : z \mapsto -z$  yields a singular **Kummer surface**  $A/\langle i \rangle$ . This is not a manifold, since the involution has  $2^4 = 16$  fixed points, the 2-torsion points of  $A$ .

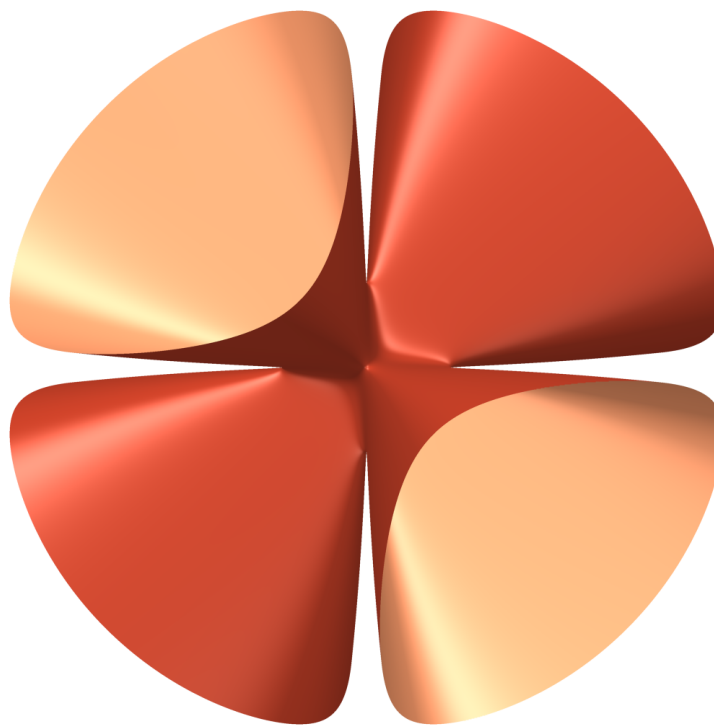


Figure B.3.1: The K3 surface  $x^4 + y^4 + z^4 - t^4 + 60xyzt = 0$  in  $\mathbb{P}^3$ .

Our first task is to change  $A/\langle t \rangle$  at these singularities in a controlled way to make it into a manifold. Locally in coordinates around a fixed point, the involution looks like  $(z_1, z_2) \mapsto (-z_1, -z_2)$ . The invariant functions  $u = z_1^2, w = z_1 z_2, v = z_2^2$  obey the relation  $uv = w^2$  and one deduces that the quotient looks locally like a cone given by these equations. Its vertex at the origin is an ordinary double point. The latter can be resolved by a blowing up process in  $\mathbb{C}^3$ . This means that one replaces the origin of  $\mathbb{C}^3$  with the  $\mathbb{P}^2$  parametrizing the directions at the origin. Explicitly, one takes the closure  $\tilde{\mathbb{C}}^3$  in  $\mathbb{C}^3 \times \mathbb{P}^2$  of the graph of the tautological map sending  $(u, v, w) \in \mathbb{C}^3 - \{0\}$  to  $(U : V : W) = (u : v : w)$ . The projection onto the first factor induces a holomorphic map  $\pi : \tilde{\mathbb{C}}^3 \rightarrow \mathbb{C}^3$  which is biholomorphic away from the origin and  $D = \pi^{-1}(0, 0, 0) = (0, 0, 0) \times \mathbb{P}^2$  is a hypersurface, the so-called exceptional divisor. One thus obtains a smooth manifold which intersects  $D$  in a smooth conic and thus  $\simeq \mathbb{P}^1$ . Doing this for all 16 singularities results in a smooth surface  $\text{Km}(A)$  where the 16 singularities have been replaced by 16 rational curves  $E_j$ . One can show that their cohomology classes  $e_j \in H^2(\text{Km}(A), \mathbb{Z})$  are roots, that is,  $e_j \cdot e_j = -2$ , where the dot is the intersection pairing. Let us for clarity assemble

the maps in the above construction in a commutative diagram

$$\begin{array}{ccc}
 \tilde{A} & \xrightarrow{\tilde{\pi}} & A \quad \circlearrowright i \\
 \downarrow & & \downarrow \\
 \text{Km}(A) & \xrightarrow{\pi} & A/\langle \iota \rangle.
 \end{array}$$

Here  $\tilde{\pi} : \tilde{A} \rightarrow A$  is the blow-up map with respect to the sixteen two-torsion points of the torus  $A$ , and which covers  $\pi$ .

Next, we calculate the **Betti numbers**. First note that there are no non-zero invariant holomorphic 1-forms on  $A$  and hence no holomorphic 1-forms on  $\text{Km}(A)$ . Thus  $b_1(\text{Km}(A)) = 0$  by the Hodge decomposition (B.3). Secondly,  $\text{Km}(A)$  admits a nowhere vanishing holomorphic 2-form: the 2-form  $dz_1 \wedge dz_2$  on  $\mathbb{C}^2$  is invariant under translations and the involution  $(z_1, z_2) \mapsto (-z_1, -z_2)$ , and so descends to the (singular) Kummer surface. It is not hard to see that it lifts to  $\text{Km}(A)$  as a nowhere zero holomorphic two-form. Hence the canonical bundle of  $\text{Km}(A)$  is trivial. Now, since  $\text{Km}(A)$  is known to be simply connected, it follows that the Kummer surface is a K3.

Let us compute  $b_2(\text{Km}(A))$  explicitly. Since the Euler number is the alternating sum of the Betti numbers  $b_j$ , and since  $b_0 = b_4 = 1$  while  $b_1 = b_3 = 0$ , to calculate  $b_2$  it suffices to calculate the Euler number  $e = 2 + b_2$ . To do this we exploit additivity of the Euler number: if  $Z$  is a closed subset of a compact manifold  $X$ , we have  $e(X) = e(X - Z) + e(Z)$ . So, if we remove from the torus  $A$  the 16 two-torsion points we get a manifold with Euler number  $0 - 16$ . Taking the quotient by a fixed point free involution halves this number to  $-8$  and inserting the 16 exceptional curves, which are two-spheres with Euler number 2 (a conic is isomorphic to  $\mathbb{P}^1$ ) yields  $e(\text{Km}(A)) = -8 + 16 \cdot 2 = 24$  and hence  $b_2(\text{Km}(A)) = 22$ .

5. An **Enriques surface** is a surface with  $p_g = b_1 = 0$  and  $K^{\otimes 2}$  trivial (hence its class is a torsion class with zero self-intersection). The universal cover can be shown to be a K3 surface which doubly covers the surface. Since  $p_g = q = 0$  and  $c_1^2 = K^2 = 0$ , from (B.5) we find  $c_2 = 2 + b_2 = 12$  and hence  $b_2 = h^{1,1} = 10$ . Then we deduce from Lemma B.2.4 that the intersection lattice has signature  $(1, 9)$ . It is also even. This is the case since all classes are algebraic and since for a divisor  $D$  the genus formula (B.7) shows that  $D^2 = D^2 + D \cdot K$  is even. Consequently, the intersection lattice is isometric to  $\Lambda_{\text{Enr}} = U \oplus E_8(-1)$ .

**Example** ([19, 4.18]). Let  $(x_1 : y_1 : z_1 : x_2 : y_2 : z_2)$  be projective coordinates in  $\mathbb{P}^5$  and define

$$\iota(x_1 : y_1 : z_1 : x_2 : y_2 : z_2) = (x_1 : y_1 : z_1 : -x_2 : -y_2 : -z_2).$$

An invariant quadric is of the form  $Q'(x_1, y_1, z_1) + Q''(x_2, y_2, z_2)$ . For a generic choice of three such quadrics, the intersection is a smooth surface and the calculation rules for complete intersections tell us that this is a K3 surface. Note that the fixed point set of  $\iota$  consists of the two planes  $x_i = y_i = z_i = 0$ ,  $i = 1, 2$ , and three invariant quadrics cut out three conics on each of these planes and so their



intersection is empty for a generic choice of the quadrics. If this is the case, the involution acts on the intersection without fixed points. By what we just said, the quotient is an Enriques surface. All Enriques surfaces can be shown to either arise in this way or they are, in a technical sense, “limits” of such surfaces; in particular they are all algebraic.

## B.4 Period Domains

Since intersection form on a surface  $X$  by definition comes from the wedge product of (closed) forms and taking the wedge of two type  $(2, 0)$ -classes is zero while for a single class  $\omega \neq 0$  of type  $(2, 0)$  the product  $\frac{1}{4}\omega \wedge \bar{\omega}$  is the volume form, the *Riemann bilinear relations* result:

$$S_X(u, u') = 0, \quad u, u' \in H^{2,0}(X) \quad (\text{B.8})$$

$$S_X(u, \bar{u}) > 0, \quad u \in H^{2,0}(X), u \neq 0. \quad (\text{B.9})$$

Secondly, since  $\alpha \wedge \beta = 0$  if  $\alpha$  is a 2-form of type  $(2, 0)$  and  $\beta$  a 2-form of type  $(1, 1)$ , we see that  $H^{2,0}(X)$  and  $H^{1,1}(X)$  are orthogonal. The Hodge decomposition (B.3), shows then that

$$\begin{aligned} H^{1,1}(X) &= H_{\mathbb{R}}^{1,1}(X) \otimes \mathbb{C} = [H^{1,1}(X) \cap H^2(X, \mathbb{R})]_{\mathbb{C}} \\ H^{2,0}(X) \oplus H^{0,2}(X) &= H_{\mathbb{R}}^{1,1}(X)^{\perp} \otimes \mathbb{C}. \end{aligned}$$

By (B.9) the intersection pairing on the second space, a real space of dimension  $2p_g(X)$ , is positive definite. Type considerations further show that under the intersection pairing one has

$$H^{2,0}(X)^{\perp} = H^{2,0}(X) \oplus H^{1,1}(X).$$

This implies that the Hodge decomposition on the  $\mathbb{C}$ -quadratic space  $H_X \otimes \mathbb{C}$  is completely determined by  $H^{2,0}(X)$  alone. This subspace defines a point in the Grassmann variety of  $p_g$ -dimensional subspaces of  $H^2(X, \mathbb{C})$  which captures the Hodge structure on  $H^2(X)$ .

This can be rephrased using the abstract concept of “Hodge structure”:

**Definition B.4.1.** 1. A *Hodge structure* of weight 2 on a free  $\mathbb{Z}$ -module  $L$  of finite rank consists of a decomposition

$$L_{\mathbb{C}} = L^{2,0} \oplus L^{1,1} \oplus L^{0,2},$$

such that  $L^{2,0}$  is the complex conjugate of  $L^{0,2}$  and  $L^{1,1}$  is self-conjugate. This implies that there exist subspaces  $L$  and  $L''$  of  $L_{\mathbb{R}}$  such that

$$L_{\mathbb{R}} = L' \oplus L'', \quad L'_{\mathbb{C}} = L^{1,1}, \quad L''_{\mathbb{C}} = L^{2,0} + L^{0,2}.$$

2. If  $b$  is a non-degenerate integral form on  $L$  we say that  $L$  is **polarized by  $b$** , if the two Riemann bilinear relations (B.8) and (B.9) hold.<sup>5</sup>
3. A polarized weight 2 Hodge structure is said to be of **K3 type** if  $\dim L^{2,0} = 1$  and  $L' \subset L_{\mathbb{R}}$  is of Lorentzian type, that is, has signature  $(1, \dim L' - 1)$ .

Polarized weight 2 Hodge structures on  $(L, b)$  with fixed Hodge number  $h^{2,0} \neq 0$  are in one to one correspondence with points of the corresponding **period domain**

$$D(L, b) = \{[P] \in \text{Gr}(h^{2,0}, L_{\mathbb{C}}) \mid P \text{ is } b_{\mathbb{C}}\text{-isotropic, and } b_{\mathbb{C}}(u, \bar{u}) > 0 \text{ for all } u \in P - \{0\}\}.$$

Here,  $[P]$  denotes the point in the Grassmann variety  $\text{Gr}(h^{2,0})$  corresponding to the subspace  $P$  of  $L_{\mathbb{C}}$ . If we have a Hodge structure of K3 type, then the Grassmann variety is just the projective space of lines  $[u]$  in  $L_{\mathbb{C}}$  and one can rewrite the period domain as

$$D(L, b) = \{[u] \in \mathbb{P}(L_{\mathbb{C}}) \mid b_{\mathbb{C}}(u, u) = 0, \text{ and } b_{\mathbb{C}}(u, \bar{u}) > 0 \}. \tag{B.10}$$

Period domains admit descriptions as a homogeneous domains. The form  $b$  has signature  $(r_+, r_-)$  with  $r_+ = 2h^{2,0} + 1$ ,  $r_- = h^{1,1} - 1$  and the group  $O(r_+, r_-)$  acts transitively on  $D(L, b)$  with isotropy group  $SO(r_+ - 1) \times O(1, r_-)$ :

$$\begin{aligned} D(L, b) &= O(r_+, r_-)/SO(r_+ - 1) \times O(1, r_-) \\ &= SO(r_+, r_-)/SO(r_+ - 1) \times SO(1, r_-). \end{aligned} \tag{B.11}$$

One deduces from Proposition 13.3.7 that  $D(L, b)$  is connected.

Coming back to the intersection lattice, via a choice of isometry  $\varphi : H_X \xrightarrow{\sim} L$ , the polarized Hodge structure can be transported to  $L$ . Such a **marking** determines a point in the period domain  $D(L)$ , the **period point**  $\{\varphi(H^{2,0}(X)) \subset L_{\mathbb{C}}\} \in \text{Gr}(p_g, L_{\mathbb{C}})$ .

## B.5 Surface Classification

**Minimal models.** Classification of surfaces begins with a reduction to minimal surfaces. To explain this, we need the concept of a **(-1)-curve**<sup>6</sup>  $E$  on a complex algebraic surface; by definition  $E$  is a smooth rational curve with  $E \cdot E = -1$ . Such a curve arises under the process of blowing up a surface at a point. To describe this, we assume that we have chosen coordinates  $(u, v)$  in an open subset  $U$  on the surface such that the point  $p$  is the origin. Now consider

$$\tilde{U} := \{((u, v), (U : V)), \in U \times \mathbb{P}^1 \mid (u : v) = (U : V)\}$$

<sup>5</sup>Usually, a polarized Hodge structure of weight two on  $L$  is such that  $b_{\mathbb{R}}$  is positive definite on  $L''$  and negative definite on  $L'$ . This is the case for the orthogonal complement of a hyperplane class inside the intersection lattice of a projective surface, the so-called primitive cohomology.

<sup>6</sup>Also called “exceptional curve of the first kind”.

and let  $\sigma : \tilde{U} \rightarrow U$  be induced by the projection onto the first factor. Then  $\tilde{U}$  contains the curve  $E := (0, 0) \times \mathbb{P}^1$  which by  $\sigma$  gets contracted to the point  $p$  while  $\sigma$  is biholomorphic outside  $E$ . One can show that  $E \cdot E = -1$ . Castelnuovo's contractibility criterion (see [15, Thm. III (4,1)] or [19, II.17]) tells us that, conversely, a  $(-1)$ -curve in a surface  $\tilde{X}$  can be contracted to give a point  $p$  on a smooth surface  $X$  and  $\tilde{X}$  is the blow-up of  $x$  in the point  $p$ . It follows then that any complex algebraic surface has a (not necessarily unique) minimal model, a **minimal surface** which one obtains after blowing down successively all  $(-1)$ -curves. See [15, Thm. III(4.5)].

**Example B.5.1.** Let  $p, q \in \mathbb{P}^2$  be two distinct points and let  $L$  be the line connecting  $p$  and  $q$ . Blowing up  $\mathbb{P}^2$  in  $p$  and  $q$  transforms the line  $L$  in an exceptional curve.<sup>7</sup> Blowing down this curve yields  $\mathbb{P}^1 \times \mathbb{P}^1$  and this procedure shows that  $\mathbb{P}^2$  and  $\mathbb{P}^1 \times \mathbb{P}^1$  are two distinct minimal models within the same birationality class.

We frequently need to compare the cohomology of a surface and of its blow-up. The result we shall use is the following special case of a more general result, a proof of which can be found e.g. in [88, Section 4.6].

**Lemma B.5.2.** *Let  $X$  be a compact complex surface,  $\sigma : \tilde{X} \rightarrow X$  the blow-up in a point  $p$  and  $E = \sigma^{-1}p$  the exceptional curve. Recalling (B.2) for the notation, we have the following cohomological results:*

1.  $\sigma^* : H^2(X, \mathbb{Z}) \rightarrow H^2(\tilde{X}, \mathbb{Z})$  is an injection;
2.  $H_{\tilde{X}} \simeq H_X \oplus \langle -1 \rangle$ , where the second summand is spanned by the class of  $E$ .

**Intermezzo on the Kodaira dimension.** In this subsection we broaden our scope and change notation accordingly:  $X$  stands for a compact Kähler variety and  $L$  for a holomorphic line bundle on  $X$ . Assuming  $L$  has holomorphic sections, a choice of a basis  $\{s_0, s_1, \dots, s_N\}$  for the vector space of holomorphic sections defines the meromorphic map

$$f_L : X \dashrightarrow \mathbb{P}^N \\ x \mapsto (s_0(x) : s_1(x) : \dots : s_N(x)).$$

This is not defined at points where all sections of  $L$  vanish.

If  $f_L$  is everywhere defined and is an embedding,  $L$  is called very ample and likewise for a divisor  $D$  with  $L = \mathcal{O}_X(D)$ . Lastly,  $L$  (or  $D$ ) is called ample if for some positive  $m$  the bundle  $L^{\otimes m}$  (or the divisor  $mD$ ) is very ample. This implies that  $L \cdot C > 0$  for all curves  $C \subset X$ , since  $L \cdot (mC)$  is the degree of the curve  $C$  as embedded in  $\mathbb{P}^N$  by means of  $f_{L^{\otimes m}}$ . Similarly, if  $X$  has dimension  $d$ , we have  $\underbrace{L \cdots L}_{d \text{ times}} > 0$ . We conclude that if  $d = 2$ , for  $D$  ample, we have  $D \cdot C > 0$  and  $D^2 > 0$ .

The converse is the Kleiman criterion: a divisor  $D$  on a surface with positive self-intersection and such that  $D \cdot C > 0$  for all curves  $C$  is an ample divisor.

<sup>7</sup>In technical terms, this is the “proper” transform of  $L$ .

The *canonical bundle*  $K_X$  of  $X$  is the line bundle associated to the sheaf  $\Omega_X^n$  of holomorphic  $n$ -forms where  $n = \dim X$ . A divisor whose line bundle is  $K_X$  is called a *canonical divisor*, also denoted by  $K_X$ . The  $m$ -th tensor power of  $K_X$  is the  $m$ -th *pluricanonical bundle* and we set

$$P_m(X) = h^0(K_X^{\otimes m}), \quad \text{the } m\text{-th plurigenus of } X.$$

These numbers determine the Kodaira dimension:

**Definition B.5.3.** Let  $X$  be a compact complex variety. The *Kodaira dimension* of  $X$  is the number

$$\kappa(X) = \begin{cases} -\infty & \text{if } P_m(X) = 0 \text{ for all } m \in \mathbb{N} \\ \max_{m \in \mathbb{Z}_{>0}} \dim f_{K_X^{\otimes m}}(X) & \text{otherwise.} \end{cases}$$

**On the classification.** To explain the classification of minimal Kähler surfaces, we need some terminology.

1. A *bielliptic surface*<sup>8</sup> is a surface with  $b_2 = 2$  admitting a holomorphic, locally trivial fibre bundle structure over an elliptic curve with fibre an elliptic curve. These are all of the form  $E \times C/G$ , with  $E$  and  $C$  elliptic,  $G \subset C$  a finite group of translations acting on  $E$  not only by translations. There are only 7 possible groups  $G$  (see [15, Ch. V. 5 BII]). The canonical bundle is not trivial: it has no sections.
2. A *properly elliptic surface* is a surface  $X$  of Kodaira dimension 1 admitting an elliptic fibration, i.e., a holomorphic map  $f : X \rightarrow C$  with general fibre an elliptic curve.
3. A *surface of general type* is a surface  $X$  with  $\kappa(X) = 2$ . Its minimal model can be characterized as being a non-rational surface with  $c_1^2 > 0$ . See [15, IV, Table 10].

We now can state the classification theorem.

**Theorem B.5.4** (Enriques–Kodaira classification). *Every minimal compact Kähler surface belongs to exactly one of the following classes ordered according to their Kodaira dimension  $\kappa$ :*

<sup>8</sup>In older literature the terminology *hyperelliptic surface* is used.

$\kappa$	Class		$b_1$	$c_1^2$	$c_2$
$-\infty$	<ul style="list-style-type: none"> <li>• minimal rational surfaces</li> <li>• ruled surfaces over a curve of genus <math>g &gt; 0</math></li> </ul>	<i>all algebraic</i>	0	8 or 9	4 or 3
		<i>all algebraic</i>	$2g$	$8(1 - g)$	$4(1 - g)$
0	<ul style="list-style-type: none"> <li>• Two-dimensional tori</li> <li>• K3 surfaces</li> <li>• Enriques surfaces</li> <li>• bielliptic surfaces</li> </ul>		4	0	0
			0	0	24
		<i>all algebraic</i>	0	0	12
		<i>all algebraic</i>	2	0	0
1	<ul style="list-style-type: none"> <li>• minimal properly elliptic surfaces</li> </ul>			0	$\geq 0$
2	<ul style="list-style-type: none"> <li>• surfaces of general type</li> </ul>	<i>all algebraic</i>		$> 0$	$> 0$

**Historical and Bibliographical Notes.** The classification of algebraic surfaces over a field of characteristic zero goes back to F. Enriques [71]. For modern accounts see e.g. [19]. The extension of the classification to compact complex surfaces is completely due to K. Kodaira. See the monograph [15] by W. Barth, K. Hulek, C. Peters and A. van de Ven for an overall exposition.

## Quadratic Forms: Specialized Topics

### C.1 On Witt's Extension Theorem

$R$  is a local ring with maximal ideal  $\mathfrak{m}$  in which 2 is not invertible,  $k = R/\mathfrak{m}$ .

In this section we present an elaborated English version of the material in M. Kneser's book [122, I.4] on Witt's theorems. These results are important for the local study of quadratic forms at the prime 2, but we could not find a treatment in the English language elsewhere.

Recall that for any  $R$ -module  $V$  equipped with a symmetric form  $b$  the correlation map  $b_V : V \rightarrow V^*$  is defined by sending  $x \in V$  to the functional  $b_V(x)$  which on  $y \in V$  has the value  $b(x, y)$ . The form  $b$  is non-degenerate, respectively unimodular, precisely if  $b_V$  is injective, respectively bijective. If  $W \subset V$  is an  $R$ -submodule, restricting this functional to  $W$  gives a map  $\beta_W : V \rightarrow W^*$ .

Assume from now on that  $V$  is a free  $R$ -module of finite rank and  $W \subset V$  a free submodule.

**Lemma C.1.1.** *Let  $\{w_1, \dots, w_r\}$  be a basis of  $W$ . Then  $\beta_W$  is surjective if and only if there exists vectors  $v_1, \dots, v_r \in V$  with  $b(w_i, v_j) = \delta_{ij}$ . If  $\beta_W(Z) = W^*$  for some submodule  $Z \subset W$ , then we may assume that the vectors  $v_i$  belong to  $Z$ .*

A quadratic form  $q$  on  $V$  is non-degenerate precisely if its polar form  $b_q$  is non-degenerate. Recall also that any vector  $x \in V$  with  $q(x)$  a unit defines a reflection  $\sigma_x : V \rightarrow V$  given by  $y \mapsto y - b_q(x, y)q(x)^{-1}x$ . The quadratic form  $q$  on an  $R$ -module  $V$  induces the  $k$ -valued quadratic form  $\bar{q}$  on  $\bar{V} = V \otimes_R k = V/\mathfrak{m}V$  defined by  $\bar{q}(\bar{x}) = q(x) \bmod \mathfrak{m}$  and  $q$  is unimodular if and only if the form  $\bar{q}$  is unimodular (see § 6.3.B, Example 6).

**Proposition C.1.2.** *Let  $(V, q)$  be a quadratic inner product space over  $R$  of finite rank, and  $W, W', Z$  submodules. Let  $W, W'$  be free and assume that*

$$\beta_W(Z) = W^*, \quad \beta_{W'}(Z) = W'^*. \quad (\text{C.1})$$

Suppose  $t : W \xrightarrow{\cong} W'$  is an isometry such that

$$t(x) - x \in Z \text{ for all } x \in W. \quad (\text{C.2})$$

Then  $t$  extends to an isometry  $\tilde{t} : V \xrightarrow{\cong} V$  such that  $\tilde{t} = \text{id}$  on the orthogonal complement of  $Z$ . Moreover,  $\tilde{t}$  is a product of reflections in vectors of  $Z$  if we are

in one of the following cases:

$$k \neq \mathbb{F}_2 \quad \text{and} \quad \bar{q}(\bar{Z}) \neq 0, \quad (\text{C.3})$$

$$k = \mathbb{F}_2 \quad \text{and} \quad \bar{q}(\bar{Z}^\perp) \neq 0. \quad (\text{C.4})$$

Taking  $Z = V$  gives an unconditional extension of  $t$  to  $V$  which generalizes Corollary 7.2.8:

**Corollary C.1.3** (Witt's extension theorem over local rings). *Let  $(V, q)$  be a quadratic inner product space over  $R$  of finite rank,  $W, W'$  primitive free submodules such that  $\beta_W$  and  $\beta_{W'}$  are surjective (this is in particular the case for unimodular submodules  $W$  and  $W'$ ) and let  $t : W \rightarrow W'$  be an isometry. Then  $t$  extends to an isometry of  $V$ . If  $k \neq \mathbb{F}_2$ , then this extension is a product of hyperplane reflections.*

*Remark.* 1. As we have observed (see Remark 7.2.9.1), Witt's extension theorem is equivalent to Witt's cancellation theorem 7.2.7. The proof of this does not depend on 2 being invertible or not, and so Witt's cancellation theorem likewise holds over any local ring.

2. We may take  $W = W'$  which implies that in case  $k \neq \mathbb{F}_2$ , every isometry is a product of hyperplane reflections. Below we discuss the case  $k = \mathbb{F}_2$ . See Theorem C.1.4.

*Proof of Proposition C.1.2.* The extra condition on  $Z$  gives some flexibility enabling to prove the proposition first under the restrictive conditions (C.3) and (C.4) on the field  $k$ . So we first assume we are in one of these cases and then show the result. We shall demonstrate by induction on  $r := \text{rank}(W) = \text{rank}(W')$  that in this situation  $t$  can be written as a product of reflections in vectors of  $Z$  and hence provides the desired extension. Finally we show how to handle the situation if we are not in one of the cases (C.3) or (C.4). In the proof we simplify notation and use  $b = b_q$  for the polar form of  $q$ .

**Step 1:**  $r = 1$ . Then  $W = Rw, W' = Rw'$  and (by assumption)  $t(w) = w' = w + z$ ,  $z \in Z$ . We claim:

$$b(w, z) = -q(z), \quad b(w + z, z) = q(z), \quad (\text{C.5})$$

To see this, note that since  $t$  is an isometry,  $q(w) = q(w + z)$  and so  $b(w, z) = q(w + z) - q(w) - q(z) = -q(z)$ , proving the first equality. From  $b(z, z) = 2q(z)$  the second equality follows.

- In case  $q(z) \in R^\times$ , it follows from  $b(w, z) = -q(z)$  that  $t(w) = w + z = \sigma_z(w)$ . The isometry  $\sigma_z$  on  $V$  thus extends  $t$ . Since  $\sigma_z(y) = y$  for  $y \in Z^\perp$ ,  $t$  extends as a reflection in an element from  $Z$  inducing the identity on  $Z^\perp$  showing the proposition in this case.
- Suppose now that  $q(z)$  is not a unit. We search for  $x \in Z$ ,  $q(x)$  a unit, which gives a reflection  $\sigma_x$ . We introduce  $x' = w' - \sigma_x(w)$  which we rewrite as

$$x' = b(w, x)q(x)^{-1}x + z \quad (\text{and so } x' \in Z \text{ if } x \in Z). \quad (\text{C.6})$$

Moreover, since

$$q(x') = (b(w, x)b(w, x) + b(z, x)) \cdot q(x)^{-1} + q(z),$$

one finds

$$q(x') = b(w, x)b(w', x)q(x)^{-1} + q(z). \quad (\text{C.7})$$

Now assume that in addition to  $q(x)$  being invertible, also  $q(x')$  is invertible. From (C.6), (C.5) and (C.7) we get

$$\begin{aligned} b(x', w') &= b(x, w)b(x, w')q(x)^{-1} + b(z, w') \\ &= b(x, w)b(x, w')q(x)^{-1} + q(z) = q(x'). \end{aligned}$$

It follows that  $\sigma_{x'}(w') = w' - b(x', w')q(x')^{-1}x' = w' - x' = \sigma_x(w)$  and hence  $\tilde{t} := \sigma_{x'} \circ \sigma_x$  is the desired extension of  $t$ .

To complete Step 1, it suffices to find  $x \in Z$  such that both  $q(x)$  and  $q(x')$  are invertible, i.e., are not in the maximal ideal  $\mathfrak{m} \subset R$ . Taking into account (C.7) and remembering that  $q(z)$  is not a unit, we see that it suffices to assure that  $x \in Z$  exists with the following properties:

$$q(x) \notin \mathfrak{m}, \quad b(w, x) \notin \mathfrak{m}, \quad b(w', x) \notin \mathfrak{m}.$$

The last two conditions can be regarded as statements about the sets

$$\begin{aligned} H &= \{x \in Z \mid b(x, w) \equiv 0 \pmod{\mathfrak{m}}\} \\ H' &= \{x \in Z \mid b(x, w') \equiv 0 \pmod{\mathfrak{m}}\}. \end{aligned}$$

By assumption, the functional on  $W$  which has value 1 on the basis  $w$  of  $W$  is of the form  $x \mapsto b(x, s)$  for some  $s \in Z$ . In other words  $1 = b(w, s)$  and so  $s \notin H$  and  $\bar{s} \notin \bar{H}$  (with  $\bar{H} \subset \bar{V} = V/\mathfrak{m}$ ). Hence  $\bar{H}$  is a hyperplane in  $\bar{Z}$ , and likewise for  $\bar{H}'$  (using that  $\beta_Z(W') = (W')^*$ ). Since  $Z \rightarrow \bar{Z}$  is surjective, it thus suffices to show that  $\bar{q}$  is not identically zero on

$$\bar{Z}_0 := \bar{Z} - [\bar{H} \cup \bar{H}']$$

so that we may take  $x \in Z$  such that  $\bar{x} \in \bar{Z}_0$  with  $\bar{q}(\bar{x}) \neq 0$ . Note that for all scalars  $a \in k$  and all  $\bar{x} \in \bar{H} \cap \bar{H}'$  and  $\bar{y} \in \bar{Z}_0 = \bar{Z} - [\bar{H} \cup \bar{H}']$ , the vector  $a\bar{x} + \bar{y} \in \bar{Z}$  does not belong to  $\bar{H} \cup \bar{H}'$ . So, if we assume that on the contrary,  $\bar{q}|_{\bar{Z}_0} = 0$ , we would have for all  $a \in k$

$$0 = \bar{q}(a\bar{x} + \bar{y}) = a^2\bar{q}(\bar{x}) + a\bar{b}(\bar{x}, \bar{y}) + \bar{q}(\bar{y}).$$

We now distinguish the cases in which (C.3) or (C.4) hold. Supposing that (C.3) holds,  $k$  has three or more elements and so in that case

$$\bar{q}(\bar{x}) = \bar{b}(\bar{x}, \bar{y}) = \bar{q}(\bar{y}) = 0. \quad (\text{C.8})$$

Since  $b(w, z) = -q(z)$  and  $q(z) \in \mathfrak{m}$ , one has  $\bar{b}(\bar{w}, \bar{z}) = 0$  so that  $\bar{z} \in \bar{H}$ , and similarly  $\bar{z} \in \bar{H}'$ . But then, by the above argument,  $\bar{b}(\bar{z}, \bar{y}) = 0$  for all  $\bar{y} \in \bar{Z}_0$  and



hence  $\bar{b}(\bar{z}, \bar{Z}) = 0$  since the complement of two hyperplanes generates the entire vector space. Since  $w' = w + z$ , this implies  $\bar{H} = \bar{H}'$  (by the definition of  $\bar{H}$  and  $\bar{H}'$ ) and so every vector of  $\bar{Z}$  either belongs to  $\bar{H} \cap \bar{H}' = \bar{H}$  or to  $\bar{Z}_0 = \bar{Z} - \bar{H}$ , yielding  $\bar{q}(\bar{Z}) = 0$  by (C.8). This contradicts (C.3). So  $\bar{q}|_{\bar{Z}_0}$  is not identically zero.

Next, suppose that (C.4) holds (and  $\bar{q}|_{\bar{Z}_0} = 0$ ), so in particular  $k = \mathbb{F}_2$ . Assuming that  $\bar{x}, \bar{y} \in \bar{Z} \cap (\bar{Z})^\perp$ , then (C.8) still holds. From the definition of  $\bar{H}$  and  $\bar{H}'$  it follows that  $\bar{H} \cap \bar{Z}^\perp = \bar{H}' \cap \bar{Z}^\perp$ . So every vector from  $\bar{Z}^\perp$  either belongs to  $\bar{H} \cap \bar{H}'$  or to  $\bar{Z}_0$  and, as before,  $\bar{q}$  is identically zero on  $\bar{Z}^\perp$  which contradicts (C.4).

**Step 2: induction.** Now assume  $r > 1$ . We choose a basis  $\mathbf{W} = \{w_1, \dots, w_r\}$  for  $W$ . By assumption (C.1), and Lemma C.1.1 there are vectors  $z_1, \dots, z_r$  in  $Z$  such that  $b(w_i, z_j) = \delta_{ij}$ . These span a subspace  $H \subset Z$  and  $Z = H \oplus H'$ ,  $H' = Z \cap W^\perp$ . Moreover,  $\{z_1, \dots, z_r\}$  is a basis of  $Z$  modulo  $H'$ . By induction,  $t$  restricted to the span of the vectors  $w_1, \dots, w_{r-1}$  extends as a product  $s$  of reflections in vectors of  $Z$  (by assumption (C.3) or (C.4)). Replacing  $t$  with  $s^{-1}t$  we then may assume that  $t(w_i) = w_i$  for  $i = 1, \dots, r-1$ . This implies that for all  $w \in W$  one has  $b(t(w) - w, w_i) = b(t(w), t(w_i)) - b(w, w_i) = 0$ ,  $i = 1, \dots, r-1$ . In particular,  $t(w_r) - w_r$  is perpendicular to  $w_1, \dots, w_{r-1}$ . Adding a suitable multiple of  $z_r$  to  $t(w_r) - w_r$  we obtain an element in  $W^\perp \cap Z$ . So  $t(w_r) - w_r \in Z_0 := R \cdot z_r + H'$  and hence

$$t(w) - w \in Z_0 \text{ for all } w \in W. \quad (\text{C.9})$$

The idea now is to replace  $W, W', Z$  with  $W_0 := R \cdot w_r$ ,  $W'_0 = R \cdot t(w_r)$  and  $Z_0$ . By (C.9) the condition (C.2) holds for  $W_0$  and  $Z_0$ . Clearly, (C.1) holds for  $W_0$  and  $Z_0$ . It also holds for  $W'_0$  and  $Z_0$  as we see as follows. First of all, (C.1) holds for  $t(W) = W'$  by assumption, and so there exists  $z' \in Z$  with  $b(t(w_r), z') = 1$  while  $z'$  is perpendicular to  $t(w_i) = w_i$ ,  $i = 1, \dots, r-1$ . On the other hand  $z' - b(z', w_r)z_r$  belongs to  $Z$  and is orthogonal to  $w_r$  (and hence to all  $w_j$ ) and so belongs to  $H' = Z \cap W^\perp$ . In other words,  $z' \in Z_0$  and  $b(z', t(w_r)) = 1$ .

If the remaining conditions would hold, then by the argument for  $r = 1$ , the linear map  $t$  would extend to an isometry of  $V$  inducing the identity on  $Z_0^\perp \supset Z^\perp$ . Since  $z_r$  and  $H' = Z \cap W^\perp$  are orthogonal to  $w_1, \dots, w_{r-1}$  it would then follow that  $t = \text{id}$  on the span of  $w_1, \dots, w_{r-1}$  and so is an extension of  $t$  which is a product of reflections in vectors in  $Z_0 \subset Z$ .

So, if in addition either (C.3) or (C.4) holds (but now for  $Z_0$  which requires adapting the basis for  $W$  from which the vectors  $z_1, \dots, z_r$  were constructed), the result would follow. Hence we are left to show that either (C.3) or (C.4) hold in the present situation.

By the original assumption (C.3), respectively (C.4) for  $Z$ , there is a vector  $\bar{x} \in \bar{Z}$ , respectively  $\bar{x} \in \bar{Z}^\perp$  with  $\bar{q}(\bar{x}) \neq 0$ . In the second case we are done since  $Z_0^\perp \supset Z^\perp$ . In the first case we choose a vector  $\bar{z}_r \in \bar{Z} - \bar{H}'$  in such a way that  $\bar{x} \in k \cdot \bar{z}_r + \bar{H}' = \bar{Z}_0$ . We show now that another basis  $\mathbf{W}$  for  $W$  can be constructed so that the above argument still applies. First, observing that  $\dim(\bar{Z}/\bar{Z}_0) = r-1$ , choose  $\bar{z}_j$ ,  $j = 2, \dots, r$  so that  $\{\bar{z}_1, \dots, \bar{z}_r\}$  is a basis of  $\bar{Z}$  modulo  $\bar{Z}_0$ . Representing vectors  $z_1, \dots, z_r$  give a basis for  $Z$  modulo  $Z_0$ . Then for  $\mathbf{W}$  we take the basis  $\{w_1, \dots, w_r\}$  of  $W$  dual to  $\{z_1, \dots, z_r\}$ . Leaving  $H'$  unchanged, the previous argument now

applies to  $H = \text{span}(z_1, \dots, z_r)$ , and the new basis  $\mathbf{W}$ .

**Disposing of condition (C.3), respectively (C.4).** We enlarge  $V$  to  $\widetilde{V} := V \oplus U$ , where  $U$  is a hyperbolic plane over  $R$ , say with standard basis  $\{e, f\}$ ,  $q(e) = q(f) = 0, b(e, f) = 1$ . Since  $q(e + f) = 1$  either (C.3) or (C.4) holds with respect to  $\widetilde{Z} := Z \oplus R \cdot (e + f)$ . Setting  $\widetilde{W} := W \oplus R \cdot e, \widetilde{W}' := W' \oplus R \cdot e$ , (C.1) and (C.2) hold for the triple  $(\widetilde{W}, \widetilde{W}', \widetilde{Z})$ . We apply the previous argument in this setting to  $t' = t + \text{id}_{R \cdot e}$ . We get an extension  $\widetilde{t}'$  which leaves  $e$  invariant. Since  $b(\widetilde{Z}, e - f) = 0$ , it also leaves  $e - f$  and hence the summand  $U$  invariant. Then  $\widetilde{t}'$  has the shape  $\widetilde{t} \oplus \text{id}_U$  so that  $\widetilde{t}$  is the desired extension of  $t$ .  $\square$

We shall next use Proposition C.1.2 to extend the Cartan–Dieudonné theorem 7.2.4 to quadratic inner product spaces over local rings where 2 is not invertible.

**Theorem C.1.4** (Cartan–Dieudonné over local rings). *Every isometry of a quadratic inner product space  $(V, q)$  over a local ring  $(R, \mathfrak{m})$  is a product of hyperplane reflections, except if  $k = R/\mathfrak{m} = \mathbb{F}_2$ ,  $\text{rank}(V) = 4$  with quadratic form isometric to  $x^2 + xy + y^2 + u^2 + uv + v^2$  or if  $k = R/\mathfrak{m} = \mathbb{F}_2$ ,  $\text{rank}(V) = 2$ .*

*Proof.* If  $k \neq \mathbb{F}_2$  the result follows from Corollary C.1.3 (take  $W = W' = Z = V$ ) and so we may assume that  $k = \mathbb{F}_2$ . With  $t$  an isometry, we distinguish several cases:

**Case 1: There exists  $x \in V$  with  $q(x) \notin \mathfrak{m}$  and such that  $t(x) = x$ .** Since  $q(x) \notin \mathfrak{m}$  the submodule  $R \cdot x$  is free and hence  $V = R \cdot x \oplus W$  for some free submodule  $W$ . We can apply Proposition C.1.2 to  $t|_W, W' := t(W)$  and  $Z := x^\perp$  since first of all  $t$  restricts to  $t : Z \xrightarrow{\cong} Z$  since  $t(x) = x$ . Secondly the condition that  $\beta_W(Z) = W^*$  is satisfied since any functional on  $W$  can be extended by defining it to be zero on  $x$ , and the resulting element  $u \in V$  that represents this functional evidently belongs to  $Z$ . Similarly  $\beta_{W'}(Z) = (W')^*$  since  $\beta_W(z) = t^* \cdot \beta_{W'} \cdot t(z), z \in Z$ , so that surjectivity of  $\beta_W : Z \rightarrow W^*$  implies surjectivity of  $\beta_{W'} : Z \rightarrow (W')^*$ .

Since  $\bar{x} \in \overline{Z}^\perp$  and  $\bar{q}(\bar{x}) \neq 0$ , (C.4) applies. So there exists a product of reflections of vectors in  $Z$  which extends  $t|_W$ . Such reflections leave  $Z^\perp = Rx$  invariant and so  $t$  itself is a product of reflections.

**Case 2: No vector  $x \in V$  with  $q(x) \notin \mathfrak{m}$  is left invariant by  $t$ .** The idea is to search for a product  $\tilde{t}$  of reflections so that  $\tilde{t}(x) = t(x)$ , where  $x$  is any vector with  $q(x) \notin \mathfrak{m}$ . If such  $\tilde{t}$  exists,  $\tilde{t}^{-1} \cdot t$  leaves  $x$  invariant and Case 1 shows that it is a product of reflections, and hence so is  $t$ . Such  $\tilde{t}$  exists by Proposition C.1.2 applied to  $(W = R \cdot x, W' = R \cdot t(x), Z)$  if a submodule  $Z \subset V$  exists satisfying the conditions (C.1), (C.2), (C.4) required to apply this proposition to  $t|_W$ . Such a submodule can be found as follows. Take any  $y \in V$  with  $q(y) \notin \mathfrak{m}$  and provisionally set

$$Z := y^\perp + \mathfrak{m} \cdot V.$$

Reducing mod  $\mathfrak{m}$  shows that  $\overline{Z} = \overline{y}^\perp$  and so  $\overline{y}$  belongs to  $\overline{Z}^\perp$  and since  $\bar{q}(\overline{y}) \neq 0$ , condition (C.4) holds. Now observe that condition (C.2), reading  $t(x) - x \in Z$  can be phrased as

$$\overline{y} \in H = [\overline{t(x)} - \overline{x}]^\perp \subset \overline{V}.$$

Next, condition (C.1) stating in this case that  $b(x, Z) = b(t(x), Z) = R$  translates as  $\bar{b}(\bar{x}, \bar{Z}) = k = \mathbb{F}_2$  and similarly for  $t(x)$ . Since  $\bar{Z} = \bar{y}^\perp$ , the vanishing of  $\bar{b}(\bar{x}, \bar{y}^\perp)$  would be equivalent to  $\bar{x} \in (\bar{y}^\perp)^\perp = \mathbb{F}_2 \cdot \bar{y}$ , and so we need  $\bar{y} \neq \bar{x}$ , and similarly we need  $t(x) \neq \bar{y}$ .

Summarizing, conditions (C.1), (C.2) (C.4) hold if we can find a non-isotropic  $\bar{y} \in H = [t(x) - \bar{x}]^\perp$  distinct from  $\bar{x}$  and from  $t(x)$ . Since  $H$  may or may not contain the non-isotropic vectors  $\bar{x}$  or  $t(x)$ , this is possible if  $H$  contains more than 2 non-isotropic vectors.

Observe that since  $\bar{q}$  is unimodular,  $\bar{V} \simeq \bigoplus^m U_k$  or  $\bar{V} \simeq \bigoplus^m U_k \oplus V_k$ , where  $V_k$  is represented by the form  $x^2 + xy + y^2$  (see e.g. Theorem 8.3.3). Note that  $H = \bar{V}$  or  $H$  is a hyperplane in  $\bar{V}$ , and so for the count we may assume that  $H$  is a hyperplane, say  $H = h^\perp$ . If  $h$  is isotropic, then we may assume that  $h$  belongs to some summand  $U_k$  (here we use Witt's extension theorem C.1.3 and the fact that  $V_k$  does not contain isotropic vectors). If  $h$  is not isotropic, then again by Corollary C.1.3 we may assume that  $h$  belongs to some summand  $U_k$  or to the summand  $V_k$  (in the second case). Hence either  $\bar{q}|_H \simeq \bigoplus^{m-1} U_k \oplus \langle 1 \rangle$ ,  $\bar{q}|_H \simeq \bigoplus^{m-1} U_k \oplus \langle 0 \rangle$  (in the first case),  $\bar{q}|_H \simeq \bigoplus^m U_k \oplus \langle 1 \rangle$ ,  $\bar{q}|_H \simeq \bigoplus^m U_k \oplus \langle 0 \rangle$  (in the second case). Then by the results of Section 16.3, the number of non-isotropic vectors on  $H$  is at least  $2^{2m-3}$ ,  $\dim \bar{V} = 2m$ . So, if  $m \geq 3$  we can find 3 non-isotropic vectors.

In case  $\dim \bar{V} = 4$  we can easily see that only if  $\bar{V} = \bigoplus^2 U_k$  and  $H$  is such that  $\bar{q}|_H \simeq U_k \oplus \langle 0 \rangle$ , there are precisely 2 non-isotropic vectors. This can indeed occur: take  $H$  the diagonal in  $\bigoplus^2 U_k$ . Since  $\bigoplus^2 U_k \simeq \bigoplus^2 V_k$  (this follows like equation (I) in Appendix C.3.A), we can apply the observation of Example 7.2.6.1: exchanging the two summands (an obvious isometry) is not a product of reflections.  $\square$

## C.2 Index Invariants for Torsion Forms

We present the material from [156, Ch.III] on invariants for torsion forms which is used in § C.3.A to refine the normal form classification in the 2-primary case.

**Generalized Gauss Sums.** Let  $(G, q)$  be a non-degenerate quadratic torsion group. The invariant  $\tau_8(q)$  is the mod 8 index of a non-degenerate integral quadratic lattice of which  $q$  is the discriminant form. We saw in Section 12.2 that this is a well-defined invariant. In this section we discuss an alternative approach to the index modulo 8 which is based on Gauss sums of the form

$$\gamma_{(G,q)} := \frac{1}{\sqrt{|G|}} \sum_{x \in G} \exp(2\pi i q(x)) \in \mathbb{C}.$$

This obviously is an invariant of  $(G, q)$ . It figures in the following result which is equivalent to Corollary 12.2.4:

**Theorem C.2.1** (Milgram). *Let  $L$  be a non-degenerate integral quadratic lattice with discriminant form  $(G, q)$ . Then  $\gamma_{(G,q)} = \rho_8^{\tau_8(q)}$ ,  $\rho_8 = \exp(2\pi i/8)$ .<sup>1</sup>*

There are further generalized Gauss sum invariants for possibly degenerate quadratic forms  $q$  on a finite Abelian group  $G$ , namely

$$\gamma_{(G,q)}(f) = \frac{1}{\sqrt{|G|}} \sum_{x \in G} \exp 2\pi i (f \circ q(x)),$$

which involve a  $\mathbb{Z}$ -homomorphism  $f : \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$ . Taking for  $f$  the identity we get back the invariant  $\gamma_{(G,q)}$ . If  $f$  is multiplication with an integer  $N$ , then  $N \cdot q$  is also a torsion quadratic form, but, even if  $q$  is non-degenerate, the new form  $N \cdot q$  can be a degenerate quadratic form.

The basic properties of Gauss sums for possibly degenerate quadratic forms are:

**Proposition C.2.2.** (1) *If  $\iota : (G, q) \simeq (G', q')$  is an isometry of torsion quadratic forms and  $f, f' : \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$  homomorphisms for which  $f' \circ q' \circ \iota = f \circ q$ , then  $\gamma_{(G',q')}(f') = \gamma_{(G,q)}(f)$ .*

(2) *Let  $(G, q) = (G', q') \oplus (G'', q'')$ , then for all homomorphisms  $f : \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$  one has  $\gamma_{(G,q)}(f) = \gamma_{(G',q')}(f) \cdot \gamma_{(G'',q'')}(f)$ .*

(3) *If  $H$  is a totally isotropic subgroup of  $(G, q)$  then  $\gamma_{(G,q)} = \sqrt{|H|} \frac{1}{\sqrt{|G/H^\perp|}} \cdot \gamma_{(H^\perp/H, q)}$ . If, moreover,  $(G, q)$  is non-degenerate, then  $\gamma_{(G,q)} = \gamma_{(H^\perp/H, q)}$ .*

(4) *The quotient group<sup>2</sup>  $\bar{G} = G/\text{rad}(q)$  with induced quadratic form  $\bar{q}$  satisfies  $\gamma_{(G,q)}(f) = \sqrt{|\text{rad}(q)|} \cdot \gamma_{(\bar{G}, \bar{q})}(f)$  for every homomorphism  $f : \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$ .*

(5) *Suppose that  $\text{rad}(q) \neq G^\perp$ , then  $\gamma_{(G,q)}(\text{id}) = \gamma_{(G,q)}(\text{id}) = 0$ .*

*Proof.* (1) is clear since one sums the complex numbers  $\exp 2\pi i (f \circ q(x))$  over all  $x \in G$ , and  $\iota$  translates this into summing the complex numbers  $\exp 2\pi i (f' \circ q'(x'))$ ,  $x' \in G'$ .

(2) This follows since  $|G| = |G'| \cdot |G''|$  and  $q(x+y) = q(x) + q(y) + b(x, y) = q(x) + q(y)$  if  $x \in G', y \in G''$ .

(3) Let  $b$  be the polar form of  $q$ . Choose a complete set  $\{x_1, \dots, x_m\}$  of  $m = |G/H|$  representatives for  $G/H$ , such that the set  $\{x_1, \dots, x_m\} \cap H^\perp$  is a complete set of representatives for  $H^\perp/H$ , and sum over  $x_j + y, j = 1, \dots, m, y \in H$ . This gives

$$\gamma_{(G,q)} = \frac{1}{\sqrt{|G|}} \cdot \sum_{x_j} \exp(2\pi i q(x_j)) \cdot \sum_{y \in H} \exp(2\pi i b(x_j, y)).$$

The (restricted) adjoint map  $G \rightarrow \text{Hom}(H, \mathbb{Q}/\mathbb{Z})$  sending  $x_j$  to  $b(x_j, -)|_H$  is the zero map if and only if every  $x_j \in H^\perp$ . In that case  $\sum_{y \in H} \exp(2\pi i b(x_j, y)) = |H|$ . Otherwise,  $b(x_j, H)$  is a torsion subgroup of  $\mathbb{Q}/\mathbb{Z}$ , say of order  $m$ , and  $\sum_{y \in H} \exp(2\pi i b(x_j, y))$  is a sum over all  $m$ -th roots of unity, each counted  $|H|/m$

<sup>1</sup>A nice short proof of Milgram's theorem can be found in [151, Appendix 4].

<sup>2</sup>Recall that the radical  $\text{rad}(q)$  is the subgroup of the null-space  $G^\perp$  of the polar form of  $q$  on which  $q$  is identically zero.

times, and hence contributes zero. In other words, using  $|G/H| = |G/H^\perp| \cdot |H^\perp/H|$ , we find

$$\begin{aligned} \gamma_{(G,q)} &= \frac{1}{\sqrt{|G|}} \cdot |H| \cdot \sum_{x_j \in H^\perp} \exp(2\pi i q(x_j)) \\ &= \sqrt{|H|} \cdot \frac{1}{\sqrt{|G/H|}} \cdot \sum_{x_j \in H^\perp} \exp(2\pi i q(x_j)) = \sqrt{|H|} \frac{1}{\sqrt{|G/H^\perp|}} \cdot \gamma_{(H^\perp/H,q)}. \end{aligned}$$

In the non-degenerate situation one has  $|H| = |G/H^\perp|$  and the last assertion of (3) follows.

(4) Clearly,  $\text{rad}(q)$  is isotropic for the quadratic form  $f \circ q$  on  $G$  while  $(\text{rad}(q))^\perp = G$ . But then, by (3),

$$\gamma_{(G,q)}(f) = \gamma_{(G,f \circ q)} = \sqrt{|\text{rad}(q)|} \cdot \gamma_{(\bar{G}, f \circ \bar{q})} = \sqrt{|\text{rad}(q)|} \cdot \gamma_{(\bar{G}, \bar{q})}(f).$$

(5) By (4) we may assume that  $\text{rad}(q) = 0$ . Now  $G = G^\perp \oplus H$  for any supplement  $H$  of  $G^\perp$  in  $G$ , and so by (2) it suffices to show that  $\gamma_{(G^\perp,q)} = 0$ . We first show that  $G^\perp$  has only one non-zero element  $x \in G^\perp$ . If  $x$  would be 2-divisible, say  $x = 2y$ , then  $q(2x) = 4q(x) = 2b(y, y) = b(x, y) = 0$  and  $x \in \text{rad}(q)$ , contrary to assumption. Now observe that  $q : G^\perp \rightarrow \mathbb{Q}/\mathbb{Z}$  is additive, since  $q(u+v) = q(u) + q(v) + b(u, v) = q(u) + q(v)$  for all  $u, v \in G^\perp$ . Hence  $4q(x) = q(2x) = q(x+x) = 2q(x)$  and  $q(x) \equiv \frac{1}{2} \pmod{\mathbb{Z}}$ . If  $x' \in G^\perp$  is also a non-zero element, we find  $q(x-x') = 0$  and so,  $x = x'$  since  $\text{rad}(q) = 0$ . In other words  $G^\perp = \{0, x\}$  and  $\exp(2\pi i q(0)) = 1$  while  $\exp(2\pi i q(x)) = -1$ .  $\square$

**Calculating Index Invariants.** Viewing powers  $p^\ell$  as homomorphisms from  $\mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$ , the Gauss sums lead to generalized index invariants  $\gamma_{(G,q)}(p^\ell)$  for  $p$ -primary torsion forms. We calculate their values on the basic building blocks  $\langle u \cdot p^{-k} \rangle$ ,  $u$  a unit mod  $p$ ,  $u_k, v_k$ :

**Proposition C.2.3.** (1) *Let  $p$  be a prime and  $G = \mathbb{Z}/p^k\mathbb{Z}$ ,  $k \geq 1$ . Then*

$$\gamma_{(G, \langle u \cdot p^{-k} \rangle)}(p^\ell) = \begin{cases} p^{k/2} & \text{if } \ell > k \\ p^{\ell/2} & \text{if } \ell = k, \quad p \neq 2 \\ 0 & \text{if } \ell = k, \quad p = 2 \\ p^{\ell/2} \cdot \gamma_{(G, \langle u \cdot p^{-(k-\ell)} \rangle)} & \text{if } \ell < k \end{cases}$$

(2) *For  $u_k, v_k$ ,  $G = \mathbb{Z}/2^k\mathbb{Z} \oplus \mathbb{Z}/2^k\mathbb{Z}$ , we have*

$$\gamma_{(G, u_k)}(2^\ell) = \begin{cases} 2^k & \text{if } \ell \geq k \\ 2^\ell \cdot \gamma_{(G, u_{k-\ell})} & \text{if } \ell < k \end{cases} \quad \text{and} \quad \gamma_{(G, v_k)}(2^\ell) = \begin{cases} 2^k & \text{if } \ell \geq k \\ 2^\ell \cdot \gamma_{(G, v_{k-\ell})} & \text{if } \ell < k \end{cases}$$

*Proof.* (1) The form  $q' = p^\ell \langle u \cdot p^{-k} \rangle$  is identically zero if  $\ell > k$ , and so by Proposition C.2.2.4,  $\gamma_{(G,q')} = \sqrt{|G|} = p^{k/2}$ .

Let  $e$  generate the cyclic group  $\mathbb{Z}/p^k\mathbb{Z}$ . For  $p$  odd and  $\ell < k$ , one has  $(G, q')^\perp = \text{rad}(q') = \langle p^{k-\ell} \cdot e \rangle$ , and the induced form on  $G/(G, q')^\perp \simeq \mathbb{Z}/p^{k-\ell}\mathbb{Z}$  is given by  $x \mapsto \frac{1}{2} \cdot u \cdot p^{\ell-k} x^2$ . The same argument holds for  $p = 2$  and  $\ell < k$ .

Finally, if  $p = 2$  and  $k = \ell$ ,  $\text{rad}(q') \subsetneq (G, q')^\perp$  and so by Proposition C.2.2(5) we get  $\gamma_{(G, q')} = 0$  in this case.

(2) The proof is similar to (1), but here for  $\ell < k$  one has  $G^\perp = \text{rad}(q) \simeq \mathbb{Z}/2^\ell\mathbb{Z} \oplus \mathbb{Z}/2^\ell\mathbb{Z}$ . □

Let  $G = \bigoplus_j H_j$  with  $H_j$  homogeneous  $p$ -primary of exponent  $j$  and length  $r_j$ . The above calculations suggest to introduce

**Definition C.2.4.**  $\rho_G(\ell) = \sum_{j \leq \ell} j \cdot r_j + \ell \cdot \sum_{j > \ell} r_j$ ,  $\sigma_\ell(G, q) = \gamma_{(G, q)}(p^\ell) \cdot p^{-\frac{1}{2}\rho_G(\ell)}$ .

**Corollary C.2.5.** (1). Let  $p$  be a prime and  $G = \mathbb{Z}/p^k\mathbb{Z}$ . Then

$$\sigma_\ell(G, \langle u \cdot p^{-k} \rangle) = \begin{cases} 1 & \text{if } \ell > k \\ 1 & \text{if } \ell = k, \quad p \neq 2 \\ 0 & \text{if } \ell = k, \quad p = 2 \\ \gamma_{(G, \langle u \cdot p^{-(k-\ell)} \rangle)} & \text{if } \ell < k. \end{cases}$$

(2) For  $u_k, v_k$ ,  $G = \mathbb{Z}/2^k\mathbb{Z} \oplus \mathbb{Z}/2^k\mathbb{Z}$ , we have

$$\sigma_\ell(G, u_k) = \begin{cases} 1 & \text{if } \ell \geq k \\ \gamma_{(G, u_{k-\ell})} & \text{if } \ell < k \end{cases} \quad \text{and} \quad \sigma_\ell(G, v_k) = \begin{cases} 1 & \text{if } \ell \geq k \\ \gamma_{(G, v_{k-\ell})} & \text{if } \ell < k. \end{cases}$$

Table C.2.1: Values of  $\sigma_\ell(q)$ .

$p$ odd, $q = \langle u \cdot p^{-k} \rangle$	$\left(\frac{u}{p}\right)$	$k - \ell > 0$ even	$k - \ell > 0$ odd	$\ell = k$	$\ell > k$
$p \equiv 1 \pmod 8$	1	1	1	1	1
	-1	1	-1	1	1
$p \equiv -1 \pmod 8$	1	1	<b>i</b>	1	1
	-1	1	<b>-i</b>	1	1
$p \equiv 3 \pmod 8$	1	1	<b>-i</b>	1	1
	-1	1	<b>i</b>	1	1
$p \equiv -3 \pmod 8$	1	1	-1	1	1
	-1	1	1	1	1
$p = 2$	$u \pmod 8$	$k - \ell > 0$ even	$k - \ell > 0$ odd	$\ell = k$	$\ell > k$
$q = \langle u \cdot 2^{-k} \rangle$	1	$\rho_8$	$\rho_8$	0	1
	-1	$-\rho_8^3$	$-\rho_8^3$	0	1
	3	$\rho_8^3$	$-\rho_8^3$	0	1
	-3	$-\rho_8$	$\rho_8$	0	1
$q = u_k$		1	1	1	1
$q = v_k$		1	-1	1	1

Table C.2.1 has been established using the tables from Propositions 12.3.2 and 12.3.3 for the index modulo 8.

### C.3 Normal Forms for 2-Primary Torsion Quadratic Forms

We present some of the material from [156, Ch.IV] on the normal form classification for 2-primary torsion forms. The results of the first section below are used in the main body of the book.

**C.3.A The homogeneous case.** For  $p$  odd, we gave the normal forms for (homogeneous)  $p$ -primary torsion forms in Section 11.1, but we did not give a unique normal form in case  $p = 2$ . Recall that the normal form decomposition we established in Section 11.2 used the isometries I,II,III of Lemma 11.2.1. In Section 14.6 we also used another relation, relation IV. Here we shall prove these relations which we state again for convenience.

As usual, there are similar relations for torsion quadratic forms where  $2^k$  is replaced by  $2^{-k}$ ,  $U_k$  and  $V_k$  by  $u_k$  and  $v_k$ . In what follows  $u, u', u''$  are units in  $\mathbb{Z}_2$ . Note that  $uu' + uu'' + u'u''$  is a unit and can be checked to assume only the values 3 and  $-1$  modulo 8. Further isometries involving lattices of different exponents are stated as Lemma C.3.3.

$$U_k \oplus U_k \simeq V_k \oplus V_k, \quad k \geq 0, \tag{I}$$

$$\langle u \rangle \oplus \langle u' \rangle \oplus \langle u'' \rangle (2^k) \simeq \begin{cases} V_k \oplus \langle (u + u' + u'') \cdot 2^k \rangle \\ \text{in case } uu' + uu'' + u'u'' \equiv 3 \pmod{8} \\ U_k \oplus \langle (u + u' + u'') \cdot 2^k \rangle \\ \text{in case } uu' + uu'' + u'u'' \equiv -1 \pmod{8} \end{cases} \quad k \geq 0 \tag{II}$$

$$\langle u \rangle \oplus \langle u' \rangle (2^k) \simeq \langle -3u \rangle \oplus \langle -3u' \rangle (2^k), \quad k \geq 0 \tag{III}$$

$$U_k \oplus (\langle u \rangle \oplus \langle u' \rangle) (2^k) \simeq V_k \oplus (\langle u - 2 \rangle \oplus \langle u' + 2 \rangle) (2^k), \quad u \equiv u' \pmod{4}, k \geq 1. \tag{IV}$$

*Proof.* For the verifications that follow, we use base changes. In each case the conditions are such that the proposed change of basis matrix is invertible in  $\mathbb{Z}_2$ . It suffices to verify each relation for the smallest value of the integer  $k$ .

(I) Use  $V_k(-1) \simeq V_k$  by Lemma 10.1.2 and

$$C \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} C^T = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & -2 & -1 \\ 0 & 0 & -1 & -2 \end{pmatrix}, \text{ with } C = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & -1 & -1 & 0 \\ 1 & -1 & 0 & -1 \end{pmatrix}.$$

(II) First make a change of basis:

$$C \begin{pmatrix} u & 0 & 0 \\ 0 & u' & 0 \\ 0 & 0 & u'' \end{pmatrix} C^T = \begin{pmatrix} u + u' + u'' & 0 & 0 \\ 0 & u(u')^2 + u^2u' & uu'u'' \\ 0 & uu'u'' & u(u'')^2 + u^2u'' \end{pmatrix},$$

where  $C = \begin{pmatrix} 1 & 1 & 1 \\ u' & -u & 0 \\ u'' & 0 & -u \end{pmatrix}$ . Since  $u, u', u''$  are units,  $u(u')^2 + u^2u'$  and  $u(u'')^2 + u^2u''$  are even, say  $u(u')^2 + u^2u' = 2a$  and  $u(u'')^2 + u^2u'' = 2c$  and  $uu'u'' = b$  is

odd. So, by Lemma 10.1.2 the binary form with matrix  $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ , which splits off, is indecomposable. Moreover, it is isometric to  $U$  if and only if  $\frac{1}{4} \cdot 4ac = \frac{1}{2} (u(u')^2 + u^2u') \cdot \frac{1}{2} (u(u'')^2 + u^2u'')$  is even. Since a square of a unit is 1 modulo 8, we find  $(u(u')^2 + u^2u') \cdot (u(u'')^2 + u^2u'') \equiv 1 + (uu' + uu'' + u'u'') \pmod{8}$ . Hence, in this setting  $ac$  is even if and only if  $uu' + uu'' + u'u'' \equiv -1 \pmod{8}$ , which proves the isometry for  $k = 0$ .

(III) This uses that in  $D(\mathbb{Z}_2)$  we have  $u + 4u' = 5u$  and so also  $uu'(u + 4u') = 5u^2u' = 5u'$  which implies

$$\begin{pmatrix} 1 & 2 \\ 2u' & -u \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & u' \end{pmatrix} \begin{pmatrix} 1 & 2u' \\ 2 & -u \end{pmatrix} = \begin{pmatrix} u + 4u' & 0 \\ 0 & uu'(u + 4u') \end{pmatrix} \simeq \begin{pmatrix} 5u & 0 \\ 0 & 5u' \end{pmatrix},$$

which proves the relation for  $k = 0$ .

(IV) We have

$$C \begin{pmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 2u & 0 \\ 0 & 0 & 0 & 2u' \end{pmatrix} C^T = \begin{pmatrix} 4 & 2 & 0 & 0 \\ 2 & 2(u + u') & 0 & 0 \\ 0 & 0 & 2a & b \\ 0 & 0 & b & 2c \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ -u & u & 1 & 0 \\ -u' & u' & 0 & 1 \end{pmatrix},$$

$$a = -2u^2 + u, \quad b = -4uu', \quad c = -2(u')^2 + u'.$$

To the matrix  $\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}$  we apply Lemma 10.1.2. So the corresponding form is decomposable. Also  $a = -2u^2 + u \equiv u - 2 \pmod{8}$ ,  $c \equiv u' - 2$  so that

$$d = ac - \frac{1}{4}b^2 \equiv (u - 2)(u' - 2) - 4(uu')^2 \equiv uu' - 2(u + u') \pmod{8}.$$

But since  $u \equiv u' \pmod{4}$  we get

$$ad \equiv (u - 2)(uu' - 4u') \equiv u' - 4 + 2uu' \equiv u' + 4 + 2u^2 \equiv u' + 2 \pmod{8},$$

which shows the claim for  $k = 1$ .  $\square$

For classification purposes one further invariant will be used, the reduced discriminant  $\delta$ , introduced in Section 9.1.B. We recall that  $\delta$  is a well defined integer mod 8 if  $k \geq 2$  and mod 4 in case  $k = 1$ . We are now ready to establish a finer normal form:

**Proposition C.3.1.** *Let  $(G, q)$  be a homogeneous 2-primary quadratic torsion group of exponent  $k$  and length  $\ell(G)$ . Then*

(1)  $q \simeq w_k \oplus^b v_k \oplus^c u_k$ , where  $w_k$  is an orthogonal direct sum of  $a$  cyclic groups,  $a \leq 2$ ,  $b \leq 1$ ,  $c = \frac{1}{2}(\ell(G) - a) - b$ , and where  $a$  is an isometry invariant of  $q$ .

(2) If  $a = 2, b = 0$ , then  $w_k$  is isometric to one of the following:

$$\begin{aligned} &\langle 2^{-k} \rangle \oplus \langle 2^{-k} \rangle, \quad \langle -2^{-k} \rangle \oplus \langle -2^{-k} \rangle, \quad \text{with } \delta(q) = 1 \\ &\langle -2^{-k} \rangle \oplus \langle 3 \cdot 2^{-k} \rangle, \quad \langle 2^{-k} \rangle \oplus \langle -3 \cdot 2^{-k} \rangle \quad \text{with } \delta(q) = -3 \\ &\langle 2^{-k} \rangle \oplus \langle -2^{-k} \rangle, \quad \text{with } \delta(q) = -1 \\ &\langle 2^{-k} \rangle \oplus \langle 3 \cdot 2^{-k} \rangle, \quad \text{with } \delta(q) = 3. \end{aligned}$$



(3) If  $a = 2, b = 1$ , one may assume that  $w_k \oplus v_k$  is one of the following:

$$\begin{aligned} &\langle 2^{-k} \rangle \oplus \langle 3 \cdot 2^{-k} \rangle \oplus v_k \text{ with } \delta(q) = 1 \\ &\langle 2^{-k} \rangle \oplus \langle -2^{-k} \rangle \oplus v_k \text{ with } \delta(q) = -3. \end{aligned}$$

*Proof.* Since we proved the relations I–III, (1) follows from the discussion in Section 11.2. To make further reductions, we use relation (III). To show (2), we use relation (I) to eliminate 4 of the 10 possible decomposable length 2 quadratic torsion groups of exponent  $k$ . Finally, (3) follows from relation (IV) since if one of the first four possibilities of (2) comes with a copy of  $v_k$ , the copy of  $v_k$  can be exchanged with a copy of  $u_k$ .  $\square$

A normal form as in Proposition C.3.1 is called a **reduced homogeneous normal form**. Such normal forms are collected in the following table.

Table C.3.1: Reduced homogeneous normal forms  $q = \oplus^a \langle u \cdot 2^{-k} \rangle \oplus \oplus^b v_k \oplus \oplus^{\frac{1}{2}(\ell(G)-a)-b} u_k$  for dyadic forms  $(G, q)$ ,  $G \simeq (\mathbb{Z}/2^k\mathbb{Z})^{\ell(G)}$ .

$q'$	$a$	$b$	$\ell(G) \bmod 2$	$(-1)^{\frac{1}{2}(\ell(G)-a)}\delta(q)$	$\sigma_{k-1}(q)$
$\langle 2^{-k} \rangle$	1	0	1	1	$\rho_8$
$\langle -3 \cdot 2^{-k} \rangle \oplus v_k$	1	1	1	1	$-\rho_8$
$\langle 2^{-k} \rangle \oplus \langle -2^{-k} \rangle$	2	0	0	1	1
$\langle 2^{-k} \rangle \oplus \langle 3 \cdot 2^{-k} \rangle \oplus v_k$	2	1	0	1	-1
$\langle -3 \cdot 2^{-k} \rangle$	1	0	1	-3	$\rho_8$
$\langle 1 \cdot 2^{-k} \rangle \oplus v_k$	1	1	1	-3	$-\rho_8$
$\langle 2^{-k} \rangle \oplus \langle 3 \cdot 2^{-k} \rangle$	2	0	0	-3	1
$\langle 2^{-k} \rangle \oplus \langle -2^{-k} \rangle \oplus v_k$	2	1	0	-3	-1
$\langle -2^{-k} \rangle$	1	0	1	-1	$-\rho_8^3$
$\langle 3 \cdot 2^{-k} \rangle \oplus v_k$	1	1	1	-1	$\rho_8^3$
$\langle -2^{-k} \rangle \oplus \langle -2^{-k} \rangle$	2	0	0	-1	$-\mathbf{i}$
$\langle 2^{-k} \rangle \oplus \langle 2^{-k} \rangle$	2	0	0	-1	$\mathbf{i}$
$\langle 3 \cdot 2^{-k} \rangle$	1	0	1	3	$-\rho_8^3$
$\langle -2^{-k} \rangle \oplus v_k$	1	1	1	3	$\rho_8^3$
$\langle -2^{-k} \rangle \oplus \langle 3 \cdot 2^{-k} \rangle$	2	0	0	3	$-\mathbf{i}$
$\langle 2^{-k} \rangle \oplus \langle -3 \cdot 2^{-k} \rangle$	2	0	0	3	$\mathbf{i}$

**Corollary C.3.2.** *Every 2-primary homogeneous quadratic form has a unique reduced normal form given in Table C.3.1. For  $k \geq 2$  these forms are mutually non-isometric. For  $k = 1$  the forms with  $\delta = 1, -3$  with corresponding remaining invariants are isometric and the same holds for forms with  $\delta = -1, 3$ .*

*Proof.* The reduced discriminant is multiplicative on homogeneous orthogonal sums and this determines its value on the reduced normal forms. Note that  $\ell(G) - a$  is even and half this number is the sum of the number of copies  $u_k$  plus  $v_k$ . The

contribution of the number of copies of  $u_k$  to  $\delta$  is therefore  $\pm(-1)^{(\ell(G)-a)/2}$  according to whether  $b = 0$  or  $b = 1$ . This implies that the contribution  $\delta'$  to  $\delta$  coming from the summands under  $q'$  in the table has to be multiplied with this factor. In other words,  $\pm\delta' \cdot (-1)^{(\ell(G)-a)/2}$  gives  $\delta$ . This explains the fifth column. Table C.2.1 can be used for the last column exhibiting  $\sigma_{k-1}$  which is likewise multiplicative on orthogonal homogeneous sums.

The table then exhibits a complete set of invariants showing the various normal forms are mutually non-isometric: forms with fixed reduced determinants  $\delta$  are in consecutive rows separated by double lines,  $a$  is a distinguishing invariant and  $\sigma_{k-1}$  is then needed to distinguish forms with the same  $\delta$  and  $a$ .

Note that for  $\delta = 1, -3$  the remaining invariants are line by line the same and likewise for  $\delta = -1, 3$ . For  $k = 1$  the corresponding forms are the same which should be the case since here  $\delta$  is only well defined modulo 4.  $\square$

### C.3.B The non-homogeneous case.

**Further relations.** In Section C.3.A we presented the relations (I)–(IV) which are valid for homogeneous lattices. As announced, there are further relations between non-homogeneous lattices:

**Lemma C.3.3.** *Let  $u, u', u''$  be units in  $\mathbb{Z}_2$ . Then the following relations hold between non-homogeneous dyadic forms.*

$$\langle u \cdot 2^{k-1} \rangle \oplus U_k \simeq \langle -3u \cdot 2^{k-1} \rangle \oplus V_k \text{ for } k \geq 1 \quad (\text{V})$$

$$U_{k-1} \oplus \langle u \cdot 2^k \rangle \simeq \langle 3u \cdot 2^k \rangle \oplus V_{k-1} \text{ for } k \geq 1 \quad (\text{VI})$$

$$\langle u \cdot 2^{k-1} \rangle \oplus \langle u' \cdot 2^k \rangle \simeq \langle (u + 2u') \cdot 2^{k-1} \rangle \oplus \langle (u' + 2u) \cdot 2^k \rangle \text{ for } k \geq 1, \quad (\text{VII})$$

$$(\langle u \rangle \oplus \langle u' \rangle)(2^{k-1}) \oplus \langle 2^k \rangle \simeq (\langle u + 2 \rangle \oplus \langle u' - 2 \rangle)(2^{k-1}) \oplus \langle -3 \cdot 2^k \rangle \quad (\text{VIII})$$

$$\text{if } u \equiv u' \pmod{4}, \quad k \geq 1.$$

$$\langle u \cdot 2^{k-2} \rangle \oplus \langle u' \cdot 2^k \rangle \simeq \langle -3u \cdot 2^{k-2} \rangle \oplus \langle -3u' \cdot 2^k \rangle, \text{ for } k \geq 3. \quad (\text{IX})$$

Similar relations hold for their quadratic torsion forms, that is, for the 2-primary quadratic torsion groups where the exponents  $2^j$  are replaced by  $2^{-j}$ , and for  $u_k$  and  $v_k$  instead of  $U_k$  and  $V_k$ , respectively.

*Proof.* (V). This uses the computation

$$\begin{pmatrix} 1 & 1 & 1 \\ -2 & u & 0 \\ -2 & 0 & u \end{pmatrix} \begin{pmatrix} u & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & -2 & -2 \\ 1 & u & 0 \\ 1 & 0 & u \end{pmatrix} = \begin{pmatrix} u+4 & 0 & 0 \\ 0 & 2^2 \cdot u & 2(u^2+2u) \\ 0 & 2(u^2+2u) & 2 \cdot 2u \end{pmatrix}.$$

Since  $u + 4 \equiv -3u \pmod{8}$  and using Lemma 10.1.2.2 for the second summand, the claim follows for  $k = 1$ .

(VI). This can be proved in a similar way, using the computation

$$\begin{pmatrix} 2 & 2 & 1 \\ u & 0 & -1 \\ 0 & u & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2u \end{pmatrix} \begin{pmatrix} 2 & u & 0 \\ 2 & 0 & u \\ 1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 2(u+2) & 0 & 0 \\ 0 & 2u & u^2+2u \\ 0 & u^2+2u & 2u \end{pmatrix}.$$

As in the proof of (V) this gives the result for  $k = 1$ .

(VII). We have

$$\begin{pmatrix} 1 & 1 \\ -2u' & u \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & 2u' \end{pmatrix} \begin{pmatrix} 1 & -2u' \\ 1 & u \end{pmatrix} = \begin{pmatrix} u+2u' & 0 \\ 0 & 2(u'u^2+2uu'^2) \end{pmatrix},$$

which gives the result since  $u^2 \equiv (u')^2 \equiv 1 \pmod{8}$ .

(VIII). First, note that

$$\begin{pmatrix} 1 & 0 & 1 \\ -2 & 0 & u \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} u & 0 & 0 \\ 0 & u' & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -2 & 0 \\ 0 & 0 & 1 \\ 1 & u & 0 \end{pmatrix} = \begin{pmatrix} u+2 & 0 & 0 \\ 0 & 2(u^2+2u) & 0 \\ 0 & 0 & u' \end{pmatrix}.$$

Then use (VII) to see that  $\langle 2(u^2+2u) \rangle \oplus \langle u' \rangle$  is isometric to  $\langle u'+2u^2+4u \rangle \oplus \langle 2u^2+4u+4u' \rangle$ . Since  $u \equiv u' \pmod{4}$ , we have  $u'+2u^2+4u \equiv u'+2+4u \equiv 5u'+2 \equiv u'-2 \pmod{8}$  and  $2u^2+4u+4u' \equiv 2 \pmod{8} \equiv -3 \times 2 \pmod{8}$ , so that this form is isometric to  $\langle -3 \cdot 2 \rangle \oplus \langle u'-2 \rangle$ , which proves the formula for  $k = 1$ .

(IX). This uses

$$\begin{pmatrix} 1 & 1 \\ -4u' & u \end{pmatrix} \begin{pmatrix} 2u & 0 \\ 0 & 8u' \end{pmatrix} \begin{pmatrix} 1 & -4u' \\ 1 & u \end{pmatrix} = \begin{pmatrix} 2(u+4u') & 0 \\ 0 & 8uu'(u+4u') \end{pmatrix} \simeq \begin{pmatrix} 2 \cdot -3u & 0 \\ 0 & 8 \cdot -3u' \end{pmatrix},$$

where we make changes by using different representations in  $D(\mathbb{Z}_2)$  of elements on the diagonal. This completes the proof for  $k = 3$ .  $\square$

*Remark C.3.4.* The relations (V)–(IX) from Lemma C.3.3 involving different exponents give further reductions of non-homogeneous forms whose homogeneous summands are already in reduced normal form. These relations affect three consecutive exponents. Starting with the largest exponent and going down, this gives a new reduced normal form as is shown in [156, Ch.4.4]. Furthermore, as a consequence, every 2-primary quadratic torsion form and every quadratic dyadic lattice has a reduced normal form and no two such forms are isometric.

## References

- [1] ALLCOCK, D. Congruence subgroups and Enriques surface automorphisms. *J. Lond. Math. Soc. (2)* 98 (2018), 1–11. 419
- [2] ARBARELLO, E., CORNALBA, M., GRIFFITHS, P. A., AND HARRIS, J. *Geometry of algebraic curves. Vol. I*, vol. 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985. 301, 306
- [3] ARF, C. Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. *J. Reine Angew. Math* 183 (1941), 148–167. 179
- [4] ARNOL'D, V. I. Local normal forms of functions. *Invent. Math.* 35 (1976), 87–109. 337
- [5] ARNOL'D, V. I., VASIL'EV, V. A., GORYUNOV, V. V., AND LYASHKO, G. V. *Singularity Theory I*, second ed. Springer-Verlag, Berlin, 1998. 334, 335, 336, 340
- [6] ARTEBANI, M., AND SARTI, A. Non-symplectic automorphisms of order 3 on K3 surfaces. *Math. Ann.* 342, 4 (2008), 903–921. 405
- [7] ARTEBANI, M., SARTI, A., AND TAKI, S. K3 surfaces with non-symplectic automorphisms of prime order. *Math. Z.* 268, 1-2 (2011), 507–533. With an appendix by Shigeyuki Kondō. 405
- [8] ARTIN, E. *Geometric Algebra*, repr. of the orig., publ. by Interscience Publ. Inc., New York (1957) ed. Dover Publ. Inc., Mineola, New York, 2009. 165
- [9] ARTIN, M. Supersingular K3 surfaces. *Ann. Sci. École Norm. Sup. (4)* 7 (1974), 543–567 (1975). 361
- [10] ARTIN, M., GROTHENDIECK, A., VERDIER, J. L., DELIGNE, P., AND SAINT-DONAT, B., Eds. *Séminaire de géométrie algébrique du Bois-Marie 1963–1964. Théorie des topos et cohomologie étale des schémas. (SGA 4). Tome 1: Théorie des topos. Exposés I à IV. 2e éd*, vol. 269 of *Lecture Notes in Mathematics*. Springer, Cham, 1972. 357
- [11] ARTIN, M., GROTHENDIECK, A., VERDIER, J. L., DELIGNE, P., AND SAINT-DONAT, B., Eds. *Séminaire de géométrie algébrique du Bois-Marie 1963–1964. Théorie des topos et cohomologie étale des schémas (SGA 4). Tome 2. Exposes V à VIII*, vol. 270 of *Lect. Notes Math.* Springer, Cham, 1972. 357
- [12] ARTIN, M., GROTHENDIECK, A., VERDIER, J. L., DELIGNE, P., AND SAINT-DONAT, B., Eds. *Séminaire de géométrie algébrique du Bois-Marie*

- 1963–1964. *Théorie des topos et cohomologie étale des schémas (SGA 4). Tome 3. Exposés IX à XIX*, vol. 305 of *Lecture Notes in Mathematics*. Springer, Cham, 1973. 357
- [13] ASH, A., MUMFORD, D., RAPOPORT, M., AND TAI, Y.-S. *Smooth compactifications of locally symmetric varieties*, second ed. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 2010. With the collaboration of Peter Scholze. 361
- [14] BAILY, W., AND BOREL, A. Compactification of arithmetic quotients of bounded symmetric domains. *Ann. of Math. (2)* 84 (1966), 442–528. 347, 352
- [15] BARTH, W., HULEK, K., PETERS, C., AND VAN DE VEN, A. *Compact Complex Surfaces*, second enlarged ed. No. 4 in *Ergebn. der Math. 3. Folge*. Springer-Verlag, Berlin etc., 2004. 65, 68, 107, 108, 109, 110, 118, 126, 142, 342, 345, 346, 347, 348, 361, 388, 408, 415, 419, 436, 437, 438, 439, 444, 445, 446
- [16] BARTH, W., AND PETERS, C. Automorphisms of Enriques surfaces. *Invent. Math.* 73 (1983), 383–411. 4, 415, 419
- [17] BEAUVILLE, A. Sur le nombre maximum de points doubles d’une surface dans  $\mathbf{P}^3$  ( $\mu(5) = 31$ ). In *Journées de Géométrie Algébrique d’Angers, Juillet 1979/Algebraic Geometry, Angers, 1979* (Alphen aan den Rijn–Germantown, Md., 1980), Sijthoff & Noordhoff, pp. 207–215. 2, 126, 130, 142
- [18] BEAUVILLE, A. Le groupe de monodromie des familles universelles d’hypersurfaces et d’intersections complètes. In *Complex analysis and algebraic geometry (Göttingen, 1985)*, no. 1194 in *Lecture Notes in Math*. Springer-Verlag, 1986, pp. 8–18. 326, 340, 341
- [19] BEAUVILLE, A. *Complex algebraic surfaces*, second edition ed. Cambridge University Press, Cambridge, 1996. 437, 438, 441, 444, 446
- [20] BELCASTRO, S.-M. *Picard lattices of families of K3 surfaces*. ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–University of Michigan. 113
- [21] BELCASTRO, S.-M. Picard lattices of families of K3 surfaces. *Comm. Algebra* 30, 1 (2002), 61–82. 113
- [22] BERTIN, J. Réseaux de Kummer et surfaces K3. *Invent. Math.* 93 (1988), 267–284. 405
- [23] BOMBIERI, E., AND MUMFORD, D. Enriques’ classification of surfaces in char.  $p$ . II. In *Complex analysis and algebraic geometry*. 1977, pp. 23–42. 357, 358

- 
- [24] BORCHERDS, R. Automorphism groups of Lorentzian lattices. *J. Algebra* 111, 1 (1987), 133–153. 313, 314
- [25] BOREL, A., AND HARISH-CHANDRA. Arithmetic subgroups of algebraic groups. *Bull. Amer. Math. Soc.* 67 (1961), 579–583. 366
- [26] BOURBAKI, N. *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Ch. IV: Groupes de Coxeter et systèmes de Tits. Ch. V: Groupes engendrés par des réflexions. Ch. VI: systèmes de racines.*, vol. 1337 of *Actualités Scientifiques et Industrielles*. Hermann, Paris, 1968. 91, 92, 117, 310, 311, 382, 416
- [27] BRAGG, D., AND LIEBLICH, M. Perfect points on curves of genus 1 and consequences for supersingular K3 surfaces. *Compos. Math.* 158, 5 (2022), 1052–1083. 362
- [28] BRANDT, H. Zur Zahlentheorie der Quaternionen. *Jahresber. Dtsch. Math.-Ver.* 53 (1943), 23–57. 142
- [29] BRIESKORN, E. Singular elements of semi-simple algebraic groups. In *Actes du Congrès International des Mathématiciens (Nice, 1970)* (Paris, 1971), vol. 2, Gauthier-Villars, pp. 279–284. 130
- [30] BRODY, E. J. The topological classification of the lens spaces. *Ann. Math.* 71 (1960), 163–184. 117
- [31] BROWDER, W. The Kervaire invariant of framed manifolds and its generalization. *Ann. of Math. (2)* 90 (1969), 157–186. 299
- [32] BROWN, K. S. *Cohomology of groups*, vol. 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original. 431, 432
- [33] BURNS, JR., D., AND RAPOPORT, M. On the Torelli problem for kählerian K-3 surfaces. *Ann. Sci. École Norm. Sup. (4)* 8 (1975), 235–273. 349, 350, 351, 361
- [34] CARTAN, E. *The theory of spinors*. Dover Publications, Inc., New York, 1981. With a foreword by Raymond Streater, A reprint of the 1966 English translation, Dover Books on Advanced Mathematics. 169
- [35] CARTAN, H. Quotient d'un espace analytique par un groupe d'automorphismes. In *Algebraic geometry and topology*. Princeton University Press, Princeton, N. J., 1957, pp. 90–102. A symposium in honor of S. Lefschetz,. 371, 385, 398
- [36] CASSELS, J. W. S. *Rational Quadratic Forms*. L. N. M. Monographs. Academic Press Inv., London, 1978. 1, 20, 51, 52, 58, 168, 169, 206, 227, 228, 256, 257, 258, 265, 266, 267, 268, 275, 423, 424, 425

- 
- [37] CATANESE, F. Babbage's conjecture, contact of surfaces, symmetric determinantal varieties and applications. *Invent. Math.* 63, 3 (1981), 433–465. 126
- [38] CHENEVIER, G. The infinite fern and families of quaternionic modular forms lecture 6. [http://gaetan.chenevier.perso.math.cnrs.fr/coursIHP/chenevier\\_lecture6.pdf](http://gaetan.chenevier.perso.math.cnrs.fr/coursIHP/chenevier_lecture6.pdf) (2010). 141
- [39] CLIFFORD, W. Preliminary Sketch of Biquaternions. *Proc. Lond. Math. Soc.* 4 (1871/73), 381–395. 256
- [40] COBLE, A. B. *Algebraic geometry and theta functions*, vol. 10 of *American Mathematical Society Colloquium Publications*. A. M. S., Providence, R.I., 1982. Reprint of the 1929 edition. 306
- [41] COHN, H., KUMAR, A., MILLER, S. D., RADCHENKO, D., AND VIAZOVSKA, M. The sphere packing problem in dimension 24. *Ann. of Math. (2)* 185 (2017), 1017–1033. 54
- [42] CONWAY, J. H. The automorphism group of the 26-dimensional even unimodular Lorentzian lattice. *J. Algebra* 80, 1 (1983), 159–163. 314
- [43] CONWAY, J. H., AND SLOANE, N. J. A. Low-Dimensional Lattices. IV. The Mass Formula. *Proc. Royal Soc. London. Series A, Math. and Phys. Sc* 419 (1988). 55
- [44] CONWAY, J. H., AND SLOANE, N. J. A. *Sphere packings, lattices and groups (with additional contributions by E. Bannai, R. Borcherds, J. Leech, S. Norton, A. Odlyzko, R. Parker, L. Queen and B. Venkov)*, third ed., vol. 290 of *Grundlehren der Math.* Springer-Verlag, Berlin, 1999. 54, 55, 124
- [45] COSSEC, F., AND DOLGACHEV, I. On automorphisms of nodal Enriques surfaces. *Bull. Amer. Math. Soc.* 12 (1985), 247–249. 419
- [46] COSSEC, F., DOLGACHEV, I., AND LIEDTKE, C. Enriques surfaces, I. preprint, May 2020. Appendix by S. Kondō. 419
- [47] COXETER, H. S. M. *Regular polytopes*. Dover Publications, Inc., New York, 1973. 90, 91
- [48] DIEUDONNÉ, J. Pseudo-discriminant and Dickson invariant. *Pacific. J. Math.* 5 (1955), 907–910. 256, 306
- [49] DIEUDONNÉ, J. *Sur les groupes classiques*, nouveau tirage ed. Paris: Hermann, 1998. 169
- [50] DOLD, A. *Lectures on algebraic topology*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the 1972 edition. 399
- [51] DOLGACHEV, I. On automorphisms of Enriques surfaces. *Invent. Math.* (1984), 1–60. 4, 419

- 
- [52] DOLGACHEV, I. *Classical Algebraic Geometry*. Cambridge Univ. Press., Cambridge, 2012. 117, 340
- [53] DOLGACHEV, I., AND KONDO, S. Enriques surfaces, II. preprint, May 2020. 419
- [54] DONALDSON, S. K. An application of gauge theory to four-dimensional topology. *J. Differential Geom.* 18 (1983), 279–315. 65, 68
- [55] DONALDSON, S. K. Irrationality and the  $h$ -cobordism conjecture. *J. Differential Geom.* 26, 1 (1987), 141–168. 68
- [56] DURFEE, A. H. Bilinear and quadratic forms on torsion modules. *Advances in Math.* 25 (1977), 133–164. 3, 58, 161, 193, 206, 219, 242
- [57] DURFEE, A. H. Fifteen characterizations of rational double points and simple critical points. *Enseign. Math. (2)* 25, 1-2 (1979), 131–163. 108
- [58] DYE, R. H. On the Arf invariant. *J. of Algebra* 53 (1978), 36–39. 179
- [59] EBELING, W. Arithmetic monodromy groups. *Math. Ann.* 264 (1983), 241–255. 341
- [60] EBELING, W. On the monodromy groups of singularities. In *Singularities, (Arcata, Calif.), Part 1* (1983), vol. 40 of *Proc. Sympos. Pure Math.*, Amer. Math. Soc., Providence, R.I., pp. 327–336. 323, 327, 341
- [61] EBELING, W. An arithmetic characterisation of the symmetric monodromy groups of singularities. *Invent. Math.* 77 (1984), 85–99. 323, 338, 341
- [62] EBELING, W. *The monodromy groups of isolated singularities of complete intersections*, vol. 1293 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1987. 323, 341
- [63] EBELING, W. Vanishing lattices and monodromy groups of isolated complete intersection singularities. *Invent. Math.* 90 (1987), 653–668. 329, 336, 341
- [64] EBELING, W. *Lattices and Codes*. Advanced Lectures in Math. Vieweg, Braunschweig, Wiesbaden, 1994. 56, 119, 122, 123, 124, 135, 136, 141
- [65] EBELING, W., AND GUSEĬN-ZADE, S. Coxeter-Dynkin diagrams of the complete intersection singularities  $Z_9$  and  $Z_{10}$ . *Math. Z.* 218 (1995), 549–562. 341
- [66] EICHLER, M. Note zur Theorie der Kristallgitter. *Math. Ann.* 125 (1952), 51–55. 56
- [67] EICHLER, M. *Quadratische Formen und orthogonale Gruppen*, second ed. (1974) ed. Springer-Verlag, Berlin-New York, 1952. 1, 4, 323



- 
- [68] ELDUQUE, A., AND RODRIGO-ESCUADERO, A. Clifford algebras as twisted group algebras and the Arf invariant. *Adv. Appl. Clifford Algebr.* 28, 2 (2018), Paper No. 41, 15. 246
- [69] ELKIES, N. On Mordell–Weil lattices. Arbeitstagung Bonn, 1990. 113, 118
- [70] ELMAN, R., KARPENKO, N., AND MERKURJEV, A. *The algebraic and geometric theory of quadratic forms*, vol. 56 of *A. M. S. Coll. Pub.* American Math. Soc., Providence, RI., 2008. 5
- [71] ENRIQUES, F. *Le Superficie Algebriche*. Nicola Zanichelli, Bologna, 1949. 58, 446
- [72] ESSELMANN, F. Über die maximale Dimension von Lorentz-Gittern mit coendlicher Spiegelungsgruppe. *J. Number Theory* 61, 1 (1996), 103–144. 312
- [73] FREEDMAN, M. The topology of four-dimensional manifolds. *J. Diff. Geo.* 17 (1982), 357–454. 64, 68
- [74] FUJIKI, A. Finite automorphism groups of complex tori of dimension two. *Publ. Res. Inst. Math. Sci.* 24 (1988), 1–97. 405
- [75] GALLUZZI, F., LOMBARDO, G., AND PETERS, C. Automorphs of indefinite binary quadratic forms and K3-surfaces with Picard number 2. *Rendiconti Mat. Torino* 68 (2010), 57–77. 365
- [76] GARBAGNATI, A. Symplectic automorphisms on Kummer surfaces. *Geom. Dedicata* 145 (2010), 219–232. 405
- [77] GARBAGNATI, A. The dihedral group  $\mathcal{D}_5$  as a group of symplectic automorphisms on K3 surfaces. *Proc. Amer. Math. Soc.* 139, 6 (2011), 2045–2055. 405
- [78] GARBAGNATI, A. On K3 surface quotients of K3 or Abelian surfaces. *Canad. J. Math.* 69 (2017), 338–372. 406
- [79] GARBAGNATI, A., AND MONTAÑEZ, Y. P. Order 3 symplectic automorphisms on K3 surfaces. *Math. Z.* 301, 1 (2022), 225–253. 383
- [80] GARBAGNATI, A., AND SARTI, A. Symplectic automorphisms of prime order on K3 surfaces. *J. Algebra* 318, 1 (2007), 323–350. 405
- [81] GARBAGNATI, A., AND SARTI, A. Elliptic fibrations and symplectic automorphisms on K3 surfaces. *Comm. Algebra* 37, 10 (2009), 3601–3631. 405
- [82] GARBAGNATI, A., AND SARTI, A. On symplectic and non-symplectic automorphisms of K3 surfaces. *Rev. Mat. Iberoam.* 29, 1 (2013), 135–162. 405
- [83] GEEMEN, B. V., AND SARTI, A. Nikulin involutions on K3 surfaces. *Math. Z.* 255 (2007), 731–753. 393, 405

- 
- [84] GERSTEIN, L. J. *Basic quadratic forms*, vol. 60 of *Graduate Studies in Mathematics*. Amer. Math. Soc., Providence, R.I., 2008. 5
- [85] GOLAY, M. J. E. Notes on digital coding. *Proc. IRE.* 37 (1949), 657. 141
- [86] GREENBERG, M. *Lectures on algebraic topology*. W. A. Benjamin, Inc., New York-Amsterdam, 1967. 66, 100
- [87] GRIFFITHS, P. Periods of integrals on algebraic manifolds I, II. *Amer. J. Math.* 90 (1968), 568–626; 805–865. 345, 349
- [88] GRIFFITHS, P., AND HARRIS, J. *Principles of Algebraic Geometry*. Wiley-Interscience [John Wiley & Sons], New York, 1978. 301, 302, 306, 374, 434, 444
- [89] GRIFFITHS, P. A. Periods of integrals on algebraic manifolds. III. Some global differential-geometric properties of the period mapping. *Inst. Hautes Études Sci. Publ. Math.*, 38 (1970), 125–180. 349
- [90] HAMILTON, W. R. On Quaternions; or on a new System of Imaginaries in Algebra. Letter to John T. Graves. 17 October 1843, 1843. 142, 256
- [91] HAMMING, R. W. Error detecting and error correcting codes. *Bell System Tech. J.* 29 (1950), 147–160. 141
- [92] HARRIS, J. Theta-characteristics on algebraic curves. *Trans. Amer. Math. Soc.* 271, 2 (1982), 611–638. 305
- [93] HASHIMOTO, K. Finite symplectic actions on the  $K3$  lattice. *Nagoya Math. J.* 206 (2012), 99–153. 405
- [94] HATCHER, A. *Algebraic Topology*. Cambridge University Press, Cambridge, 2002. 100, 102, 103, 399, 400, 402, 403, 431
- [95] HECKMAN, G. Coxetergroups <https://www.math.ru.nl/~heckman/CoxeterGroups.pdf>. 355
- [96] HELGASON, S. *Differential Geometry and Symmetric Spaces*. Academic Press, New York, London, 1962. 254
- [97] HIRZEBRUCH, F. Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei komplexen Veränderlichen. *Math. Ann.* 126 (1953), 1–22. 118
- [98] HIRZEBRUCH, F. *Topological Methods in Algebraic Geometry*, vol. 131 of *Grundlehre der Math. Wiss.* Springer Verlag, Berlin etc., 1966. 435
- [99] HIRZEBRUCH, F., NEUMANN, W. D., AND KOH, S. S. *Differentiable manifolds and quadratic forms*. Marcel Dekker, Inc., New York, 1971. 100, 103, 117, 118, 206, 242

- 
- [100] HORIKAWA, E. On the periods of Enriques surfaces. I. *Math. Ann.* 234, 1 (1978), 73–88. 419
- [101] HORIKAWA, E. On the periods of Enriques surfaces. II. *Math. Ann.* 235, 3 (1978), 217–246. 419
- [102] HUDSON, R. *Kummer's quartic surface*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1990. With a foreword by W. Barth, Revised reprint of the 1905 original. 141
- [103] HUMPHREYS, J. E. *Introduction to Lie algebras and representation theory*. No. 9 in Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1972. 81, 91, 311
- [104] HUSEMOLLER, D. *Fibre bundles*. McGraw-Hill book company, New York etc., 1966. 256
- [105] HUYBRECHTS, D. *Complex geometry. An introduction*. Universitext. Springer-Verlag, Berlin, 2005. 434, 435, 439
- [106] HUYBRECHTS, D. *Lectures on K3 Surfaces*. Cambridge Univ. Press, Cambridge, 2016. 342, 344, 345, 347, 361, 362, 365, 405
- [107] IANO-FLETCHER, A. R. Working with weighted complete intersections. In *Explicit birational geometry of 3-folds*, vol. 281 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 2000, pp. 101–173. 112, 113
- [108] JAFFE, D. B., AND RUBERMAN, D. A sextic surface cannot have 66 nodes. *J. Algebraic Geom.* 6, 1 (1997), 151–168. 142
- [109] JAMES, D. G. On Witt's theorem for unimodular quadratic forms. *Pacific J. Math.* 26 (1968), 303–316. 291
- [110] JANSSEN, W. A. M. Skew-symmetric vanishing lattices and their monodromy groups. *Math. Ann.* 266 (1983), 17–22. 341
- [111] JARVIS, F. *Algebraic Number Theory*. Springer Cham, Heidelberg, 2014. 131, 134
- [112] JONES, B. W. *The Arithmetic Theory of Quadratic Forms*, vol. 10 of *Carcus Monograph Series*. The Math. Assoc. of America, Buffalo, N. Y., 1950. 1
- [113] JONES, G., AND JONES, J. *Elementary Number Theory*. Undergraduate Math. Series. Springer Verlag, London, 1998. 421
- [114] JUNG, H. W. E. Darstellung der Funktionen eines algebraischen Körpers zweier unabhängigen Veränderlichen  $x, y$  in der Umgebung einer Stelle  $x = a, y = b$ . *J. Reine Angew. Math.* 133 (1908), 289–314. 118
- [115] KALKER, A. *Cubic fourfolds with fifteen ordinary double points*. PhD thesis, Rijksuniversiteit Leiden, 1986. 142

- 
- [116] KNEBUSCH, M. Grothendieck- und Witttringe von nichtausgearteten symmetrischen Bilinearformen. *S.-B. Heidelb. Akad. Wiss. Math.-Natur. Kl. 1969/70* (1969/1970), 93–157. 161, 169
- [117] KNESER, M. Zur Theorie der Kristallgitter. *Math. Ann.* 127 (1954), 105–106. 56
- [118] KNESER, M. Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen. *Arch. Math.* 7 (1956), 323–332. 58
- [119] KNESER, M. Klassenzahlen definiter quadratischer Formen. *Arch. Math.* 8 (1957), 241–250. 54, 122, 392
- [120] KNESER, M. Normalteiler ganzzahliger Spingruppen. *J. Reine Angew. Math.* 311/312 (1979), 191–214. 315
- [121] KNESER, M. Erzeugung ganzzahliger orthogonaler Gruppen durch Spiegelungen. *Math. Ann.* 255 (1981), 453–462. 315, 316, 323
- [122] KNESER, M. *Quadratische Formen, Revised and edited in collaboration with R. Scharlau*. Springer-Verlag, Berlin, 2002. 19, 21, 58, 161, 165, 166, 169, 179, 275, 292, 300, 306, 423, 424, 447
- [123] KNUS, M.-A. *Quadratic and Hermitian forms over rings*, vol. 294 of *Grundle. der Math. Wissenschaften*. Springer-Verlag, Berlin, 1991. 5
- [124] KODAIRA, K. On compact complex analytic surfaces. I. *Ann. of Math. (2)* 71 (1960), 111–152. 118, 348
- [125] KODAIRA, K. On compact analytic surfaces. II, III. *Ann. of Math. (2)* 77 (1963), 563–626; *ibid.* 78 (1963), 1–40. 118
- [126] KONDŌ, S. Enriques surfaces with finite automorphism groups. *Japan. J. Math. (N.S.)* 12 (1986), 191–282. 419
- [127] KONDŌ, S. Automorphisms of algebraic K3 surfaces which act trivially on Picard groups. *J. Math. Soc. Japan* 44, 1 (1992), 75–98. 367
- [128] KONDŌ, S. Niemeier lattices, Mathieu groups, and finite groups of symplectic automorphisms of K3 surfaces. *Duke Math. J.* 92 (1998), 593–603. 373, 405
- [129] KONDŌ, S. *K3 surfaces*, vol. 32 of *EMS Tracts in Mathematics*. EMS Publishing House, Berlin, 2020. 362, 419
- [130] KULIKOV, V. S. Degenerations of K3 surfaces and Enriques surfaces. *Izv. Akad. Nauk SSSR Ser. Mat.* 41 (1977), 1008–1042, 1199. 361
- [131] KULIKOV, V. S. Surjectivity of the period mapping for K3 surfaces. *Uspehi Mat. Nauk* 32, 257–258 (1977). 361
- [132] LAM, T. Y. *The algebraic theory of quadratic forms*. Math. Lect. Note Series. W. A. Benjamin, Inc., Reading, Mass, 1973. 4

- 
- [133] LAM, T. Y. *Introduction to quadratic forms over fields*, vol. 67 of *Graduate Studies in Math.* Amer. Math. Soc., Providence, R.I., 2005. 4
- [134] LAMOTKE, K. The topology of complex projective varieties after S. Lefschetz. *Topology* 20 (1981), 15–51. 333, 336, 339
- [135] LANG, S. *Introduction to differentiable manifolds*, second ed. Universitext. Springer-Verlag, New York, 2002. 401
- [136] LATIMER, C. G. The classes of integral sets in a quaternion algebra. *Duke Math. J.* 3 (1937), 237–247. 142
- [137] LAWSON, H. B., AND MICHELSON, M.-L. *Spin Geometry*. Princeton Univ. Press, Princeton, 1989. 245, 247, 250, 251, 254, 256
- [138] LEFSCHETZ, S. *L'Analysis Situs et la Géométrie Algébrique*. Gauthier-Villars, Paris, 1924. 338
- [139] LIEDTKE, C. Lectures on Supersingular K3 Surfaces and the Crystalline Torelli Theorem. In *K3 Surfaces and Their Moduli*, vol. 315 of *Progress in Mathematics*. Birkhäuser, 2016, pp. 171–235. 362
- [140] LINT, J. H. v. *Introduction to Coding Theory*, second edition ed., vol. 86 of *GTM*. Springer-Verlag, Berlin etc., 92. 119, 124
- [141] LIPSCHITZ, R. Principes d'un calcul algébrique qui contient comme espèces particulières le calcul des quantités imaginaires et des quaternions. *Bull. Sci. Math., II. Sér.* 11 (1887), 115–120. 256
- [142] LOOIJENGA, E. *Isolated Singular Points on Complete Intersections*, vol. 77 of *London Math. Soc. Lecture Note Series*. Cambridge Univ. Press., Cambridge, 1984. 334, 336
- [143] LOOIJENGA, E. New compactifications of locally symmetric varieties. In *Proceedings of the 1984 Vancouver conference in algebraic geometry* (1986), vol. 6 of *CMS Conf. Proc.*, Amer. Math. Soc., Providence, RI, pp. 341–364. 352, 361
- [144] LOOIJENGA, E., AND PETERS, C. Torelli theorems for Kähler K3-surfaces. *Compos. Math.* 42 (1981), 145–186. 321
- [145] LORENZ, F. *Quadratische Formen über Körpern*. Lecture Notes in Mathematics, Vol. 130. Springer-Verlag, Berlin-New York, 1970. 169
- [146] MACHIDA, N., AND OGUIISO, K. On K3 surfaces admitting finite non-symplectic group actions. *J. Math. Sci. Univ. Tokyo* 5, 2 (1998), 273–297. 367
- [147] MASSUYEAU, G. An introduction to the abelian Reidemeister torsion of three-dimensional manifolds. *Ann. Math. Blaise Pascal* 18:1 18 (2011), 61–140. 117

- 
- [148] MILNE, J. S. *Étale cohomology*. Princeton Mathematical Series, No. 33. Princeton University Press, Princeton, N.J., 1980. 357
- [149] MILNOR, J. Eigenvalues of the Laplace operator on certain manifolds. *Proc. Nat. Acad. Sci. U.S.A.* 51 (1964), 542. 55, 56
- [150] MILNOR, J. *Lectures on the h-cobordism theorem*. Notes by L. Siebenmann and J. Sondow. Princeton University Press, Princeton, N.J., 1965. 64
- [151] MILNOR, J., AND HUSEMOLLER, D. *Symmetric Bilinear Forms*, vol. 73 of *Ergebn. der Math. und ihrer Grenzgebiete. 3. Folge*. Springer Verlag, Berlin, 1973. 1, 2, 52, 53, 68, 161, 168, 169, 453
- [152] MILNOR, J., AND STASHEFF, J. *Characteristic Classes*, vol. 76 of *Ann. of Math. Studies*. Princeton Univ. Press, Princeton, N.J., 1974. 54, 66
- [153] MINKOWSKI, H. Untersuchungen über quadratische Formen I. Bestimmung der Anzahl verschiedener Formen, welche ein gegebenes Genus enthält. *Acta Math.* 7 (1885), 201–258. 54
- [154] MIRANDA, R., AND MORRISON, D. R. The number of embeddings of integral quadratic forms I. *Proc. Japan Acad. Ser. A Math. Sci.* 61 (1985), 317–320. v
- [155] MIRANDA, R., AND MORRISON, D. R. The number of embeddings of integral quadratic forms II. *Proc. Japan Acad. Ser. A Math. Sci.* 62 (1986), 29–32. v
- [156] MIRANDA, R., AND MORRISON, D. R. Embeddings of Integral Quadratic Forms. Preprint. <http://web.math.ucsb.edu/~drm/manuscripts/eiqf.pdf>, 2009. v, 23, 45, 58, 193, 206, 216, 272, 275, 306, 452, 456, 460
- [157] MOISE, E. E. Affine structures in 3-manifolds. V. The triangulation theorem and Hauptvermutung. *Ann. of Math. (2)* 56 (1952), 96–114. 117
- [158] MORRISON, D. R. On K3 surfaces with large Picard number. *Invent. Math.* 75 (1984), 105–121. 4, 142, 348, 361, 395, 396, 405
- [159] MUKAI, S. Finite groups of automorphisms of K3 surfaces and the Mathieu group. *Invent. Math.* 94 (1988), 183–221. 372, 405
- [160] MUKAI, S., AND NAMIKAWA, Y. Automorphisms of Enriques surfaces which act trivially on the cohomology groups. *Invent. Math.* 77 (1984), 383–397. 414
- [161] MUKAI, S., AND OHASHI, H. Finite groups of automorphisms of Enriques surfaces and the Mathieu group  $M_{12}$ . <https://arxiv.org/pdf/1410.7535.pdf>, 2014. 414
- [162] MULLER, D. E. Application of Boolean algebra to switching circuit design and to error detection. *Trans. I.R.E. EC-3* 3 (1954), 6–12. 141

- 
- [163] MUMFORD, D. The topology of normal singularities of an algebraic surface and a criterion for simplicity. *Publications mathématiques de l'I.H.É.S.* 9 (1961), 5–22. 107
- [164] MUMFORD, D. Theta characteristics of an algebraic curve. *Ann. Sci. École Norm. Sup. (4)* 4 (1971), 181–192. 305, 306
- [165] NAMIKAWA, Y. Surjectivity of period map for K3 surfaces. In *Surjectivity of period map for K3 surfaces*, vol. 39 of *Progr. Math.* Birkhäuser Boston, Boston, MA, 1983. 361
- [166] NAMIKAWA, Y. Periods of Enriques surfaces. *Math. Ann.* 270, 2 (1985), 201–222. 419
- [167] NIEMEIER, H.-V. Definite quadratische Formen der Dimension 24 und Diskriminante 1. *J. Number Theory* 5 (1973), 142–178. 55, 58
- [168] NIKULIN, V. V. Kummer surfaces. *Izv. Akad. Nauk SSSR Ser. Mat.* 39, 2 (1975), 278–293, 471. v, 2, 142, 388, 405
- [169] NIKULIN, V. V. Finite groups of automorphisms of Kählerian K3 surfaces. (Russian). *Trudy Moskov. Mat. Obshch.* 38 (1979), 75–137. v, 142, 275, 351, 375, 376, 379, 404, 405
- [170] NIKULIN, V. V. Quotient-groups of groups of automorphisms of hyperbolic forms of subgroups generated by 2-reflections. (russian). *Dokl. Akad. Nauk SSSR* 248, 6 (1979), 1307–1309. v, 323, 365
- [171] NIKULIN, V. V. Integral symmetric bilinear forms and some of their geometric applications. *Math. USSR Izv. Integral symmetric bilinear forms and some of their geometric* 49, 4 (1980), 103–167. v, 1, 4, 30, 47, 48, 58, 216, 229, 232, 237, 240, 242, 280, 291
- [172] NIKULIN, V. V. On quotient groups of the automorphism groups of hyperbolic forms by the subgroups generated by 2-reflections. algebraic-geometric applications. In *Current problems in mathematics*, vol. 18. Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1981, pp. 3–114. v, 312, 313, 314, 320, 323, 365, 405, 415, 419
- [173] NIKULIN, V. V. Description of automorphism groups of Enriques surfaces. (Russian). *Dokl. Akad. Nauk SSSR* 227 (1984), 1324–1327. v, 418, 419
- [174] OGUSO, K. On Jacobian fibrations on the Kummer surfaces of the product of nonisogenous elliptic curves. *J. Math. Soc. Japan* 41, 4 (1989), 651–680. 384
- [175] OGUS, A. Supersingular K3 crystals. In *Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II* (1979), vol. 64 of *Astérisque*, Soc. Math. France, Paris, pp. 3–86. 362

- 
- [176] OGUS, A. A crystalline Torelli theorem for supersingular K3 surfaces. In *Arithmetic and geometry Vol. II* (Boston, 1983), vol. 36 of *Progress in Math.*, Birkhäuser Boston. 361, 362
- [177] O'MEARA, O. T. *Introduction to Quadratic Forms*, second edition (1971); reprint (2000) ed. Grundle. der math. Wissensch. Springer Verlag, Berlin etc., 1971. 1, 142, 165
- [178] ÖNSIPER, H., AND SERTÖZ, S. Generalized Shioda-Inose structures on K3 surfaces. *Manuscripta Math.* 98, 4 (1999), 491–495. 406
- [179] OVSIENKO, V. Real Clifford Algebras and Quadratic Forms over  $\mathbb{F}_2$ : Two Old Problems Become One. *The Mathematical Intelligencer* 38, 3 (June 2016), 1–5. 246
- [180] PALL, G. On generalized quaternions. *Trans. Am. Math. Soc.* 59 (1946), 280–280. 142
- [181] PEARLSTEIN, G., AND PETERS, C. A remarkable class of elliptic surfaces of amplitude 1 in weighted projective space. <https://arxiv.org/pdf/2302.09358.pdf> (02 2023). 113
- [182] PERSSON, U., AND PINKHAM, H. Degeneration of surfaces with trivial canonical bundle. *Ann. of Math. (2)* 113 (1981), 45–66. 361
- [183] PETERS, C. Introduction to the theory of compact complex surfaces. In *Differential geometry, global analysis, and topology (Halifax, NS, 1990)*, vol. 12 of *CMS Conf. Proc.* Amer. Math. Soc., Providence, RI, 1991, pp. 129–156. 68
- [184] PETERS, C. On complex surfaces with definite intersection form. *New York Journal of Mathematics* 27 (2021), 840–847. 68
- [185] PETERS, C. On the maximal number of du Val singularities for a K3 surface. *Geometriae Dedicata* (2021). 142, 388
- [186] PETERS, C., AND STEENBRINK, J. *Mixed Hodge Theory*, vol. 52 of *Ergebn. der Math.* Springer Verlag, Berlin, 2008. 387, 396
- [187] PETERS, C., AND STERK, H. On K3 double planes covering Enriques surfaces. *Math. Ann.* 371 (2018), 1–11. 418, 419
- [188] PFISTER, A. *Quadratic forms with applications to algebraic geometry and topology*, vol. 217 of *London Math. Soc. Lecture Note Series.* Cambr. Univ. Press, Cambridge, 1995. 5
- [189] PJATECKIĀ-ŠAPIRO, I. I., AND ŠAFAREVIČ, I. R. Torelli's theorem for algebraic surfaces of type K3. *Izv. Akad. Nauk SSSR Ser. Mat.* 35 (1971), 530–572. 361, 365



- 
- [190] REED, I. S. A class of multiple-error-correcting codes and the decoding scheme. *Trans. IRE. EM 4 4* (1954), 38–49. 141
- [191] REIDEMEISTER, K. Homotopieringe und Linsenräume. *Abh. Math. Semin. Hamb. Univ 11* (1935), 102–109. 117
- [192] REINER, I. Integral representations of cyclic groups of prime order. *Proc. Amer. Math. Soc. 8* (1957), 142–146. 384
- [193] REYE, T. Die Geometrie der Lage. Erste Abteilung. 3<sup>te</sup> Auflage. Leipzig. Baumgärtner. XIV u. 248 S. (1886)., 1886. 419
- [194] RIEMANN, B. Theorie der Abel’schen Functionen. *J. Reine Angew. Math. 54* (1857), 115–155. 306
- [195] RIEMANN, B. Ueber das Verschwinden der  $\vartheta$ -Functionen. *J. Reine Angew. Math. 65* (1866), 161–172. 306
- [196] ROHLIN, V. A. New results in the theory of four-dimensional manifolds. *Doklady Akad. Nauk SSSR (N.S.) 84* (1952), 221–224. 66
- [197] ROULLEAU, X. On generalized Kummer surfaces and the orbifold Bogomolov-Miyaoka-Yau inequality. Preprint <https://arxiv.org/abs/1708.09358> [math.AG], 2017. 406
- [198] ROULLEAU, X. An atlas of K3 surfaces with finite automorphism group. *Épjournal Géom. Algébrique 6* (2022), Art. 19, 95. 365
- [199] RUDAKOV, A. N., AND ŠAFAREVIČ, I. R. Supersingular K3 surfaces over fields of characteristic 2. *Izv. Akad. Nauk SSSR Ser. Mat. 42*, 2 (1978), 848–869. 4, 359, 360, 361, 362
- [200] SCATTONE, F. On the compactification of moduli spaces for algebraic K3 surfaces. *Mem. Amer. Math. Soc. 70*, 374 (1987), x+86. 361
- [201] SCHARLAU, W. *Quadratic and Hermitian forms*, vol. 270 of *Grundl. der math. Wissensch.* Springer Verlag, Berlin etc., 1985. 5, 169
- [202] SCHÜTT, M., AND SHIODA, T. *Mordell–Weil Lattices*. No. 70 in *Ergebn. der Math. 3. Folge*. Springer Nature, Singapore, 2019. 54, 112, 113, 114, 115, 116, 117, 118
- [203] SEIFERT, H., AND THRELFALL, W. *Lehrbuch der Topologie*. Chelsea publishing company, New York, 1934. 58, 101, 103, 117
- [204] SERRE, J.-P. *A course in arithmetic*. Springer Verlag, Berlin etc., 1973. 2, 54, 55, 56, 70, 77, 78, 227, 232, 422, 423, 424, 425, 426, 427, 428
- [205] SERRE, J.-P. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. 375

- 
- [206] SHAH, J. A complete moduli space for  $K3$  surfaces of degree 2. *Ann. of Math. (2)* 112, 3 (1980), 485–510. 352
- [207] SHIMADA, I. Rational double points on supersingular  $K3$  surfaces. *Math. Comp.* 73, 248 (2004), 1989–2017. 142
- [208] SHIMADA, I. Supersingular  $K3$  surfaces in characteristic 2 as double covers of a projective plane. *Asian J. Math.* 8, 3 (2004), 531–586. 142
- [209] SHIODA, T. An example of unirational surfaces in characteristic  $p$ . *Math. Ann.* 211 (1974), 233–236. 361
- [210] SHIODA, T. On the Mordell–Weil lattices. *Comment. Math. Univ. St. Pauli* 39 (1990), 211–240. 113, 114, 118
- [211] SHIODA, T., AND INOSE, H. On singular  $K3$  surfaces. In *Complex analysis and algebraic geometry* (Tokyo, 1977), Iwanami Shoten, pp. 119–136. 395, 397, 405
- [212] SIEGEL, C. L. Über Die Analytische Theorie Der Quadratischen Formen I. *Ann. of Math. (2)* 36 (1935), 527–606. 1, 54
- [213] SIEGEL, C. L. Über Die Analytische Theorie Der Quadratischen Formen II. *Ann. of Math. (2)* 37 (1936), 230–263. 1
- [214] SIEGEL, C. L. Über Die Analytische Theorie Der Quadratischen Formen III. *Ann. of Math. (2)* 38 (1937), 212–291. 1
- [215] SIEGEL, C. L. *Gesammelte Abhandlungen. I.* Springer Collected Works in Mathematics. Springer, Heidelberg, 2015. Edited by Komaravolu Chandrasekharan and Hans Maaß, Reprint of the 1966 edition [ MR0197270]. 4
- [216] SIEGEL, C. L. *Gesammelte Abhandlungen. II.* Springer Collected Works in Mathematics. Springer, Heidelberg, 2015. Edited by Komaravolu Chandrasekharan and Hans Maaß, Reprint of the 1966 edition [ MR0197270]. 4
- [217] SIEGEL, C. L. *Gesammelte Abhandlungen. III.* Springer Collected Works in Mathematics. Springer, Heidelberg, 2015. Edited by Komaravolu Chandrasekharan and Hans Maaß, Reprint of the 1966 edition [ MR0197270], Original publication incorrectly given as 1979 edition on the title page. 4
- [218] SIEGEL, C. L. *Gesammelte Abhandlungen. IV.* Springer Collected Works in Mathematics. Springer, Heidelberg, 2015. Edited by Komaravolu Chandrasekharan and Hans Maaß, Reprint of the 1979 edition [ MR0543842], Original publication incorrectly given as 1966 edition on the title page. 4
- [219] SPANIER, E. H. *Algebraic topology*. Springer-Verlag, New York, 1995. Corrected reprint of the 1966 original. 401
- [220] STERK, H. Finiteness results for algebraic  $K3$  surfaces. *Math. Z.* 189 (1985), 507–513. 366, 405

- [221] SYLVESTER, J. A demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real orthogonal substitutions to the form of a sum of positive and negative squares. *Philos. Mag. IV* (1852), 138–142. 179
- [222] TAUSSKY, O. The discriminant matrices of an algebraic number field. *J. London Math. Soc. 1* (1968), 152–154. 132
- [223] TAYLOR, D. E. *The geometry of the classical groups*, vol. 9 of *Sigma Ser. Pure Math.* Berlin: Heldermann Verlag, 1992. 298, 428
- [224] THURSTON, W. P. *Three-dimensional geometry and topology. Vol. 1*, vol. 35 of *Princeton Mathematical Series*. Princeton Univ. Press, Princeton, N.J., 1997. 118
- [225] TIETZE, H. Über die topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten. *Monatshefte f. Math. und Phys. 19* (1908), 1–118. 117
- [226] TODOROV, A. N. Applications of the Kähler-Einstein-Calabi-Yau metric to moduli of K3 surfaces. *Invent. Math. 61* (1980), 251–265. 361
- [227] TOGLIATTI, E. G. Una notevole superficie de 5<sup>o</sup> ordine con soli punti doppi isolati. *Vierteljschr. Naturforsch. Ges. Zürich. Beiblatt (Festschrift Rudolf Fueter) 85* (1940), 127–132. 131
- [228] UENO, K. A remark on automorphisms of Enriques surfaces. *J. Fac. Sci. Univ. Tokyo Sect. I A Math 23* (1976), 149–165. 385
- [229] VAL, P. D. On isolated singularities of surfaces which do not affect the conditions of adjunction (part I.). *Math. Proc. Cambridge Phil. Soc. 30* (1934), 453–459. 118
- [230] VAL, P. D. On isolated singularities of surfaces which do not affect the conditions of adjunction (part II.). *Math. Proc. Cambridge Phil. Soc. 30* (1934), 460–465. 118
- [231] VAL, P. D. On isolated singularities of surfaces which do not affect the conditions of adjunction (part III.). *Math. Proc. Cambridge Phil. Soc. 30* (1934), 483–491. 118
- [232] VAN KAMPEN, E. R. Invariants derived from looping coefficients. *Am. J. of Math. 60*, 3 (1938), 595–610. 193, 339
- [233] VIAZOVSKA, M. The sphere packing problem in dimension 8. *Ann. of Math. (2) 185* (2017), 991–1015. 54
- [234] VIGNÉRAS, M.-F. *Arithmétique des algèbres de quaternions*, vol. 800 of *Lecture Notes in Mathematics*. Springer Verlag, Berlin etc., 1980. 138, 142
- [235] VINBERG, È. B. The groups of units of certain quadratic forms. *Mat. Sb. (N.S.) 87(129)* (1972), 18–36. 355

- 
- [236] VINBERG, È. B. Some arithmetical discrete groups in Lobačevskiĭ spaces. In *Discrete subgroups of Lie groups and applications to moduli (Internat. Colloq., Bombay, 1973)*, Tata Inst. Fundam. Res. Stud. Math., No. 7. Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press, Bombay, 1975, pp. 323–348. 354
- [237] VINBERG, È. B. Discrete reflection groups in Lobachevsky spaces. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)* (1984), PWN, Warsaw, pp. 593–601. 323
- [238] VINBERG, È. B. Hyperbolic groups of reflections. *Uspekhi Mat. Nauk* 40, 1(241) (1985), 29–66, 255. 323
- [239] VINBERG, È. B., AND KAPLINSKAJA, I. M. The groups  $O_{18,1}(\mathbb{Z})$  and  $O_{19,1}(\mathbb{Z})$ . *Dokl. Akad. Nauk SSSR* 238, 6 (1978), 1273–1275. 312, 323
- [240] VINBERG, È. B., AND SHVARTSMAN, O. V. Discrete groups of motions of spaces of constant curvature. In *Geometry, II*, vol. 29 of *Encyclopaedia Math. Sci.* Springer, Berlin, 1993, pp. 139–248. 312, 323
- [241] VOIGHT, J. M. *Quaternion algebras*, vol. 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] ©2021. 142
- [242] WAERDEN, B. L. v. D. *Algebra. Vol. 2*. Frederick Ungar Publishing Co, New York, 1970. 420
- [243] WAHL, J. Nodes on sextic hypersurfaces in  $\mathbb{P}^3$ . *J. Differential Geom.* 48, 3 (1998), 439–444. 142
- [244] WALL, C. T. C. On the orthogonal groups of unimodular quadratic forms. *Math. Ann.* 147 (1962), 328–338. 291
- [245] WALL, C. T. C. Quadratic forms on finite groups and related topics. *Topology* 2 (1963), 281–298. 2, 45, 117, 193, 242
- [246] WATSON, G. L. *Integral quadratic forms*, vol. 51 of *Cambridge Tracts in Math. and Math. Physics*. Cambr. Univ. Press, Cambridge, 1960. 1
- [247] WEIBEL, C. A. *An introduction to homological algebra*, vol. 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994. 431
- [248] WEIL, A. *Oeuvres scientifiques/collected papers. II. 1951–1964*. Springer Collected Works in Mathematics. Springer, Heidelberg, 2014. Reprint of the 2009 [MR2883739] and 1979 [MR0537935] editions. 58, 256
- [249] WENDLAND, K. Consistency of orbifold conformal field theories on K3. *Adv. Theor. Math. Phys* 5 (2001), 429–456. 405
- [250] WHITEHEAD, J. H. C. On incidence matrices, nuclei and homotopy type. *Ann. Math.* 42 (1941), 1197–1237. 99

- [251] WITT, E. Theorie der quadratischen Formen in beliebigen Körpern. *J. Reine Angew. Math.* 176 (1937), 31–44. 1, 169
- [252] WITT, E. *Collected papers. Gesammelte Abhandlungen.* Springer-Verlag, Berlin, 1998. With an essay by Günter Harder on Witt vectors, Edited and with a preface in English and German by Ina Kersten. 4
- [253] XIAO, G. Non-symplectic involutions of a K3 surface. <https://arxiv.org/abs/alg-geom/9512007>, 1995. 367
- [254] ZARISKI, O. A theorem on the Poincaré group of an algebraic hypersurface. *Ann. of Math. (2)* 38, 1 (1937), 131–141. 339
- [255] ZHANG, D.-Q. *Automorphisms of K3 surfaces*, vol. 39 of *AMS/IP Stud. Adv. Math.* Amer. Math. Soc., Providence, R.I., 2007, pp. 379–392. 367

# Index

- 1-curve, 443
- $\mu$ -invariant, 102
- $\sigma$ -invariant, 60
- 11/8 conjecture, 67
  
- Abel's theorem, 303
- Abel–Jacobi map, 303
- adjoint map, 149
- adjunction formula, 437
- alternating form, 144, 428
- ample cone, 344
- anisotropic
  - (totally) — submodule, 146
- Arf invariant, 172, 247, 296, 305
  - democratic interpretation, 299
- Artin invariant, 358
- Artin–Schreier
  - map, 172, 177
  - polynomial, 177
  
- binary form, 17, 153, 159, 177, 197
- bitangents of a smooth quartic curve, 304
  
- canonical bundle formula, 109
- Cartan–Dieudonné theorem
  - on reflections, 164
- Cartan–Leray spectral sequences, 432
- characteristic element, 60
- class number of a genus, 51
- Clifford algebra, 245
  - real —, 246
- Clifford group, 249
- code
  - doubly even —, 122
  - Golay —, 123, 135
  - Hamming —, 122
  - isotropic —, 120
  - Reed–Muller —, 124
  - self-dual —, 120
  - weight, 119
- compactification
  - SBB-compactification, 352
- cone
  - ample —, 344
  - Kähler, 343
  - light —, 295
  - positive, 343
- connected sum, 64
- contiguous chain of orthonormal bases, 71
- continued fraction, 93
- correlation morphism, 28, 149
- Coxeter group/graph, 89
- cyclic
  - group actions, 107
- cyclotomic field, 134
  
- deformation
  - miniversal —, 334
- Dickson invariant, 161, 297
- discriminant
  - of ring of integers, 132
  - form, 30
  - group, 28
  - locus, 334
  - of a lattice, 17, 150
  - of a symmetric bilinear form, 15
  - reduced —, 183
- doubly even code, 122
- Du Val singularity, 108
- dual graph, 107
- Dynkin diagram, 24, 79, 90
  - generalized —, 324
  - of type *A-D-E* and semi-definite extensions, 82
  - of type  $B_n$ , 91
  - of type  $\tilde{B}_n, \tilde{C}_n$ , 91
  - of type  $E_8$ , 24
  - of type  $F_4$ , 90
  - of type  $\tilde{F}_4, \tilde{G}_2$ , 92
  - of type  $G_2$ , 90
  - of type  $T_{p,q,r}$ , 80, 313, 329

- of type  $T_{p,q,r}^1$ , 329  
 Eichler–Siegel transformation, 317, 416  
 Eisenstein–Hermite theorem, 48  
 elementary divisors, 31, 420  
 embeddings  
   equivalent —, 166, 279  
 Enriques  
   involution, 386  
   lattice, 57, 81  
   lattice — involution, 407  
   surface, 441  
 equivalence  
   of forms, 25, 145  
   of lattices, 25, 259  
   proper — of lattices, 259  
 euclidean algorithm, 93  
 even form, 18, 144  
 exceptional divisor, 107  
 fibration  
   elliptic —, 109  
   relatively minimal —, 109  
   surface —, 109  
 form  
   semi-unimodular —, 151, 176  
 Freedman’s theorem, 64  
 genus  
   class number, 51  
 genus (of a lattice), 43, 259  
   characterization, 215  
   existence, 229  
   invariant, 216, 238  
 genus (of a variety)  
   — formula for curves, 437  
   geometric —, 434  
 Gram matrix, 14, 150  
 graph  
    $\Gamma_{\mathbf{a}}$ , 92  
   dual —, 107  
   lattice associated to —, 23  
 group (co)homology, 431  
 group action, 399  
 Gysin  
   homomorphism, 387, 399  
   sequence, 401  
 Hamilton quaternions, 136, 246, 249  
 Hasse  
   invariant, 69, 205  
   principle, 47, 69, 77  
 Hasse–Minkowski theorem, 77  
 height pairing, 114  
 Hensel’s lemma, 426  
 Hesse pencil, 115  
 Hilbert  
   product formula, 428  
   symbol, 426  
 Hirzebruch surface, 438  
 Hodge  
   decomposition, 434  
   index theorem for surfaces, 436  
   numbers, 434  
   structure (weight 2), 442  
   structure of K3 type, 443  
 homotopy type, 99  
 hyperbolic  
    $R$ -module, 155  
   plane, 70, 152, 153  
   space, 295  
 hyperbolic plane, 17  
 hyperplane reflection, 26, 158  
 indecomposable lattice, 54, 56  
 index  
   modulo 16, 102  
   modulo 8, 48, 222  
   of a sublattice, 18  
   of a lattice, 23  
   of an inner product space, 171  
 index theorem, 435  
   Hodge — for surfaces, 436  
 inner product space, 15, 151  
 integral  
   (symmetric) lattice, 17  
   quadratic form, 19  
   quadratic lattice, 19  
 intersection form, 64  
 invariant factors, 420  
 involution  
   Enriques —, 386

- Kummer —, 388  
 Nikulin —, 129, 386, 391  
 type of —, 385  
 irregularity, 434  
 isometric  
   embedding, 25  
   forms, 145  
   vector spaces, 17  
 isometry  
   — of lattices, 25  
   group, 157  
   of  $R$ -modules, 145  
   of vector spaces, 17  
 isospectral tori, 56  
 isotropic  
   subspace, 20  
   totally —, 146  
   vector, 20, 73  
 isotropic torsion subgroup, 31  
  
 Jacobi inversion, 303  
 jacobian of a curve, 301  
 Jordan splitting, 200  
  
 $K$ -generic period point, 367  
 K3 lattice, 57  
 K3 surface, 438  
    $S$ -marking, 347  
   marking, 344  
   strong marking, 350  
 K3 type  
   Hodge structure of —, 443  
 Kähler  
   metric/form, 434  
 Kodaira dimension, 445  
 Kodaira's list of singular elliptic fibers,  
   110  
 Kummer  
   involution, 388  
   lattice, 128, 388  
   surface, 389, 439  
 Kuranishi family (of K3 surfaces), 349  
  
 lattice  
   2-elementary —, 36, 274  
    $R$ - —, 144  
    $\Gamma_n$ , 24  
    $\Gamma_{16}$  and  $E_8 \oplus E_8$ , 216  
    $p$ -elementary —, 35, 120, 272  
   equivalence, 259  
   overlattice, 276  
   Borcherd —, 314  
   dual —, 28  
   dyadic —, 46  
   Enriques —, 57, 81  
   hexagonal —, 115  
   hyperbolic —, 22  
   indecomposable —, 54, 56  
   integral —, 17, 144  
   K3 —, 57  
   Kummer —, 128  
   Leech —, 54, 55, 123, 314  
   Lorentz —, 84, 313  
   Lorentzian —, 312, 313  
   Milnor —, 333  
   Mordell–Weil —, 114  
   Néron–Severi —, 437  
   neighbour —, 34  
   Niemeier —, 55, 124, 135, 314, 372  
   Nikulin —, 129  
   non-degenerate  $p$ -adic —, 42  
   non-degenerate —, 18, 20  
   overlattice, 37  
    $p$ -adic —, 42, 144  
   Picard —, 437  
   primitive —, 18  
   reflective —, 310  
   root —, 24, 79, 88  
   transcendental —, 437  
   trivial – (of elliptic fibration), 111  
   unimodular  $p$ -adic —, 42  
   unimodular —, 18  
   vanishing —, 325  
   length of torsion module, 421  
   lens space, 99  
   linking pairing, 101  
   localization of an integral lattice, 44, 217  
  
 Mathieu group, 123, 372  
 Meyer's theorem, 77  
 Milgram's theorem, 453  
 Milnor



- fiber/fibration, 333
  - number, 333
- mod  $n$  reduction map, 309
- module
  - free —, 420
  - torsion —, 420
- moduli space
  - for Enriques surfaces, 408
  - for K3 surfaces, 347
- monodromy group
  - associated to a singularity, 336
  - of singularity, 333
- Mordell–Weil
  - group/lattice, 114
  - rank, 114, 117
- Néron–Severi group/lattice, 437
- Nikulin
  - involution, 129, 375, 377, 386, 391
  - lattice, 129, 375, 394
- nodal
  - class, 343
  - curve, 126, 343
  - type of an Enriques surface, 413
- non-degenerate
  - symmetric form, 146
- norm form, 132, 153, 159, 177
- normal form
  - of a 2-primary torsion form, 211
  - of a  $p$ -adic lattice, 207
  - of a dyadic lattice, 211
  - reduced homogeneous —, 458
- null-space, 20, 146
- number field, 131
- odd form, 18, 144
- ordered basis of torsion module, 181
- orientation
  - $q^\pm$ - —, 294
  - of a vector space, 293
- orthogonal
  - complement, 16, 20, 146
  - group, 157
  - reduced — group, 253
- overlattice, 37, 276
- $p$ -adic
  - lattice, 194
    - homogeneous — of exponent  $k$ , 200
    - Jordan splitting, 200
    - normal form, 207
  - topology, 423
  - valuation, 422
- $p$ -elementary lattice, 35, 120, 272
- $p$ -primary torsion module, 420
- parity (of a lattice), 18
- period domain, 442
- period map for K3 surfaces, 345
- Picard
  - group, 301
  - lattice, 437
  - number, 346, 437
  - variety, 301
- pin group, 253
- polar form, 14, 144
- polarization
  - of K3-surface, 347
- polarized Hodge structure (weight 2), 443
- primitive
  - vector, 18, 152
- primitive closure, 19
- primitive cohomology, 338
- quadratic
  - form, 14
  - integral — form, 19
  - integral — lattice, 19
  - $R$ -module, 144
  - torsion form, 145, 208
- quadratic module
  - semi-unimodular —, 151
- quaternion algebra
  - Hamilton —, 136, 246, 249
- quintic with 31 nodes, 130
- quotient singularity, 108
- $R$ -lattice, 144
- radical, 16, 20
  - of a quadratic  $R$ -module, 146
- reduced discriminant

- of torsion bilinear (quadratic) form, 183
- reduction
  - homomorphisms, 159
  - mod  $p$  (of a lattice), 59
- reflection, 25, 88, 158, 244, 255, 259
  - Cartan–Dieudonné theorem, 164
  - existence of  $p$ -adic —, 198
  - hyperplane —, 26, 158
- reflection group
  - $A_n, D_n, E_n$ , 310
  - $F_4$ , 91
  - $G_6$ , 90
- regular form, 149
- Riemann’s
  - constant, 303
  - singularity theorem, 303
  - theorem, 303
  - theta function, 302
- Riemann–Mumford relation, 305
- ring of integers of a number field, 132
- Rohlin’s theorem, 66
- root, 27
  - associated to reflection, 308
  - lattice, 27
  - Leech —, 314
  - sublattice, 308
- root lattice
  - $A_n(-1)$ , 79, 82
  - $D_n(-1)$ , 81
  - $E_n(-1), \tilde{A}_n(-1), \tilde{D}_n(-1), \tilde{E}_n(-1)$ , 82
  - of type  $E_8$ , 24, 25
- rotation, 25, 158
  - characteristic 2, 298
- Satake–Baily–Borel compactification, 352
- scaled form, 146
- semi-discriminant, 151
- semi-symplectic
  - automorphism, 414
- semi-unimodular
  - form, 151, 176
- semi-universal unfolding, 334
- Shioda–Inose structure, 394
- sign structure, 293
- signature, 23, 171
- singularity
  - adjacent —, 334
  - deformation theory, 334
  - du Val —, 108
  - exceptional unimodal —, 337
  - hyperbolic —, 335, 336
  - $m$ -modal —, 334
  - quotient —, 108
  - rational —, 108
  - unimodal —, 334
- skew symmetric
  - form, 144
- socle (of special set of roots), 326
- spin
  - group, 253
- spinor
  - equivalence, 260
  - genus, 260
  - norm, 251, 255
    - $\epsilon$ —, 293
    - signed —, 293
- stable equivalence, 219
- sublattice, 18
  - primitive —, 18, 152
  - primitive closure, 18
- supersingular K3 surface, 360
- surface
  - bi-elliptic —, 445
  - elliptic —, 109, 438, 445
  - Enriques —, 441
  - Hirzebruch —, 438
  - K3 —, 438
  - Kummer —, 439
  - minimal —, 443
  - of general type, 445
  - rational —, 438
  - ruled —, 438
  - singularity, 106
- Sylow decomposition, 420
- Sylvester’s law, 23, 170
- symmetric
  - $R$ -module, 151
  - bilinear form, 14
  - torsion form, 145
- symmetric form

- 
- over rings, 144
  - symplectic
    - automorphism, 364, 414
    - form, 144, 428
    - group, 428
    - pair, 428
    - space, 428
  - Ternary form, 139
  - theta
    - characteristic (odd or even), 303
    - divisor, 302
    - function, 55, 302
  - Tjurina number, 334
  - Torelli's theorem for K3 surfaces, 345
  - Torsion group
    - ordered basis, 32
  - torsion group
    - symmetric/quadratic —, 30, 43
  - torsion module
    - ordered basis, 181
  - trace form, 131, 153
  - transcendental lattice, 437
  - transfer homomorphism, 399
  - transvection, 429
    - symplectic —, 157
  - type I,II 2-elementary lattice, 36, 187, 193, 274, 360
  - unimodular
    - $R$ -module, 149
    - form, 18, 65, 150
    - lattice, 18, 42
  - vanishing
    - cycle, 333
    - lattice, 325
  - variable homology, 338
  - Vinberg–Dynkin diagram, 356
  - weak approximation, 424
  - Weil
    - pairing, 304
    - reciprocity, 301
  - Weyl
    - chamber, 311
  - Weyl group, 27, 308, 325
  - Witt
    - cancellation theorem, 165
    - decomposition, 27, 167
    - extension theorem, 166
    - group, 169
    - index, 27, 168
    - ring, 169