

CENTRAL SIMPLE ALGEBRAS AND GALOIS COHOMOLOGY

Philippe Gille and Tamás Szamuely

Preface

This book provides a comprehensive and up-to-date introduction to the theory of central simple algebras over arbitrary fields, emphasizing methods of Galois cohomology and (mostly elementary) algebraic geometry. The central result is the Merkurjev-Suslin theorem. As we see it today, this fundamental theorem is at the same time the culmination of the theory of Brauer groups of fields initiated by Brauer, Noether, Hasse and Albert in the 1930's, and a starting point of motivic cohomology theory, a domain which is at the forefront of current research in algebraic geometry and K-theory – suffice it here to mention the recent spectacular results of Voevodsky, Suslin, Rost and others. As a gentle ascent towards the Merkurjev-Suslin theorem, we cover the basic theory of central simple algebras, methods of Galois descent and Galois cohomology, Severi-Brauer varieties, residue maps and finally, Milnor K-theory and K-cohomology. These chapters also contain a number of noteworthy additional topics. The last chapter of the book rounds off the theory by presenting the results in positive characteristic. For an overview of the contents of each chapter we refer to their introductory sections.

Prerequisites. The book should be accessible to a graduate student or a nonspecialist reader with a solid training in algebra including Galois theory and basic commutative algebra, but no homological algebra. Some familiarity with algebraic geometry is also helpful. Most of the text can be read with a basic knowledge corresponding to, say, the first volume of Shafarevich's text. To help the novice, we summarize in an appendix the results from algebraic geometry we need. The first three sections of Chapter 8 require some familiarity with schemes, and in the proof of one technical statement we are forced to use techniques from Quillen K-theory. However, these may be skipped in a first reading by those willing to accept some 'black boxes'.

Acknowledgments

Our first words of thanks go to Jean-Louis Colliot-Thélène and Jean-Pierre Serre, from whom we learned much of what we know about the subject and who, to our great joy, have also been the most assiduous readers of the manuscript, and suggested many improvements. Numerous other colleagues helped us with their advice during the preparation of the text, or spotted inaccuracies in previous versions. Thanks are due to Spencer Bloch, Jean-Benoît Bost, Irene Bouw, Gábor Braun, Ferenc Bródy, Jérôme Burési, Baptiste Calmès, Mathieu Florence, Ofer Gabber, Skip Garibaldi, Luc Illusie, Bruno Kahn, Max-Albert Knus, David Leep, David Madore, Alexander Merkurjev, Ján Mináč, Arturo Pianzola, Peter Roquette, Joël Riou, Christophe Soulé, Jean-Pierre Tignol, Burt Totaro and Stefan Wewers.

Parts of the book formed the basis of a graduate course by the first author at Université de Paris-Sud and of a lecture series by the two authors at the Alfréd Rényi Institute. We thank both audiences for their pertinent questions and comments, and in particular Endre Szabó who shared his geometric insight with us. Most of the book was written while the first author visited the Rényi Institute in Budapest with a Marie Curie Intra-European Fellowship. The support of the Commission and the hospitality of the Institute are gratefully acknowledged. Last but not least, we are indebted to Diana Gillooly for assuring us a smooth and competent publishing procedure.

Contents

1	Quaternion Algebras	11
1.1	Basic Properties	11
1.2	Splitting over a Quadratic Extension	15
1.3	The Associated Conic	17
1.4	A Theorem of Witt	20
1.5	Tensor Products of Quaternion Algebras	23
2	Central Simple Algebras and Galois Descent	29
2.1	Wedderburn's Theorem	29
2.2	Splitting Fields	32
2.3	Galois Descent	36
2.4	The Brauer Group	42
2.5	Cyclic Algebras	46
2.6	Reduced Norms and Traces	51
2.7	A Basic Exact Sequence	53
2.8	K_1 of Central Simple Algebras	55
3	Techniques From Group Cohomology	65
3.1	Definition of Cohomology Groups	65
3.2	Explicit Resolutions	72
3.3	Relation to Subgroups	76
3.4	Cup-products	84
4	The Cohomological Brauer Group	97
4.1	Profinite Groups and Galois Groups	97
4.2	Cohomology of Profinite Groups	103
4.3	The Cohomology Exact Sequence	108
4.4	The Brauer Group Revisited	113
4.5	Index and Period	118
4.6	The Galois Symbol	124
4.7	Cyclic Algebras and Symbols	127

5	Severi-Brauer varieties	133
5.1	Basic Properties	134
5.2	Classification by Galois cohomology	136
5.3	Geometric Brauer Equivalence	140
5.4	Amitsur's Theorem	145
5.5	An Application: Making Central Simple Algebras Cyclic	151
6	Residue Maps	155
6.1	Cohomological Dimension	156
6.2	C_1 -Fields	161
6.3	Cohomology of Laurent Series Fields	167
6.4	Cohomology of Function Fields of Curves	172
6.5	Application to Class Field Theory	178
6.6	Application to the Rationality Problem: The Method	182
6.7	Application to the Rationality Problem: The Example	189
6.8	Residue Maps with Finite Coefficients	194
6.9	The Faddeev Sequence with Finite Coefficients	199
7	Milnor K-Theory	207
7.1	The Tame Symbol	207
7.2	Milnor's Exact Sequence and the Bass-Tate Lemma	214
7.3	The Norm Map	220
7.4	Reciprocity Laws	229
7.5	Applications to the Galois Symbol	235
7.6	The Galois Symbol Over Number Fields	242
8	The Merkurjev-Suslin Theorem	251
8.1	Gersten Complexes in Milnor K-theory	252
8.2	Properties of Gersten Complexes	256
8.3	A Property of Severi-Brauer Varieties	260
8.4	Hilbert's Theorem 90 for K_2	267
8.5	The Merkurjev-Suslin Theorem: A Special Case	275
8.6	The Merkurjev-Suslin Theorem: The General Case	280
9	Symbols in Positive Characteristic	289
9.1	The Theorems of Teichmüller and Albert	290
9.2	Differential Forms and p -torsion in the Brauer Group	296
9.3	Logarithmic Differentials and Flat p -Connections	300
9.4	Decomposition of the de Rham Complex	307
9.5	The Bloch-Gabber-Kato Theorem: Statement and Reductions	311
9.6	Surjectivity of the Differential Symbol	314

9.7 Injectivity of the Differential Symbol	321
Appendix: A Breviary of Algebraic Geometry	333
A.1 Affine and Projective Varieties	333
A.2 Maps Between Varieties	336
A.3 Function Fields and Dimension	338
A.4 Divisors	341
A.5 Complete Local Rings	343
A.6 Discrete Valuations	346
A.7 Derivations	350
A.8 Differential forms	354
Bibliography	361
Index	377

Chapter 1

Quaternion Algebras

As a prelude to the book, we present here our main objects of study in the simplest case, that of quaternion algebras. Many concepts that will be ubiquitous in the sequel, such as division algebras, splitting fields or norms appear here in a concrete and elementary context. Another important notion we shall introduce is that of the conic associated with a quaternion algebra; these are the simplest examples of Severi-Brauer varieties, objects to which a whole chapter will be devoted later. In the second part of the chapter two classic theorems from the 1930's are proven: a theorem of Witt asserting that the associated conic determines a quaternion algebra up to isomorphism, and a theorem of Albert that gives a criterion for the tensor product of two quaternion algebras to be a division algebra. The discussion following Albert's theorem will lead us to the statement of one of the main theorems proven later in the book, that of Merkurjev concerning division algebras of period 2.

The basic theory of quaternion algebras goes back to the 19th century. The original references for the main theorems of the last two sections are Witt [1] and Albert [1], [5], respectively.

1.1 Basic Properties

In this book we shall study finite dimensional algebras over a field. Here by an algebra over a field k mean a k -vector space equipped with a not necessarily commutative but associative k -linear multiplication. All k -algebras will be tacitly assumed to have a unit element.

Historically the first example of a finite dimensional noncommutative algebra over a field was discovered by W. R. Hamilton during a walk with his wife (presumably doomed to silence) on 16 October 1843. It is the *algebra of quaternions*, a 4-dimensional algebra with basis $1, i, j, k$ over the field \mathbf{R}

of real numbers, the multiplication being determined by the rules

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji = k.$$

This is in fact a *division algebra* over \mathbf{R} , which means that each nonzero element x has a two-sided multiplicative inverse, i.e. an element y with $xy = yx = 1$. Hamilton proved this as follows.

For a quaternion $q = x + yi + zj + wk$, introduce its *conjugate*

$$\bar{q} = x - yi - zj - wk$$

and its *norm* $N(q) = q\bar{q}$. A computation gives $N(q) = x^2 + y^2 + z^2 + w^2$, so if $q \neq 0$, the quaternion $\bar{q}/N(q)$ is an inverse for q .

We now come to an easy generalisation of the above construction. *Henceforth in this chapter, unless otherwise stated, k will denote a field of characteristic not 2.*

Definition 1.1.1 For any two elements $a, b \in k^\times$ define the (*generalised*) *quaternion algebra* (a, b) as the 4-dimensional k -algebra with basis $1, i, j, ij$, multiplication being determined by

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

One calls the set $\{1, i, j, ij\}$ a *quaternion basis* of (a, b) .

Remark 1.1.2 The isomorphism class of the algebra (a, b) depends only on the classes of a and b in $k^\times/k^{\times 2}$, because the substitution $i \mapsto ui, j \mapsto vj$ induces an isomorphism

$$(a, b) \xrightarrow{\sim} (u^2a, v^2b)$$

for all $u, v \in k^\times$. This implies in particular that the algebra (a, b) is isomorphic to (b, a) ; indeed, mapping $i \mapsto abj, j \mapsto abi$ we get

$$(a, b) \cong (a^2b^3, a^3b^2) \cong (b, a).$$

Given an element $q = x + yi + zj + wij$ of the quaternion algebra (a, b) , we define its *conjugate* by

$$\bar{q} = x - yi - zj - wij.$$

The map $(a, b) \rightarrow (a, b)$ given by $q \mapsto \bar{q}$ is an anti-automorphism of the k -algebra (a, b) , i.e. it is a k -vector space automorphism of (a, b) satisfying $\overline{(q_1q_2)} = \bar{q}_2\bar{q}_1$. Moreover, we have $\bar{\bar{q}} = q$; an anti-automorphism with this property is called an *involution* in ring theory.

We define the *norm* of $q = x + yi + zj + wij$ by $N(q) = q\bar{q}$. A calculation yields

$$N(q) = x^2 - ay^2 - bz^2 + abw^2 \in k, \quad (1)$$

so $N : (a, b) \rightarrow k$ is a *nondegenerate quadratic form*. The computation

$$N(q_1q_2) = q_1q_2\bar{q}_2\bar{q}_1 = q_1N(q_2)\bar{q}_1 = N(q_1)N(q_2)$$

shows that the norm is a multiplicative function, and the same argument as for Hamilton's quaternions yields:

Lemma 1.1.3 *An element q of the quaternion algebra (a, b) is invertible if and only if it has nonzero norm. Hence (a, b) is a division algebra if and only if the norm $N : (a, b) \rightarrow k$ does not vanish outside 0.*

Remark 1.1.4 In fact, one can give an intrinsic definition of the conjugation involution (and hence of the norm) on a quaternion algebra (a, b) which does not depend on the choice of the basis $(1, i, j, ij)$. Indeed, call an element q of (a, b) a *pure quaternion* if $q^2 \in k$ but $q \notin k$. A straightforward computation shows that a nonzero $q = x + yi + zj + wij$ is a pure quaternion if and only if $x = 0$. Hence a general q can be written uniquely as $q = q_1 + q_2$ with $q_1 \in k$ and q_2 pure, and conjugation is given by $\bar{q} = q_1 - q_2$. Moreover, a pure quaternion q satisfies $N(q) = -q^2$.

Example 1.1.5 (The matrix algebra $M_2(k)$)

Besides the classical Hamilton quaternions, the other basic example of a quaternion algebra is the k -algebra $M_2(k)$ of 2×2 matrices. Indeed, the assignment

$$i \mapsto I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j \mapsto J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}$$

defines an isomorphism $(1, b) \cong M_2(k)$, because the matrices

$$\text{Id} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad J = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad IJ = \begin{bmatrix} 0 & b \\ -1 & 0 \end{bmatrix} \quad (2)$$

generate $M_2(k)$ as a k -vector space, and they satisfy the relations

$$I^2 = \text{Id}, \quad J^2 = b\text{Id}, \quad IJ = -JI.$$

Definition 1.1.6 A quaternion algebra over k is called *split* if it is isomorphic to $M_2(k)$ as a k -algebra.

Proposition 1.1.7 *For a quaternion algebra (a, b) the following statements are equivalent.*

1. *The algebra (a, b) is split.*
2. *The algebra (a, b) is not a division algebra.*
3. *The norm map $N : (a, b) \rightarrow k$ has a nontrivial zero.*
4. *The element b is a norm from the field extension $k(\sqrt{a})|k$.*

Of course, instead of (4) another equivalent condition is that a is a norm from the field extension $k(\sqrt{b})|k$.

Proof: The implication (1) \Rightarrow (2) is obvious and (2) \Rightarrow (3) was proven in Lemma 1.1.3. For (3) \Rightarrow (4) we may assume a is not a square in k , for otherwise the claim is obvious. Take a nonzero quaternion $q = x + yi + zj + wi$ with norm 0. Then equation (1) implies $(z^2 - aw^2)b = x^2 - ay^2$, and so in particular $z^2 - aw^2 = (z + \sqrt{a}w)(z - \sqrt{a}w) \neq 0$, for otherwise a would be a square in k . Denoting by $N_{K|k}$ the field norm from $K = k(\sqrt{a})$ we get

$$b = N_{K|k}(x + \sqrt{a}y)N_{K|k}(z + \sqrt{a}w)^{-1},$$

whence (4) by multiplicativity of $N_{K|k}$. Finally, we shall show assuming (4) that $(a, b) \cong (1, 4a^2)$, whence (1) by the isomorphism in Example 1.1.5. To see this, we may again assume that a is not a square in k . If b is a norm from K , then so is b^{-1} , so by (4) and our assumption on a we find $r, s \in k$ satisfying $b^{-1} = r^2 - as^2$. Putting $u = rj + sij$ thus yields $u^2 = br^2 - abs^2 = 1$. Moreover, one verifies that $ui = -iu$, which implies that the element $v = (1+a)i + (1-a)ui$ satisfies $uv = (1+a)ui + (1-a)i = -vu$ and $v^2 = (1+a)^2a - (1-a)^2a = 4a^2$. Passing to the basis $(1, u, v, uv)$ thus gives the required isomorphism $(a, b) \cong (1, 4a^2)$. \square

Remark 1.1.8 Over a field of characteristic 2 one defines the generalised quaternion algebra $[a, b]$ by the presentation

$$[a, b] = \langle i, j \mid i^2 + i = a, j^2 = b, ij = ji + j \rangle$$

where $a \in k$ and $b \in k^\times$. This algebra has properties analogous to those in the above proposition (see Exercise 4).

1.2 Splitting over a Quadratic Extension

We now prove a structure theorem for division algebras of dimension 4. Recall first that the center $Z(A)$ of a k -algebra A is the k -subalgebra consisting of elements $x \in A$ satisfying $xy = yx$ for all $y \in A$. By assumption we have $k \subset Z(A)$; if this inclusion is an equality, one says that A is *central* over k . If A is a division algebra, then $Z(A)$ is a field. We then have:

Proposition 1.2.1 *A 4-dimensional central division algebra D over k is isomorphic to a quaternion algebra.*

We first prove:

Lemma 1.2.2 *If D contains a commutative k -subalgebra isomorphic to a nontrivial quadratic field extension $k(\sqrt{a})$ of k , then D is isomorphic to a quaternion algebra (a, b) for suitable $b \in k^\times$.*

Proof: A k -subalgebra as in the lemma contains an element q with $q^2 = a \in k$. By assumption, q is not in the center k of A and hence the inner automorphism of A given by $x \mapsto q^{-1}xq$ has exact order 2. As a k -linear automorphism of A , it thus has -1 as an eigenvalue, which means that there exists $r \in A$ such that $qr + rq = 0$. The elements $1, q, r, qr$ are linearly independent over k , for otherwise left multiplication by q would show that $qr = -rq$ lies in the k -span of 1 and q , but then it would commute with q , whereas they anticommute. The relation $qr + rq = 0$ then implies that the k -linear automorphism $x \mapsto r^{-2}xr^2$ leaves all four basis elements $1, q, r$ and qr fixed. Thus r^2 belongs to the center of A which is k by assumption. The lemma follows by setting $r^2 = b \in k^\times$. \square

Proof of Proposition 1.2.1: Let d be an element of $D \setminus k$. As D is finite dimensional over k , the powers $\{1, d, d^2, \dots\}$ are linearly dependent, so there is a polynomial $f \in k[x]$ with $f(d) = 0$. As D is a division algebra, it has no zero divisors and we may assume f irreducible. This means there is a k -algebra homomorphism $k[x]/(f) \rightarrow D$ which realises the field $k(d)$ as a k -subalgebra of D . Now the degree $[k(d) : k]$ cannot be 1 as $d \notin k$, and it cannot be 4 as D is not commutative. Hence $[k(d) : k] = 2$, and the lemma applies. \square

The crucial ingredient in the above proof was the existence of a quadratic extension $k(\sqrt{a})$ contained in D . Observe that the algebra $D \otimes_k k(\sqrt{a})$ then splits over $k(\sqrt{a})$. In fact, it follows from basic structural results to be proven

in the next chapter (Lemma 2.2.2 and Wedderburn's theorem) that any 4-dimensional central k -algebra for which there exists a quadratic extension of k with this splitting property is a division algebra or a matrix algebra.

It is therefore interesting to characterise those quadratic extensions of k over which a quaternion algebra splits.

Proposition 1.2.3 *Consider a quaternion algebra A over k , and fix an element $a \in k^\times \setminus k^{\times 2}$. The following statements are equivalent:*

1. A is isomorphic to the quaternion algebra (a, b) for some $b \in k^\times$.
2. The $k(\sqrt{a})$ -algebra $A \otimes_k k(\sqrt{a})$ is split.
3. A contains a commutative k -subalgebra isomorphic to $k(\sqrt{a})$.

Proof: To show (1) \Rightarrow (2), note that $(a, b) \otimes_k k(\sqrt{a})$ is none but the quaternion algebra (a, b) defined over the field $k(\sqrt{a})$. But a is a square in $k(\sqrt{a})$, so $(a, b) \cong (1, b)$, and the latter algebra is isomorphic to $M_2(k(\sqrt{a}))$ by Example 1.1.5. Next, if A is split, the same argument shows that (1) always holds, so to prove (3) \Rightarrow (1) one may assume A is nonsplit, in which case Lemma 1.2.2 applies.

The implication (2) \Rightarrow (3) is easy in the case when $A \cong M_2(k)$: one chooses an isomorphism $M_2(k) \cong (1, a)$ as in Example 1.1.5 and takes the subfield $k(J)$, where J is the basis element with $J^2 = a$. We now assume A is nonsplit, and extend the quaternion norm N on A to $A \otimes_k k(\sqrt{a})$ by base change. Applying part (3) of Proposition 1.1.7 to $A \otimes_k k(\sqrt{a})$ one gets that there exist elements $q_0, q_1 \in A$, not both 0, with $N(q_0 + \sqrt{a}q_1) = 0$. Denote by $B : A \otimes_k k(\sqrt{a}) \times A \otimes_k k(\sqrt{a}) \rightarrow k(\sqrt{a})$ the symmetric bilinear form associated with N (recall that it is defined by $B(x, y) = (N(x + y) - N(x) - N(y))/2$ and satisfies $B(x, x) = N(x)$). We get

$$0 = B(q_0 + \sqrt{a}q_1, q_0 + \sqrt{a}q_1) = N(q_0) + aN(q_1) + 2\sqrt{a}B(q_0, q_1).$$

Now note that since $q_0, q_1 \in A$, the elements $B(q_0, q_1)$ and $N(q_0) + aN(q_1)$ both lie in k . So it follows from the above equality that

$$N(q_0) = -aN(q_1) \quad \text{and} \quad 2B(q_0, q_1) = q_0\bar{q}_1 + q_1\bar{q}_0 = 0.$$

Here $N(q_0), N(q_1) \neq 0$ as A is nonsplit. The element $q_2 := q_0\bar{q}_1 \in A$ satisfies

$$q_2^2 = q_0\bar{q}_1q_0\bar{q}_1 = -q_0\bar{q}_0q_1\bar{q}_1 = -N(q_0)N(q_1) = aN(q_1)^2.$$

The square of the element $q := q_2N(q_1)^{-1}$ is then precisely a , so mapping \sqrt{a} to q embeds $k(\sqrt{a})$ into A . \square

We conclude this section by another characterisation of the quaternion norm.

Proposition 1.2.4 *Let (a, b) be a quaternion algebra over a field k , and let $K = k(\sqrt{a})$ be a quadratic splitting field for (a, b) . Then for all $q \in (a, b)$ and all K -isomorphisms $\phi : (a, b) \otimes_k K \xrightarrow{\sim} M_2(K)$ we have $N(q) = \det(\phi(q))$.*

Proof: First note that $\det(\phi(q))$ does not depend on the choice of ϕ . Indeed, if $\psi : (a, b) \otimes_k K \xrightarrow{\sim} M_2(K)$ is a second isomorphism, then $\phi \circ \psi^{-1}$ is an automorphism of $M_2(K)$. But it is well-known that all K -automorphisms of $M_2(K)$ are of the form $M \rightarrow CMC^{-1}$ for some invertible matrix C (check this by hand or see Lemma 2.4.1 for a proof in any dimension), and that the determinant map is invariant under such automorphisms.

Now observe that by definition the quaternion norm on $(a, b) \otimes_k K$ restricts to that on (a, b) . Therefore to prove the proposition it is enough to embed (a, b) into $M_2(K)$ via ϕ and check that on $M_2(K)$ the quaternion norm (which is intrinsic by Remark 1.1.4) is given by the determinant. For this, consider a basis of $M_2(K)$ as in (2) with $b = 1$ and write

$$\begin{aligned} \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} &= \left(\frac{a_1 + a_4}{2}\right) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \left(\frac{a_1 - a_4}{2}\right) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + \\ &+ \left(\frac{a_2 + a_3}{2}\right) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \left(\frac{a_2 - a_3}{2}\right) \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \end{aligned}$$

Then equation (1) yields

$$\begin{aligned} N\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\right) &= \left(\frac{a_1 + a_4}{2}\right)^2 - \left(\frac{a_1 - a_4}{2}\right)^2 - \left(\frac{a_2 + a_3}{2}\right)^2 + \left(\frac{a_2 - a_3}{2}\right)^2 \\ &= a_1a_4 - a_2a_3 = \det\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\right). \end{aligned}$$

□

1.3 The Associated Conic

We now introduce another important invariant of a quaternion algebra (a, b) , the *associated conic* $C(a, b)$. By definition, this is the projective plane curve defined by the homogeneous equation

$$ax^2 + by^2 = z^2 \tag{3}$$

where x, y, z are the homogeneous coordinates in the projective plane \mathbf{P}^2 . In the case of $(1, 1) \xrightarrow{\sim} M_2(k)$ we get the usual circle

$$x^2 + y^2 = z^2.$$

Remark 1.3.1 In fact, the conic $C(a, b)$ is canonically attached to the algebra (a, b) and does not depend on the choice of a basis. To see why, note first that the conic $C(a, b)$ is isomorphic to the conic $ax^2 + by^2 = abz^2$ via the substitution $x \mapsto by, y \mapsto ax, z \mapsto abz$ (after substituting, divide the equation by ab). But $ax^2 + by^2 - abz^2$ is exactly the square of the pure quaternion $xi + yj + zij$ and hence is intrinsically defined by Remark 1.1.4.

This observation also shows that if two quaternion algebras (a, b) and (c, d) are isomorphic as k -algebras, then the conics $C(a, b)$ and $C(c, d)$ are also isomorphic over k . Indeed, constructing an isomorphism $(a, b) \cong (c, d)$ is equivalent to finding a k -basis in (a, b) that satisfies the multiplicative rule in (c, d) .

Recall from algebraic geometry that the conic $C(a, b)$ is said to have a k -rational point if there exist $x_0, y_0, z_0 \in k$, not all zero, that satisfy equation (3) above.

We can now give a complement to Proposition 1.1.7.

Proposition 1.3.2 *The quaternion algebra (a, b) is split if and only if the conic $C(a, b)$ has a k -rational point.*

Proof: If (x_0, y_0, z_0) is a k -rational point on $C(a, b)$ with $y_0 \neq 0$, then $b = (z_0/y_0)^2 - a(x_0/y_0)^2$ and part (4) of Proposition 1.1.7 is satisfied. If y_0 happens to be 0, then x_0 must be nonzero and we get similarly that a is a norm from the extension $k(\sqrt{b})|k$. Conversely, if $b = r^2 - as^2$ for some $r, s \in k$, then $(s, 1, r)$ is a k -rational point on $C(a, b)$. \square

Remark 1.3.3 Again, the proposition has a counterpart in characteristic 2; see Exercise 4.

Example 1.3.4 For $a \neq 1$, the projective conic $ax^2 + (1 - a)y^2 = z^2$ has the k -rational point $(1, 1, 1)$, hence the quaternion algebra $(a, 1 - a)$ splits by the proposition. This innocent-looking fact is a special case of the so-called *Steinberg relation* for symbols that we shall encounter later.

Remark 1.3.5 It is a well-known fact from algebraic geometry that a smooth projective conic defined over a field k is isomorphic to the projective line \mathbf{P}^1 over k if and only if it has a k -rational point. The isomorphism is given by

taking the line joining a point P of the conic to some fixed k -rational point O and then taking the intersection of this line with \mathbf{P}^1 embedded as, say, some coordinate axis in \mathbf{P}^2 . In such a way we get another equivalent condition for the splitting of a quaternion algebra, which will be substantially generalised later.

In the remainder of this section we give examples of how Proposition 1.3.2 can be used to give easy proofs of splitting properties of quaternion algebras over special fields.

Example 1.3.6 Let k be the finite field with q elements (q odd). Then any quaternion algebra (a, b) over k is split.

To see this, it suffices by Proposition 1.3.2 to show that the conic $C(a, b)$ has a k -rational point. We shall find a point (x_0, y_0, z_0) with $z_0 = 1$. As the multiplicative group of k is cyclic of order $q-1$, there are exactly $1 + (q-1)/2$ squares in k , including 0. Thus the sets $\{ax^2 : x \in k\}$ and $\{1 - by^2 \mid y \in k\}$ both have cardinality $1 + (q-1)/2$, hence must have an element in common.

The next two examples concern the field $k(t)$ of rational functions over a field k , which is by definition the fraction field of the polynomial ring $k[t]$. Note that sending t to 0 induces a k -homomorphism $k[t] \rightarrow k$; we call it the *specialisation* map attached to t .

Example 1.3.7 Let (a, b) a quaternion algebra over k . Then (a, b) is split over k if and only if $(a, b) \otimes_k k(t)$ is split over $k(t)$.

Here necessity is obvious. For sufficiency, we assume given a point (x_t, y_t, z_t) of $C(a, b)$ defined over $k(t)$. As the equation (3) defining $C(a, b)$ is homogeneous, we may assume after multiplication by a suitable element of $k(t)$ that x_t, y_t, z_t all lie in $k[t]$ and one of them has nonzero constant term. Then specialisation gives a k -point $(x_t(0), y_t(0), z_t(0))$ of $C(a, b)$.

Finally we give an example of a splitting criterion for a quaternion algebra over $k(t)$ that does not come from k .

Example 1.3.8 For $a \in k^\times$ the $k(t)$ -algebra (a, t) is split if and only if a is a square in k .

Here sufficiency is contained in Example 1.1.5. For necessity, assume given a $k(t)$ -point (x_t, y_t, z_t) of $C(a, b)$ as above. Again we may assume x_t, y_t, z_t are all in $k[t]$. If x_t and z_t were both divisible by t , then equation (3) would imply the same for y_t , so after an eventual division we may assume they are not. Then setting $t = 0$ gives $ax_t^2(0) = z_t(0)^2$ and so $a = x_t^2(0)^{-1}z_t(0)^2$ is a square.

1.4 A Theorem of Witt

In this section we prove an elegant theorem which characterises isomorphisms of quaternion algebras by means of the function fields of the associated conics. Recall that the function field of an algebraic curve C is the field $k(C)$ of rational functions defined over some Zariski open subset of C . In the concrete case of a conic $C(a, b)$ as in the previous section, the simplest way to define it is to take the fraction field of the integral domain $k[x, y]/(ax^2 + by^2 - 1)$ (this is also the function field of the affine curve of equation $ax^2 + by^2 = 1$).

A crucial observation for the sequel is the following.

Remark 1.4.1 The quaternion algebra $(a, b) \otimes_k k(C(a, b))$ is always split over $k(C(a, b))$. Indeed, the conic $C(a, b)$ always has a point over this field, namely $(x, y, 1)$ (where we also denote by x, y their images in $k(C(a, b))$). This point is called the *generic point* of the conic.

Now we can state the theorem.

Theorem 1.4.2 (Witt) *Let $Q_1 = (a_1, b_1)$, $Q_2 = (a_2, b_2)$ be quaternion algebras, and let $C_i = C(a_i, b_i)$ be the associated conics. The algebras Q_1 and Q_2 are isomorphic over k if and only if the function fields $k(C_1)$ and $k(C_2)$ are isomorphic over k .*

Remark 1.4.3 It is known from algebraic geometry that two smooth projective curves are isomorphic if and only if their function fields are. Thus the theorem states that *two quaternion algebras are isomorphic if and only if the associated conics are isomorphic as algebraic curves.*

In Chapter 5 we shall prove a broad generalisation of the theorem, due to Amitsur. We now begin the proof by the following easy lemma.

Lemma 1.4.4 *If (a, b) is a quaternion algebra and $c \in k^\times$ is a norm from the field extension $k(\sqrt{a})|k$, then $(a, b) \cong (a, bc)$.*

Proof: By hypothesis, we may write $c = x^2 - ay^2$ with $x, y \in k$. Hence we may consider c as the norm of the quaternion $q = x + yi + 0j + 0ij$ and set $J = qj = xj + yij$. Then J is a pure quaternion satisfying

$$iJ + Ji = 0, \quad J^2 = -N(J) = -N(q)N(j) = bc,$$

and $1, i, J, iJ$ is a basis of (a, b) over k (by a similar argument as in the proof of Lemma 1.2.1). The lemma follows. \square

Proof of Theorem 1.4.2: Necessity follows from Remark 1.3.1, so it is enough to prove sufficiency. If both Q_1 and Q_2 are split, the theorem is obvious. So we may assume one of them, say Q_1 , is nonsplit. By Remark 1.4.1 the algebra $Q_1 \otimes_k k(C_1)$ is split, hence so is the algebra $Q_1 \otimes_k k(C_2)$ by assumption. If Q_2 is split, then $k(C_2)$ is a rational function field, and therefore Q_1 is also split by Example 1.3.7.

So we may assume that both algebras are nonsplit. In particular a_1 is not a square in k , and the algebra $Q_1 \otimes_k L$ becomes split over the quadratic extension $L := k(\sqrt{a_1})$. For brevity's sake, we write C instead of C_1 in the sequel. The field $L(C) = L \otimes_k k(C)$ is the function field of the curve C_L obtained by extension of scalars from C ; this curve is isomorphic to the projective line over L , and hence $L(C)$ is isomorphic to the rational function field $L(t)$. As $Q_2 \otimes_k L(C)$ is split over $L(C)$ by assumption, Example 1.3.7 again yields that $Q_2 \otimes_k L$ must be split over L . Proposition 1.2.3 then implies that $Q_2 \xrightarrow{\sim} (a_1, c)$ for some $c \in k^\times$. As $Q_2 \otimes_k k(C)$ is split over $k(C)$ (again by assumption and Remark 1.4.1), it follows from Proposition 1.1.7 that $c = N_{L(C)/k(C)}(f)$ for some $f \in L(C)^\times$.

Our goal is to identify the function f in order to compute c . Recall (e.g. from Section A.4 of the Appendix) that the group $\text{Div}(C_L)$ of divisors on C_L is defined as the free abelian group generated by the closed points of C_L (in this case they correspond to irreducible polynomials in $L(t)$, plus a point at infinity). There is a *divisor map* $\text{div} : L(C)^\times \rightarrow \text{Div}(C_L)$ associating to a function the divisor given by its zeroes and poles, and a *degree map* given by $\sum m_i P_i \mapsto \sum m_i [\kappa(P_i) : L]$, where $\kappa(P_i)$ is the residue field of the closed point P_i . The two maps fit into an exact sequence

$$0 \rightarrow L(C)^\times / L^\times \xrightarrow{\text{div}} \text{Div}(C_L) \xrightarrow{\text{deg}} \mathbf{Z} \rightarrow 0, \quad (4)$$

corresponding in our case to the decomposition of rational functions into products of irreducible polynomials and their inverses.

The Galois group $\text{Gal}(L|K) = \{1, \sigma\}$ acts on this exact sequence as follows (see Remark A.4.5 of the Appendix). On $L(C)$ it acts via its action on L (but note that under the isomorphism $L(C) \cong L(t)$ this action does *not* induce the similar action on the right hand side!). On $\text{Div}(C_L)$ it acts by sending a closed point P to its conjugate $\sigma(P)$. Finally, it acts trivially on \mathbf{Z} , making the maps of the sequence $\text{Gal}(L|K)$ -equivariant.

Now consider the map $(1 + \sigma) : \text{Div}(C_L) \rightarrow \text{Div}(C_L)$. By additivity of the divisor map, we have

$$(1 + \sigma)\text{div}(f) = \text{div}(f\sigma(f)) = \text{div}(c) = 0,$$

as c is a constant. On the other hand, as σ has order 2, we have a natural

direct sum decomposition

$$\operatorname{Div}(C_L) = \left(\bigoplus_{P=\sigma(P)} \mathbf{Z}P \right) \oplus \left(\bigoplus_{P \neq \sigma(P)} \mathbf{Z}P \right),$$

where σ acts trivially on the first summand, and exchanges P and $\sigma(P)$ in the second. Writing $\operatorname{div}(f) = E_1 + E_2$ according to this decomposition, we get

$$0 = (1 + \sigma)\operatorname{div}(f) = 2E_1 + (1 + \sigma)E_2.$$

This implies that $E_1 = 0$ and E_2 is of the form $\sum(m_i P_i - m_i \sigma(P_i))$ for some closed points P_1, \dots, P_r and $m_i \neq 0$. Setting $D = \sum m_i P_i$, we may therefore write

$$\operatorname{div}(f) = (1 - \sigma)D.$$

Let d be the degree of D . The point $P_0 := (1 : 0 : \sqrt{a_1})$ is an L -rational point of our conic C_L , whose equation is $a_1 x^2 + b_1 y^2 = z^2$. Exact sequence (4) therefore shows that there exists $g \in L(C)^\times$ such that

$$D - dP_0 = \operatorname{div}(g).$$

It follows that

$$\operatorname{div}(f) = \operatorname{div}(g\sigma(g)^{-1}) + d(1 - \sigma)P_0.$$

Replacing f by $f\sigma(g)g^{-1}$, we get a function still satisfying $c = N_{L(C)|k(C)}(f)$, but with

$$\operatorname{div}(f) = d(1 - \sigma)P_0. \quad (5)$$

We are now able to identify the function f up to a constant. We first claim that the rational function $h := (z - \sqrt{a_1}x)y^{-1} \in L(C)^\times$ satisfies

$$\operatorname{div}(h) = (1 : 0 : \sqrt{a_1}) - (1 : 0 : -\sqrt{a_1}) = (1 - \sigma)P_0. \quad (6)$$

Indeed, let $P = (x_0 : y_0 : z_0)$ be a pole of h (over an algebraic closure \bar{k}). Then we must have $y_0 = 0$ and hence $P = (1 : 0 : \pm\sqrt{a_1})$; in particular, P is an L -rational point. But by the equation of C we have $h = b_1 y(z + \sqrt{a_1}z)^{-1}$, so $(1 : 0 : \sqrt{a_1})$ is a zero of h and not a pole. Therefore $(1 : 0 : -\sqrt{a_1})$ is the only pole of h and similarly $(1 : 0 : \sqrt{a_1})$ is its only zero. Comparing formulae (5) and (6), we get from the left exactness of sequence (4) that $f = c_0 h^d$ for some constant $c_0 \in L^\times$. We compute

$$c = N_{L(C)|k(C)}(f) = N_{L|k}(c_0)N_{L(C)|k(C)}(h)^d = N_{L|k}(c_0) \left(\frac{z^2 - a_1 x^2}{y^2} \right)^d = N_{L|k}(c_0) b_1^d.$$

So Lemma 1.4.4 implies

$$Q_2 \cong (a_1, c) \cong (a_1, b_1^d).$$

By our assumption Q_2 is nonsplit, so d is odd and $Q_2 \cong (a_1, b_1)$, as desired. \square

1.5 Tensor Products of Quaternion Algebras

Now we step forward and consider higher dimensional k -algebras, where k is still assumed to be a field of characteristic not 2. The simplest of these are *biquaternion algebras*, which are by definition those k -algebras that are isomorphic to a tensor product of two quaternion algebras over k .

We begin with two lemmas that are very helpful in calculations. The first is well-known:

Lemma 1.5.1 *The tensor product of two matrix algebras $M_n(k)$ and $M_m(k)$ over k is isomorphic to the matrix algebra $M_{nm}(k)$.*

Proof: Perhaps the simplest proof is to note that given k -endomorphisms $\phi \in \text{End}_k(k^n)$ and $\psi \in \text{End}_k(k^m)$, the pair (ϕ, ψ) induces an element $\phi \otimes \psi$ of $\text{End}_k(k^n \otimes_k k^m)$. The resulting map $\text{End}_k(k^n) \otimes \text{End}_k(k^m) \rightarrow \text{End}_k(k^n \otimes_k k^m)$ is obviously injective, and it is surjective e.g. by dimension reasons. \square

Lemma 1.5.2 *Given elements $a, b, b' \in k^\times$ we have an isomorphism*

$$(a, b) \otimes_k (a, b') \xrightarrow{\sim} (a, bb') \otimes_k M_2(k).$$

Proof: Denote by $(1, i, j, ij)$ and $(1, i', j', i'j')$ quaternion bases of (a, b) and (a, b') , respectively, and consider the k -subspaces

$$A_1 = k(1 \otimes 1) \oplus k(i \otimes 1) \oplus k(j \otimes j') \oplus k(ij \otimes j'),$$

$$A_2 = k(1 \otimes 1) \oplus k(1 \otimes j') \oplus k(i \otimes i'j') \oplus k((-b'i) \otimes i')$$

of $(a, b) \otimes_k (a, b')$. One checks that A_1 and A_2 are both closed under multiplication and hence are subalgebras of $(a, b) \otimes_k (a, b')$. By squaring the basis elements $i \otimes 1, j \otimes j'$ and $1 \otimes j', i \otimes i'j'$ we see that A_1 and A_2 are isomorphic to the quaternion algebras (a, bb') and $(b', -a^2b')$, respectively. But this latter algebra is isomorphic to $(b', -b')$, which is split because the conic $C(b', -b')$ has the k -rational point $(1, 1, 0)$.

Now consider the map $\rho : A_1 \otimes_k A_2 \rightarrow (a, b) \otimes_k (a, b')$ induced by the k -bilinear map $(x, y) \rightarrow xy$. Inspection reveals that all standard basis elements of $(a, b) \otimes_k (a, b')$ lie in the image of ρ , so it is surjective and hence induces the required isomorphism for dimension reasons. \square

Corollary 1.5.3 *For a quaternion algebra (a, b) the tensor product algebra $(a, b) \otimes_k (a, b)$ is isomorphic to the matrix algebra $M_4(k)$.*

Proof: The case $b = b'$ of the previous lemma and Example 1.1.5 give

$$(a, b) \otimes_k (a, b) \cong (a, b^2) \otimes_k M_2(k) \cong (a, 1) \otimes_k M_2(k) \cong M_2(k) \otimes_k M_2(k),$$

and we conclude by Lemma 1.5.1. \square

A biquaternion algebra $A = Q_1 \otimes_k Q_2$ is equipped with an involution σ defined as the product of the conjugation involutions on Q_1 and Q_2 , i.e. by setting $\sigma(q_1 \otimes q_2) = \bar{q}_1 \otimes \bar{q}_2$ and extending by linearity. We remark that the involution σ is not canonical but depends on the decomposition $A \cong Q_1 \otimes_k Q_2$. For $i = 1, 2$ denote by Q_i^- the subspace of pure quaternions in Q_i (cf. Remark 1.1.4).

Lemma 1.5.4 *Let V be the k -subspace of A consisting of elements satisfying $\sigma(a) = -a$, and W the subspace of those with $\sigma(a) = a$. One has a direct sum decomposition $A = V \oplus W$, and moreover one may write*

$$V = (Q_1^- \otimes_k k) \oplus (k \otimes_k Q_2^-) \quad \text{and} \quad W = k \oplus (Q_1^- \otimes_k Q_2^-).$$

Proof: One has $V \cap W = 0$. Moreover, there are natural inclusions

$$(Q_1^- \otimes_k k) \oplus (k \otimes_k Q_2^-) \subset V \quad \text{and} \quad k \oplus (Q_1^- \otimes_k Q_2^-) \subset W.$$

For dimension reasons these must be isomorphisms and $V \oplus W$ must be the whole of A . \square

Denote by N_1 and N_2 the quaternion norms on Q_1 and Q_2 , respectively, and consider the quadratic form

$$\phi(x, y) = N_1(x) - N_2(y) \tag{7}$$

on V , called an *Albert form* of A . Again it depends on the decomposition $A \cong Q_1 \otimes_k Q_2$.

Theorem 1.5.5 (Albert) *For a biquaternion algebra $A \cong Q_1 \otimes_k Q_2$ over k , the following statements are equivalent:*

1. The algebra A is not a division algebra.
2. There exist $a, b, b' \in k^\times$ such that $Q_1 \xrightarrow{\sim} (a, b)$ and $Q_2 \xrightarrow{\sim} (a, b')$.
3. The Albert form (7) has a nontrivial zero on A .

Proof: For the implication (2) \Rightarrow (3), note that the assumption in (2) implies that there exist pure quaternions $q_i \in Q_i^-$ with $q_i^2 = -N_i(q_i) = a$ for $i = 1, 2$, and hence $\phi(q_1, q_2) = 0$. For (3) \Rightarrow (1), assume there is a nontrivial relation $\phi(q_1, q_2) = 0$ in pure quaternions. Note that q_1 and q_2 commute, because the components Q_1 and Q_2 centralise each other in the tensor product $Q_1 \otimes_k Q_2$. Hence we have $0 = \phi(q_1, q_2) = q_1^2 - q_2^2 = (q_1 + q_2)(q_1 - q_2)$, which implies that A cannot be a division algebra.

For the hardest implication (1) \Rightarrow (2) assume (2) is false, and let us prove that $A \cong Q_1 \otimes_k Q_2$ is a division algebra. If (2) is false, then both Q_1 and Q_2 are division algebras (otherwise say $b' = 1$ and suitable a, b will do). Denote by K_i a quadratic extension of K contained in Q_i for $i = 1, 2$. By our assumption that (2) is false, Proposition 1.2.3 implies that K_1 splits Q_1 but not Q_2 , and similarly for K_2 . Therefore both $K_1 \otimes_k Q_2$ and $K_2 \otimes_k Q_1$ are division algebras. It will suffice to show that each nonzero $\alpha \in A$ has a left inverse α_l , for then the conjugate $\alpha_r := \sigma(\sigma(\alpha)_l)$ is a right inverse for α , and $\alpha_l = \alpha_l \alpha \alpha_r = \alpha_r$. Moreover, it is enough to find $\alpha^* \in A$ such that $\alpha^* \alpha$ is a nonzero element lying in either $K_1 \otimes_k Q_2$ or $Q_1 \otimes_k K_2$, for then $\alpha^* \alpha$ has a left inverse, and so does α . Fix a quaternion basis $\{1, i, j, ij\}$ for Q_2 such that $K_2 = k(j)$. We can then write

$$\alpha = (\beta_1 + \beta_2 j) + (\beta_3 + \beta_4 j) ij$$

with suitable $\beta_i \in Q_1$. We may assume that $\gamma := \beta_3 + \beta_4 j \neq 0$, for otherwise α lies in $Q_1 \otimes_k K_2$ already. Then γ^{-1} exists in $Q_1 \otimes_k K_2$, and after replacing α by $\gamma^{-1} \alpha$ we are reduced to the case when $\alpha = \beta_1 + \beta_2 j + ij$. If β_1 and β_2 commute, then $k(\beta_1, \beta_2)$ is either k or a quadratic extension $K|k$ contained in Q_1 . Thus $\alpha \in Q_2$ or $\alpha \in K \otimes_k Q_2$, and we are done in this case. So we may assume $\beta_1 \beta_2 - \beta_2 \beta_1 \neq 0$. We then contend that $\alpha^* := \beta_1 - \beta_2 j - ij$ is a good choice. Indeed, we compute

$$\begin{aligned} \alpha^* \alpha &= (\beta_1 - \beta_2 j - ij)(\beta_1 + \beta_2 j + ij) = (\beta_1 - \beta_2 j)(\beta_1 + \beta_2 j) - (ij)^2 = \\ &= \beta_1^2 - \beta_2^2 j^2 - (ij)^2 + (\beta_1 \beta_2 - \beta_2 \beta_1) j, \end{aligned}$$

where the second equality holds since ij commutes with β_1, β_2 (for the same reason as above), and anticommutes with j . Since j^2 and $(ij)^2$ lie in k and $\beta_1 \beta_2 - \beta_2 \beta_1 \neq 0$, this shows $\alpha^* \alpha \in (Q_1 \otimes_k K_2) \setminus \{0\}$, as required. \square

Remark 1.5.6 The above proof, taken from Lam [1], is a variant of Albert's original argument. For other proofs of the theorem, valid in all characteristics, see Knus [1] as well as Tits [1] (for the equivalence (1) \Leftrightarrow (2)).

The theorem makes it possible to give concrete examples of biquaternion division algebras, such as the following one.

Example 1.5.7 Let k be a field of characteristic $\neq 2$ as usual, and let F be the purely transcendental extension $k(t_1, t_2, t_3, t_4)$. Then the biquaternion algebra

$$(t_1, t_2) \otimes_F (t_3, t_4)$$

is a division algebra over F .

To see this, we have to check that the Albert form has no nontrivial zero. Assume it does. Then by formula (1) for the quaternion norm we have a nontrivial solution of the equation

$$-t_1x_1^2 - t_2x_2^2 + t_1t_2x_{1,2}^2 + t_3x_3^2 + t_4x_4^2 - t_3t_4x_{3,4}^2 = 0 \quad (8)$$

in the variables $x_1, x_2, x_{1,2}, x_3, x_4, x_{3,4}$. By multiplying with a rational function we may assume $x_1, x_2, x_{1,2}, x_3, x_4, x_{3,4}$ are all in $k(t_1, t_2, t_3)[t_4]$ and one of them is not divisible by t_4 .

Assume that $x_1, x_2, x_{1,2}, x_3$ are all divisible by t_4 . Then t_4^2 must divide $t_4x_4^2 - t_3t_4x_{3,4}^2$, so t_4 divides $x_4^2 - t_3x_{3,4}^2$. Setting $t_4 = 0$ produces a solution of the equation $x^2 - t_3y^2 = 0$ with $x, y \in k(t_1, t_2, t_3)$ not both 0, which implies that t_3 is a square in $k(t_1, t_2, t_3)$; this is a contradiction. So one of the $x_1, x_2, x_{1,2}, x_3$ is not divisible by t_4 , and by setting $t_4 = 0$ in equation (8) we get a nontrivial solution of the equation

$$-t_1y_1^2 - t_2y_2^2 + t_1t_2y_{1,2}^2 + t_3y_3^2 = 0$$

with entries in $k(t_1, t_2, t_3)$. A similar argument as before then shows that there is a nontrivial solution of the equation

$$-t_1z_1^2 - t_2z_2^2 + t_1t_2z_{1,2}^2 = 0$$

over the field $k(t_1, t_2)$. Applying the same trick one last time, we see that the equation

$$t_1w_1^2 = 0$$

has a nontrivial solution in $k(t_1)$, which finally yields a contradiction.

In general, we say that a finite dimensional division algebra D over a field k has *period 2* if $D \otimes_k D$ is isomorphic to a matrix algebra over k . Quaternion algebras have this property by Corollary 1.5.3. Also, applying Lemma 1.5.1 we see that tensor products of division algebras of period 2 are again of period 2.

According to Proposition 1.2.1, a 4-dimensional central division algebra over k is in fact a quaternion algebra. Moreover, in 1932 Albert proved that a 16-dimensional central division algebra of period 2 is isomorphic to a biquaternion algebra. Thus it was plausible to conjecture that a central division algebra of period 2 and dimension 4^m is always a tensor product of m quaternion algebras. However, in 1979 Amitsur, Rowen and Tignol [1] produced a 64-dimensional central division algebra of period 2 which is not a tensor product of quaternion algebras.

Therefore the following theorem of Merkurjev [1], which is one of the highlights of this book, is all the more remarkable.

Theorem 1.5.8 (Merkurjev) *Let D be a central division algebra of period 2 over a field k . There exist positive integers m_1, m_2, n and quaternion algebras Q_1, \dots, Q_n over k such that there is an isomorphism*

$$D \otimes_k M_{m_1}(k) \cong Q_1 \otimes_k Q_2 \otimes_k \cdots \otimes_k Q_n \otimes_k M_{m_2}(k).$$

EXERCISES

1. Let Q be a quaternion algebra over k . Show that the conjugation involution is the only linear map $\sigma : Q \rightarrow Q$ such that $\sigma(1) = 1$ and $\sigma(q)q \in k$ for all $q \in Q$.
2. Show that a quaternion algebra is split if and only if it has a basis (e, f, g, h) in which the norm is given by $(xe + yf + zg + wh) \mapsto xy - zw$. (In the language of quadratic forms, this latter property means that the norm form is *hyperbolic*.)
3. Let Q be a quaternion algebra over k , and let $K|k$ be a quadratic extension embedded as a k -subalgebra in Q . Verify that one has $N(q) = N_{K|k}(q)$ for all $q \in K$, where N is the quaternion norm and $N_{K|k}$ is the field norm. [*Hint*: Extend a suitable k -basis of K to a quaternion basis of Q .]
4. Let k be a field of characteristic 2, and let $[a, b]$ the quaternion algebra of Remark 1.1.8. Show that the following are equivalent:
 - $[a, b] \cong M_2(k)$.

- $[a, b]$ is not a division algebra.
 - The element b is a norm from the extension $k(\alpha)|k$, where α is a root of the equation $x^2 + x = a$.
 - The projective conic $ax^2 + by^2 = z^2 + zx$ has a k -rational point.
5. Determine those prime numbers p for which the quaternion algebra $(-1, p)$ is split over the field \mathbf{Q} of rational numbers.
6. (Chain lemma) Assume that the quaternion algebras (a, b) and (c, d) are isomorphic. Show that there exists an $e \in k^\times$ such that

$$(a, b) \cong (e, b) \cong (e, d) \cong (c, d).$$

[*Hint:* Consider the symmetric bilinear form $B(q_1, q_2) := \frac{1}{2}(q_1\bar{q}_2 + q_2\bar{q}_1)$ on the subspace $B_0 \subset (a, b)$ of elements $q \in (a, b)$ satisfying $q + \bar{q} = 0$. Note that $i, j, I, J \in B_0$, where $1, i, j, ij$ and $1, I, J, IJ$ are the standard bases of $(a, b) \cong (c, d)$ with $i^2 = a, j^2 = b, ij = -ji$ and $I^2 = c, J^2 = d, IJ = -JI$. Take an element $\varepsilon \in B_0 \setminus \{0\}$ with $B(\varepsilon, j) = B(\varepsilon, J) = 0$ and set $e = \varepsilon^2$.]

Chapter 2

Central Simple Algebras and Galois Descent

In this chapter we treat the basic theory of central simple algebras from a modern viewpoint. The main point we would like to emphasize is that, as a consequence of Wedderburn's theorem, we may characterise central simple algebras as those finite dimensional algebras which become isomorphic to some full matrix ring over a finite extension of the base field. We then show that this extension can in fact be chosen to be a Galois extension, which enables us to exploit a powerful theory in our further investigations, that of Galois descent. Using descent we can give elegant treatments of such classical topics as the construction of reduced norms or the Skolem-Noether theorem. The main invariant concerning central simple algebras is the Brauer group which classifies all finite dimensional central division algebras over a field. Using Galois descent, we shall identify it with a certain first cohomology set equipped with an abelian group structure.

The foundations of the theory of central simple algebras go back to the great algebraists of the dawn of the 20th century; we merely mention here the names of Wedderburn, Dickson and Emmy Noether. The Brauer group appears in the pioneering paper of the young Richard Brauer [1]. Though Galois descent had been implicitly used by algebraists in the early years of the 20th century and Châtelet had considered special cases in connection with Diophantine equations, it was André Weil who first gave a systematic treatment with applications to algebraic geometry in mind (Weil [2]). The theory in the form presented below was developed by Jean-Pierre Serre, and finally found a tantalizing generalisation in the general descent theory of Grothendieck ([1], [2]).

2.1 Wedderburn's Theorem

Let k be a field. We assume throughout that all k -algebras under consideration are finite dimensional over k . A k -algebra A is called *simple* if it has

no (two-sided) ideal other than 0 and A . Recall moreover from the previous chapter that A is *central* if its center equals k .

Here are the basic examples of central simple algebras.

Example 2.1.1 A division algebra over k is obviously simple. Its center is a field (indeed, inverting the relation $xy = yx$ gives $y^{-1}x^{-1} = x^{-1}y^{-1}$ for all $y \in D, x \in Z(D)$). Hence D is a central simple algebra over $Z(D)$.

As concrete examples (besides fields), we may cite nonsplit quaternion algebras: these are central over k by definition and division algebras by Proposition 1.1.7.

The next example shows that split quaternion algebras are also simple.

Example 2.1.2 If D is a division algebra over k , the ring $M_n(D)$ of $n \times n$ matrices over D is simple for all $n \geq 1$. Checking this is an exercise in matrix theory. Indeed, we have to show that the two-sided ideal $\langle M \rangle$ in $M_n(D)$ generated by a nonzero matrix M is $M_n(D)$ itself. Consider the matrices E_{ij} having 1 as the j -th element of the i -th row and zero elsewhere. Since each element of $M_n(D)$ is a D -linear combination of the E_{ij} , it suffices to show that $E_{ij} \in \langle M \rangle$ for all i, j . But in view of the relation $E_{ki}E_{ij}E_{jl} = E_{kl}$ we see that it is enough to show $E_{ij} \in \langle M \rangle$ for *some* i, j . Now choose i, j so that the j -th element in the i -th row of M is a nonzero element m . Then $m^{-1}E_{ii}ME_{jj} = E_{ij}$, and we are done.

Noting the easy fact that in a matrix ring the center can only contain scalar multiples of the identity matrix, we get that $M_n(D)$ is a central simple algebra over $Z(D)$.

The main theorem on simple algebras over a field provides a converse to the above example.

Theorem 2.1.3 (Wedderburn) *Let A be a finite dimensional simple algebra over a field k . Then there exist an integer $n \geq 1$ and a division algebra $D \supset k$ so that A is isomorphic to the matrix ring $M_n(D)$. Moreover, the division algebra D is uniquely determined up to isomorphism.*

The proof will follow from the next two lemmas. Before stating them, let us recall some basic facts from module theory. First, a nonzero A -module M is *simple* if it has no A -submodules other than 0 and M .

Example 2.1.4 Let us describe the simple left modules over $M_n(D)$, where D is a division algebra. For all $1 \leq r \leq n$, consider the subring $I_r \subset M_n(D)$ formed by matrices $M = [m_{ij}]$ with $m_{ij} = 0$ for $j \neq r$. These

are left ideals in $M_n(D)$ and a simple argument with the matrices E_{ij} of Example 2.1.2 shows that they are also *minimal* with respect to inclusion, i.e. simple $M_n(D)$ -modules. Moreover, we have $M_n(D) = \bigoplus I_r$ and the I_r are all isomorphic as $M_n(D)$ -modules. Finally, if M is a simple $M_n(D)$ -module, it must be a quotient of $M_n(D)$, but then the induced map $\bigoplus I_r \rightarrow M$ must induce an isomorphism with some I_r . Thus all simple left $M_n(D)$ -modules are isomorphic to (say) I_1 .

Next, an *endomorphism* of a left A -module M over a ring A is an A -homomorphism $M \rightarrow M$; these form a ring $\text{End}_A(M)$ where addition is given by the rule $(\phi + \psi)(x) = \phi(x) + \psi(x)$ and multiplication by composition of maps. If A is a k -algebra, then so is $\text{End}_A(M)$, for multiplication by an element of k defines an element in the center of $\text{End}_A(M)$. In the case when A is a division algebra, M is a left vector space over A , so the usual argument from linear algebra shows that choosing a basis of M induces an isomorphism $\text{End}_A(M) \cong M_n(A)$, where n is the dimension of M over A .

The module M is equipped with a left module structure over $\text{End}_A(M)$, multiplication being given by the rule $\phi \cdot x = \phi(x)$ for $x \in M, \phi \in \text{End}_A(M)$.

Lemma 2.1.5 (Schur) *Let M be a simple module over a k -algebra A . Then $\text{End}_A(M)$ is a division algebra.*

Proof: The kernel of a nonzero endomorphism $M \rightarrow M$ is an A -submodule different from M , hence it is 0. Similarly, its image must be the whole of M . Thus it is an isomorphism, which means it has an inverse in $\text{End}_A(M)$. \square

Now let M be a left A -module with endomorphism ring $D = \text{End}_A(M)$. As remarked above, M is naturally a left D -module, hence one may also consider the endomorphism ring $\text{End}_D(M)$. One defines a ring homomorphism $\lambda_M : A \rightarrow \text{End}_D(M)$ by sending $a \in A$ to the endomorphism $x \mapsto ax$ of M . This is indeed a D -endomorphism, for if $\phi : M \rightarrow M$ is an element of D , one has $\phi \cdot ax = \phi(ax) = a\phi(x) = a\phi \cdot x$ for all $x \in M$.

Lemma 2.1.6 (Rieffel) *Let L be a nonzero left ideal in a simple k -algebra A , and put $D = \text{End}_A(L)$. Then the map $\lambda_L : A \rightarrow \text{End}_D(L)$ defined above is an isomorphism.*

Note that in a ring A a left ideal is none but a submodule of the left A -module A .

Proof: Since $\lambda_L \neq 0$, its kernel is a proper two-sided ideal of A . But A is simple, so λ_L is injective. For surjectivity, we show first that $\lambda_L(L)$ is a left ideal in $\text{End}_D(L)$. Indeed, let $\phi \in \text{End}_D(L)$ and $l \in L$. Then $\phi \cdot \lambda_L(l)$ is the map $x \mapsto \phi(lx)$. But for all $x \in L$, the map $y \mapsto yx$ is an A -endomorphism of L , i.e. an element of D . As ϕ is a D -endomorphism, we have $\phi(lx) = \phi(l)x$, and so $\phi \cdot \lambda_L(l) = \lambda_L(\phi(l))$.

Now observe that the right ideal LA generated by L is a two-sided ideal, hence $LA = A$. In particular, we have $1 = \sum l_i a_i$ with $l_i \in L$, $a_i \in A$. Hence for $\phi \in \text{End}_D(L)$ we have $\phi = \phi \cdot 1 = \phi \lambda_L(1) = \sum \phi \lambda_L(l_i) \lambda_L(a_i)$. But since $\lambda_L(L)$ is a left ideal, we have here $\phi \lambda_L(l_i) \in \lambda_L(L)$ for all i , and thus $\phi \in \lambda_L(A)$. \square

Proof of Theorem 2.1.3: As A is finite dimensional, a descending chain of left ideals must stabilize. So let L be a minimal left ideal; it is then a simple A -module. By Schur's lemma, $D = \text{End}_A(L)$ is a division algebra, and by Rieffel's lemma we have an isomorphism $A \cong \text{End}_D(L)$. The discussion before Lemma 2.1.5 then yields an isomorphism $\text{End}_D(L) \cong M_n(D)$, where n is the dimension of L over D (it is finite as L is already finite dimensional over k).

For the unicity statement, assume that D and D' are division algebras for which $A \cong M_n(D) \cong M_m(D')$ with suitable integers n, m . By Example 2.1.4, the minimal left ideal L then satisfies $D^n \cong L \cong D'^m$, whence a chain of isomorphisms $D \cong \text{End}_A(D^n) \cong \text{End}_A(L) \cong \text{End}_A(D'^m) \cong D'$. \square

Corollary 2.1.7 *Let k be an algebraically closed field. Then every central simple k -algebra is isomorphic to $M_n(k)$ for some $n \geq 1$.*

Proof: By the theorem it is enough to see that there is no finite dimensional division algebra $D \supset k$ other than k . For this, let d be an element of $D \setminus k$. As in the proof of Corollary 1.2.1 we see that there is an irreducible polynomial $f \in k[x]$ and a k -algebra homomorphism $k[x]/(f) \rightarrow D$ whose image contains d . But k being algebraically closed, we have $k[x]/(f) \cong k$. \square

2.2 Splitting Fields

The last corollary enables one to give an alternative characterisation of central simple algebras.

Theorem 2.2.1 *Let k be a field and A a finite dimensional k -algebra. Then A is a central simple algebra if and only if there exist an integer $n > 0$ and a finite field extension $K|k$ so that $A \otimes_k K$ is isomorphic to the matrix ring $M_n(K)$.*

We first prove:

Lemma 2.2.2 *Let A be a finite dimensional k -algebra, and $K|k$ a finite field extension. The algebra A is central simple over k if and only if $A \otimes_k K$ is central simple over K .*

Proof: If I is a nontrivial (two-sided) ideal of A , then $I \otimes_k K$ is a nontrivial ideal of $A \otimes_k K$ (e.g. for dimension reasons); similarly, if A is not central, then neither is $A \otimes_k K$. Thus if $A \otimes_k K$ is central simple, then so is A .

Using Wedderburn's theorem, for the converse it will be enough to consider the case when $A = D$ is a division algebra. Under this assumption, if w_1, \dots, w_n is a k -basis of K , then $1 \otimes w_1, \dots, 1 \otimes w_n$ yields a D -basis of $D \otimes_k K$ as a left D -vector space. Given an element $x = \sum \alpha_i (1 \otimes w_i)$ in the center of $D \otimes_k K$, for all $d \in D$ the relation $x = (d^{-1} \otimes 1)x(d \otimes 1) = \sum (d^{-1} \alpha_i d)(1 \otimes w_i)$ implies $d^{-1} \alpha_i d = \alpha_i$ by the linear independence of the $1 \otimes w_i$. As D is central over k , the α_i must lie in k , so $D \otimes_k K$ is central over K . Now if J is a nonzero ideal in $D \otimes_k K$ generated by elements z_1, \dots, z_r , we may assume the z_i to be D -linearly independent and extend them to a D -basis of $D \otimes_k K$ by adjoining some of the $1 \otimes w_i$, say $1 \otimes w_{r+1}, \dots, 1 \otimes w_n$. Thus for $1 \leq i \leq r$ we may write

$$1 \otimes w_i = \sum_{j=r+1}^n \alpha_{ij} (1 \otimes w_j) + y_i,$$

where y_i is some D -linear combination of the z_i and hence an element of J . Here y_1, \dots, y_r are D -linearly independent (because so are $1 \otimes w_1, \dots, 1 \otimes w_r$), so they form a D -basis of J . As J is a two-sided ideal, for all $d \in D$ we must have $d^{-1} y_i d \in J$ for $1 \leq i \leq r$, so there exist $\beta_{il} \in D$ with $d^{-1} y_i d = \sum \beta_{il} y_l$. We may rewrite this relation as

$$(1 \otimes w_i) - \sum_{j=r+1}^n (d^{-1} \alpha_{ij} d)(1 \otimes w_j) = \sum_{l=1}^r \beta_{il} (1 \otimes w_l) - \sum_{l=1}^r \beta_{il} \sum_{j=r+1}^n \alpha_{lj} (1 \otimes w_j),$$

from which we get as above, using the independence of the $1 \otimes w_j$, that $\beta_{ii} = 1$, $\beta_{il} = 0$ for $l \neq i$ and $d^{-1} \alpha_{ij} d = \alpha_{ij}$, i.e. $\alpha_{ij} \in k$ as D is central. This means that J can be generated by elements of K (viewed as a k -subalgebra of $D \otimes_k K$ via the embedding $w \mapsto 1 \otimes w$). As K is a field, we must have $J \cap K = K$, so $J = D \otimes_k K$. This shows that $D \otimes_k K$ is simple. \square

Proof of Theorem 2.2.1: Sufficiency follows from the above lemma and Example 2.1.2. For necessity, note first that denoting by \bar{k} an algebraic closure of k , the lemma together with Corollary 2.1.7 imply that $A \otimes_k \bar{k} \cong M_n(\bar{k})$ for some n . Now observe that for every finite field extension K of k

contained in \bar{k} , the inclusion $K \subset \bar{k}$ induces an injective map $A \otimes_k K \rightarrow A \otimes_k \bar{k}$ and $A \otimes_k \bar{k}$ arises as the union of the $A \otimes_k K$ in this way. Hence for a sufficiently large finite extension $K|k$ contained in \bar{k} the algebra $A \otimes_k K$ contains the elements $e_1, \dots, e_{n^2} \in A \otimes_k \bar{k}$ corresponding to the standard basis elements of $M_n(\bar{k})$ via the isomorphism $A \otimes_k \bar{k} \cong M_n(\bar{k})$, and moreover the elements a_{ij} occurring in the relations $e_i e_j = \sum a_{ij} e_i$ defining the product operation are also contained in K . Mapping the e_i to the standard basis elements of $M_n(K)$ then induces a K -isomorphism $A \otimes_k K \cong M_n(K)$. \square

Corollary 2.2.3 *If A is a central simple k -algebra, its dimension over k is a square.*

Definition 2.2.4 A field extension $K|k$ over which $A \otimes_k K$ is isomorphic to $M_n(K)$ for suitable n is called a *splitting field* for A . We shall also employ the terminology *A splits over K* or *K splits A* .

The integer $\sqrt{\dim_k A}$ is called the *degree* of A .

The following proposition, though immediate in the case of a perfect base field, is crucial for our considerations to come.

Proposition 2.2.5 (Noether, Köthe) *A central simple k -algebra has a splitting field separable over k .*

Proof: Assume there exists a central simple k -algebra A which does not split over any finite separable extension $K|k$. Fix separable and algebraic closures $k^s \subset \bar{k}$ of k . By the same argument as at the end of the proof of Theorem 2.2.1, the k^s -algebra $A \otimes_k k^s$ does not split over k^s , hence by Wedderburn's theorem it is isomorphic to some matrix algebra $M_n(D)$, where D is a division algebra over k^s different from k^s . Let $d > 1$ be the dimension of D over k^s . Then by Corollary 2.1.7 we have $D \otimes_{k^s} \bar{k} \cong M_d(\bar{k})$. Regarding the elements of $M_d(\bar{k})$ as \bar{k} -points of affine d^2 -space \mathbf{A}^{d^2} , elements of D correspond to the points of \mathbf{A}^{d^2} defined over k^s . As D is a division algebra, its nonzero elements give rise to invertible matrices in $M_d(\bar{k})$; in particular, they have nonzero determinant. Now the map which sends an element of $M_d(\bar{k})$ viewed as a point of $\mathbf{A}^{d^2}(\bar{k})$ to its determinant is given by a polynomial P in the variables x_1, \dots, x_{d^2} ; note that $P \in k^s[x_1, \dots, x_{d^2}]$ as its coefficients are all 1 or -1 . Hence our assumption means that the hypersurface $H \subset \mathbf{A}^{d^2}$ defined by the vanishing of P contains no points defined over k^s except for the origin. But this contradicts the basic fact from algebraic geometry (see Appendix, Proposition A.1.1) according to which in an algebraic variety defined over a separably closed field k^s the points defined over k^s form a Zariski dense subset; indeed, such a subset is infinite if the variety has positive dimension. \square

Corollary 2.2.6 *A finite dimensional k -algebra A is a central simple algebra if and only if there exist an integer $n > 0$ and a finite Galois field extension $K|k$ so that $A \otimes_k K$ is isomorphic to the matrix ring $M_n(K)$.*

Proof: This follows from Theorem 2.2.1, Proposition 2.2.5 and the well-known fact from Galois theory according to which every finite separable field extension embeds into a finite Galois extension. \square

Remarks 2.2.7

1. It is important to bear in mind that if A is a central simple k -algebra of degree n which does not split over k but splits over a finite Galois extension $K|k$ with group G , then the isomorphism $A \otimes_k K \cong M_n(K)$ is *not* G -equivariant if we equip $M_n(K)$ with the usual action of G coming from its action on K . Indeed, were it so, we would get an isomorphism $A \cong M_n(k)$ by taking G -invariants.
2. In traditional accounts, Proposition 2.2.5 is proven by showing that the separable splitting field can actually be chosen among the field extensions of k that are k -subalgebras of A . We shall prove this stronger fact later in Proposition 4.5.4. However, it is not always possible to realize a Galois splitting field in such a way, as shown by a famous counterexample by Amitsur (see Amitsur [2] or Pierce [1]; see also Brussel [1] for counterexamples over $\mathbf{Q}(t)$ and $\mathbf{Q}((t))$). Central simple algebras containing a Galois splitting field are called *crossed products* in the literature.

We finally discuss a method for finding Galois splitting fields among k -subalgebras of A . The basic idea is contained in the following splitting criterion, inspired by the theory of maximal tori in reductive groups.

Proposition 2.2.8 *A central simple algebra A of degree n over a field k is split if and only if it contains a k -subalgebra isomorphic to the direct product $k^n = k \times \cdots \times k$.*

For the proof we need a well-known property of matrix algebras.

Lemma 2.2.9 *The k -subalgebras in $M_n(k)$ that are isomorphic to k^n are conjugate to the subalgebra of diagonal matrices.*

Proof: Giving a k -subalgebra isomorphic to k^n is equivalent to specifying n elements e_1, \dots, e_n that form a system of orthogonal idempotents, i.e. satisfy $e_i^2 = 1$ for all i and $e_i e_j = 0$ for $i \neq j$. Identifying $M_n(k)$ with the endomorphism algebra of an n -dimensional k -vector space V , we may regard the e_i as projections to 1-dimensional subspaces V_i in a direct product decomposition $V = V_1 \oplus \dots \oplus V_n$ of V . Choosing a vector space isomorphism $V \cong k^n$ sending V_i to the i -th component of $k^n = k \oplus \dots \oplus k$ gives rise to the required conjugation. \square

Proof of Proposition 2.2.8: Of course $M_n(k)$ contains subalgebras isomorphic to k^n , whence the necessity of the condition. Conversely, assume given a k -algebra embedding $i : k^n \rightarrow A$, and let e_1, \dots, e_n be the images of the standard basis elements of k^n . By Rieffel's Lemma it will be enough to show that Ae_1 is a simple left A -module and that the natural map $k \rightarrow \text{End}_A(Ae_1)$ is an isomorphism. If k is algebraically closed, then $A \cong M_n(k)$ by Corollary 2.1.7. Lemma 2.2.9 then enables us to assume that i is the standard diagonal embedding $k^n \subset M_n(k)$, for which the claim is straightforward. If k is not algebraically closed, we pass to an algebraic closure and deduce the result by dimension reasons. \square

Corollary 2.2.10 *Let A be a central simple k -algebra containing a commutative k -subalgebra K which is a Galois field extension of k of degree n . Then K is a splitting field for A .*

Proof: By Galois theory, the K -algebra $K \otimes_k K$ is isomorphic to K^n (see the discussion after the statement of Lemma 2.3.8 below), and thus is a K -subalgebra of $A \otimes_k K$ to which the proposition applies. \square

2.3 Galois Descent

Corollary 2.2.6 makes it possible to classify central simple algebras using methods of Galois theory. Here we present such a method, known as *Galois descent*.

We shall work in a more general context, that of *vector spaces V equipped with a tensor Φ of type (p, q)* . By definition, Φ is an element of the tensor product $V^{\otimes p} \otimes_k (V^*)^{\otimes q}$, where $p, q \geq 0$ are integers and V^* is the dual space $\text{Hom}_k(V, k)$. Note the natural isomorphism

$$V^{\otimes p} \otimes_k (V^*)^{\otimes q} \cong \text{Hom}_k(V^{\otimes q}, V^{\otimes p})$$

coming from the general formula $\text{Hom}_k(V, k) \otimes_k W \cong \text{Hom}_k(V, W)$.

Examples 2.3.1 The following special cases will be the most important for us:

- The trivial case $\Phi = 0$ (with any p, q). This is just V with no additional structure.
- $p = 1, q = 1$. In this case Φ is given by a k -linear endomorphism of V .
- $p = 0, q = 2$. Then Φ is the tensor product of two k -linear functions, i.e. a k -bilinear form $V \otimes_k V \rightarrow k$.
- $p = 1, q = 2$. This case corresponds to a k -bilinear map $V \otimes_k V \rightarrow V$.

Note that the theory of associative algebras is contained in the last example, for the multiplication in such an algebra A is given by a k -bilinear map $A \otimes_k A \rightarrow A$ satisfying the associativity condition.

So consider pairs (V, Φ) of k -vector spaces equipped with a tensor of fixed type (p, q) as above. A k -isomorphism between two such objects (V, Φ) and (W, Ψ) is given by a k -isomorphism $f : V \xrightarrow{\sim} W$ of k -vector spaces such that $f^{\otimes q} \otimes (f^{*-1})^{\otimes p} : V^{\otimes p} \otimes_k (V^*)^{\otimes q} \rightarrow W^{\otimes p} \otimes_k (W^*)^{\otimes q}$ maps Φ to Ψ . Here $f^* : W^* \xrightarrow{\sim} V^*$ is the k -isomorphism induced by f .

Now fix a finite Galois extension $K|k$ with Galois group $G = \text{Gal}(K|k)$. Denote by V_K the K -vector space $V \otimes_k K$ and by Φ_K the tensor induced on V_K by Φ . In this way we associate with (V, Φ) a K -object (V_K, Φ_K) . We say that (V, Φ) and (W, Ψ) become isomorphic over K if there exists a K -isomorphism between (V_K, Φ_K) and (W_K, Ψ_K) . In this situation, (W, Ψ) is also called a $(K|k)$ -twisted form of (V, Φ) or a twisted form for short.

Now Galois theory enables one to classify k -isomorphism classes of twisted forms as follows. Given a k -automorphism $\sigma : K \rightarrow K$, tensoring by V gives a k -automorphism $V_K \rightarrow V_K$ which we again denote by σ . Each K -linear map $f : V_K \rightarrow W_K$ induces a map $\sigma(f) : V_K \rightarrow W_K$ defined by $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$. If f is a K -isomorphism from (V_K, Φ_K) to (W_K, Ψ_K) , then so is $\sigma(f)$. The map $f \rightarrow \sigma(f)$ preserves composition of automorphisms, hence we get a left action of $G = \text{Gal}(K|k)$ on the group $\text{Aut}_K(\Phi)$ of K -automorphisms of (V_K, Φ_K) . Moreover, given two k -objects (V, Φ) and (W, Ψ) as well as a K -isomorphism $g : (V_K, \Phi_K) \xrightarrow{\sim} (W_K, \Psi_K)$, one gets a map $G \rightarrow \text{Aut}_K(\Phi)$ associating $a_\sigma = g^{-1} \circ \sigma(g)$ to $\sigma \in G$. The map a_σ satisfies the fundamental relation

$$a_{\sigma\tau} = a_\sigma \cdot \sigma(a_\tau) \quad \text{for all } \sigma, \tau \in G. \quad (1)$$

Indeed, we compute

$$a_{\sigma\tau} = g^{-1} \circ \sigma(\tau(g)) = g^{-1} \circ \sigma(g) \circ \sigma(g^{-1}) \circ \sigma(\tau(g)) = a_\sigma \cdot \sigma(a_\tau).$$

Next, let $h : (V_K, \Phi_K) \xrightarrow{\sim} (W_K, \Psi_K)$ be another K -isomorphism, defining $b_\sigma := h^{-1} \circ \sigma(h)$ for $\sigma \in G$. Then a_σ and b_σ are related by

$$a_\sigma = c^{-1} b_\sigma \sigma(c), \quad (2)$$

where c is the K -automorphism $h^{-1} \circ g$. We abstract this in a general definition:

Definition 2.3.2 Let G be a group and A another (not necessarily commutative) group on which G acts on the left, i.e. there is a map $(\sigma, a) \rightarrow \sigma(a)$ satisfying $\sigma(ab) = \sigma(a)\sigma(b)$ and $\sigma\tau(a) = \sigma(\tau(a))$ for all $\sigma, \tau \in G$ and $a, b \in A$. Then a *1-cocycle* of G with values in A is a map $\sigma \mapsto a_\sigma$ from G to A satisfying the relation (1) above. Two 1-cocycles a_σ and b_σ are called *equivalent* or *cohomologous* if there exists $c \in A$ such that the relation (2) holds.

One defines the *first cohomology set* $H^1(G, A)$ of G with values in A as the quotient of the set of 1-cocycles by the equivalence relation (2). It is a *pointed set*, i.e. a set equipped with a distinguished element coming from the trivial cocycle $\sigma \mapsto 1$, where 1 is the identity element of A . We call this element the *base point*.

In our concrete situation, we see that the class $[a_\sigma]$ in $H^1(G, \text{Aut}_K(\Phi))$ of the 1-cocycle a_σ associated with the K -isomorphism $g : (V_K, \Phi_K) \xrightarrow{\sim} (W_K, \Psi_K)$ depends only on (W, Ψ) but not on the map g . This enables us to state the main theorem of this section.

Theorem 2.3.3 *For a k -object (V, Φ) consider the pointed set $TF_K(V, \Phi)$ of twisted $(K|k)$ -forms of (V, Φ) , the base point being given by (V, Φ) . Then the map $(W, \Psi) \rightarrow [a_\sigma]$ defined above yields a base point preserving bijection*

$$TF_K(V, \Phi) \leftrightarrow H^1(G, \text{Aut}_K(\Phi)).$$

Before proving the theorem, we give some immediate examples, leaving the main application (that to central simple algebras) to the next section.

Example 2.3.4 (Hilbert's Theorem 90) Consider first the case when V has dimension n over k and Φ is the trivial tensor. Then $\text{Aut}_K(\Phi)$ is just the group $\text{GL}_n(K)$ of invertible $n \times n$ matrices. On the other hand, two n -dimensional vector k -spaces that are isomorphic over K are isomorphic already over k , so we get:

$$H^1(G, \text{GL}_n(K)) = \{1\}. \quad (3)$$

This statement is due to Speiser. The case $n = 1$ is usually called Hilbert's Theorem 90 in the literature, though Hilbert only considered the case when

$K|k$ is a cyclic extension of degree n . In this case, denoting by σ a generator of $G = \text{Gal}(K|k)$, every 1-cocycle is determined by its value a_σ on σ . Applying the cocycle relation (1) inductively we get $a_{\sigma^i} = a_\sigma \sigma(a_\sigma) \dots \sigma^{i-1}(a_\sigma)$ for all $1 \leq i \leq n$. In particular, for $i = n$ we get $a_\sigma \sigma(a_\sigma) \dots \sigma^{n-1}(a_\sigma) = a_1 = 1$ (here the second equality again follows from the cocycle relation applied with $\sigma = \tau = 1$). But $a_\sigma \sigma(a_\sigma) \dots \sigma^{n-1}(a_\sigma)$ is by definition the norm of a_σ for the extension $K|k$. Now formula (3) together with the coboundary relation (2) imply the original form of Hilbert's Theorem 90:

In a cyclic field extension $K|k$ with $\text{Gal}(K|k) = \langle \sigma \rangle$ each element of norm 1 is of the form $\sigma(c)c^{-1}$ with some $c \in K$.

Example 2.3.5 (Quadratic forms) As another example, assume k is of characteristic different from 2, and take V to be n -dimensional and Φ a tensor of type (0,2) coming from a nondegenerate symmetric bilinear form \langle, \rangle on V . Then $\text{Aut}_K(\Phi)$ is the group $O_n(K)$ of orthogonal matrices with respect to \langle, \rangle and we get from the theorem that there is a base point preserving bijection

$$TF_K(V, \langle, \rangle) \leftrightarrow H^1(G, O_n(K)).$$

This bijection is important for the classification of quadratic forms.

To prove the theorem, we construct an inverse to the map $(W, \Psi) \mapsto [a_\sigma]$. This is based on the following general construction.

Construction 2.3.6 Let A be a group equipped with a left action by another group G . Suppose further that X is a set on which both G and A act in a compatible way, i.e. we have $\sigma(a(x)) = (\sigma(a))(\sigma(x))$ for all $x \in X$, $a \in A$ and $\sigma \in G$. Assume finally given a 1-cocycle $\sigma \mapsto a_\sigma$ of G with values in A . Then we define the *twisted action of G on X by the cocycle a_σ* via the rule

$$(\sigma, x) \mapsto a_\sigma(\sigma(x)).$$

This is indeed a G -action, for the cocycle relation yields

$$a_{\sigma\tau}(\sigma\tau(x)) = a_\sigma \sigma(a_\tau)(\sigma\tau(x)) = a_\sigma \sigma(a_\tau \tau(x)).$$

If X is equipped with some algebraic structure (e.g. it is a group or a vector space), and G and A act on it by automorphisms, then the twisted action is also by automorphisms. The notation ${}_a X$ will mean X equipped with the twisted G -action by the cocycle a_σ .

Remark 2.3.7 Readers should be warned that the above construction can only be carried out on the level of cocycles and *not* on that of cohomology

classes: equivalent cocycles give rise to different twisted actions in general. For instance, take $G = \text{Gal}(K|k)$, $A = X = \text{GL}_n(K)$, acting on itself by inner automorphisms. Then twisting the usual G -action on $\text{GL}_n(K)$ by the trivial cocycle $\sigma \mapsto 1$ does not change anything, whereas if $\sigma \mapsto a_\sigma$ is a 1-cocycle with a_σ a noncentral element for some σ , then $a_\sigma^{-1}\sigma(x)a_\sigma \neq \sigma(x)$ for a noncentral x , so the twisted action is different. But a 1-cocycle $G \rightarrow \text{GL}_n(K)$ is equivalent to the trivial cocycle by Example 2.3.4.

Now the idea is to take a cocycle a_σ representing some cohomology class in $H^1(G, \text{Aut}_K(\Phi))$ and to apply the above construction with $G = \text{Gal}(K|k)$, $A = \text{Aut}_K(\Phi)$ and $X = V_K$. The main point is then to prove that taking the invariant subspace $({}_aV_K)^G$ under the twisted action of G yields a twisted form of (V, Φ) .

We show this first when Φ is trivial (i.e. we in fact prove Hilbert's Theorem 90). The statement to be checked then boils down to:

Lemma 2.3.8 (Speiser) *Let $K|k$ be a finite Galois extension with group G and V a K -vector space equipped with a semi-linear G -action, i.e. a G -action satisfying*

$$\sigma(\lambda v) = \sigma(\lambda)\sigma(v) \quad \text{for all } \sigma \in G, v \in V \text{ and } \lambda \in K.$$

Then the natural map

$$\lambda : V^G \otimes_k K \rightarrow V$$

is an isomorphism, where the superscript G denotes invariants under G .

Before proving the lemma, let us recall a consequence of Galois theory. Let $K|k$ be a Galois extension as in the lemma, and consider two copies of K , the first one equipped with trivial G -action, and the second one with the action of G as the Galois group. Then the tensor product $K \otimes_k K$ (endowed with the G -action given by $\sigma(a \otimes b) \cong a \otimes \sigma(b)$) decomposes as a direct sum of copies of K :

$$K \otimes_k K \cong \bigoplus_{\sigma \in G} Ke_\sigma,$$

where G acts on the right hand side by permuting the basis elements e_σ . To see this, write $K = k[x]/(f)$ with f some monic irreducible polynomial $f \in k[x]$, and choose a root α of f in K . As $K|k$ is Galois, f splits in $K[x]$ as a product of linear terms of the form $(x - \sigma(\alpha))$ for $\sigma \in G$. Thus using a special case of the Chinese Remainder Theorem for rings (which is easy to prove directly) we get

$$K \otimes_k K \cong K[x]/(f) \cong K[x]/\left(\prod_{\sigma \in G} (x - \sigma(\alpha))\right) \cong \bigoplus_{\sigma \in G} K[x]/(x - \sigma(\alpha)),$$

whence a decomposition of the required form.

Proof: Consider the tensor product $V \otimes_k K$, where the second factor K carries trivial G -action and V the G -action of the lemma. It will be enough to prove that the map $\lambda_K : (V \otimes_k K)^G \otimes_k K \rightarrow V \otimes_k K$ is an isomorphism. Indeed, by our assumption about the G -actions we have $(V \otimes_k K)^G \cong V^G \otimes_k K$, and hence we may identify λ_K with the map $(V^G \otimes_k K) \otimes_k K \rightarrow V \otimes_k K$ obtained by tensoring with K . Therefore if λ had a nontrivial kernel A (resp. a nontrivial cokernel B), then λ_K would have a nontrivial kernel $A \otimes_k K$ (resp. a nontrivial cokernel $B \otimes_k K$).

Now by the Galois-theoretic fact recalled above, the $K \otimes_k K$ -module $V \otimes_k K$ decomposes as a direct sum $V \otimes_k K \cong \bigoplus W e_\sigma$, with $\sigma(e_1) = e_\sigma$ for $\sigma \in G$. It follows that $(V \otimes_k K)^G = W e_1$, whence we derive the required isomorphism $(V \otimes_k K)^G \otimes_k K \cong \bigoplus W e_\sigma \cong V \otimes_k K$. \square

Remark 2.3.9 We could have argued directly for λ , by remarking that K decomposes as a product $K = \bigoplus k e_\sigma$ with $\sigma(e_1) = e_\sigma$ according to the normal basis theorem of Galois theory. The above proof, inspired by flat descent theory, avoids the use of this nontrivial theorem.

Proof of Theorem 2.3.3: As indicated above, we take a 1-cocycle a_σ representing some cohomology class in $H^1(G, \text{Aut}_K(\Phi))$ and consider the invariant subspace $W := ({}_a V_K)^G$. Next observe that $\sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$ (as Φ_K comes from the k -tensor Φ) and also $a_\sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$ (as $a_\sigma \in \text{Aut}_K(\Phi)$). Hence $a_\sigma \sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$, which means that Φ_K comes from a k -tensor on W . Denoting this tensor by Ψ , we have defined a k -object (W, Ψ) . Speiser's lemma yields an isomorphism $W \otimes_k K \cong V_K$, and by construction this isomorphism identifies Ψ_K with Φ_K . Thus (W, Ψ) is indeed a twisted form of (V, Φ) . If $a_\sigma = c^{-1} b_\sigma \sigma(c)$ with some 1-cocycle $\sigma \mapsto b_\sigma$ and $c \in \text{Aut}_K(\Phi)$, we get from the definitions $({}_b V_K)^G = c(W)$, which is a k -vector space isomorphic to W . To sum up, we have a well-defined map $H^1(G, \text{Aut}_K(\Phi)) \rightarrow TF_K(V, \Phi)$. The kind reader will check that this map is the inverse of the map $(W, \Psi) \mapsto [a_\sigma]$ of the theorem. \square

Remark 2.3.10 There is an obvious variant of the above theory, where instead of a single tensor Φ one considers a whole family of tensors on V . The K -automorphisms to be considered are then those preserving all tensors in the family, and twisted forms are vector spaces W isomorphic to V over K such that the family of tensors on W_K goes over to that on V_K via the K -isomorphism. The descent theorem in this context is stated and proven in the same way as Theorem 2.3.3.

2.4 The Brauer Group

Now we come to the classification of central simple algebras. First we recall a well-known fact about matrix rings:

Lemma 2.4.1 *Over a field K all automorphisms of the matrix ring $M_n(K)$ are inner, i.e. given by $M \mapsto CMC^{-1}$ for some invertible matrix C .*

Proof: Consider the minimal left ideals I_r of $M_n(K)$ described in Example 2.1.4. They are permuted by each automorphism $\lambda \in \text{Aut}(M_n(K))$. Replacing λ by a conjugate with a suitable matrix E_{ij} (see Example 2.1.2), we may actually assume $\lambda(I_1) = I_1$. Let e_1, \dots, e_n be the standard basis of K^n . Mapping a matrix $M \in I_1$ to Me_1 induces an isomorphism $I_1 \cong K^n$ of K -vector spaces, and thus λ induces an automorphism of K^n . As such, it is given by an invertible matrix C . We get that for all $M \in M_n(K)$, the endomorphism of K^n defined in the standard basis by $\lambda(M)$ has matrix CMC^{-1} , whence the lemma. \square

Corollary 2.4.2 *The automorphism group of $M_n(K)$ is the projective general linear group $\text{PGL}_n(K)$.*

Proof: There is a natural homomorphism $\text{GL}_n(K) \rightarrow \text{Aut}(M_n(K))$ mapping $C \in \text{GL}_n(K)$ to the automorphism $A \mapsto CAC^{-1}$. It is surjective by the lemma, and its kernel consists of the center of $\text{GL}_n(K)$, i.e. the subgroup of scalar matrices. \square

Now take a finite Galois extension $K|k$ as before, and let $CSA_K(n)$ denote the set of k -isomorphism classes of central simple k -algebras of degree n split by K . We regard it as a pointed set, the base point being the class of the matrix algebra $M_n(k)$.

Theorem 2.4.3 *There is a base point preserving bijection*

$$CSA_K(n) \leftrightarrow H^1(G, \text{PGL}_n(K)).$$

Proof: By Corollary 2.2.6 the central simple k -algebras of degree n are precisely the twisted forms of the matrix algebra $M_n(k)$. To see this, note that as explained in Example 2.3.1, an n^2 -dimensional k -algebra can be considered as an n^2 -dimensional k -vector space equipped with a tensor of type (1,2) satisfying the associativity condition. But on a twisted form of $M_n(k)$ the tensor defining the multiplication automatically satisfies the associativity condition. Hence Theorem 2.3.3 applies and yields a bijection of pointed sets

$CSA_K(n) \leftrightarrow H^1(G, \text{Aut}(M_n(K)))$. The theorem now follows by Corollary 2.4.2. \square

Our next goal is to classify all central simple k -algebras split by K by means of a single cohomology set. This should then carry a product operation, for tensor product induces a natural commutative and associative product operation on the set of isomorphism classes of central simple algebras, as shown by the following lemma.

Lemma 2.4.4 *If A and B are central simple k -algebras split by K , then so is $A \otimes_k B$.*

Proof: In view of the isomorphism $(A \otimes_k K) \otimes_K (B \otimes_k K) \cong (A \otimes_k B) \otimes_k K$ and Theorem 2.2.1, it is enough to verify the isomorphism of matrix algebras $M_n(K) \otimes_K M_m(K) \cong M_{nm}(K)$. This was done in Lemma 1.5.1. \square

By the lemma, we have a product operation

$$CSA_K(n) \times CSA_K(m) \rightarrow CSA_K(mn)$$

induced by the tensor product. Via the bijection of Theorem 2.4.3, this should correspond to a product operation

$$H^1(G, \text{PGL}_n(K)) \times H^1(G, \text{PGL}_m(K)) \rightarrow H^1(G, \text{PGL}_{nm}(K)) \quad (4)$$

on cohomology sets. To define this product directly, note that the map

$$\text{End}_K(K^n) \otimes \text{End}_K(K^m) \rightarrow \text{End}_K(K^n \otimes K^m)$$

given by $(\phi, \psi) \mapsto \phi \otimes \psi$ restricts to a product operation

$$\text{GL}_n(K) \times \text{GL}_m(K) \rightarrow \text{GL}_{nm}(K)$$

on invertible matrices which preserves scalar matrices, whence a product

$$\text{PGL}_n(K) \times \text{PGL}_m(K) \rightarrow \text{PGL}_{nm}(K).$$

This induces a natural product on cocycles, whence the required product operation (4).

Next observe that for all $n, m > 0$ there are natural injective maps $\text{GL}_n(K) \rightarrow \text{GL}_{nm}(K)$ mapping a matrix $M \in \text{GL}_n(K)$ to the block matrix given by m copies of M placed along the diagonal and zeros elsewhere. As usual, these pass to the quotient modulo scalar matrices and finally induce maps

$$\lambda_{nm} : H^1(G, \text{PGL}_n(K)) \rightarrow H^1(G, \text{PGL}_{nm}(K))$$

on cohomology. Via the bijection of Theorem 2.4.3, the class of a central simple algebra A in $H^1(G, \mathrm{PGL}_n(K))$ is mapped to the class of $A \otimes_k M_m(k)$ by λ_{mn} .

Lemma 2.4.5 *The maps λ_{mn} are injective for all $m, n > 0$.*

Proof: Assume A and A' are central simple k -algebras with $A \otimes_k M_m(k) \cong A' \otimes_k M_m(k)$. By Wedderburn's theorem they are matrix algebras over division algebras D and D' , respectively, hence so are $A \otimes_k M_m(k)$ and $A' \otimes_k M_m(k)$. But then $D \cong D'$ by the unicity statement in Wedderburn's theorem, so finally $A \cong A'$ by dimension reasons. \square

The lemma prompts the following construction.

Construction 2.4.6 Two central simple k -algebras A and A' are called *Brauer equivalent* or *similar* if $A \otimes_k M_m(k) \cong A' \otimes_k M_{m'}(k)$ for some $m, m' > 0$. This defines an equivalence relation on the union of the sets $CSA_K(n)$. We denote the set of equivalence classes by $\mathrm{Br}(K|k)$ and the union of the sets $\mathrm{Br}(K|k)$ for all finite Galois extensions by $\mathrm{Br}(k)$.

Remarks 2.4.7 Brauer equivalence enjoys the following basic properties.

1. One sees from the definition that each Brauer equivalence class contains (up to isomorphism) a unique division algebra. Thus we can also say that $\mathrm{Br}(K|k)$ classifies division algebras split by K .
2. It follows from Wedderburn's theorem and the previous remark that if A and B are two Brauer equivalent k -algebras of the same dimension, then $A \cong B$.

The set $\mathrm{Br}(K|k)$ (and hence also $\mathrm{Br}(k)$) is equipped with a product operation induced by tensor product of k -algebras; indeed, the tensor product manifestly preserves Brauer equivalence.

Proposition 2.4.8 *The sets $\mathrm{Br}(K|k)$ and $\mathrm{Br}(k)$ equipped with the above product operation are abelian groups.*

Before proving the proposition, we recall a notion from ring theory: the *opposite algebra* A° of a k -algebra A is the k -algebra with the same underlying k -vector space as A , but in which the product of two elements x, y is given by the element yx with respect to the product in A . If A is central simple over k , then so is A° .

Proof: Basic properties of the tensor product imply that the product operation is commutative and associative. Now let A represent a class in $\text{Br}(K|k)$; we show that the class of A° yields an inverse. To see this, define a k -linear map $A \otimes_k A^\circ \rightarrow \text{End}_k(A)$ by sending $\sum a_i \otimes b_i$ to the k -linear endomorphism $x \mapsto \sum a_i x b_i$. This map is manifestly nonzero, and hence injective, because $A \otimes_k A^\circ$ is simple by Lemma 2.4.4. Thus it is an isomorphism for dimension reasons. \square

Definition 2.4.9 We call $\text{Br}(K|k)$ equipped with the above product operation the *Brauer group of k relative to K* and $\text{Br}(k)$ the *Brauer group of k* .

Now define the set $H^1(G, \text{PGL}_\infty)$ as the union for all n of the sets $H^1(G, \text{PGL}_n(K))$ via the inclusion maps λ_{mn} , equipped with the product operation coming from (4) (which is manifestly compatible with the maps λ_{mn}). Also, observe that for a Galois extension $L|k$ containing K , the natural surjection $\text{Gal}(L|k) \rightarrow \text{Gal}(K|k)$ induces injective maps

$$H^1(\text{Gal}(K|k), \text{PGL}_n(K)) \rightarrow H^1(\text{Gal}(L|k), \text{PGL}_n(K))$$

for all n , and hence also injections

$$\iota_{LK} : H^1(\text{Gal}(K|k), \text{PGL}_\infty) \rightarrow H^1(\text{Gal}(L|k), \text{PGL}_\infty).$$

Fixing a separable closure k_s of k , we define $H^1(k, \text{PGL}_\infty)$ as the union over all Galois extensions $K|k$ contained in k_s of the groups $H^1(\text{Gal}(K|k), \text{PGL}_\infty)$ via the inclusion maps ι_{LK} . The arguments above then yield:

Corollary 2.4.10 *The sets $H^1(G, \text{PGL}_\infty)$ and $H^1(k, \text{PGL}_\infty)$ equipped with the product operation coming from (4) are abelian groups, and there are natural group isomorphisms*

$$\text{Br}(K|k) \cong H^1(G, \text{PGL}_\infty) \quad \text{and} \quad \text{Br}(k) \cong H^1(k, \text{PGL}_\infty).$$

Remark 2.4.11 The sets $H^1(G, \text{PGL}_\infty)$ are not cohomology sets of G in the sense defined so far, but may be viewed as cohomology sets of G with values in the *direct limit* of the groups $\text{PGL}_n(K)$ via the maps λ_{mn} . Still, this coefficient group is fairly complicated. Later we shall identify $\text{Br}(K|k)$ with the second cohomology *group* of G with values in the multiplicative group K^\times , a group that is much easier to handle.

2.5 Cyclic Algebras

We are now in the position for introducing a class of algebras that will play a central role in this book.

Construction 2.5.1 (Cyclic algebras) Let $K|k$ be a cyclic Galois extension with Galois group $G \cong \mathbf{Z}/m\mathbf{Z}$. In the sequel we fix one such isomorphism $\chi : G \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z}$; it is a character of G . Furthermore, let $b \in k^\times$ be given. We associate with these data a central simple algebra over k which is a $K|k$ -twisted form of the matrix algebra $M_m(k)$. To do so, consider the matrix

$$\tilde{F}(b) = \begin{bmatrix} 0 & 0 & \cdots & 0 & b \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \in \mathrm{GL}_m(k).$$

We denote by $F(b)$ its image in the group $\mathrm{PGL}_m(k)$. A computation shows that $\tilde{F}(b)^m = b \cdot I_m$, and hence $F(b)^m = 1$; in fact, the element $F(b)$ has exact order m in $\mathrm{PGL}_m(k)$.

Now consider the homomorphism $\mathbf{Z}/m\mathbf{Z} \rightarrow \mathrm{PGL}_m(k)$ defined by sending 1 to $F(b)$. Embedding $\mathrm{PGL}_m(k)$ into $\mathrm{PGL}_m(K)$ and composing by χ we thus get a 1-cocycle

$$z(b) : G \rightarrow \mathrm{PGL}_m(K).$$

We now equip the matrix algebra $M_m(K)$ with the twisted G -action ${}_{z(b)}M_m(K)$ coming from $z(b)$ (see Construction 2.3.6) and take G -invariants. By Theorem 2.4.3 (and its proof), the resulting k -algebra is a central simple algebra split by K . We denote it by (χ, b) , and call it the *cyclic algebra* associated with χ and b .

We now come to the definition of cyclic algebras originally proposed by Dickson.

Proposition 2.5.2 *The algebra (χ, b) can be described by the following presentation. There is an element $y \in (\chi, b)$ such that (χ, b) is generated as a k -algebra by K and y , subject to the relations*

$$y^m = b, \quad \lambda y = y\sigma(\lambda) \tag{5}$$

for all $\lambda \in K$, where σ is the generator of G mapped to 1 by χ .

In particular, we see that K is a commutative k -subalgebra in (χ, b) which is *not* contained in the center.

Proof: Denote by A the k -algebra given by the presentation of the proposition and define a k -algebra homomorphism $j : A \rightarrow M_m(K)$ by setting

$$j(y) = \tilde{F}(b) \quad \text{and} \quad j(\lambda) = \text{diag}(\lambda, \sigma(\lambda), \dots, \sigma^{m-1}(\lambda)) \quad \text{for } \lambda \in K.$$

(where $\text{diag}(\dots)$ means the diagonal matrix with the indicated entries), and extending k -linearly. To see that this is indeed a homomorphism, one checks by direct computation that the relation

$$j(\lambda)\tilde{F}(b) = \tilde{F}(b)j(\sigma(\lambda)) \tag{6}$$

holds for all $\lambda \in K$; the relation $\tilde{F}(b)^m = b$ has already been noted above. Next we check that the image of j lands in (χ, b) . For this, recall that by definition the elements of ${}_{z(b)}M_m(K)^G$ are those matrices M which satisfy $\tilde{F}(b)\sigma(M)\tilde{F}(b)^{-1} = M$. This relation is obviously satisfied by $j(y) = \tilde{F}(b)$ as it is in $M_m(k)$, and for the $j(\lambda)$ it follows from relation (6) above, which proves the claim. Finally, we have to check that j is an isomorphism. For dimension reasons it is enough to check surjectivity, which in turn can be done after tensoring by K . The image of $j \otimes \text{id}_K$ in $(\chi, b) \otimes_k K \cong M_m(K)$ is the K -subalgebra generated by $\tilde{F}(b)$ and the diagonal subalgebra $K \oplus \dots \oplus K$. If $E_{i,j}$ is the usual basis of $M_m(K)$, it therefore remains to check that the $E_{i,j}$'s belong to this subalgebra for $i \neq j$. This is achieved by computing $E_{i,j} = \tilde{F}(b)^{i-j} E_{j,j}$ for $i \neq j$. \square

The following proposition provides a kind of a converse to the previous one.

Proposition 2.5.3 *Assume that A is a central simple k -algebra of degree m containing a k -subalgebra K which is a cyclic Galois field extension of degree m . Then A is isomorphic to a cyclic algebra given by a presentation of the form (5).*

The crucial point in the proof is the following statement.

Lemma 2.5.4 *Under the assumptions of the proposition there exists $y \in A^\times$ such that*

$$y^{-1}xy = \sigma(x)$$

for all $x \in K$, where σ is a generator of $G = \text{Gal}(K|k)$.

Proof: In order to avoid confusing notation, we take another extension \tilde{K} of k isomorphic to K and put $\tilde{G} := \text{Gal}(\tilde{K}|k)$. By Proposition 2.2.8 the algebra $A \otimes_k \tilde{K}$ is split, as it contains the \tilde{K} -subalgebra $K \otimes_k \tilde{K} \cong \tilde{K}^m$. The embedding $K \otimes_k \tilde{K} \rightarrow A \otimes_k \tilde{K}$ is \tilde{G} -equivariant, where \tilde{G} acts on $K \otimes_k \tilde{K}$ via the second factor. On the other hand, the group G acts on $K \otimes_k \tilde{K}$ via the first factor, and the two actions commute. As seen before the proof of Lemma 2.3.8, under the isomorphism $K \otimes_k \tilde{K} \cong \tilde{K}^m$ the action of G corresponds to permuting the components on the right hand side. Under the diagonal embedding $K \otimes_k \tilde{K} \rightarrow A \otimes_k \tilde{K} \cong M_m(\tilde{K})$ we may identify permutation of the components of the diagonal with conjugation by a permutation matrix, so we find an element $y \in \text{GL}_m(\tilde{K}) \cong (A \otimes_k \tilde{K})^\times$ satisfying

$$\sigma(x) = y^{-1}xy \text{ for all } x \in K \otimes_k \tilde{K}. \quad (7)$$

We now show that we may choose y in the subgroup $A^\times \subset (A \otimes_k \tilde{K})^\times$, which will conclude the proof of the lemma.

For all $\tilde{\tau} \in \tilde{G}$ and $x \in K$ (where we view K embedded into $K \otimes_k \tilde{K}$ via the first factor), we have

$$\sigma(x) = \sigma(\tilde{\tau}(x)) = \tilde{\tau}(\sigma(x)) = \tilde{\tau}(y^{-1})\tilde{\tau}(x)\tilde{\tau}(y) = \tilde{\tau}(y)^{-1}x\tilde{\tau}(y),$$

using that the two actions commute and that \tilde{G} acts trivially on K . Thus $z_{\tilde{\tau}} := y\tilde{\tau}(y)^{-1}$ satisfies $z_{\tilde{\tau}}^{-1}xz_{\tilde{\tau}} = x$ for all $x \in K$. It follows that $z_{\tilde{\tau}}$ lies in $Z_A(K) \otimes_k \tilde{K}$, where $Z_A(K)$ stands for the centralizer of K in A . The natural embedding $K \rightarrow Z_A(K)$ is an isomorphism, as one sees by passing to the split case and counting dimensions. Thus the function $\tilde{\tau} \mapsto z_{\tilde{\tau}}$ has values in $(K \otimes_k \tilde{K})^\times$, and moreover it is a 1-cocycle for \tilde{G} by construction.

Now observe that the group $H^1(\tilde{G}, (K \otimes_k \tilde{K})^\times)$ is trivial. Indeed, the group $(K \otimes_k \tilde{K})^\times$ is the automorphism group of the $K \otimes_k \tilde{K}$ -algebra $K \otimes_k \tilde{K}$, so by Theorem 2.3.3 the group $H^1(\tilde{G}, (K \otimes_k \tilde{K})^\times)$ classifies those K -algebras B for which $B \otimes_k \tilde{K} \cong K \otimes_k \tilde{K}$. But these K -algebras must be isomorphic to K by dimension reasons, whence the claim. In view of this claim we find $y_0 \in (K \otimes_k \tilde{K})^\times$ such that $y\tilde{\tau}(y)^{-1} = y_0\tilde{\tau}(y_0)^{-1}$ for all $\tilde{\tau} \in \tilde{G}$. Up to replacing y by $y_0^{-1}y$ in the equation (7), we may thus assume that $\tilde{\tau}(y) = y$ for all $\tilde{\tau}$, i.e. $y \in A^\times$, as required. \square

Proof of Proposition 2.5.3: We first prove that the element y of the previous lemma satisfies $y^m \in k$. To see this, apply formula (7) to $\sigma(x)$ in place of x , with $x \in K$. It yields $\sigma^2(x) = y^{-2}xy^2$, so iterating $m - 1$ times we obtain $x = \sigma^m(x) = y^{-m}xy^m$. Thus y^m commutes with all $x \in K$ and hence lies in K by the equality $Z_A(K) = K$ noted above. Now apply (7) with $x = y^m$ to obtain $\sigma(y^m) = y^m$, i.e. $y^m \in k$.

Setting $b := y^m$, to conclude the proof it remains to show that the elements of K and the powers of y generate A . For this it suffices to check that the elements $1, y, \dots, y^{m-1}$ are K -linearly independent in A , where K acts by right multiplication. If not, take a nontrivial K -linear relation $\sum y^i \lambda_i = 0$ with a minimal number of nonzero coefficients. This minimal number is at least 2, so after reindexing we may assume $\lambda_0, \lambda_1 \neq 0$. Choose $c \in K^\times$ with $c \neq \sigma(c)$. Using equation (7) and its iterates we may write $\sum y^i \sigma^i(c) \lambda_i = c(\sum y^i \lambda_i) = 0$. It follows that $\sum y^i (c \lambda_i - \sigma^i(c) \lambda_i) = 0$ is a shorter nontrivial relation, a contradiction. \square

In special cases one gets even nicer presentations for cyclic algebras. One of these is when m is invertible in k , and k contains a primitive m -th root of unity ω . In this case, for $a, b \in k^\times$ define the k -algebra $(a, b)_\omega$ by the presentation

$$(a, b)_\omega = \langle x, y \mid x^m = a, y^m = b, xy = \omega yx \rangle.$$

In the case $m = 2$, $\omega = -1$ one gets back the generalised quaternion algebras of the previous chapter.

Another case is when k is of characteristic $p > 0$ and $m = p$. In this case for $a \in k$ and $b \in k^\times$ consider the presentation

$$[a, b] = \langle x, y \mid x^p - x = a, y^p = b, xy = y(x + 1) \rangle.$$

Note that the equation $x^p - x = a$ defines a cyclic Galois extension of degree p whose Galois group is given by the substitutions $\alpha \mapsto \alpha + i$ ($0 \leq i \leq p-1$) for some root α . In the case $p = 2$ this definition is coherent with that of Remark 1.1.8.

Corollary 2.5.5

1. Assume that k contains a primitive m -th root of unity and that we may write K in the form $K = k(\sqrt[m]{a})$ with some m -th root of an element $a \in k$. Let $\chi : \text{Gal}(K|k) \cong \mathbf{Z}/m\mathbf{Z}$ be the isomorphism sending the automorphism $\sigma : \sqrt[m]{a} \mapsto \omega \sqrt[m]{a}$ to 1. Then for all $b \in k^\times$ there is an isomorphism of k -algebras

$$(a, b)_\omega \cong (\chi, b).$$

2. Similarly, assume that k has characteristic $p > 0$, $m = p$ and $K|k$ is a cyclic Galois extension defined by a polynomial $x^p - x + a$ for some $a \in k$. Fix a root α of $x^p - x - a$ and let $\chi : \text{Gal}(K|k) \cong \mathbf{Z}/p\mathbf{Z}$ be the isomorphism sending the automorphism $\sigma : \alpha \mapsto \alpha + 1$ to 1. Then for all $b \in k^\times$ there is an isomorphism of k -algebras

$$[a, b] \cong (\chi, b).$$

In particular, $(a, b)_\omega$ and $[a, b]$ are central simple algebras split by K .

Proof: In (1), one gets the required isomorphism by choosing as generators of (χ, b) the element $x = \sqrt[m]{a}$ and the y given by the proposition above. In (2), one chooses $x = \alpha$ and y as in the proposition. \square

Remark 2.5.6 In fact, we shall see later that according to Kummer theory (Corollary 4.3.9) in the presence of a primitive m -th root of unity one may write an arbitrary degree m cyclic Galois extension $K|k$ in the form $K = k(\sqrt[m]{a})$, as in the corollary above. Similarly, Artin-Schreier theory (Remark 4.3.13 (1)) shows that a cyclic Galois extension of degree p in characteristic $p > 0$ is generated by a root of some polynomial $x^p - x - a$.

In the previous chapter we have seen that the class of a nonsplit quaternion algebra has order 2 in the Brauer group. More generally, the class of a cyclic division algebra $(a, b)_\omega$ as above has order m ; we leave the verification of this fact as an exercise to the reader. Thus the class of a tensor product of degree m cyclic algebras has order dividing m in the Brauer group. The remarkable fact is the converse:

Theorem 2.5.7 (Merkurjev-Suslin) *Assume that k contains a primitive m -th root of unity ω . Then a central simple k -algebra whose class has order dividing m in $\text{Br}(k)$ is Brauer equivalent to a tensor product*

$$(a_1, b_1)_\omega \otimes_k \cdots \otimes_k (a_i, b_i)_\omega$$

of cyclic algebras.

This generalises Merkurjev's theorem from the end of Chapter 1. In fact, Merkurjev and Suslin found this generalisation soon after the first result of Merkurjev. It is this more general statement whose proof will occupy a major part of this book.

Here is an interesting corollary of the Merkurjev-Suslin theorem of which no elementary proof is known presently.

Corollary 2.5.8 *For k and A as in the theorem above, there exist elements $a_1, \dots, a_i \in k^\times$ such that the extension $k(\sqrt[m]{a_1}, \dots, \sqrt[m]{a_i})|k$ splits A . In particular, A is split by a Galois extension with solvable Galois group.*

2.6 Reduced Norms and Traces

We now discuss a construction which generalises the quaternion norm encountered in the previous chapter.

Construction 2.6.1 (Reduced norms and traces) Let A be a central simple k -algebra of degree n . Take a finite Galois splitting field $K|k$ with group G and choose a K -isomorphism $\phi : M_n(K) \xrightarrow{\sim} A \otimes_k K$. Recall that the isomorphism ϕ is not compatible with the action of G . However, if we twist the usual action of G on $M_n(K)$ by the 1-cocycle $\sigma \mapsto a_\sigma$ with $a_\sigma = \phi^{-1} \circ \sigma(\phi)$ associated with A by the descent construction, then we get an isomorphism ${}_a M_n(K) \xrightarrow{\sim} A \otimes_k K$ that is already G -equivariant, whence an isomorphism $({}_a M_n(K))^G \cong A$.

Now consider the determinant map $\det : M_n(K) \rightarrow K$. For all $\sigma \in G$, lifting a_σ to an invertible matrix $C_\sigma \in \mathrm{GL}_n(K)$ we get

$$\det(C_\sigma \sigma(M) C_\sigma^{-1}) = \det(\sigma(M)) = \sigma(\det(M))$$

by multiplicativity of the determinant and its compatibility with the usual G -action. Bearing in mind that the twisted G -action on ${}_a M_n(K)$ is given by $(\sigma, M) \rightarrow a_\sigma \sigma(M) a_\sigma^{-1}$, this implies that the map $\det : {}_a M_n(K) \rightarrow K$ is compatible with the action of G . So by taking G -invariants and using the isomorphism above we get a map $\mathrm{Nrd} : A \rightarrow k$, called the *reduced norm map*. On the subgroup A^\times of invertible elements of A it restricts to a group homomorphism $\mathrm{Nrd} : A^\times \rightarrow k^\times$.

The above construction does not depend on the choice of ϕ , for changing ϕ amounts to replacing a_σ by an equivalent cocycle, i.e. replacing the matrix C above by some $D^{-1}CD$, which does not affect the determinant. The construction does not depend on the choice of K either, as one sees by embedding two Galois splitting fields K, L into a bigger Galois extension $M|k$.

By performing the above construction using the trace of matrices instead of the determinant, one gets a homomorphism $\mathrm{Trd} : A \rightarrow k$ of additive groups called the *reduced trace map*.

The reduced norm map is a generalisation of the norm map for quaternion algebras, as one sees from Proposition 1.2.4. Just like the quaternion norm, it enjoys the following property:

Proposition 2.6.2 *In a central simple k -algebra A an element $a \in A$ is invertible if and only if $\mathrm{Nrd}(a) \neq 0$. Hence A is a division algebra if and only if Nrd restricts to a nowhere vanishing map on $A \setminus 0$.*

Proof: If a is invertible, it corresponds to an invertible matrix via any isomorphism $\phi : A \otimes_K K \cong M_n(K)$, which thus has nonzero determinant. For the converse, consider ϕ as above and assume an element $a \in A$ maps to a matrix with nonzero determinant. It thus has an inverse $b \in M_n(K)$. Now in any ring the multiplicative inverse of an element is unique (indeed, if b' is another inverse, one has $b = bab' = b'$), so for an automorphism $\sigma_A \in \text{Aut}_k(A \otimes_k K)$ coming from the action of an element $\sigma \in \text{Gal}(K|k)$ on K we have $\sigma_A(b) = b$. As A is the set of fixed elements of all the σ_A , this implies $b \in A$. \square

We now elucidate the relation with other norm and trace maps. Recall that given a finite dimensional k -algebra A , the *norm* and the *trace* of an element $a \in A$ are defined as follows: one considers the k -linear mapping $L_a : A \rightarrow A$ given by $L_a(x) = ax$ and puts

$$N_{A|k}(a) := \det(L_a), \quad \text{tr}_{A|k}(a) := \text{tr}(L_a).$$

By definition, these norm and trace maps are insensitive to change of the base field.

Proposition 2.6.3 *Let A be a central simple k -algebra of degree n .*

1. *One has $N_{A|k} = (\text{Nrd}_A)^n$ and $\text{tr}_{A|k} = n \text{Trd}_A$.*
2. *Assume that K is a commutative k -subalgebra of A which is a degree n field extension of k . For any $x \in K$ one has*

$$\text{Nrd}_A(x) = N_{K|k}(x) \quad \text{and} \quad \text{Trd}_A(x) = \text{tr}_{K|k}(x).$$

Proof: To prove (1) we may assume, up to passing to a splitting field of A , that $A = M_n(k)$. The required formulae then follow from the fact that for $M \in M_n(k)$, the matrix of the multiplication-by- M map L_M with respect to the standard basis of $M_n(k)$ is the block diagonal matrix $\text{diag}(M, \dots, M)$.

To check (2), note first that as a K -vector space the algebra A is isomorphic to the direct power K^n . For $x \in K$ we thus have $N_{A|k}(x) = (N_{K|k}(x))^n$ and $\text{tr}_{A|k}(x) = n \text{tr}_{K|k}(x)$. By part (1) there exists an n -th root of unity $\omega(x)$ such that $\text{Nrd}_A(x) = \omega(x)N_{K|k}(x)$. To show that $\omega(x) = 1$ we use the following trick. Performing base change from k to $k(t)$ and applying the previous formula to $t + x \in K(t)^\times$ yields the equality

$$\text{Nrd}_A(t + x) = \omega(t + x)N_{K|k}(t + x).$$

Since $\text{Nrd}_A(t + x)$ and $N_{K|k}(t + x)$ are monic polynomials in t , we obtain $\omega(t + x) = 1$, and therefore $\text{Nrd}_A(t + x) = N_{K|k}(t + x)$. We then get the desired

formula $\text{Nrd}_A(x) = N_{K|k}(x)$ by specialising this polynomial identity to $t = 0$. To handle the trace formula $\text{Trd}_A(x) = \text{tr}_{K|k}(x)$, it then suffices to look at the coefficients of t in the polynomial identity $\text{Nrd}_A(1 + tx) = N_{K|k}(1 + tx)$.

□

We conclude by the following result that we shall need later. For a generalisation, see Exercise 8.

Proposition 2.6.4 *Let k be a field, and let A be a central division algebra of prime degree p over k . An element $c \in k^\times$ is a reduced norm from A^\times if and only if $c \in N_{K|k}(K^\times)$ for some k -subalgebra $K \subset A$ which is a degree p field extension of k and moreover a splitting field for A .*

Proof: Sufficiency follows from part (2) of the previous proposition. To check necessity, take $a \in A^\times$ such that $c = \text{Nrd}(a)$. If $a \notin k$, let K be the k -subalgebra generated by a , which is necessarily a degree p field extension of k since A is a division algebra of degree p . If $a \in k$, take K to be any degree p subfield of A obtained in the above way. Since $A \otimes_k K$ contains $K \otimes_k K$ which is not a division algebra, $A \otimes_k K$ itself is not a division algebra and thus can only be isomorphic to the matrix algebra $M_p(K)$ by Wedderburn's theorem. Thus K is a degree p splitting field for A , and we again conclude by part (2) of the above proposition. □

2.7 A Basic Exact Sequence

In this section we first establish a formal proposition which, combined with the descent method, is a main tool in computations.

Proposition 2.7.1 *Let G be a group and*

$$1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$$

an exact sequence of groups equipped with a G -action, the maps being G -homomorphisms. Then there is an exact sequence of pointed sets

$$1 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C).$$

By definition, an exact sequence of pointed sets is a sequence in which the kernel of each map equals the image of the previous one, the kernel being the subset of elements mapping to the base point.

Proof: The only nonobvious points are the definition of the map $\delta : C^G \rightarrow H^1(G, A)$ and the exactness of the sequence at the third and fourth terms. To define δ , take an element $c \in C^G$ and lift it to an element $b \in B$ via the surjection $B \rightarrow C$. For all $\sigma \in G$ the element $b\sigma(b)^{-1}$ maps to 1 in C because $c = \sigma(c)$ by assumption, so it lies in A . Immediate calculations then show that the map $\sigma \mapsto b\sigma(b)^{-1}$ is a 1-cocycle and that modifying b by an element of A yields an equivalent cocycle, whence a well-defined map δ as required, sending elements coming from B^G to 1. The relation $\delta(c) = 1$ means by definition that $b\sigma(b)^{-1} = a^{-1}\sigma(a)$ for some $a \in A$, so c lifts to the G -invariant element ab in B . This shows the exactness of the sequence at the third term, and the composition $C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B)$ is trivial by construction. Finally, that a cocycle $\sigma \mapsto a_\sigma$ with values in A becomes trivial in $H^1(G, B)$ means that $a_\sigma = b^{-1}\sigma(b)$ for some $b \in B$, and modifying $\sigma \mapsto a_\sigma$ by an A -coboundary we may choose b so that its image c in C is fixed by G ; moreover, the cohomology class of $\sigma \mapsto a_\sigma$ depends only on c . \square

As a first application, we derive a basic theorem on central simple algebras.

Theorem 2.7.2 (Skolem-Noether) *All automorphisms of a central simple algebra are inner, i.e. given by conjugation by an invertible element.*

Proof: Let A be a central simple k -algebra of degree n and K a finite Galois splitting field of A . Denoting by A^\times the subgroup of invertible elements of A and using Lemma 2.4.1 we get an exact sequence

$$1 \rightarrow K^\times \rightarrow (A \otimes_k K)^\times \rightarrow \text{Aut}_K(A \otimes_k K) \rightarrow 1$$

of groups equipped with a $G = \text{Gal}(K|k)$ -action, where the second map maps an invertible element to the inner automorphism it defines. Proposition 2.7.1 then yields an exact sequence

$$1 \rightarrow k^\times \rightarrow A^\times \rightarrow \text{Aut}_k(A) \rightarrow H^1(G, K^\times),$$

where the last term is trivial by Hilbert's Theorem 90. The theorem follows. \square

As another application, we derive from Proposition 2.7.1 a useful cohomological characterisation of reduced norms. First a piece of notation: for a central simple algebra A , we denote by $\text{SL}_1(A)$ the multiplicative subgroup of elements of reduced norm 1.

Proposition 2.7.3 *Let A be a central simple k -algebra split by a finite Galois extension $K|k$ of group G . There is a canonical bijection of pointed sets*

$$H^1(G, \text{SL}_1(A \otimes_k K)) \leftrightarrow k^\times / \text{Nrd}(A^\times).$$

For the proof we need a generalisation of Example 2.3.4.

Lemma 2.7.4 *For A , K and G as above, we have $H^1(G, (A \otimes_k K)^\times) = 1$.*

Proof: Let M be a left A -module with $\dim_k M = \dim_k A$. Then M is isomorphic to the left A -module A . Indeed, since $A \cong M_n(D)$ by Wedderburn's theorem, it is isomorphic to a direct sum of the minimal left ideals I_r introduced in Example 2.1.4; these are all isomorphic simple A -modules. As M is finitely generated over A , there is a surjection $A^N \rightarrow M$ for some $N > 0$, so M must be isomorphic to a direct sum of copies of I_r as well and hence isomorphic to A for dimension reasons.

On the other hand, multiplication by an element of A is an endomorphism of M as a k -vector space. By the second example in Example 2.3.1 combined with Remark 2.3.10, the module M can thus be considered as a k -object (M, Φ) to which the theory of Section 2.3 applies. Now $M \otimes_k K$ is an $A \otimes_k K$ -module of rank 1, and hence isomorphic to $A \otimes_k K$ as above. An automorphism of $A \otimes_k K$ as a left module over itself is given by right multiplication by an invertible element, thus $\text{Aut}_K(M \otimes_k K) \cong (A \otimes_k K)^\times$. The lemma then follows from Theorem 2.3.3 (more precisely, from its variant in Remark 2.3.10). \square

Proof of Proposition 2.7.3: Applying Proposition 2.7.1 to the exact sequence

$$1 \rightarrow \text{SL}_1(A \otimes_k K) \rightarrow (A \otimes_k K)^\times \xrightarrow{\text{Nrd}} K^\times \rightarrow 1$$

we get an exact sequence

$$A^\times \xrightarrow{\text{Nrd}} k^\times \rightarrow H^1(G, \text{SL}_1(A \otimes_k K)) \rightarrow H^1(G, (A \otimes_k K)^\times),$$

where the last term is trivial by the lemma above. \square

2.8 K_1 of Central Simple Algebras

The main result of this section is a classical theorem of Wang on commutator subgroups of division algebras. Following the present-day viewpoint, we discuss it within the framework of the K-theory of rings. Therefore we first define the group K_1 for a ring.

Construction 2.8.1 Given a not necessarily commutative ring R with unit and a positive integer n , consider the group $\text{GL}_n(R)$ of $n \times n$ invertible matrices over R . For each n there are injective maps $i_{n,n+1} : \text{GL}_n(R) \rightarrow \text{GL}_{n+1}(R)$

given by

$$i_{n,n+1}(A) := \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}. \quad (8)$$

Let $\mathrm{GL}_\infty(R)$ be the union of the tower of embeddings

$$\mathrm{GL}_1(R) \subset \mathrm{GL}_2(R) \subset \mathrm{GL}_3(R) \subset \cdots,$$

given by the maps $i_{n,n+1}$. (Note that this definition of GL_∞ is *not* compatible with the definition of PGL_∞ introduced in Section 2.4.)

We define the group $K_1(R)$ as the quotient of $\mathrm{GL}_\infty(R)$ by its commutator subgroup $[\mathrm{GL}_\infty(R), \mathrm{GL}_\infty(R)]$. This group is sometimes called the *Whitehead group* of R . It is functorial with respect to ring homomorphisms, i.e. a map $R \rightarrow R'$ of rings induces a map $K_1(R) \rightarrow K_1(R')$.

For calculations the following description of the commutator subgroup $[\mathrm{GL}_\infty(R), \mathrm{GL}_\infty(R)]$ is useful. A matrix in $\mathrm{GL}_n(R)$ is called *elementary* if all of its diagonal entries are equal to 1 and moreover it has at most one nonzero off-diagonal entry. We denote by $E_{ij}(r)$ the elementary matrix with r in the i -th row and j -th column and by $E_n(R)$ the subgroup of $\mathrm{GL}_n(R)$ generated by elementary matrices. The maps $i_{n,n+1}$ preserve these subgroups, whence a subgroup $E_\infty(R) \subset \mathrm{GL}_\infty(R)$.

Proposition 2.8.2 (Whitehead's Lemma) *The subgroup $E_\infty(R)$ is precisely the commutator subgroup $[\mathrm{GL}_\infty(R), \mathrm{GL}_\infty(R)]$ of $\mathrm{GL}_\infty(R)$.*

The proof uses the following lemma.

Lemma 2.8.3 *Any upper triangular $n \times n$ matrix with 1's in the diagonal is a product of elements of $E_n(R)$. A similar statement holds for lower triangular matrices.*

Proof: It suffices to treat the case of an upper triangular matrix $A = [a_{ij}]$. Multiplication on the right by the elementary matrix $E_{12}(-a_{12})$ produces a matrix $A' = [a'_{ij}]$ with $a'_{12} = 0$. Then multiplication by $E_{23}(-a_{23})$ produces $A'' = [a''_{ij}]$ with $a''_{12} = a''_{23} = 0$. Continuing the process we get a matrix $B = [b_{ij}]$ which is still upper triangular with 1's in the diagonal but has 0's in the subdiagonal $j = i + 1$. Then multiplication by $E_{13}(-b_{13})$ annihilates the first element of the subdiagonal $j = i + 2$. Continuing the process we finally arrive at the identity matrix. \square

Proof of Theorem 2.8.2: The relation $E_{ij}(r) = [E_{ik}(r), E_{kj}(1)]$ for distinct i, j and k is easily checked by matrix multiplication and shows that $E_\infty(R)$ is contained in $[E_\infty(R), E_\infty(R)] \subset [GL_\infty(R), GL_\infty(R)]$. To show $[GL_\infty(R), GL_\infty(R)] \subset E_\infty(R)$, we embed $GL_n(R)$ into $GL_{2n}(R)$ and for $A, B \in GL_n(R)$ compute

$$\begin{bmatrix} ABA^{-1}B^{-1} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} AB & 0 \\ 0 & B^{-1}A^{-1} \end{bmatrix} \begin{bmatrix} A^{-1} & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} B^{-1} & 0 \\ 0 & B \end{bmatrix}.$$

All terms on the right are of similar shape. Denoting by I_n the identity matrix, another computation shows that

$$\begin{bmatrix} A & 0 \\ 0 & A^{-1} \end{bmatrix} = \begin{bmatrix} I_n & A \\ 0 & I_n \end{bmatrix} \begin{bmatrix} I_n & 0 \\ -A^{-1} & I_n \end{bmatrix} \begin{bmatrix} I_n & A \\ 0 & I_n \end{bmatrix} \begin{bmatrix} 0 & -I_n \\ I_n & 0 \end{bmatrix} \quad (9)$$

and similarly for the other terms. The first three terms on the right hand side are upper or lower triangular matrices with 1's in the diagonal, so the lemma applies. For the fourth, notice that

$$\begin{bmatrix} 0 & -I_n \\ I_n & 0 \end{bmatrix} = \begin{bmatrix} I_n & -I_n \\ 0 & I_n \end{bmatrix} \begin{bmatrix} I_n & 0 \\ I_n & I_n \end{bmatrix} \begin{bmatrix} I_n & -I_n \\ 0 & I_n \end{bmatrix},$$

so the lemma applies again. \square

Using Whitehead's lemma we may easily calculate K_1 -groups of fields.

Proposition 2.8.4 *For a field k the natural map $k^\times = GL_1(k) \rightarrow GL_\infty(k)$ induces an isomorphism $k^\times \xrightarrow{\sim} K_1(k)$.*

Proof: We first show surjectivity. It is well known from linear algebra that a matrix in $M_n(k)$ may be put in diagonal form by means of elementary row and column operations, i.e. by multiplication with suitable elementary matrices. Thus by Whitehead's lemma each element of $K_1(k)$ may be represented by some diagonal matrix. But any diagonal matrix may be expressed as a product of a diagonal matrix of the form $\text{diag}(b, 1, \dots, 1)$ and diagonal matrices of the form $\text{diag}(1, \dots, 1, a, a^{-1}, 1, \dots, 1)$. The same matrix calculation that establishes formula (9) shows that the latter are products of elementary matrices, so the class in $K_1(k)$ is represented by $\text{diag}(b, 1, \dots, 1)$, whence the required surjectivity.

To show injectivity one considers the determinant maps $GL_n(k) \rightarrow k^\times$. They are compatible with the transition maps $i_{n,n+1}$, and therefore they define a homomorphism $\det_\infty : GL_\infty(k) \rightarrow k^\times$ which is a splitting of the the surjection $k^\times \rightarrow K_1(k)$ studied above. The proposition follows. \square

Remarks 2.8.5

1. More generally, for a division ring D one can consider the map

$$D^\times / [D^\times, D^\times] \rightarrow K_1(D)$$

induced by the map $D^\times = \mathrm{GL}_1(D) \rightarrow \mathrm{GL}_\infty(D)$ and show that it is an isomorphism. The proof of surjectivity goes by the same argument as above (since diagonalisation of matrices by elementary row and column transformations also works over a division ring). The proof of injectivity is also the same, except that one has to work with the *Dieudonné determinant*, a noncommutative generalisation of the usual determinant map (see e.g. Pierce [1], §16.5).

2. Another, much easier, generalisation is the following: the isomorphism of the proposition also holds for finite direct products $k_1 \times \cdots \times k_r$ of fields. This follows from the proposition and the general formula

$$K_1(R \times R') \cong K_1(R) \times K_1(R'),$$

valid for arbitrary rings R and R' , which is a consequence of the definition of K_1 .

Consider now for $n, m \geq 1$ the maps $i_{n, nm} : M_n(R) \rightarrow M_{nm}(R)$ given by

$$i_{n,m}(A) := \begin{bmatrix} A & 0 \\ 0 & I_{nm-n} \end{bmatrix}.$$

By functoriality, the map $i_{1,m}$ induces a map $K_1(R) \rightarrow K_1(M_m(R))$.

Lemma 2.8.6 *The above map $K_1(R) \rightarrow K_1(M_m(R))$ is an isomorphism.*

This map is sometimes called the Morita isomorphism because of its relation with Morita equivalence in ring theory. In the case of a central simple algebra A it shows that the isomorphism class of $K_1(A)$ only depends on the Brauer class of A .

Proof: For all $n \geq 1$, the diagram

$$\begin{array}{ccccc} \mathrm{GL}_n(R) & \xrightarrow{i_{1,m^*}} & \mathrm{GL}_n(M_m(R)) & \cong & \mathrm{GL}_{nm}(R) \\ i_{n,nm} \downarrow & & i_{n,nm} \downarrow & & i_{nm,nm^2} \downarrow \\ \mathrm{GL}_{nm}(R) & \xrightarrow{i_{1,m^*}} & \mathrm{GL}_{nm}(M_m(R)) & \cong & \mathrm{GL}_{nm^2}(R) \end{array}$$

commutes, so the map $\mathrm{GL}_\infty(R) \rightarrow \mathrm{GL}_\infty(M_m(R))$ is an isomorphism. This isomorphism preserves the commutator subgroups, whence the lemma. \square

The lemma enables us to construct a norm map for K_1 of k -algebras.

Construction 2.8.7 Let A be a k -algebra and $K|k$ a field extension of degree n . Denote by A_K the base change $A \otimes_k K$. We construct a norm map $N_{K|k} : K_1(A_K) \rightarrow K_1(A)$ as follows. Fixing an isomorphism $\phi : \mathrm{End}_k(K) \cong M_n(k)$ gives rise to a composite map

$$\phi_* : A_K = A \otimes_k K \rightarrow A \otimes_k \mathrm{End}_k(K) \xrightarrow{id \otimes \phi} A \otimes_k M_n(k) \cong M_n(A).$$

We then define the norm map $N_{K|k}$ as the composite

$$K_1(A_K) \xrightarrow{\phi_*} K_1(M_n(A)) \xrightarrow{\sim} K_1(A),$$

where the second map is the inverse of the isomorphism of the previous lemma. Since the conjugation action of the group $\mathrm{GL}_n(k)$ (and even of $\mathrm{GL}_n(A)$) on $M_n(A)$ induces a trivial action on $K_1(M_n(A))$, we conclude that the map above is independent of the choice of ϕ .

Proposition 2.8.8 *In the situation above the composite map*

$$K_1(A) \rightarrow K_1(A_K) \xrightarrow{N_{K|k}} K_1(A)$$

is multiplication by $n = [K : k]$.

Proof: The composite $K_1(A) \rightarrow K_1(A_K) \rightarrow K_1(M_n(A))$ is induced by the map $A \rightarrow A \otimes_k M_n(k)$ sending a matrix M to the block diagonal matrix $\mathrm{diag}(M, \dots, M)$. The same argument with formula (9) as in the proof of Proposition 2.8.4 shows that the class of $\mathrm{diag}(M, \dots, M)$ in $K_1(A)$ equals that of $\mathrm{diag}(M^n, 1, \dots, 1)$, whence the claim. \square

We now focus on the case of a central simple k -algebra A and construct reduced norm maps on K_1 -groups. Given an integer $n \geq 1$, we denote by $\mathrm{Nrd}_n : \mathrm{GL}_n(A) \rightarrow k^\times$ the composite

$$\mathrm{GL}_n(A) \cong \mathrm{GL}_1(M_n(A)) \xrightarrow{\mathrm{Nrd}_{M_n(A)}} k^\times.$$

Lemma 2.8.9 *For all integers $n \geq 1$, the diagram*

$$\begin{array}{ccc} \mathrm{GL}_n(A) & \xrightarrow{i_{n,n+1}} & \mathrm{GL}_{n+1}(A) \\ \mathrm{Nrd}_n \downarrow & & \mathrm{Nrd}_{n+1} \downarrow \\ k^\times & \xrightarrow{id} & k^\times \end{array}$$

commutes.

Proof: By the construction of reduced norm maps, it is enough to check commutativity after base change to a Galois splitting field of k . There the diagram becomes

$$\begin{array}{ccc} \mathrm{GL}_{nm}(k) & \xrightarrow{i_{nm,(n+1)m}} & \mathrm{GL}_{(n+1)m}(k) \\ \det \downarrow & & \det \downarrow \\ k^\times & \xrightarrow{\mathrm{id}} & k^\times, \end{array}$$

and commutativity is straightforward. \square

By the lemma, the collection of reduced norm homomorphisms $\mathrm{Nrd}_n : \mathrm{GL}_n(A) \rightarrow k^\times$ gives rise to a map $\mathrm{Nrd}_\infty : \mathrm{GL}_\infty(A) \rightarrow k^\times$ which induces a map

$$\mathrm{Nrd} : K_1(A) \rightarrow k^\times$$

called the *reduced norm map* for K_1 .

By construction, its composite with the natural map $A^\times \rightarrow K_1(A)$ induced by $A^\times = \mathrm{GL}_1(A) \rightarrow \mathrm{GL}_\infty(A)$ is the usual reduced norm $\mathrm{Nrd} : A^\times \rightarrow k^\times$. Thus for all positive n the isomorphism $K_1(A) \cong K_1(M_n(A))$ of Lemma 2.8.6 yields the following remarkable fact:

Corollary 2.8.10 (Dieudonné) *For a central simple k -algebra A we have*

$$\mathrm{Nrd}(A^\times) = \mathrm{Nrd}_n(\mathrm{GL}_n(A))$$

for all $n \geq 1$.

We note the following compatibility property.

Proposition 2.8.11 *For a central simple k -algebra A and a finite field extension $K|k$ the diagram*

$$\begin{array}{ccc} K_1(A_K) & \xrightarrow{N_{K|k}} & K_1(A) \\ \mathrm{Nrd}_{A_K} \downarrow & & \mathrm{Nrd}_A \downarrow \\ K^\times & \xrightarrow{N_{K|k}} & k^\times \end{array}$$

commutes.

Proof: Again this can be checked after base change to a Galois splitting field of A . After such a base change the field K may not remain a field any more, but may become a finite product of fields. Still, the definition of the norm map $N_{K|k} : K_1(A_K) \rightarrow K_1(A)$ immediately generalises to this setting, so we are reduced to checking the commutativity of the diagram

$$\begin{array}{ccc} K_1(M_m(K)) & \xrightarrow{N_{K|k}} & K_1(M_m(k)) \\ \det \downarrow & & \det \downarrow \\ K^\times & \xrightarrow{N_{K|k}} & k^\times \end{array}$$

where m is the degree of A . By Lemma 2.8.6 and Remark 2.8.5 (2) both vertical maps are isomorphisms. The composite map

$$K^\times \cong K_1(M_m(K)) \longrightarrow K_1(M_m(k)) \cong k^\times$$

is nothing but the composite

$$K^\times \rightarrow \text{End}_k(K) \xrightarrow{\det} k,$$

which is indeed the norm map $N_{K|k}$. The lemma follows. \square

Denote by $SK_1(A)$ the kernel of the reduced norm map $\text{Nrd} : K_1(A) \rightarrow k^\times$. The proposition shows that for each finite extension $K|k$ there is a norm map

$$N_{K|k} : SK_1(A_K) \rightarrow SK_1(A).$$

We now come to the main theorem of this section.

Theorem 2.8.12 (Wang) *If A is a central simple k -algebra of prime degree p , then $SK_1(A) = 0$.*

Proof: The case when A is split is immediate from Lemma 2.8.6 and Proposition 2.8.4, so we may assume that A is a division algebra. By Remark 2.8.5 (1) the natural map $A^\times/[A^\times, A^\times] \rightarrow K_1(A)$ is surjective, so each element of $SK_1(A)$ may be represented by some element $a \in A^\times$ of trivial reduced norm. If $a \notin k$, let $L \subset A$ be the k -subalgebra generated by a ; it is a degree p field extension of k . Otherwise take L to be any degree p extension of k contained in A . By Proposition 2.6.3 (2) we have $N_{L|k}(a) = 1$. The algebra $A_L := A \otimes_k L$ contains the subalgebra $L \otimes_k L$ which is not a division algebra, hence neither is A_L . Since $\deg_L(A_L) = p$, Wedderburn's theorem shows that

$A \otimes_k L$ must be split. By the split case we have $SK_1(A_L) = 0$, hence the composite map

$$SK_1(A) \rightarrow SK_1(A_L) \xrightarrow{N_{L|k}} SK_1(A_L)$$

is trivial. Proposition 2.8.8 then implies that $pSK_1(A) = 0$. We now distinguish two cases.

Case 1: The extension $L|k$ is separable. Take a Galois closure $\tilde{L}|k$ of L and denote by $K|k$ the fixed field of a p -Sylow subgroup in $\text{Gal}(\tilde{L}|k)$. Since $\text{Gal}(\tilde{L}|k)$ is a subgroup of the symmetric group S_p , the extension $\tilde{L}|K$ is a cyclic Galois extension of degree p . By Proposition 2.8.8 the composite

$$SK_1(A) \rightarrow SK_1(A_K) \xrightarrow{N_{K|k}} SK_1(A)$$

is multiplication by $[K : k]$ which is prime to p . But we know that $pSK_1(A) = 0$, so the map $SK_1(A) \rightarrow SK_1(A_K)$ is injective. Up to replacing k by K and L by \tilde{L} , we may thus assume that $L|k$ is cyclic of degree p . Let σ be a generator of $\text{Gal}(L|k)$. According to the classical form of Hilbert's Theorem 90 (Example 2.3.4), there exists $c \in L^\times$ satisfying $a = c^{-1}\sigma(c)$. On the other hand, L is a subfield of A which has degree p over k , so by Lemma 2.5.4 we find $b \in A^\times$ with $b^{-1}cb = \sigma(c)$. Hence $a = c^{-1}\sigma(c) = c^{-1}b^{-1}cb$ is a commutator in A^\times , and as such yields a trivial element in $SK_1(A)$.

Case 2: The extension $L|k$ is purely inseparable. In this case $N_{L|k}(x) = x^p = 1$ and thus $(x - 1)^p = 0$. Since A is a division algebra, we must have $x = 1$, and the result follows. \square

Remarks 2.8.13

1. With a little more knowledge of the theory of central simple algebras the theorem can be generalised to division algebras of arbitrary squarefree degree. See Chapter 4, Exercise 9.
2. In the same paper (Wang [1]) that contains the above theorem, Wang showed that over a number field the group $SK_1(A)$ is trivial for an arbitrary central simple algebra A . However, this is not so over an arbitrary field. Platonov [1] constructed examples of algebras A of degree p^2 for all primes p such that $SK_1(A) \neq 0$. For further work on $SK_1(A)$, see Merkurjev [4] and Suslin [3].

EXERCISES

1. Prove that the tensor product $D_1 \otimes_k D_2$ of two division algebras of coprime degrees is a division algebra. [*Hint:* Apply Rieffel's lemma to a minimal left ideal L in $D_1 \otimes_k D_2$. Then show that $\dim_k(D_1 \otimes_k D_2) = \dim_k L$.]
2. Determine the cohomology set $H^1(G, \mathrm{SL}_n(K))$ for a finite Galois extension $K|k$ with group G .
3. Let $K|k$ be a finite Galois extension with group G , and let $B(K) \subset \mathrm{GL}_2(K)$ be the subgroup of upper triangular matrices.
 - (a) Identify the quotient $\mathrm{GL}_2(K)/B(K)$ as a G -set with $\mathbf{P}^1(K)$, the set of K -points of the projective line.
 - (b) Show that $H^1(G, B(K)) = 1$. [*Hint:* Exploit Proposition 2.7.1.]
 - (c) Denote by K^+ the additive group of K . Show that $H^1(G, K^+) = 1$. [*Hint:* Observe that sending an element $a \in K^+$ to the 2×2 matrix (a_{ij}) with $a_{11} = a_{22} = 1, a_{21} = 0$ and $a_{12} = a$ defines a G -equivariant embedding $K^+ \rightarrow B(K)$.]
4. Let k be a field containing a primitive m -th root of unity ω . Take $a, b \in k^\times$ satisfying the condition in Proposition 2.5.5 (1). Prove that the class of the cyclic algebra $(a, b)_\omega$ has order dividing m in the Brauer group of k .
5. Show that the class of the cyclic algebra $(a, 1 - a)_\omega$ is trivial in the Brauer group for all $a \in k^\times$.
6. Show that the following are equivalent for a central simple k -algebra A :
 - A is split.
 - The reduced norm map $\mathrm{Nrd} : (A \otimes_k F)^\times \rightarrow F^\times$ is surjective for all field extensions $F|k$.
 - t is a reduced norm from the algebra $A \otimes_k k((t))$.
7. Let A be a central simple k -algebra of degree n . Assume that there exists a finite extension $K|k$ of degree prime to n that is a splitting field of A . Show that A is split. [*Hint:* Use the last statement of the previous exercise.]
8. Let A be a central simple k -algebra, and let $K|k$ be a finite field extension which splits A . Show that $N_{K|k}(K^\times) \subset \mathrm{Nrd}(A^\times)$. [*Hint:* Use Propositions 2.8.4 and 2.8.11 (2).]
9. Let k be an infinite field, and A a central simple k -algebra of degree n .
 - (a) Show that the set $[A^\times, A^\times]$ is Zariski dense in A viewed as an n^2 -dimensional affine space. [*Hint:* Argue as in the proof of Proposition 2.2.5.]

- (b) Given $a \in A^\times$, show that there exist $x, y \in A^\times$ such that the k -subalgebra of A generated by $a[x, y]$ is of dimension n .
10. Show that for a central simple algebra over an infinite field k the subgroup $\text{Nrd}(A^\times) \subset k^\times$ is generated by the subgroups $N_{K|k}(K^\times)$ with $K|k$ running over the finite field extensions which split A . [*Hint*: Reduce to the case of a division algebra and use the previous exercise.]

Chapter 3

Techniques From Group Cohomology

In order to pursue our study of Brauer groups, we need some basic notions from the cohomology theory of groups with abelian coefficient modules. This is a theory which is well-documented in the literature; we only establish here the facts we shall need in the sequel, for the ease of the reader. In particular, we establish the basic exact sequences, construct cup-products and study the maps relating the cohomology of a group to that of a subgroup or a quotient. In accordance with the current viewpoint in homological algebra, we emphasize the use of complexes and projective resolutions, rather than that of explicit cocycles and the technique of dimension-shifting (though the latter are also very useful).

As already said, the subject matter of this chapter is fairly standard and almost all facts may already be found in the first monograph written on homological algebra, that of Cartan and Eilenberg [1]. Some of the constructions were first developed with applications to class field theory in view. For instance, Shapiro's lemma first appears in a footnote to Weil [1], then with a (two-page) proof in Hochschild-Nakayama [1].

3.1 Definition of Cohomology Groups

Let G be a group. By a (*left*) G -module we shall mean an abelian group A equipped with a left action by G . Notice that this is the same as giving a left module over the integral group ring $\mathbf{Z}[G]$: indeed, for elements $\sum n_\sigma \sigma \in \mathbf{Z}[G]$ and $a \in A$ we may define $(\sum n_\sigma \sigma)a := \sum n_\sigma \sigma(a)$ and conversely, a $\mathbf{Z}[G]$ -module structure implies in particular the existence of “multiplication-by- σ ” maps on A for all $\sigma \in G$. We say that A is a *trivial* G -module if G acts trivially on A , i.e. $\sigma a = a$ for all $\sigma \in G$ and $a \in A$. By a G -homomorphism we mean a homomorphism $A \rightarrow B$ of abelian groups compatible with the G -action. Denote by $\text{Hom}_G(A, B)$ the set of G -homomorphisms $A \rightarrow B$; it is an abelian group under the natural addition of homomorphisms. Recall also

that we denote by A^G the subgroup of G -invariant elements in a G -module A .

We would like to define for all G -modules A and all integers $i \geq 0$ abelian groups $H^i(G, A)$ subject to the following three properties.

1. $H^0(G, A) = A^G$ for all G -modules A .
2. For all G -homomorphisms $A \rightarrow B$ there exist canonical maps

$$H^i(G, A) \rightarrow H^i(G, B)$$

for all $i \geq 0$.

3. Given a short exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

of G -modules, there exists an infinite long exact sequence

$$\dots \rightarrow H^i(G, A) \rightarrow H^i(G, B) \rightarrow H^i(G, C) \rightarrow H^{i+1}(G, A) \rightarrow \dots$$

of abelian groups, starting from $i = 0$.

In other words, we would like to generalise the $H^1(G, A)$ introduced in the previous chapter to higher dimensions, and in particular we would like to continue the long exact sequence of Proposition 2.7.1 to an infinite sequence. This is known to be possible only when A is commutative; for non-commutative A reasonable definitions have been proposed only for $i = 2$ and 3, but we shall not consider them here.

To construct the groups $H^i(G, A)$ we begin by some reminders concerning left modules over a ring R which is not necessarily commutative but has a unit element 1. Recall that a (*cohomological*) *complex* A^\bullet of R -modules is a sequence of R -module homomorphisms

$$\dots \xrightarrow{d^{i-1}} A^i \xrightarrow{d^i} A^{i+1} \xrightarrow{d^{i+1}} A^{i+2} \xrightarrow{d^{i+2}} \dots$$

for all $i \in \mathbf{Z}$, satisfying $d^{i+1} \circ d^i = 0$ for all i . For $i < 0$ we shall also use the convention $A_{-i} := A^i$. We introduce the notations

$$Z^i(A^\bullet) := \ker(d^i), \quad B^i(A^\bullet) := \operatorname{Im}(d^{i-1}) \quad \text{and} \quad H^i(A^\bullet) := Z^i(A^\bullet)/B^i(A^\bullet).$$

The complex A^\bullet is said to be *acyclic* or *exact* if $H^i(A^\bullet) = 0$ for all i .

A *morphism of complexes* $\phi : A^\bullet \rightarrow B^\bullet$ is a collection of homomorphisms $\phi^i : A^i \rightarrow B^i$ for all i such that the diagrams

$$\begin{array}{ccc} A^i & \longrightarrow & A^{i+1} \\ \phi^i \downarrow & & \downarrow \phi^{i+1} \\ B^i & \longrightarrow & B^{i+1} \end{array}$$

commute for all i . By this defining property, a morphism of complexes $A^\bullet \rightarrow B^\bullet$ induces maps $H^i(A^\bullet) \rightarrow H^i(B^\bullet)$ for all i . A *short exact sequence of complexes* is a sequence of morphisms of complexes

$$0 \rightarrow A^\bullet \rightarrow B^\bullet \rightarrow C^\bullet \rightarrow 0$$

such that the sequences

$$0 \rightarrow A^i \rightarrow B^i \rightarrow C^i \rightarrow 0$$

are exact for all i . Now we have the following basic fact which gives the key to the construction of cohomology groups satisfying property 3 above.

Proposition 3.1.1 *Let*

$$0 \rightarrow A^\bullet \rightarrow B^\bullet \rightarrow C^\bullet \rightarrow 0$$

be a short exact sequence of complexes of R -modules. Then there is a long exact sequence

$$\dots \rightarrow H^i(A^\bullet) \rightarrow H^i(B^\bullet) \rightarrow H^i(C^\bullet) \xrightarrow{\partial} H^{i+1}(A^\bullet) \rightarrow H^{i+1}(B^\bullet) \rightarrow \dots$$

The map ∂ is usually called the *connecting homomorphism* or the *(co)-boundary map*.

For the proof of the proposition we need the following equally basic lemma.

Lemma 3.1.2 (The Snake Lemma) *Given a commutative diagram of R -modules*

$$\begin{array}{ccccccc} A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' \end{array}$$

with exact rows, there is an exact sequence

$$\ker(\alpha) \rightarrow \ker(\beta) \rightarrow \ker(\gamma) \rightarrow \operatorname{coker}(\alpha) \rightarrow \operatorname{coker}(\beta) \rightarrow \operatorname{coker}(\gamma).$$

Proof: The construction of all maps in the sequence is immediate, except for the map $\partial : \ker(\gamma) \rightarrow \operatorname{coker}(\alpha)$. For this, lift $c \in \ker(\gamma)$ to $b \in B$. By commutativity of the right square, the element $\beta(b)$ maps to 0 in C' , hence it comes from a unique $a' \in A'$. Define $\partial(c)$ as the image of a' in $\operatorname{coker}(\alpha)$. Two choices of b differ by an element $a \in A$ which maps to 0 in $\operatorname{coker}(\alpha)$, so ∂ is well-defined. Checking exactness is left as an exercise to the readers. \square

Proof of Proposition 3.1.1: Applying the Snake Lemma to the diagram

$$\begin{array}{ccccccc}
 A^i/B^i(A^\bullet) & \longrightarrow & B^i/B^i(B^\bullet) & \longrightarrow & C^i/B^i(C^\bullet) & \longrightarrow & 0 \\
 & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\
 0 & \longrightarrow & Z^{i+1}(A^\bullet) & \longrightarrow & Z^{i+1}(B^\bullet) & \longrightarrow & Z^{i+1}(C^\bullet)
 \end{array}$$

yields a long exact sequence

$$H^i(A^\bullet) \rightarrow H^i(B^\bullet) \rightarrow H^i(C^\bullet) \rightarrow H^{i+1}(A^\bullet) \rightarrow H^{i+1}(B^\bullet) \rightarrow H^{i+1}(C^\bullet),$$

and the proposition is obtained by splicing these sequences together. \square

We also have to recall the notion of *projective* R -modules. By definition, these are R -modules P for which the natural map $\text{Hom}(P, A) \rightarrow \text{Hom}(P, B)$ given by $\lambda \rightarrow \alpha \circ \lambda$ is surjective for every *surjection* $\alpha : A \rightarrow B$.

Lemma 3.1.3

1. *The R -module R is projective.*
2. *Arbitrary direct sums of projective modules are projective.*

Proof: For the first statement, given an R -homomorphism $\lambda : R \rightarrow B$ and a surjection $A \rightarrow B$, lift λ to an element of $\text{Hom}(R, A)$ by lifting $\lambda(1)$ to an element of A . The second statement is immediate from the compatibility of Hom -groups with direct sums in the first variable. \square

Recall also that a *free* R -module is by definition an R -module isomorphic to a (possibly infinite) direct sum of copies of the R -module R . The above lemma then yields:

Corollary 3.1.4 *A free R -module is projective.*

Example 3.1.5 Given an R -module A , define a free R -module $F(A)$ by taking an infinite direct sum of copies of R indexed by the elements of A . One has a surjection $\pi_A : F(A) \rightarrow A$ induced by mapping 1_a to a , where 1_a is the element of $F(A)$ with 1 in the component corresponding to $a \in A$ and 0 elsewhere.

As a first application of this example, we prove the following lemma:

Lemma 3.1.6 *An R -module P is projective if and only if there exist an R -module M and a free R -module F with $P \oplus M \cong F$.*

Proof: For sufficiency, extend a map $\lambda : P \rightarrow B$ to F by defining it to be 0 on M and use projectivity of F . For necessity, take F to be the free R -module $F(P)$ associated with P in the above example. We claim that we have an isomorphism as required, with $M = \ker(\pi_P)$. Indeed, as P is projective, we may lift the identity map of P to a map $\pi : P \rightarrow F(P)$ with $\pi_P \circ \pi = \text{id}_P$. \square

For each R -module A there exist *projective resolutions*, i.e. infinite exact sequences

$$\cdots \rightarrow P_2 \rightarrow P_1 \rightarrow P_0 \rightarrow A \rightarrow 0$$

with P_i projective. One may take, for instance, P_0 to be the free R -module $F(A)$ defined in the example above; in particular, we get a surjection $p_0 : P_0 \rightarrow A$. Once P_i and $p_i : P_i \rightarrow P_{i-1}$ are defined (with the convention $P_{-1} = A$), one defines P_{i+1} and p_{i+1} by applying the same construction to $\ker(p_i)$ in place of A .

Now the basic fact concerning projective resolutions is:

Lemma 3.1.7 *Assume given a diagram*

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & A & \longrightarrow & 0 \\ & & & & & & & & & & \downarrow \alpha \\ \cdots & \longrightarrow & B_2 & \xrightarrow{b_2} & B_1 & \xrightarrow{b_1} & B_0 & \xrightarrow{b_0} & B & \longrightarrow & 0 \end{array}$$

where the upper row is a projective resolution of the R -module A and the lower row is an exact sequence of R -modules. Then there exist maps $\alpha_i : P_i \rightarrow B_i$ for all $i \geq 0$ making the diagram

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & A & \longrightarrow & 0 \\ & & \downarrow \alpha_2 & & \downarrow \alpha_1 & & \downarrow \alpha_0 & & \downarrow \alpha & & \\ \cdots & \longrightarrow & B_2 & \xrightarrow{b_2} & B_1 & \xrightarrow{b_1} & B_0 & \xrightarrow{b_0} & B & \longrightarrow & 0 \end{array}$$

commute. Moreover, if (α_i) and (β_i) are two collections with this property, there exist maps $\gamma_i : P_i \rightarrow B_{i+1}$ for all $i \geq -1$ (with the conventions $P_{-1} = A$, $\alpha_{-1} = \beta_{-1} = \alpha$) satisfying

$$\alpha_i - \beta_i = \gamma_{i-1} \circ p_i + b_{i+1} \circ \gamma_i. \quad (1)$$

Proof: To construct α_i , assume that the α_j are already defined for $j < i$, with the convention $\alpha_{-1} = \alpha$. Observe that $\text{Im}(\alpha_{i-1} \circ p_i) \subset \text{Im}(b_i)$; this is immediate for $i = 0$ and follows from $b_{i-1} \circ \alpha_{i-1} \circ p_i = \alpha_{i-2} \circ p_{i-1} \circ p_i = 0$ for

$i > 0$ by exactness of the lower row. Hence by the projectivity of P_i we may define α_i as a preimage in $\text{Hom}(P_i, B_i)$ of the map $\alpha_{i-1} \circ p_i : P_i \rightarrow \text{Im}(b_i)$. For the second statement, define $\gamma_{-1} = 0$ and assume γ_j defined for $j < i$ satisfying (1) above. This implies $\text{Im}(\alpha_i - \beta_i - (\gamma_{i-1} \circ p_i)) \subset \text{Im } b_{i+1}$ because of

$$b_i \circ (\alpha_i - \beta_i - (\gamma_{i-1} \circ p_i)) = (\alpha_{i-1} - \beta_{i-1}) \circ p_i - b_i \circ \gamma_{i-1} \circ p_i = \gamma_{i-2} \circ p_{i-1} \circ p_i = 0,$$

so we may define γ_i as a preimage of $\alpha_i - \beta_i - (\gamma_{i-1} \circ p_i) \in \text{Hom}(P_i, \text{Im}(b_{i+1}))$ in $\text{Hom}(P_i, B_{i+1})$, again using the projectivity of P_i . \square

Now we can construct the cohomology groups $H^i(G, A)$.

Construction 3.1.8 Let G be a group and A a G -module. Take a projective resolution $P_\bullet = (\cdots \rightarrow P_2 \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0)$ of the trivial G -module \mathbf{Z} . Consider the sequence $\text{Hom}_G(P_\bullet, A)$ defined by

$$\text{Hom}_G(P_0, A) \rightarrow \text{Hom}_G(P_1, A) \rightarrow \text{Hom}_G(P_2, A) \rightarrow \dots$$

where the maps $\text{Hom}_G(P_i, A) \rightarrow \text{Hom}_G(P_{i+1}, A)$ are defined by $\lambda \mapsto \lambda \circ p_{i+1}$. The fact that P_\bullet is a complex of G -modules implies that $\text{Hom}_G(P_\bullet, A)$ is a complex of abelian groups; we index it by defining $\text{Hom}_G(P_i, A)$ to be the term in degree i . We may now put

$$H^i(G, A) := H^i(\text{Hom}_G(P_\bullet, A))$$

for $i \geq 0$.

Proposition 3.1.9 *The groups $H^i(G, A)$ satisfy properties 1-3 postulated at the beginning of this section, and their isomorphism class does not depend on the choice of the resolution P_\bullet .*

Proof: Notice first that $\text{Hom}_G(\mathbf{Z}, A) \cong A^G$, the isomorphism arising from sending a G -homomorphism $\phi : \mathbf{Z} \rightarrow A$ to $\phi(1)$. On the other hand, every G -homomorphism $\mathbf{Z} \rightarrow A$ lifts to $\lambda_0 : P_0 \rightarrow A$ inducing the trivial homomorphism by composition with p_1 . Conversely, each such λ_0 defines an element of $\text{Hom}_G(\mathbf{Z}, A)$, whence property 1. Property 2 is immediate from the construction and property 3 follows from Proposition 3.1.1 applied to the sequence of complexes

$$0 \rightarrow \text{Hom}_G(P_\bullet, A) \rightarrow \text{Hom}_G(P_\bullet, B) \rightarrow \text{Hom}_G(P_\bullet, C) \rightarrow 0,$$

which is exact because the P_i are projective. For the second statement, let Q_\bullet be another projective resolution of \mathbf{Z} and apply Lemma 3.1.7 with

$A = \mathbf{Z}$, $B^\bullet = Q_\bullet$ and $\alpha = \text{id}$. We get maps $\alpha_i : P_i \rightarrow Q_i$ inducing $\alpha_i^* : H^i(\text{Hom}_G(Q_i, A)) \rightarrow H^i(\text{Hom}_G(P_i, A))$ on cohomology. Exchanging the roles of the resolutions P_\bullet and Q_\bullet we also get maps $\beta_i : Q_i \rightarrow P_i$ inducing $\beta_i^* : H^i(\text{Hom}_G(P_i, A)) \rightarrow H^i(\text{Hom}_G(Q_i, A))$. We show that the compositions $\alpha_i^* \circ \beta_i^*$ and $\beta_i^* \circ \alpha_i^*$ are identity maps. By symmetry it is enough to do this for the first one. Apply the second statement of Lemma 3.1.7 with P_i in place of B^i and the maps $\beta_i \circ \alpha_i$ and id_{P_i} in place of the α_i and β_i of the lemma. We get $\gamma_i : P_i \rightarrow P_{i+1}$ satisfying $\beta_i \circ \alpha_i - \text{id}_{P_i} = \gamma_{i-1} \circ p_i + p_{i+1} \circ \gamma_i$, whence $\lambda \circ \beta_i \circ \alpha_i - \lambda = \lambda \circ \gamma_{i-1} \circ p_i$ for a map $\lambda \in \text{Hom}_G(P_i, A)$ satisfying $\lambda \circ p_{i+1} = 0$. This means precisely that $\lambda \circ \beta_i \circ \alpha_i - \lambda$ is in the image of the map $\text{Hom}_G(P_{i-1}, A) \rightarrow \text{Hom}_G(P_i, A)$, i.e. $(\beta_i \circ \alpha_i)^* = \alpha_i^* \circ \beta_i^*$ equals the identity map of $H^i(\text{Hom}_G(P_i, A))$. \square

Remarks 3.1.10

1. The above construction is a special case of that of Ext-groups in homological algebra: for two R -modules M and N these are defined by $\text{Ext}^i(M, N) := H^i(\text{Hom}_R(P_\bullet, N))$ with a projective resolution P_\bullet of M . The same argument as above shows independence of the choice of P_\bullet . In this parlance we therefore get $H^i(G, A) = \text{Ext}_{\mathbf{Z}[G]}^i(\mathbf{Z}, A)$.
2. It follows from the definition that cohomology groups satisfy certain natural functorial properties. Namely, if

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A' & \longrightarrow & B' \end{array}$$

is a commutative diagram of G -modules, then the associated diagrams

$$\begin{array}{ccc} H^i(G, A) & \longrightarrow & H^i(G, B) \\ \downarrow & & \downarrow \\ H^i(G, A') & \longrightarrow & H^i(G, B') \end{array}$$

commute for all $i \geq 0$. Moreover, given a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

of short exact sequences, the diagrams

$$\begin{array}{ccc} H^i(G, C) & \longrightarrow & H^{i+1}(G, A) \\ \downarrow & & \downarrow \\ H^i(G, C') & \longrightarrow & H^{i+1}(G, A') \end{array}$$

coming from the functorial property and the long exact sequences commute for all $i \geq 0$.

3.2 Explicit Resolutions

To calculate the groups $H^i(G, A)$ explicitly, one uses concrete projective resolutions. The most useful of these is the following one, inspired by simplicial constructions in topology.

Construction 3.2.1 (The standard resolution) Consider for each $i \geq 0$ the $\mathbf{Z}[G]$ -module $\mathbf{Z}[G^{i+1}]$, where G^{i+1} is the $(i+1)$ -fold direct power of G and the action of G is determined by $\sigma(\sigma_0, \dots, \sigma_i) = (\sigma\sigma_0, \dots, \sigma\sigma_i)$. These are projective (in fact, free) $\mathbf{Z}[G]$ -modules, being isomorphic to $\mathbf{Z}[G]^{i+1}$. For $i > 0$ define G -homomorphisms $\delta^i : \mathbf{Z}[G^{i+1}] \rightarrow \mathbf{Z}[G^i]$ by $\delta^i = \sum_j (-1)^j s_j^i$, where $s_j^i : \mathbf{Z}[G^{i+1}] \rightarrow \mathbf{Z}[G^i]$ is the map determined by sending

$$(\sigma_0, \dots, \sigma_i) \mapsto (\sigma_0, \dots, \sigma_{j-1}, \sigma_{j+1}, \dots, \sigma_i).$$

In this way, we get a projective resolution

$$\dots \rightarrow \mathbf{Z}[G^3] \xrightarrow{\delta^2} \mathbf{Z}[G^2] \xrightarrow{\delta^1} \mathbf{Z}[G] \xrightarrow{\delta^0} \mathbf{Z} \rightarrow 0,$$

where δ^0 sends each σ_i to 1. This resolution is called the *standard resolution* of \mathbf{Z} . To see that the sequence is indeed exact, an immediate calculation shows first that $\delta^i \circ \delta^{i+1} = 0$ for all i . Then fix $\sigma \in G$ and define $h^i : \mathbf{Z}[G^{i+1}] \rightarrow \mathbf{Z}[G^{i+2}]$ by sending $(\sigma_0, \dots, \sigma_i)$ to $(\sigma, \sigma_0, \dots, \sigma_i)$. Another calculation shows $\delta^{i+1} \circ h^i + h^{i-1} \circ \delta^i = \text{id}_{\mathbf{Z}[G^{i+1}]}$, which implies $\ker(\delta^i) = \text{Im}(\delta^{i+1})$.

For a G -module A , one calls the elements of $\text{Hom}_G(\mathbf{Z}[G^{i+1}], A)$ *i-cochains*, whereas those of $Z^{i+1}(\text{Hom}_G(\mathbf{Z}[G^\bullet], A))$ and $B^{i+1}(\text{Hom}_G(\mathbf{Z}[G^\bullet], A))$ *i-cocycles* and *i-coboundaries*, respectively. We shall denote these respective groups by $C^i(G, A)$, $Z^i(G, A)$ and $B^i(G, A)$. The cohomology groups $H^i(G, A)$ then arise as the groups $H^{i+1}(\text{Hom}_G(\mathbf{Z}[G^\bullet], A))$. We shall see in the example below that for $i = 1$ we get back the notions of the previous chapter (in the commutative case).

For calculations, another expression is very useful.

Construction 3.2.2 (Inhomogeneous cochains) In $\mathbf{Z}[G^{i+1}]$ consider the particular basis elements

$$[\sigma_1, \dots, \sigma_i] := (1, \sigma_1, \sigma_1\sigma_2, \dots, \sigma_1 \dots \sigma_i).$$

From the definition of the G -action on $\mathbf{Z}[G^{i+1}]$ we get that $\mathbf{Z}[G^{i+1}]$ is none but the free $\mathbf{Z}[G]$ -module generated by the elements $[\sigma_1, \dots, \sigma_i]$. A calculation shows that on these elements the differentials δ^i are expressed by

$$\begin{aligned} \delta^i([\sigma_1, \dots, \sigma_i]) &= \sigma_1[\sigma_2, \dots, \sigma_i] + \sum_{j=1}^i (-1)^j [\sigma_1, \dots, \sigma_j\sigma_{j+1}, \dots, \sigma_i] + \\ &+ (-1)^{i+1} [\sigma_1, \dots, \sigma_{i-1}]. \end{aligned} \quad (2)$$

Therefore we may identify i -cochains with functions $[\sigma_1, \dots, \sigma_n] \mapsto a_{\sigma_1, \dots, \sigma_i}$ and compute the maps $\delta_i^* : C^{i-1}(G, A) \rightarrow C^i(G, A)$ by the formula

$$a_{\sigma_1, \dots, \sigma_{i-1}} \mapsto \sigma_1 a_{\sigma_2, \dots, \sigma_i} + \sum_{j=1}^i (-1)^j a_{\sigma_1, \dots, \sigma_j\sigma_{j+1}, \dots, \sigma_i} + (-1)^{i+1} a_{\sigma_1, \dots, \sigma_{i-1}}.$$

The functions $a_{\sigma_1, \dots, \sigma_i}$ are called *inhomogeneous cochains*.

Here is how to calculate the groups $H^i(G, A)$ in low dimensions by means of inhomogeneous cochains.

Examples 3.2.3

1. A 1-cocycle is given by a function $\sigma \mapsto a_\sigma$ satisfying $a_{\sigma_1\sigma_2} = \sigma_1 a_{\sigma_2} + a_{\sigma_1}$. It is a 1-coboundary if and only if it is of the form $\sigma \mapsto \sigma a - a$ for some $a \in A$. We thus get back the first cohomology group defined in the noncommutative situation in the previous chapter. Note that in the special case when G acts trivially on A , i.e. $\sigma(a) = a$ for all $a \in A$, we have $Z^1(G, A) = \text{Hom}(G, A)$ and $B^1(G, A) = 0$, so finally $H^1(G, A) = \text{Hom}(G, A)$.
2. A 2-cocycle is given by a function $(\sigma_1, \sigma_2) \mapsto a_{\sigma_1, \sigma_2}$ satisfying

$$\sigma_1 a_{\sigma_2, \sigma_3} - a_{\sigma_1\sigma_2, \sigma_3} + a_{\sigma_1, \sigma_2\sigma_3} - a_{\sigma_1, \sigma_2} = 0.$$

It is a 2-coboundary, i.e. an element of $\text{Im}(\partial^{1*})$ if it is of the form $\sigma_1 b_{\sigma_2} - b_{\sigma_1\sigma_2} + b_{\sigma_1}$ for some 1-cochain $\sigma \mapsto b_\sigma$.

Remark 3.2.4 Using the above description via cocycles one also gets explicit formulae for the coboundary maps $\delta^i : H^i(G, C) \rightarrow H^{i+1}(G, A)$ in long exact cohomology sequences. In particular, in the case $i = 0$ we get the same answer as in the noncommutative situation (Proposition 2.7.1): given $c \in C^G$, we lift it to an element $b \in B$, and $\delta^0(c)$ is represented by the map $\sigma \mapsto \sigma b - b$, which is readily seen to be a 1-cocycle with values in A .

Example 3.2.5 For some questions (e.g. as in the example of group extensions below) it is convenient to work with *normalised cochains*. These are obtained by considering the free resolution

$$\cdots \rightarrow L_2 \xrightarrow{\delta_n^2} L_1 \xrightarrow{\delta_n^1} L_0 \xrightarrow{\delta_n^0} \mathbf{Z} \rightarrow 0,$$

where L_i is the free G -submodule of $\mathbf{Z}[G^{i+1}]$ generated by those $[\sigma_1, \dots, \sigma_i]$ where none of the σ_j is 1. The morphisms δ_n^i are defined by the same formulae as for the δ^i in (2), except that if we happen to have $\sigma_j \sigma_{j+1} = 1$ for some j in $[\sigma_1, \dots, \sigma_i]$, we set the term involving $\sigma_j \sigma_{j+1}$ on the right hand side to 0. This indeed defines a map $L_i \rightarrow L_{i-1}$, and a calculation shows that we again have $\ker(\delta_n^i) = \text{Im}(\delta_n^{i+1})$. So we have obtained a free resolution of \mathbf{Z} and may use it for computing the cohomology of a G -module A . Elements in $\text{Hom}_G(L_i, A)$ may be identified with inhomogenous i -cochains $a_{\sigma_1, \dots, \sigma_i}$ which have the value 0 whenever one of the σ_j equals 1.

Example 3.2.6 (Group extensions) An important example of 2-cocycles arising ‘in nature’ comes from the theory of group extensions. Consider an exact sequence of groups $0 \rightarrow A \rightarrow E \rightarrow G \xrightarrow{\pi} 1$, with A abelian. The conjugation action of E on A passes to the quotient in G and gives A the structure of a G -module. Now associate with E a 2-cocycle as follows. Choose a *normalised set-theoretic section* of π , i.e. a map $s : G \rightarrow E$ with $s(1) = 1$ and $\pi \circ s = \text{id}_G$. For elements $\sigma_1, \sigma_2 \in G$ the element $a_{\sigma_1, \sigma_2} := s(\sigma_1)s(\sigma_2)s(\sigma_1\sigma_2)^{-1}$ maps to 1 in G , and therefore defines an element of A . An immediate calculation shows that $(\sigma_1, \sigma_2) \mapsto a_{\sigma_1, \sigma_2}$ is a 2-cocycle of G with values in A , which is in fact normalised, i.e. satisfies $a_{1, \sigma} = a_{\sigma, 1} = 1$ for all $\sigma \in G$. Another calculation shows that replacing s by another set-theoretic section yields a 2-cocycle with the same class in $H^2(G, A)$. In this way one associates with E a class $c(E) \in H^2(G, A)$. Furthermore, we see that in the case when there is a section s which is a group homomorphism, i.e. the extension E splits as a semidirect product of G by A , then $c(E) = 0$.

In fact, once we fix a G -action on A , we may consider the set $\text{Ext}(G, A)$ of equivalence classes of extensions E of G by A inducing the given action of G on A modulo the following equivalence relation: two extensions E and

E' are called equivalent if there is an isomorphism $\lambda : E \xrightarrow{\sim} E'$ inducing a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow \text{id} & & \downarrow \lambda & & \downarrow \text{id} & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

The map $E \mapsto c(E)$ is easily seen to preserve this equivalence relation, and in fact induces a bijection between $\text{Ext}(G, A) \rightarrow H^2(G, A)$. The inverse is constructed as follows: one represents a class in $H^2(G, A)$ by a *normalised* cocycle a_{σ_1, σ_2} and defines a group E with underlying set $A \times G$ and group law $(a_1, \sigma_1) \cdot (a_2, \sigma_2) := (a_1 + \sigma_1(a_2) + a_{\sigma_1, \sigma_2}, \sigma_1 \sigma_2)$. The cocycle relation implies that this product is associative, and the fact that a_{σ_1, σ_2} is normalised implies that $(0, 1)$ is a unit element. The element $(-\sigma^{-1}(a) - \sigma^{-1}(a_{\sigma, \sigma^{-1}}), \sigma^{-1})$ yields an inverse for (a, σ) , therefore E is indeed a group and one checks that it is an extension of G by A with $c(E) = [a_{\sigma_1, \sigma_2}]$. All this is verified by straightforward calculations which we leave the readers to carry out or to look up e.g. in Weibel [1], Section 6.6.

Remark 3.2.7 Given a homomorphism $\phi : A \rightarrow B$ of G -modules, the natural map $\phi_* : H^2(G, A) \rightarrow H^2(G, B)$ induced on cohomology has the following interpretation in terms of group extensions: the class $c(E)$ of an extension $0 \rightarrow A \xrightarrow{\iota} E \rightarrow G \rightarrow 1$ is mapped to that of the *pushforward* extension $\phi_*(E)$ defined as the quotient of $B \times E$ by the normal subgroup of elements of the form $(\phi(a), \iota(a)^{-1})$ for $a \in A$. One verifies that $\phi_*(E)$ is indeed an extension of G by B , and that $c(\phi_*(E)) = \phi_*(c(E))$ by the explicit description of the cocycle class $c(E)$ given above.

For special groups other projective resolutions may be useful for computing cohomology, as the examples of cyclic groups show.

Example 3.2.8 Let $G = \mathbf{Z}$. Then the sequence

$$0 \rightarrow \mathbf{Z}[\mathbf{Z}] \rightarrow \mathbf{Z}[\mathbf{Z}] \rightarrow \mathbf{Z} \rightarrow 0$$

gives a projective resolution of the trivial \mathbf{Z} -module \mathbf{Z} , where the second map is given by multiplication by $\sigma - 1$ for a generator σ of \mathbf{Z} considered a cyclic group, and the third one is induced by mapping σ to 1. It is immediate to check the exactness of the sequence, and for a $\mathbf{Z}[\mathbf{Z}]$ -module A we get

$$H^0(\mathbf{Z}, A) = A^\sigma, \quad H^1(\mathbf{Z}, A) = A/(\sigma - 1)A \quad \text{and} \quad H^i(\mathbf{Z}, A) = 0 \quad \text{for} \quad i > 1.$$

Example 3.2.9 Let now G be a finite cyclic group of order n , generated by an element σ . Consider the maps $\mathbf{Z}[G] \rightarrow \mathbf{Z}[G]$ defined by

$$N : a \mapsto \sum_{i=0}^{n-1} \sigma^i a \quad \text{and} \quad \sigma - 1 : a \mapsto \sigma a - a.$$

One checks easily that $\ker(N) = \text{Im}(\sigma - 1)$ and $\text{Im}(N) = \ker(\sigma - 1)$. Hence we obtain a free resolution

$$\dots \xrightarrow{N} \mathbf{Z}[G] \xrightarrow{\sigma-1} \mathbf{Z}[G] \xrightarrow{N} \mathbf{Z}[G] \xrightarrow{\sigma-1} \mathbf{Z}[G] \rightarrow \mathbf{Z} \rightarrow 0,$$

the last map being induced by $\sigma \mapsto 1$.

For a G -module A , define maps $N : A \rightarrow A$ and $\sigma - 1 : A \rightarrow A$ by the same formulae as above and put ${}_N A := \ker(N)$. Using the above resolution, one finds

$$H^0(G, A) = A^G, \quad H^{2i+1}(G, A) = {}_N A / (\sigma - 1)A \quad \text{and} \quad H^{2i+2}(G, A) = A^G / NA \quad (3)$$

for $i > 0$.

Remark 3.2.10 If $K|k$ is a finite Galois extension with cyclic Galois group G as above, the above calculation shows $H^1(G, K^\times) = {}_N K^\times / (\sigma - 1)K^\times$. The first group is trivial by Hilbert's Theorem 90 and we get back the original form of the theorem, as established in Example 2.3.4 of the previous chapter.

3.3 Relation to Subgroups

Let H be a subgroup of G and A an H -module. Then $\mathbf{Z}[G]$ with its canonical G -action is an H -module as well, and we can associate with A the G -module

$$M_H^G(A) := \text{Hom}_H(\mathbf{Z}[G], A)$$

where the action of G on an H -homomorphism $\phi : \mathbf{Z}[G] \rightarrow A$ is given by $(\sigma\phi)(g) := \phi(g\sigma)$ for a basis element g of $\mathbf{Z}[G]$. One sees that $\sigma\phi$ is indeed an H -homomorphism.

Lemma 3.3.1 *Assume moreover given a G -module M . We have a canonical isomorphism*

$$\text{Hom}_G(M, \text{Hom}_H(\mathbf{Z}[G], A)) \xrightarrow{\sim} \text{Hom}_H(M, A)$$

induced by mapping a G -homomorphism $m \rightarrow \phi_m$ in the left hand side group to the H -homomorphism $m \mapsto \phi_m(1)$.

Proof: Given an H -homomorphism $\lambda : M \rightarrow A$, consider the map $m \mapsto \lambda_m$, where $\lambda_m \in \text{Hom}_H(\mathbf{Z}[G], A)$ is the map determined by $g \mapsto \lambda(gm)$. The kind reader will check that we get an element of $\text{Hom}_G(M, \text{Hom}_H(\mathbf{Z}[G], A))$ in this way, and that the two constructions are inverse to each other. \square

Applying the lemma to the terms of a projective resolution P_\bullet of \mathbf{Z} and passing to cohomology groups, we get:

Corollary 3.3.2 (Shapiro's Lemma) *Given a subgroup H of G and an H -module A , there exist canonical isomorphisms*

$$H^i(G, M_H^G(A)) \xrightarrow{\sim} H^i(H, A)$$

for all $i \geq 0$.

The case when $H = \{1\}$ is particularly important. In this case an H -module A is just an abelian group; we denote $M_H^G(A)$ simply by $M^G(A)$ and call it the *co-induced* module associated with A .

Corollary 3.3.3 *The group $H^i(G, M^G(A))$ is trivial for all $i > 0$.*

Proof: In this case the right hand side in Shapiro's lemma is trivial (e.g. because $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Z} \rightarrow 0$ gives a projective resolution of \mathbf{Z}). \square

Remarks 3.3.4

1. It is important to note that the construction of co-induced modules is functorial in the sense that every homomorphism $A \rightarrow B$ of abelian groups induces a G -homomorphism $M^G(A) \rightarrow M^G(B)$. Of course, a similar property holds for the modules $M_H^G(A)$.
2. For a G -module A there is a natural injective map $A \rightarrow M^G(A)$ given by assigning to $a \in A$ the homomorphism $\mathbf{Z}[G] \rightarrow A$ of abelian groups induced by the mapping $\sigma \mapsto \sigma a$.
3. If G is finite, the choice of a \mathbf{Z} -basis of $\mathbf{Z}[G]$ induces a *non-canonical* isomorphism $M^G(A) \cong A \otimes_{\mathbf{Z}} \mathbf{Z}[G]$ for all abelian groups A .

Using Shapiro's lemma we may define two basic maps relating the cohomology of a group to that of a subgroup.

Construction 3.3.5 (Restriction maps) Let G be a group, A a G -module and H a subgroup of G . There are natural maps of G -modules

$$A \xrightarrow{\sim} \text{Hom}_G(\mathbf{Z}[G], A) \rightarrow \text{Hom}_H(\mathbf{Z}[G], A) = M_H^G(A),$$

the first one given by mapping $a \in A$ to the unique G -homomorphism sending 1 to a and the second by considering a G -homomorphism as an H -homomorphism. Taking cohomology and applying Shapiro's lemma we thus get maps

$$\text{Res} : H^i(G, A) \rightarrow H^i(H, A)$$

for all $i \geq 0$, called *restriction maps*. One sees that for $i = 0$ we get the natural inclusion $A^G \rightarrow A^H$.

When the subgroup H has finite index, there is a natural map in the opposite direction.

Construction 3.3.6 (Corestriction maps) Let H be a subgroup of G of finite index n and let A be a G -module.

Given an H -homomorphism $\phi : \mathbf{Z}[G] \rightarrow A$, define a new map $\mathbf{Z}[G] \rightarrow A$ by the assignment

$$\phi_H^G : x \mapsto \sum_{j=1}^n \rho_j \phi(\rho_j^{-1}x),$$

where ρ_1, \dots, ρ_n is a system of left coset representatives for H in G . This is manifestly a group homomorphism which does not depend on the choice of the ρ_j ; indeed, if we replace the system of representatives (ρ_j) by another system $(\rho_j \tau_j)$ with some $\tau_j \in H$, we get $\rho_j \tau_j \phi(\tau_j^{-1} \rho_j^{-1} x) = \rho_j \phi(\rho_j^{-1} x)$ for all j , the map ϕ being an H -homomorphism. Furthermore, the map ϕ_H^G is also a G -homomorphism, because we have for all $\sigma \in G$

$$\sum_{j=1}^n \rho_j \phi(\rho_j^{-1} \sigma x) = \sigma \left(\sum_{j=1}^n (\sigma^{-1} \rho_j) \phi((\sigma^{-1} \rho_j)^{-1} x) \right) = \sigma \left(\sum_{j=1}^n \rho_j \phi(\rho_j^{-1} x) \right),$$

as the $\sigma \rho_j$ form another system of left coset representatives.

The assignment $\phi \mapsto \phi_H^G$ thus defines a well-defined map

$$\text{Hom}_H(\mathbf{Z}[G], A) \rightarrow \text{Hom}_G(\mathbf{Z}[G], A) \cong A,$$

so by taking cohomology and applying Shapiro's lemma we get maps

$$\text{Cor} : H^i(H, A) \rightarrow H^i(G, A)$$

for all $i \geq 0$, called *corestriction maps*.

An immediate consequence of the preceding constructions is the following basic fact.

Proposition 3.3.7 *Let G be a group, H a subgroup of finite index n in G and A a G -module. Then the composite maps*

$$\text{Cor} \circ \text{Res} : H^i(G, A) \rightarrow H^i(G, A)$$

are given by multiplication by n for all $i \geq 0$.

Proof: Indeed, if $\phi : \mathbf{Z}[G] \rightarrow A$ is a G -homomorphism, then for all $x \in \mathbf{Z}[G]$ we have $\phi_H^G(x) = \sum \rho_j \phi(\rho_j^{-1}x) = \sum \rho_j \rho_j^{-1} \phi(x) = n\phi(x)$. \square

In the case $H = \{1\}$ we get:

Corollary 3.3.8 *Let G be a finite group of order n . Then the elements of $H^i(G, A)$ have finite order dividing n for all G -modules A and integers $i > 0$.*

Another basic construction is the following one.

Construction 3.3.9 (Inflation maps) Let G be a group, and H a normal subgroup. Then for a G -module A the submodule A^H of fixed elements under H is stable under the action of G (indeed, for $\sigma \in G, \tau \in H$ and $a \in A^H$ one has $\tau\sigma a = \sigma(\sigma^{-1}\tau\sigma)a = \sigma a$). Thus A^H carries a natural structure of a G/H -module.

Now take a projective resolution P_\bullet of \mathbf{Z} as a trivial G -module and a projective resolution Q_\bullet of \mathbf{Z} as a trivial G/H -module. Each Q_i can be considered as a G -module via the projection $G \rightarrow G/H$, so applying Lemma 3.1.7 with $R = \mathbf{Z}[G]$, $B^\bullet = Q_\bullet$ and $\alpha = \text{id}_{\mathbf{Z}}$ we get a morphism $P_\bullet \rightarrow Q_\bullet$ of complexes of G -modules, whence also a map $\text{Hom}_G(Q_\bullet, A^H) \rightarrow \text{Hom}_G(P_\bullet, A^H)$. Now since $\text{Hom}_G(Q_i, A^H) = \text{Hom}_{G/H}(Q_i, A^H)$ for all i , the former complex equals $\text{Hom}_{G/H}(Q_\bullet, A^H)$, so by taking cohomology we get maps $H^i(G/H, A^H) \rightarrow H^i(G, A^H)$ which do not depend on the choices of P_\bullet and Q_\bullet by the same argument as in the proof of Proposition 3.1.9. Composing with the natural map induced by the G -homomorphism $A^H \rightarrow A$ we finally get maps

$$\text{Inf} : H^i(G/H, A^H) \rightarrow H^i(G, A),$$

for all $i \geq 0$, called *inflation maps*.

Remark 3.3.10 Calculating the inflation maps in terms of the standard resolution of \mathbf{Z} , we see that inflating an i -cocycle $\mathbf{Z}[(G/H)^{i+1}] \rightarrow A^H$ amounts to taking the lifting $\mathbf{Z}[G^{i+1}] \rightarrow A^H$ induced by the projection $G \rightarrow G/H$.

Similarly, one checks that the restriction of a cocycle $\mathbf{Z}[G^{i+1}] \rightarrow A$ to a subgroup H is given by restricting it to a map $\mathbf{Z}[H^{i+1}] \rightarrow A$.

Remark 3.3.11 Given a normal subgroup H in G and a G -module A , with trivial H -action, the inflation map $\text{Inf} : H^2(G/H, A) \rightarrow H^2(G, A)$ has the following interpretation in terms of group extensions: given an extension $0 \rightarrow A \xrightarrow{\pi} E \rightarrow (G/H) \rightarrow 1$, its class $c(E)$ satisfies $\text{Inf}(c(E)) = c(\rho^*(E))$, where $\rho : G \rightarrow G/H$ is the natural projection, and $\rho^*(E)$ is the *pullback* extension $\rho^*(E)$ defined as the subgroup of $E \times G$ given by elements (e, g) satisfying $\pi(e) = \rho(g)$. One verifies that $\rho^*(E)$ is indeed an extension of G by A , and the relation $c(\rho^*(E)) = \text{Inf}(c(E))$ holds by the construction of inflation maps and that of the class $c(E)$ in Example 3.2.6.

We now turn to the last basic construction relative to subgroups.

Construction 3.3.12 (Conjugation) Let P and A be G -modules and H a *normal* subgroup of G . For each $\sigma \in G$ we define a map

$$\sigma_* : \text{Hom}_H(P, A) \rightarrow \text{Hom}_H(P, A)$$

by setting $\sigma_*(\phi)(p) := \sigma^{-1}\phi(\sigma(p))$ for each $p \in P$ and $\phi \in \text{Hom}_H(P, A)$. To see that $\sigma_*(\phi)$ indeed lies in $\text{Hom}_H(P, A)$, we compute for $\tau \in H$

$$\sigma_*(\phi)(\tau(p)) = \sigma^{-1}\phi(\sigma\tau(p)) = \sigma^{-1}\phi(\sigma\tau\sigma^{-1}\sigma(p)) = \sigma^{-1}\sigma\tau\sigma^{-1}\phi(\sigma(p)) = \tau\sigma_*(\phi)(p),$$

where we have used the normality of H in the penultimate step. As σ_*^{-1} is obviously an inverse for σ_* , we get an automorphism of the group $\text{Hom}_H(P, A)$. It follows from the definition that σ_* is the identity for $\sigma \in H$.

Now we apply the above to a projective resolution P_\bullet of the trivial G -module \mathbf{Z} . Note that this is also a resolution by projective H -modules, because $\mathbf{Z}[G]$ is free as a $\mathbf{Z}[H]$ -module (a system of coset representatives yields a basis). The construction yields an automorphism σ_* of the complex $\text{Hom}_H(P_\bullet, A)$, i.e. an automorphism in each term compatible with the G -maps in the resolution. Taking cohomology we thus get automorphisms $\sigma_*^i : H^i(H, A) \rightarrow H^i(H, A)$ in each degree $i \geq 0$, and the same method as in Proposition 3.1.9 implies that they do not depend on the choice of P_\bullet . These automorphisms are trivial for $\sigma \in H$, so we get an action of the quotient G/H on the groups $H^i(H, A)$, called the *conjugation action*.

It is worthwhile to record an explicit consequence of this construction.

Lemma 3.3.13 *Let*

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

be a short exact sequence of G -modules, and H a normal subgroup in G . The long exact sequence

$$0 \rightarrow H^0(H, A) \rightarrow H^0(H, B) \rightarrow H^0(H, C) \rightarrow H^1(H, A) \rightarrow H^1(H, B) \rightarrow \dots$$

is an exact sequence of G/H -modules, where the groups $H^i(H, A)$ are equipped with the conjugation action defined above.

Proof: This follows immediately from the fact that the conjugation action as defined above induces an isomorphism of the exact sequence of complexes

$$0 \rightarrow \text{Hom}_H(P_\bullet, A) \rightarrow \text{Hom}_H(P_\bullet, B) \rightarrow \text{Hom}_H(P_\bullet, C) \rightarrow 0$$

onto itself. \square

This lemma will be handy for establishing the following fundamental exact sequence involving inflation and restriction maps.

Proposition 3.3.14 *Let G be a group, H a normal subgroup and A a G -module. There is a natural map $\tau : H^1(H, A)^{G/H} \rightarrow H^2(G/H, A^H)$ fitting into an exact sequence*

$$\begin{aligned} 0 \rightarrow H^1(G/H, A^H) &\xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A)^{G/H} \xrightarrow{\tau} \\ &\rightarrow H^2(G/H, A^H) \xrightarrow{\text{Inf}} H^2(G, A). \end{aligned}$$

We begin the proof by the following equally useful lemma.

Lemma 3.3.15 *In the situation of the proposition we have*

$$M^G(A)^H \cong M^{G/H}(A) \quad \text{and} \quad H^j(H, M^G(A)) = 0 \quad \text{for all } j > 0.$$

Proof: The first statement follows from the chain of isomorphisms

$$M^G(A)^H = \text{Hom}(\mathbf{Z}[G], A)^H \cong \text{Hom}(\mathbf{Z}[G/H], A) = M^{G/H}(A).$$

As for the second, the already used fact that $\mathbf{Z}[G]$ is free as a $\mathbf{Z}[H]$ -module implies that $M^G(A)$ is isomorphic to a direct sum of copies of $M^H(A)$. But it follows from the definition of cohomology that $H^j(H, \bigoplus M^H(A)) \cong \bigoplus H^j(H, M^H(A))$, which is 0 by Corollary 3.3.3. \square

Proof of Proposition 3.3.14: Define C as the G -module fitting into the exact sequence

$$0 \rightarrow A \rightarrow M^G(A) \rightarrow C \rightarrow 0. \quad (4)$$

This is also an exact sequence of H -modules, so we get a long exact sequence

$$0 \rightarrow A^H \rightarrow M^G(A)^H \rightarrow C^H \rightarrow H^1(H, A) \rightarrow H^1(H, M^G(A)),$$

where the last group is trivial by the first statement of Lemma 3.3.15 and Corollary 3.3.3. Hence we may split up the sequence into two short exact sequences

$$0 \rightarrow A^H \rightarrow M^G(A)^H \rightarrow B \rightarrow 0, \quad (5)$$

$$0 \rightarrow B \rightarrow C^H \rightarrow H^1(H, A) \rightarrow 0. \quad (6)$$

Using Lemma 3.3.13 we see that these are exact sequences of G/H -modules. Taking the long exact sequence in G/H -cohomology coming from (5) we get

$$0 \rightarrow A^G \rightarrow M^G(A)^G \rightarrow B^{G/H} \rightarrow H^1(G/H, A^H) \rightarrow H^1(G/H, M^G(A)^H),$$

where the last group is trivial by Lemma 3.3.15. So we have a commutative diagram with exact rows

$$\begin{array}{ccccccc} & & & 0 & & & \\ & & & \downarrow & & & \\ 0 & \longrightarrow & A^G & \longrightarrow & M^G(A)^G & \longrightarrow & B^{G/H} \longrightarrow H^1(G/H, A^H) \rightarrow 0 \\ & & \downarrow \text{id} & & \downarrow \text{id} & & \downarrow \\ 0 & \longrightarrow & A^G & \longrightarrow & M^G(A)^G & \longrightarrow & C^G \longrightarrow H^1(G, A) \rightarrow 0 \\ & & & & & & \downarrow \\ & & & & & & H^1(H, A)^{G/H} \\ & & & & & & \downarrow \\ & & & & & & H^1(G/H, B) \end{array}$$

where second row comes from the long exact G -cohomology sequence of (4), and the column from the long exact sequence of (6). A diagram chase shows that we obtain from the diagram above an exact sequence

$$0 \rightarrow H^1(G/H, A^H) \xrightarrow{\alpha} H^1(G, A) \xrightarrow{\beta} H^1(H, A)^{G/H} \rightarrow H^1(G/H, B).$$

Here we have to identify the maps α and β with inflation and restriction maps, respectively. For α , this follows by viewing A^H and B as G -modules via the projection $G \rightarrow G/H$ and considering the commutative diagram

$$\begin{array}{ccccc} B^{G/H} & \xrightarrow{\text{id}} & B^G & \longrightarrow & C^G \\ \downarrow & & \downarrow & & \downarrow \\ H^1(G/H, A^H) & \xrightarrow{\lambda} & H^1(G, A^H) & \longrightarrow & H^1(G, A) \end{array}$$

where the composite of the maps in the lower row is by definition the inflation map. Here λ is simply given by viewing a 1-cocycle $G/H \rightarrow A^H$ as a 1-cocycle $G \rightarrow A^H$, and the diagram commutes by the functoriality of the long exact cohomology sequence. As for β , its identification with a restriction map follows from the commutative diagram

$$\begin{array}{ccc} C^G & \longrightarrow & H^1(G, A) \\ \downarrow & & \downarrow \text{Res} \\ C^H & \longrightarrow & H^1(H, A) \end{array}$$

where the left vertical map is the natural inclusion.

Now the remaining part of the required exact sequence comes from the commutative diagram

$$\begin{array}{ccccccc}
 H^1(H, A)^{G/H} & \longrightarrow & H^1(G/H, B) & \longrightarrow & H^1(G/H, C^H) & \xrightarrow{\text{Inf}} & H^1(G, C) \\
 & & \downarrow \cong & & & & \downarrow \cong \\
 & & H^2(G/H, A^H) & & \xrightarrow{\text{Inf}} & & H^2(G, A)
 \end{array}$$

where the top row, coming from (6), is exact at $H^1(G/H, B)$, and the vertical isomorphisms are induced by the long exact sequences coming from (5) and (4), using again that $M^G(A)$ and $M^G(A)^H$ have trivial cohomology. Commutativity of the diagram relies on a compatibility between inflation maps and long exact sequences which is proven in the same way as the one we have just considered for H^1 . Finally, the exactness of the sequence of the proposition at $H^2(G/H, B^H)$ comes from the exactness of the row in the above diagram, together with the injectivity of the inflation map $H^1(G/H, C^H) \rightarrow H^1(G, C)$ that we have already proven (for A in place of C). \square

Remark 3.3.16 The map τ of the proposition is called the *transgression map*. For an explicit description of τ in terms of cocycles, see Neukirch-Schmidt-Wingberg [1], Proposition 1.6.5.

Proposition 3.3.17 *In the situation of the previous proposition, let $i > 1$ be an integer and assume moreover that the groups $H^j(H, A)$ are trivial for $1 \leq j \leq i - 1$. Then there is a natural map*

$$\tau_{i,A} : H^i(H, A)^{G/H} \rightarrow H^{i+1}(G/H, A^H)$$

fitting into an exact sequence

$$\begin{array}{ccccccc}
 0 & \rightarrow & H^i(G/H, A^H) & \xrightarrow{\text{Inf}} & H^i(G, A) & \xrightarrow{\text{Res}} & H^i(H, A)^{G/H} \xrightarrow{\tau_{i,A}} \\
 & & \rightarrow & H^{i+1}(G/H, A^H) & \xrightarrow{\text{Inf}} & H^{i+1}(G, A).
 \end{array}$$

Proof: Embed A into the co-induced module $M^G(A)$ and let C_A be the cokernel of this embedding. The G -module $M^G(A)$ is an H -module in particular, and the assumption that $H^1(H, A)$ vanishes implies the exactness of the sequence $0 \rightarrow A^H \rightarrow M^G(A)^H \rightarrow C_A^H \rightarrow 0$ by the long exact cohomology sequence. This is a short exact sequence of G/H -modules, so taking the associated long exact sequence yields the first and fourth vertical maps in the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{j-1}(G/H, C_A^H) & \xrightarrow{\text{Inf}} & H^{j-1}(G, C_A) & \xrightarrow{\text{Res}} & H^{j-1}(H, C_A)^{G/H} \longrightarrow \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^j(G/H, A^H) & \xrightarrow{\text{Inf}} & H^j(G, A) & \xrightarrow{\text{Res}} & H^j(H, A)^{G/H} \longrightarrow \\
& & \xrightarrow{\tau_{j-1, C_A}} & H^j(G/H, C_A^H) & \xrightarrow{\text{Inf}} & H^j(G, C_A) & \\
& & & \downarrow & & \downarrow & \\
& & \xrightarrow{\tau_{j, A}} & H^{j+1}(G/H, A^H) & \xrightarrow{\text{Inf}} & H^{j+1}(G, A) &
\end{array}$$

where the other vertical maps come from long exact sequences associated with $0 \rightarrow A \rightarrow M^G(A) \rightarrow C_A \rightarrow 0$, and the maps $\tau_{j,A}$ and τ_{j-1, C_A} are yet to be defined. The second and fifth vertical maps are isomorphisms because $H^j(G, M^G(A)) = 0$ for $j > 0$ according to Corollary 3.3.3. Moreover, Lemma 3.3.15 shows that the groups $H^j(G/H, M^G(A)^H)$ and $H^j(H, M^G(A))$ are also trivial for $j > 0$, hence the first and fourth vertical maps and the map $H^{j-1}(H, C_A) \rightarrow H^j(H, A)$ inducing the third vertical map are isomorphisms as well. In particular, the assumption yields that $H^j(H, C_A) = 0$ for all $1 \leq j < i - 1$. By induction starting from the case $i = 1$ proven in the previous proposition, we may thus assume that the map τ_{i-1, C_A} has been defined and the upper row is exact for $j = i$. We may then define $\tau_{i,A}$ by identifying it to τ_{i-1, C_A} via the isomorphisms in the diagram, and from this obtain an exact lower row. \square

Remarks 3.3.18

1. The proposition is easy to establish using the *Hochschild-Serre spectral sequence* for group extensions (see e.g. Shatz [1] or Weibel [1]).
2. The argument proving part *b*) above is an example of a very useful technique called *dimension shifting*, which consists of proving statements about cohomology groups by embedding G -modules into co-induced modules and then using induction in long exact sequences. For other examples where this technique can be applied, see the exercises.

3.4 Cup-products

In this section we construct an associative product operation

$$H^i(G, A) \times H^j(G, B) \rightarrow H^{i+j}(G, A \otimes B), \quad (a, b) \mapsto a \cup b$$

which is *graded-commutative*, i.e. it satisfies

$$a \cup b = (-1)^{ij}(b \cup a). \quad (7)$$

Here $A \otimes B$ is the tensor product of A and B over \mathbf{Z} , equipped with the G -module structure given by $\sigma(a \otimes b) = \sigma(a) \otimes \sigma(b)$. Note that in general this is different from the tensor product of A and B over $\mathbf{Z}[G]$.

We begin the construction with general considerations on complexes. We restrict to the case of abelian groups, the only one we shall need.

Construction 3.4.1 Let A^\bullet and B^\bullet be complexes of abelian groups. We define the *tensor product complex* $A^\bullet \otimes B^\bullet$ by first considering the *double complex*

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
 \dots & \longrightarrow & A^{i-1} \otimes B^{j+1} & \longrightarrow & A^i \otimes B^{j+1} & \longrightarrow & A^{i+1} \otimes B^{j+1} \longrightarrow \dots \\
 & & \uparrow & & \uparrow & & \uparrow \\
 \dots & \longrightarrow & A^{i-1} \otimes B^j & \longrightarrow & A^i \otimes B^j & \longrightarrow & A^{i+1} \otimes B^j \longrightarrow \dots \\
 & & \uparrow & & \uparrow & & \uparrow \\
 \dots & \longrightarrow & A^{i-1} \otimes B^{j-1} & \longrightarrow & A^i \otimes B^{j-1} & \longrightarrow & A^{i+1} \otimes B^{j-1} \longrightarrow \dots \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & \vdots & & \vdots & & \vdots
 \end{array} \quad (8)$$

where the horizontal maps $\partial_{ij}^h : A^i \otimes B^j \rightarrow A^{i+1} \otimes B^j$ are given by $\partial_A^i \otimes \text{id}$ and the vertical maps $\partial_{ij}^v : A^i \otimes B^j \rightarrow A^i \otimes B^{j+1}$ by $\text{id} \otimes (-1)^i \partial_B^j$. In this way, the squares *anti-commute*, i.e. one has

$$\partial_{i,j+1}^h \circ \partial_{ij}^v = -\partial_{i+1,j}^v \circ \partial_{ij}^h.$$

Now take the *total complex* associated with this double complex. By definition, this is the complex T^\bullet with

$$T^n = \bigoplus_{i+j=n} A^i \otimes B^j$$

and $\partial^n : T^n \rightarrow T^{n+1}$ given on the component $A^i \otimes B^j$ by $\partial_{ij}^h + \partial_{ij}^v$. The above anti-commutativity then implies $\partial^{n+1} \circ \partial^n = 0$, i.e. that T^\bullet is a complex. We define T^\bullet to be the tensor product of A^\bullet and B^\bullet and denote it by $A^\bullet \otimes B^\bullet$.

We now proceed to the second step of the construction.

Construction 3.4.2 In the situation of the above construction, assume further given abelian groups A and B . Consider the complexes $\text{Hom}(A^\bullet, A)$ and $\text{Hom}(B^\bullet, B)$ whose degree i terms are $\text{Hom}(A^{-i}, A)$ and $\text{Hom}(B^{-i}, B)$, respectively, with differentials induced by those of A^\bullet and B^\bullet . We construct a product operation

$$H^i(\text{Hom}(A^\bullet, A)) \times H^j(\text{Hom}(B^\bullet, B)) \rightarrow H^{i+j}(\text{Hom}(A^\bullet \otimes B^\bullet, A \otimes B)) \quad (9)$$

as follows. Given homomorphisms $\alpha : A^{-i} \rightarrow A$ and $\beta : B^{-j} \rightarrow B$ with $i + j = n$, the tensor product $\alpha \otimes \beta$ is a homomorphism $A^{-i} \otimes B^{-j} \rightarrow A \otimes B$, and hence defines an element of the degree $i + j$ term in $\text{Hom}(A^\bullet \otimes B^\bullet, A \otimes B)$ via the diagonal embedding

$$\text{Hom}(A^{-i} \otimes B^{-j}, A \otimes B) \rightarrow \text{Hom}\left(\bigoplus_{k+l=i+j} A^{-k} \otimes B^{-l}, A \otimes B\right).$$

Here if $\alpha \in Z^i(\text{Hom}(A^\bullet, A))$ and $\beta \in Z^j(\text{Hom}(B^\bullet, B))$, then by construction of $A^\bullet \otimes B^\bullet$ we have $\alpha \otimes \beta \in Z^{i+j}(\text{Hom}(A^\bullet \otimes B^\bullet, A \otimes B))$. Moreover, if $\alpha \in B^i(\text{Hom}(A^\bullet, A))$, then $\alpha \otimes \beta \in B^{i+j}(\text{Hom}(A^\bullet \otimes B^\bullet, A \otimes B))$ (use again the diagonal embedding), and similarly for β . This defines the required map (9).

We note that if here all abelian groups carry a G -module structure for some group G and α, β are G -homomorphisms, then so is $\alpha \otimes \beta$, hence by restricting to G -homomorphisms we obtain a product

$$H^i(\text{Hom}_G(A^\bullet, A)) \times H^j(\text{Hom}_G(B^\bullet, B)) \rightarrow H^{i+j}(\text{Hom}_G(A^\bullet \otimes B^\bullet, A \otimes B)),$$

where $A \otimes B$ and $A^\bullet \otimes B^\bullet$ are endowed with the G -module structure defined at the beginning of this section.

The next step is the following key proposition. Recall that the lower numbering in a projective resolution P_\bullet is defined by $P_i := P^{-i}$.

Proposition 3.4.3 *Let G be a group, and let P_\bullet be a complex of G -modules which is a projective resolution of the trivial G -module \mathbf{Z} . Then $P_\bullet \otimes P_\bullet$ is a projective resolution of the trivial $\mathbf{Z}[G \times G]$ -module \mathbf{Z} .*

Here the terms of $P_\bullet \otimes P_\bullet$ are endowed by a $G \times G$ -action coming from

$$(\sigma_1, \sigma_2)(p_1 \otimes p_2) = \sigma_1(p_1) \otimes \sigma_2(p_2).$$

The proof is based on the following lemma.

Lemma 3.4.4 *If A^\bullet and B^\bullet are acyclic complexes of free abelian groups, then so is the complex $A^\bullet \otimes B^\bullet$.*

Similarly, if A^\bullet and B^\bullet are complexes of free abelian groups concentrated in nonpositive degrees, acyclic in negative degrees and having a free abelian group as 0-th cohomology, then so is the complex $A^\bullet \otimes B^\bullet$. Moreover, we have $H^0(A^\bullet \otimes B^\bullet) \cong H^0(A^\bullet) \otimes H^0(B^\bullet)$.

Proof: As tensor products and direct sums of free abelian groups are again free, we get that the terms of $A^\bullet \otimes B^\bullet$ are free. The proof of acyclicity is based on the fact that a subgroup of a free abelian group is again free. This implies that for all i , the subgroups $B^i(A^\bullet)$ are free, and in particular projective. Consider for all i the short exact sequences

$$0 \rightarrow Z^i(A^\bullet) \rightarrow A^i \rightarrow B^{i+1}(A^\bullet) \rightarrow 0.$$

The terms here are free abelian groups, so the sequence splits. Moreover, we have $Z^i(A^\bullet) = B^i(A^\bullet)$ by the acyclicity of A^\bullet , therefore we may rewrite the above exact sequence as

$$0 \rightarrow B^i(A^\bullet) \xrightarrow{\text{id}} B^i(A^\bullet) \oplus B^{i+1}(A^\bullet) \xrightarrow{(0, \text{id})} B^{i+1}(A^\bullet) \rightarrow 0.$$

Hence the complex A^\bullet decomposes as an infinite direct sum of complexes of the shape

$$\dots \rightarrow 0 \rightarrow 0 \rightarrow A \xrightarrow{\text{id}} A \rightarrow 0 \rightarrow 0 \rightarrow \dots,$$

and similarly, the complex B^\bullet decomposes as a direct sum of complexes

$$\dots \rightarrow 0 \rightarrow 0 \rightarrow B \xrightarrow{\text{id}} B \rightarrow 0 \rightarrow 0 \rightarrow \dots$$

As the construction of tensor products of complexes manifestly commutes with arbitrary direct sums, we are reduced to check acyclicity for the tensor product of complexes of this type. But by definition, these are complexes of the form

$$\dots \rightarrow 0 \rightarrow 0 \rightarrow A \otimes B \xrightarrow{(\text{id}, \text{id})} (A \otimes B) \oplus (A \otimes B) \xrightarrow{\text{id} - \text{id}} A \otimes B \rightarrow 0 \rightarrow 0 \rightarrow \dots,$$

or similar ones with the second identity map replaced by $-\text{id}$. The first statement is then obvious. The second one is proven by the same argument, and the description of the 0-th cohomology follows from right exactness of the tensor product. \square

Proof of Proposition 3.4.3: By definition, the P_i are direct summands in some free G -module, which is in particular a free abelian group, so they are

also free abelian groups. Hence the second statement of the lemma applies. Therefore the corollary is proven if we show that the terms of $P_\bullet \otimes P_\bullet$ are projective as $\mathbf{Z}[G \times G]$ -modules. For this, notice first the canonical isomorphism $\mathbf{Z}[G \times G] \cong \mathbf{Z}[G] \otimes_{\mathbf{Z}} \mathbf{Z}[G]$: indeed, both abelian groups are free on a basis corresponding to pairs of elements in G . Taking direct sums we get that tensor products of free $\mathbf{Z}[G]$ -modules are free $\mathbf{Z}[G \times G]$ -modules with the above $G \times G$ -action. Finally, if P_i (resp. P_j) are projective $\mathbf{Z}[G]$ -modules with direct complement Q_i (resp. Q_j) in some free $\mathbf{Z}[G]$ -module, the isomorphism

$$(P_i \oplus Q_i) \otimes (P_j \oplus Q_j) \cong (P_i \otimes P_j) \oplus (P_i \otimes Q_j) \oplus (Q_i \otimes P_j) \oplus (Q_i \otimes Q_j)$$

shows that $P_i \otimes P_j$ is a direct summand in a free $\mathbf{Z}[G \times G]$ -module, and hence it is projective. Projectivity of the terms of $P_\bullet \otimes P_\bullet$ follows. \square

Putting everything together, we can finally construct the cup-product.

Construction 3.4.5 Let A and B be G -modules, and P_\bullet a projective resolution of the trivial G -module \mathbf{Z} . Applying Construction 3.4.2 with $A^\bullet = B^\bullet = P_\bullet$ we get maps

$$H^i(\text{Hom}(P_\bullet, A)) \times H^j(\text{Hom}(P_\bullet, B)) \rightarrow H^{i+j}(\text{Hom}(P_\bullet \otimes P_\bullet, A \otimes B)).$$

By the corollary above, the complex $P_\bullet \otimes P_\bullet$ is a projective resolution of \mathbf{Z} as a $G \times G$ -module, so by definition of group cohomology we may rewrite the above as

$$H^i(G, A) \times H^j(G, B) \rightarrow H^{i+j}(G \times G, A \otimes B).$$

On the other hand, the diagonal embedding $G \rightarrow G \times G$ induces a restriction map

$$\text{Res} : H^{i+j}(G \times G, A \otimes B) \rightarrow H^{i+j}(G, A \otimes B).$$

Composing the two, we finally get an operation

$$H^i(G, A) \times H^j(G, B) \rightarrow H^{i+j}(G, A \otimes B),$$

which we call the *cup-product* map. We denote the image of two elements $a \in H^i(G, A)$ and $b \in H^j(G, B)$ by $a \cup b$. The kind reader will check that this construction does not depend on the chosen projective resolution P_\bullet .

Remarks 3.4.6

1. The construction is functorial in the sense that for a morphism $A \rightarrow A'$ of G -modules the diagram

$$\begin{array}{ccc} H^i(G, A) \times H^j(G, B) & \longrightarrow & H^{i+j}(G, A \otimes B) \\ \downarrow & & \downarrow \\ H^i(G, A') \times H^j(G, B) & \longrightarrow & H^{i+j}(G, A' \otimes B) \end{array}$$

commutes, and similarly in the second variable.

2. Given a morphism of G -modules $A \times B \rightarrow C$, we get pairings

$$H^i(G, A) \times H^j(G, B) \rightarrow H^{i+j}(G, C)$$

by composing the cup-product with the natural map

$$H^{i+j}(G, A \otimes B) \rightarrow H^{i+j}(G, C).$$

We shall also refer to these more general pairings as cup-products.

3. It follows from the construction that for $i = j = 0$ the cup-product

$$H^0(G, A) \times H^0(G, B) \rightarrow H^0(G, A \otimes B)$$

is just the natural map $A^G \otimes B^G \rightarrow (A \otimes B)^G$.

Proposition 3.4.7 *The cup-product is associative and graded-commutative, i.e. it satisfies the relation (7).*

Proof: One checks associativity by carefully following the construction. It ultimately boils down to the associativity of the tensor product; we leave the details to the reader. For graded-commutativity, we first work on the level of tensor products of complexes and compare the images of the diagonal maps

$$A^i \otimes B^j \rightarrow \bigoplus_{k+l=i+j} A^k \otimes B^l \quad \text{and} \quad B^j \otimes A^i \rightarrow \bigoplus_{k+l=i+j} B^l \otimes A^k$$

in the complexes $A^\bullet \otimes B^\bullet$ and $B^\bullet \otimes A^\bullet$, respectively. Given $a \otimes b \in A^i \otimes B^j$, the differential in $A^\bullet \otimes B^\bullet$ acts on it by $\partial_A^i \otimes \text{id}_B + (-1)^i \text{id}_A \otimes \partial_B^j$, whereas the differential of $B^\bullet \otimes A^\bullet$ acts on $b \otimes a$ by $\partial_B^j \otimes \text{id}_A + (-1)^j \text{id}_B \otimes \partial_A^i$. Therefore mapping $a \otimes b$ to $(-1)^{ij}(b \otimes a)$ induces an isomorphism of complexes

$$A^\bullet \otimes B^\bullet \xrightarrow{\sim} B^\bullet \otimes A^\bullet.$$

Applying this with $A^\bullet = B^\bullet = P_\bullet$ and performing the rest of the construction of the cup-product, we get that via the above isomorphism the elements $a \cup b$ and $(-1)^{ij}(b \cup a)$ get mapped to the same element in $H^{i+j}(G, A \otimes B)$. \square

The cup-product enjoys the following exactness property.

Proposition 3.4.8 *Given an exact sequence*

$$0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0 \quad (10)$$

of G -modules such that the tensor product over \mathbf{Z}

$$0 \rightarrow A_1 \otimes B \rightarrow A_2 \otimes B \rightarrow A_3 \otimes B \rightarrow 0 \quad (11)$$

with a G -module B remains exact, we have for all elements $a \in H^i(G, A_3)$ and $b \in H^j(G, B)$ the relation

$$\delta(a) \cup b = \delta(a \cup b)$$

in $H^{i+j+1}(G, A_1 \otimes B)$, where the δ are the connecting maps in the associated long exact sequences.

Similarly, if

$$0 \rightarrow B_1 \rightarrow B_2 \rightarrow B_3 \rightarrow 0$$

is an exact sequence of G -modules such that the tensor product over \mathbf{Z}

$$0 \rightarrow A \otimes B_1 \rightarrow A \otimes B_2 \rightarrow A \otimes B_3 \rightarrow 0$$

with a G -module A remains exact, we have for all elements $a \in H^i(G, A)$ and $b \in H^j(G, B_3)$ the relation

$$a \cup \delta(b) = (-1)^i \delta(a \cup b)$$

in $H^{i+j+1}(G, A \otimes B_1)$.

Proof: For the first statement, fix an element $b \in H^j(G, B)$. Take a projective resolution P_\bullet of the trivial G -module \mathbf{Z} and consider the sequences

$$0 \rightarrow \text{Hom}(P_\bullet, A_1) \rightarrow \text{Hom}(P_\bullet, A_2) \rightarrow \text{Hom}(P_\bullet, A_3) \rightarrow 0 \quad (12)$$

and

$$0 \rightarrow \text{Hom}(P_\bullet \otimes P_\bullet, A_1 \otimes B) \rightarrow \text{Hom}(P_\bullet \otimes P_\bullet, A_2 \otimes B) \rightarrow \text{Hom}(P_\bullet \otimes P_\bullet, A_3 \otimes B) \rightarrow 0.$$

These are exact sequences of complexes by virtue of the projectivity of the P_i and the exactness of sequences (10) and (11). Lifting b to an element $\beta \in \text{Hom}(P_j, B)$, tensor product with β yields maps

$$\text{Hom}(P_i, A_k) \rightarrow \text{Hom}(P_i \otimes P_j, A_k \otimes B)$$

for $k = 1, 2, 3$. Hence proceeding as in Construction 3.4.2 we obtain maps from the terms in the first sequence to those of the second (increasing degrees

by j), giving rise to a commutative diagram by functoriality of the cup-product construction. The connecting maps δ are obtained by applying the snake lemma to the above sequences as in Proposition 3.1.1, and one gets the first statement from the aforementioned commutativity by following the image of the element $a \in H^i(G, A)$. The proof of the second statement is similar, except that one has to replace the differentials in the complexes $\text{Hom}^\bullet(P_\bullet, B_\lambda)$ by their multiples by $(-1)^i$ in order to get a commutative diagram, by virtue of the sign convention we have taken in Construction 3.4.1. \square

We shall also need another exactness property of the cup-product.

Proposition 3.4.9 *Assume given exact sequences*

$$0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0 \quad \text{and} \quad 0 \rightarrow B_1 \rightarrow B_2 \rightarrow B_3 \rightarrow 0$$

of G -modules and a \mathbf{Z} -bilinear pairing $A_2 \times B_2 \rightarrow C$ into some G -module C , compatible with the action of G . Assume further that the restriction of this pairing to $A_1 \times B_1$ is trivial. Then it induces pairings

$$A_1 \times B_3 \rightarrow C \quad \text{and} \quad A_3 \times B_1 \rightarrow C$$

such that the induced cup-products satisfy the compatibility

$$\delta_A(\alpha) \cup \beta = (-1)^{i+1} \alpha \cup \delta_B(\beta)$$

for $\alpha \in H^i(G, A_3)$ and $\beta \in H^j(G, B_3)$, where $\delta_A : H^i(G, A_3) \rightarrow H^{i+1}(G, A_1)$ and $\delta_B : H^j(G, B_3) \rightarrow H^{j+1}(G, B_1)$ are boundary maps coming from the above short exact sequences.

Proof: Take again a projective resolution P_\bullet of the trivial G -module \mathbf{Z} , giving rise to an exact sequence of the form (12) and a similar one with the B_i . These are linked by a pairing

$$\text{Hom}(P_\bullet, A_2) \times \text{Hom}(P_\bullet, B_2) \rightarrow \text{Hom}(P_\bullet \otimes P_\bullet, C)$$

trivial on $\text{Hom}(P_\bullet, A_1) \times \text{Hom}(P_\bullet, B_1)$. Represent α and β by cocycles $\alpha_3 \in Z^i(\text{Hom}(P_\bullet, A_3))$ and $\beta_3 \in Z^j(\text{Hom}(P_\bullet, B_3))$, respectively. Recall from the proof of Proposition 3.1.1 that the class $\delta_A(\alpha)$ is constructed as follows. We first lift α_3 to an element $\alpha_2 \in \text{Hom}(P_i, A_2)$, and then take $\partial_A^i(\alpha_2)$ in $B^{i+1}(\text{Hom}(P_\bullet, A_2))$. This is an element mapping to 0 in $Z^{i+1}(\text{Hom}(P_\bullet, A_3))$ and hence coming from some $\alpha_1 \in Z^{i+1}(\text{Hom}(P_\bullet, A_1))$, and we define $\delta_A(\alpha)$ to be its class in $H^{i+1}(\text{Hom}(P_\bullet, A_1))$. By definition of our pairing, $\delta_A(\alpha) \cup \beta$ is

constructed by lifting β_3 to some $\beta_2 \in \text{Hom}(P_j, B_2)$ and then taking the image of $\partial_A^i(\alpha_2) \otimes \beta_2$ in $\text{Hom}(P_{i+1} \otimes P_j, C)$. Since α_2 comes from $Z^{i+1}(\text{Hom}(P_\bullet, A_1))$, this does not depend on the choice of the lifting β_2 , and moreover it yields a cocycle in $Z^{i+j+1}(\text{Hom}(P_\bullet \otimes P_\bullet, C))$. In a similar way, one represents $\alpha \cup \delta_B(\beta)$ by the image of $\alpha_2 \otimes \partial_B^j(\beta_2)$ in $Z^{i+j+1}(\text{Hom}(P_\bullet \otimes P_\bullet, C))$. Now viewing $\partial_A^i(\alpha_2) \otimes \beta_2 + (-1)^i \alpha_2 \otimes \partial_B^j(\beta_2)$ as an element in $Z^{i+j+1}(\text{Hom}(P_\bullet \otimes P_\bullet, C))$, we see that it is none but $\partial^{i+j}(\alpha_2 \otimes \beta_2)$, where ∂^{i+j} is the total differential of the complex. Hence it becomes 0 in $H^{i+j+1}(\text{Hom}(P_\bullet \otimes P_\bullet, C))$, which yields the required formula. \square

Finally, given a subgroup H of G (normal or of finite index if needed), the cup-product satisfies the following compatibility relations with the associated restriction, inflation and corestriction maps.

Proposition 3.4.10 *Given G -modules A and B , the following relations hold.*

1. For $a \in H^i(H, A)$ and $b \in H^j(H, B)$ we have

$$\text{Res}(a \cup b) = \text{Res}(a) \cup \text{Res}(b).$$

2. Assume H is normal in G . Then we have for $a \in H^i(G/H, A^H)$ and $b \in H^j(G/H, B^H)$

$$\text{Inf}(a \cup b) = \text{Inf}(a) \cup \text{Inf}(b).$$

3. (**Projection Formula**) Assume that H is of finite index in G . Then for $a \in H^i(H, A)$ and $b \in H^j(G, B)$ we have

$$\text{Cor}(a \cup \text{Res}(b)) = \text{Cor}(a) \cup b.$$

4. Assume H is normal in G . Then for all $\sigma \in G/H$, $a \in H^i(H, A)$ and $b \in H^j(H, B)$ we have

$$\sigma_*(a \cup b) = \sigma_*(a) \cup \sigma_*(b).$$

Proof: According to the definition of restriction maps, the first statement follows by performing the cup-product construction for the modules $M_H^G(A) = \text{Hom}_H(\mathbf{Z}[G], A)$ and $M_H^G(B) = \text{Hom}_H(\mathbf{Z}[G], B)$, and using functoriality of the construction for the natural maps $A \rightarrow M_H^G(A)$ and $B \rightarrow M_H^G(B)$. Similarly, the second statement follows by performing the cup-product construction simultaneously for the projective resolutions P_\bullet and Q_\bullet considered in the definition of inflation maps, and using functoriality. For the projection formula consider the diagram

$$\begin{array}{ccc}
\mathrm{Hom}_H(\mathbf{Z}[G], A) \times \mathrm{Hom}_H(\mathbf{Z}[G], B) & \rightarrow & \mathrm{Hom}_{H \times H}(\mathbf{Z}[G \times G], A \otimes B) \\
\downarrow & & \uparrow \\
\mathrm{Hom}_G(\mathbf{Z}[G], A) \times \mathrm{Hom}_G(\mathbf{Z}[G], B) & \rightarrow & \mathrm{Hom}_{G \times G}(\mathbf{Z}[G \times G], A \otimes B),
\end{array}$$

where the horizontal maps are induced by the tensor product, the middle vertical map is the one inducing the restriction and the two others are those inducing the corestriction maps. The diagram is commutative in the sense that starting from elements in $\mathrm{Hom}_H(\mathbf{Z}[G], A)$ and $\mathrm{Hom}_G(\mathbf{Z}[G], B)$ we get the same elements in $\mathrm{Hom}_{G \times G}(\mathbf{Z}[G \times G], A \otimes B)$ by going through the diagram in the two possible ways; this follows from the definition of the maps. The claim then again follows by performing the cup-product construction for the pairings in the two rows of the diagram and using functoriality. Finally, part (4) follows from the fact that the action of σ on $\mathrm{Hom}_H(P^\bullet, A)$ for a projective resolution P^\bullet of the trivial G -module \mathbf{Z} defined in the construction of the map σ_* is compatible with taking tensor products of resolutions. \square

We close this section with an important compatibility relation which complements the calculation of the cohomology of finite cyclic groups in Example 3.2.9.

Proposition 3.4.11 *Let G be a finite cyclic group of order n , and let χ be the element of the group $H^1(G, \mathbf{Z}/n\mathbf{Z}) \cong \mathrm{Hom}(G, \mathbf{Z}/n\mathbf{Z})$ corresponding to the identity map.*

1. Denote by $\delta : H^1(G, \mathbf{Z}/n\mathbf{Z}) \rightarrow H^2(G, \mathbf{Z})$ the boundary map coming from the short exact sequence

$$0 \rightarrow \mathbf{Z} \xrightarrow{n} \mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z} \rightarrow 0. \quad (13)$$

The element $\delta(\chi)$ is a generator of the cyclic group $H^2(G, \mathbf{Z})$.

2. If A is a G -module, the isomorphisms

$$H^i(G, A) \cong H^{i+2}(G, A)$$

of Example 3.2.9 are induced by cup-product with $\delta(\chi)$ for all $i > 0$.

3. The isomorphism

$$A^G/NA \cong H^2(G, A)$$

is induced by mapping an element of $A^G = H^0(G, A)$ to its cup-product with $\delta(\chi)$.

Proof: Recall the free resolution

$$\cdots \rightarrow \mathbf{Z}[G] \xrightarrow{\sigma^{-1}} \mathbf{Z}[G] \xrightarrow{N} \mathbf{Z}[G] \xrightarrow{\sigma^{-1}} \mathbf{Z}[G] \rightarrow \mathbf{Z} \rightarrow 0 \quad (14)$$

used to calculate the cohomology of G . To prove the first statement, it will suffice to check that the element $\delta(\chi) \in H^2(G, \mathbf{Z})$ is represented by the homomorphism $\bar{\chi} : \mathbf{Z}[G] \rightarrow \mathbf{Z}$ given by sending a generator σ of G to 1, with $\mathbf{Z}[G]$ placed in degree -2 in the above resolution. This is done by carefully going through the construction of δ , given by applying Proposition 3.1.1 to the short exact sequence of complexes arising from homomorphisms of the above resolution to the sequence (13). It yields the following: first we lift χ to the element $\psi \in \text{Hom}(\mathbf{Z}[G], \mathbf{Z})$ sending a fixed generator $\sigma \in G$ to 1. We then compose ψ by $N : \mathbf{Z}[G] \rightarrow \mathbf{Z}[G]$ to get a homomorphism with values in $n\mathbf{Z}$. The class $\delta(\chi)$ is then represented by any map $\lambda : \mathbf{Z}[G] \rightarrow \mathbf{Z}$ satisfying $n\lambda = \psi \circ N$; the map $\lambda = \bar{\chi}$ manifestly has this property.

This being said, the calculation of the cup-product with $\delta(\chi)$ is shown by the diagram

$$\begin{array}{ccccccc} \text{Hom}(\mathbf{Z}[G], A) & \xrightarrow{N_*} & \text{Hom}(\mathbf{Z}[G], A) & \xrightarrow{(\sigma^{-1})^*} & \text{Hom}(\mathbf{Z}[G], A) & \rightarrow & \cdots \\ \otimes \bar{\chi} \downarrow & & \otimes \bar{\chi} \downarrow & & \otimes \bar{\chi} \downarrow & & \\ \text{Hom}(\mathbf{Z}[G \times G], A) & \longrightarrow & \text{Hom}(\mathbf{Z}[G \times G], A) & \longrightarrow & \text{Hom}(\mathbf{Z}[G \times G], A) & \rightarrow & \cdots \\ \text{Res} \downarrow & & \text{Res} \downarrow & & \text{Res} \downarrow & & \\ \text{Hom}(\mathbf{Z}[G], A) & \xrightarrow{N_*} & \text{Hom}(\mathbf{Z}[G], A) & \xrightarrow{(\sigma^{-1})^*} & \text{Hom}(\mathbf{Z}[G], A) & \rightarrow & \cdots \end{array}$$

where the maps in the bottom line are the same as in the top one *except that the whole complex is shifted by degree 2*. But the resolution (14) is periodic by 2, whence the second statement.

The last statement is proven by a similar argument: here we represent $a \in H^0(G, A)$ by the homomorphism $\bar{a} : \mathbf{Z}[G] \rightarrow A$ sending σ to a , with $\mathbf{Z}[G]$ placed in degree 0 this time. Then it remains to observe that tensoring with \bar{a} and taking restriction along the diagonal yields the natural diagram

$$\begin{array}{ccccccc} \text{Hom}(\mathbf{Z}[G], \mathbf{Z}) & \xrightarrow{N_*} & \text{Hom}(\mathbf{Z}[G], \mathbf{Z}) & \xrightarrow{(\sigma^{-1})^*} & \text{Hom}(\mathbf{Z}[G], \mathbf{Z}) & \rightarrow & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \\ \text{Hom}(\mathbf{Z}[G], A) & \xrightarrow{N_*} & \text{Hom}(\mathbf{Z}[G], A) & \xrightarrow{(\sigma^{-1})^*} & \text{Hom}(\mathbf{Z}[G], A) & \rightarrow & \cdots \end{array}$$

corresponding to the map $\mathbf{Z} \rightarrow A$ given by sending 1 to a . \square

EXERCISES

1. Let $\phi : G_1 \rightarrow G_2$ be a homomorphism of groups, and equip each G_2 -module A with the G_1 -action induced by ϕ . Show that there exists a unique family of homomorphisms

$$\phi_A^i : H^i(G_2, A) \rightarrow H^i(G_1, A)$$

for each $i \geq 0$ such that for every short exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

of G_2 -modules the arising diagrams

$$\begin{array}{ccccccc} H^i(G_2, A) & \longrightarrow & H^i(G_2, B) & \longrightarrow & H^i(G_2, C) & \longrightarrow & H^{i+1}(G_2, A) \\ \phi_A^i \downarrow & & \phi_B^i \downarrow & & \phi_C^i \downarrow & & \phi_A^{i+1} \downarrow \\ H^i(G_1, A) & \longrightarrow & H^i(G_1, B) & \longrightarrow & H^i(G_1, C) & \longrightarrow & H^{i+1}(G_1, A) \end{array}$$

commute. [Note: This gives in particular another construction of restriction and inflation maps.]

2. Let H be a subgroup of G of finite index n and let ρ_1, \dots, ρ_n be a system of left coset representatives.

- (a) Check that the map $\text{Cor}^0 : A^H \rightarrow A^G$ given by $x \mapsto \sum_j \rho_j x$ does not depend on the choice of the ρ_j .
- (b) Show that the corestriction maps $H^i(H, A) \rightarrow H^i(G, A)$ are the only maps which coincide with the above Cor^0 for $i = 0$ and satisfy a property analogous to that of the maps ϕ_A^i of the previous exercise.

3. With notations as in the previous exercise, assume moreover that H is *normal* in G . Define for all $i \geq 0$ *norm maps* $N_{G/H} : H^i(H, A) \rightarrow H^i(H, A)$ by the formula $N_{G/H} = \sum_{j=1}^n \rho_j^*$.

- (a) Check that the above definition does not depend on the choice of the ρ_j .
- (b) Verify the formula $\text{Res} \circ \text{Cor} = N_{G/H}$.

4. Show that using the standard resolution one can give the following explicit description of the cup-product using cocycles: if $a \in H^i(G, A)$ is represented by an i -cocycle $(\sigma_1, \dots, \sigma_i) \mapsto a_{\sigma_1, \dots, \sigma_i}$ and $b \in H^j(G, B)$ is represented by a j -cocycle $(\sigma_1, \dots, \sigma_j) \mapsto b_{\sigma_1, \dots, \sigma_j}$, then $a \cup b \in H^{i+j}(G, A \otimes B)$ is represented by the $(i+j)$ -cocycle $(\sigma_1, \dots, \sigma_{i+j}) \mapsto a_{\sigma_1, \dots, \sigma_i} \otimes \sigma_1 \dots \sigma_i (b_{\sigma_{i+1}, \dots, \sigma_{i+j}})$.

5. Give an explicit interpretation of the piece

$$H^1(H, A)^{G/H} \rightarrow H^2(G/H, A^H) \xrightarrow{\text{Inf}} H^2(G, A)$$

of the exact sequence of Proposition 3.3.14 in terms of classes of group extensions. (You may assume for simplicity that H acts trivially on A .)

6. Let G be a finite cyclic group generated by $\sigma \in G$ and let A, B be G -modules.

(a) Describe directly the pairing

$$(A^G/NA) \times ({}_NB/(\sigma-1)B) \rightarrow {}_N(A \otimes B)/(\sigma-1)(A \otimes B)$$

induced by the cup-product

$$H^{2i+2}(G, A) \times H^{2j+1}(G, B) \rightarrow H^{2i+2j+1}(G, A \otimes B)$$

via the formulae of Example 3.2.9.

(b) Similar questions for the pairings

$$(A^G/NA) \times (B^G/NB) \rightarrow (A \otimes B)^G/N(A \otimes B)$$

and

$$({}_NA/(\sigma-1)A) \times ({}_NB/(\sigma-1)B) \rightarrow (A \otimes B)^G/N(A \otimes B).$$

Chapter 4

The Cohomological Brauer Group

We now apply the cohomology theory of the previous chapter to the study of the Brauer group. However, we shall have to use a slightly modified construction which takes into account the fact that the absolute Galois group of a field is determined by its finite quotients. This is the cohomology theory of profinite groups, which we develop first. As a fruit of our labours, we identify the Brauer group of a field with a second, this time commutative, cohomology group of the absolute Galois group. This makes it possible to give an easy proof of basic facts about the Brauer group, e.g. that it is a torsion group. We also treat the foundations of the theory of index and period for central simple algebras with the help of cohomology. Last but not least, one of the main objects of study in this book makes its appearance: the Galois symbol.

The cohomology theory of profinite groups was introduced in the late 1950's by John Tate, motivated by sheaf-theoretic considerations of Alexander Grothendieck. His original aim was to find the appropriate formalism for developing class field theory. Tate himself never published his work, which thus became accessible to the larger mathematical community through the famous account of Serre [4], which also contains many original contributions. It was Brauer himself who described the Brauer group as a second cohomology group, using his language of factor systems. We owe to Serre the insight that descent theory can be used to give a more conceptual proof. The Galois symbol was defined by Tate in connection with the algebraic theory of power residue symbols, a topic extensively studied in the 1960's by Bass, Milnor, Moore, Serre and others.

4.1 Profinite Groups and Galois Groups

It can be no surprise that the main application of the cohomological techniques of the previous chapter will be in the case when G is the Galois group

of a finite Galois extension. However, it will be convenient to consider the case of infinite Galois extensions as well, and first and foremost that of the extension $k_s|k$, where k_s is a separable closure of k .

Recall that a (possibly infinite) field extension $K|k$ is a Galois extension if it is separable (i.e. the minimal polynomials of all elements of K have distinct roots in an algebraic closure) and if for each element $x \in K \setminus k$ there exists a field automorphism σ of K fixing k elementwise such that $\sigma(x) \neq x$. We denote the group of k -automorphisms of K by $\text{Gal}(K|k)$ as in the finite case and call it the Galois group of $K|k$. A basic example of an infinite Galois extension is given by a separable closure k_s of k . Its Galois group is called (somewhat abusively) the *absolute Galois group* of k .

A Galois extension $K|k$ is a union of finite Galois extensions, because we may embed each simple extension $k(\alpha) \subset K$ into the splitting field of the minimal polynomial of α , which is a finite Galois extension contained in K . This fact has a capital consequence for the Galois group $\text{Gal}(K|k)$, namely that it is determined by its finite quotients. We shall prove this in Proposition 4.1.3 below, in a more precise form. To motivate its formulation, consider a tower of finite Galois subextensions $M|L|k$ contained in an infinite Galois extension $K|k$. The main theorem of Galois theory provides us with a canonical surjection $\phi_{ML} : \text{Gal}(M|k) \rightarrow \text{Gal}(L|k)$. Moreover, if $N|k$ is yet another finite Galois extension containing M , we have $\phi_{NL} = \phi_{ML} \circ \phi_{NM}$. Thus one expects that if we somehow “pass to the limit in M ”, then $\text{Gal}(L|k)$ will actually become a quotient of the infinite Galois group $\text{Gal}(K|k)$ itself. This is achieved by the following construction.

Construction 4.1.1 A (*filtered*) *inverse system* of groups $(G_\alpha, \phi_{\alpha\beta})$ consists of:

- a partially ordered set (Λ, \leq) which is directed in the sense that for all $(\alpha, \beta) \in \Lambda$ there is some $\gamma \in \Lambda$ with $\alpha \leq \gamma, \beta \leq \gamma$;
- for each $\alpha \in \Lambda$ a group G_α ;
- for each $\alpha \leq \beta$ a homomorphism $\phi_{\alpha\beta} : G_\beta \rightarrow G_\alpha$ such that we have equalities $\phi_{\alpha\gamma} = \phi_{\alpha\beta} \circ \phi_{\beta\gamma}$ for $\alpha \leq \beta \leq \gamma$.

The *inverse limit* of the system is defined as the subgroup of the direct product $\prod_{\alpha \in \Lambda} G_\alpha$ consisting of sequences (g_α) such that $\phi_{\alpha\beta}(g_\beta) = g_\alpha$ for all $\alpha \leq \beta$. It is denoted by $\varprojlim G_\alpha$; we shall not specify the inverse system in the notation when it is clear from the context. Also, we shall often say loosely that $\varprojlim G_\alpha$ is the inverse limit of the groups G_α , without special reference to the inverse system.

Plainly, this notion is not specific to the category of groups and one can define the inverse limit of sets, rings, modules, even of topological spaces in an analogous way.

We can now define a *profinite group* as an inverse limit of a system of finite groups. For a prime number p , a *pro- p group* is an inverse limit of finite p -groups.

Examples 4.1.2

1. A finite group is profinite; indeed, it is the inverse limit of the system $(G_\alpha, \phi_{\alpha\beta})$ for any directed index set Λ , with $G_\alpha = G$ and $\phi_{\alpha\beta} = \text{id}_G$.
2. Given a group G , the set of its finite quotients can be turned into an inverse system as follows. Let Λ be the index set formed by the normal subgroups of finite index partially ordered by the following relation: $U_\alpha \leq U_\beta$ iff $U_\alpha \supset U_\beta$. Then if $U_\alpha \leq U_\beta$ are such normal subgroups, we have a quotient map $\phi_{\alpha\beta} : G/U_\beta \rightarrow G/U_\alpha$. The inverse limit of this system is called the *profinite completion* of G , customarily denoted by \widehat{G} . There is a canonical homomorphism $G \rightarrow \widehat{G}$.
3. Take $G = \mathbf{Z}$ in the previous example. Then Λ is just the set $\mathbf{Z}_{>0}$, since each subgroup of finite index is generated by some positive integer m . The partial order is induced by the divisibility relation: $m|n$ iff $m\mathbf{Z} \supset n\mathbf{Z}$. The completion $\widehat{\mathbf{Z}}$ is usually called *zed hat* (or *zee hat* in the US).
4. In the previous example, taking only powers of some prime p in place of m we get a subsystem of the inverse system considered there; in fact it is more convenient to index it by the exponent of p . With this convention the partial order becomes the usual (total) order of $\mathbf{Z}_{>0}$. The inverse limit is \mathbf{Z}_p , the *additive group of p -adic integers*. This is a commutative pro- p -group. The Chinese Remainder Theorem implies that the direct product of the groups \mathbf{Z}_p for all primes p is isomorphic to $\widehat{\mathbf{Z}}$.

Now we come to the main example, that of Galois groups.

Proposition 4.1.3 *Let $K|k$ be a Galois extension of fields. Then the Galois groups of finite Galois subextensions of $K|k$ together with the homomorphisms $\phi_{ML} : \text{Gal}(M|K) \rightarrow \text{Gal}(L|k)$ form an inverse system whose inverse limit is isomorphic to $\text{Gal}(K|k)$. In particular, $\text{Gal}(K|k)$ is a profinite group.*

Proof: Only the isomorphism statement needs a proof. For this, define a group homomorphism $\phi : \text{Gal}(K|k) \rightarrow \prod \text{Gal}(L|k)$ (where the product is over all finite Galois subextensions $L|k$) by sending a k -automorphism σ of K to the direct product of its restrictions to the various subfields L indexing the product. This map is injective, since if an automorphism σ does not fix an element α of k_s , then its restriction to a finite Galois subextension containing $k(\alpha)$ is nontrivial (as we have already remarked, such an extension always exists). On the other hand, the main theorem of Galois theory assures that the image of ϕ is contained in $\varprojlim \text{Gal}(L|k)$. It is actually all of $\varprojlim \text{Gal}(L|k)$, which is seen as follows: take an element (σ_L) of $\varprojlim \text{Gal}(L|K)$ and define a k -automorphism σ of K by putting $\sigma(\alpha) = \sigma_L(\alpha)$ with some finite Galois L containing $k(\alpha)$. The fact that σ is well defined follows from the fact that by hypothesis the σ_L form a compatible system of automorphisms; finally, σ maps to $(\sigma_L) \in \varprojlim \text{Gal}(L|K)$ by construction. \square

Corollary 4.1.4 *Projection to the components of the inverse limit of the proposition yields natural surjections $\text{Gal}(K|k) \rightarrow \text{Gal}(L|k)$ for all finite Galois subextensions $L|k$ contained in K .*

Example 4.1.5 (Finite fields) Let F be a finite field and F_s a separable closure of F . It is well known that for each integer $n > 0$ the extension $F_s|F$ has a unique subextension $F_n|F$ with $[F_n : F] = n$. Moreover, the extension $F_n|F$ is Galois with group $\text{Gal}(F_n|F) \cong \mathbf{Z}/n\mathbf{Z}$, and via this isomorphism the natural projections $\text{Gal}(F_{mn}|F) \rightarrow \text{Gal}(F_n|F)$ correspond to the projections $\mathbf{Z}/mn\mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z}$. It follows that $\text{Gal}(F_s|F) \cong \widehat{\mathbf{Z}}$.

Example 4.1.6 (Laurent series fields)

As another example of a field with absolute Galois group $\widehat{\mathbf{Z}}$, we may consider the formal Laurent series field $k((t))$ over an algebraically closed field k of characteristic 0.

Here is a sketch of the proof of this fact. Take a finite extension $L|k((t))$ of degree n . As we are in characteristic 0, we may write $L = k((t))(\alpha)$ with some $\alpha \in L$. Multiplying α by a suitable element of $k[[t]]$ we may assume α satisfies an irreducible monic polynomial equation $f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ with $a_i \in k[[t]]$ and $f'(\alpha) \neq 0$. Then by the implicit function theorem for formal power series (which can be easily proven by Newton's method) we may express t as a formal power series $t = b_0 + b_1\alpha + b_2\alpha^2 + \cdots \in k[[\alpha]]$. In particular, plugging this expression into the power series expansions of the a_i and using the above equation for α we get that $b_j = 0$ for $j < n$. Next, we may find a formal power series $\tau = c_1\alpha + c_2\alpha^2 + \cdots \in k[[\alpha]]$ with $\tau^n = t$.

Indeed, comparing power series expansions we get $c_1^n = b_1$, $nc_1^{n-1}c_2 = b_2$ and so on, from which we may determine the c_i inductively. Finally, we may also express α as a power series $\alpha = d_1\tau + d_2\tau^2 + \cdots \in k[[\tau]]$, with $d_1 = c_1^{-1}$, $d_2 = -c_2c_1^{-3}$ and so on. Hence we may embed L into the Laurent series field $k((\tau))$, but this field is none but the degree n cyclic Galois extension $k((t))[\tau]$ of $k((t))$. We conclude as in the previous example.

Profinite groups are endowed with a natural topology as follows: if G is an inverse limit of a system of finite groups $(G_\alpha, \phi_{\alpha\beta})$, endow the G_α with the discrete topology, their product with the product topology and the subgroup $G \subset \prod G_\alpha$ with the subspace topology. It immediately follows from this construction that the natural projection maps $G \rightarrow G_\alpha$ are continuous and their kernels form a basis of open neighbourhoods of 1 in G (for the last statement, note that the image of each element $g \neq 1$ of G must have nontrivial image in some G_α , by definition of the inverse limit).

To state other topological properties, we need a lemma.

Lemma 4.1.7 *Let $(G_\alpha, \phi_{\alpha\beta})$ be an inverse system of groups endowed with the discrete topology. Then the inverse limit $\varprojlim G_\alpha$ is a closed topological subgroup of the product $\prod G_\alpha$.*

Proof: Take an element $g = (g_\alpha) \in \prod G_\alpha$. If $g \notin \varprojlim G_\alpha$, we have to show that it has an open neighbourhood which does not meet $\varprojlim G_\alpha$. By assumption for some α and β we must have $\phi_{\alpha\beta}(g_\beta) \neq g_\alpha$. Now take the subset of $\prod G_\alpha$ consisting of all elements with α -th component g_α and β -th component g_β . It is a suitable choice, being open (by the discreteness of the G_α and by the definition of topological product) and containing g but avoiding $\varprojlim G_\alpha$. \square

Corollary 4.1.8 *A profinite group is compact and totally disconnected (i.e. the only connected subsets are the one-element subsets). Moreover, the open subgroups are precisely the closed subgroups of finite index.*

Proof: Recall that finite groups are compact, and so is a product of compact groups, by Tikhonov's theorem. Compactness of the inverse limit then follows from the lemma, as closed subspaces of compact spaces are compact. Complete disconnectedness follows from the construction. For the second statement, note that each open subgroup U is closed since its complement is a disjoint union of cosets gU which are themselves open (the map $U \mapsto gU$ being a homeomorphism in a topological group); by compactness of G , these

must be finite in number. Conversely, a closed subgroup of finite index is open, being the complement of the finite disjoint union of its cosets which are also closed. \square

Remark 4.1.9 In fact, one may characterise profinite groups as being those topological groups which are compact and totally disconnected. See e.g. Shatz [1] for a proof.

We may now state and prove the main theorem of Galois theory for possibly infinite extensions. Observe first that if L is a subextension of a Galois extension $K|k$, then K is also a Galois extension of L and $\text{Gal}(L)$ is naturally identified with a subgroup of $\text{Gal}(k)$.

Theorem 4.1.10 (Krull) *Let L be a subextension of the Galois extension $K|k$. Then $\text{Gal}(L)$ is a closed subgroup of $\text{Gal}(K|k)$. Moreover, in this way we get a bijection between subextensions of $K|k$ and closed subgroups of $\text{Gal}(K|k)$, where open subgroups correspond to finite extensions of k contained in K .*

Proof: Take first a finite separable extension $L|k$ contained in K . Recall that we can embed it in a finite Galois extension $M|k$ contained in K (use the theorem of the primitive element to write $L = k(\alpha)$ and take the associated splitting field). Then $\text{Gal}(M|k)$ is one of the standard finite quotients of $\text{Gal}(K|k)$, and it contains $\text{Gal}(M|L)$ as a subgroup. Let U_L be the inverse image of $\text{Gal}(M|L)$ by the natural projection $\text{Gal}(K|k) \rightarrow \text{Gal}(M|k)$. Since the projection is continuous and $\text{Gal}(M|k)$ has the discrete topology, U_L is open. It thus suffices to show $U_L = \text{Gal}(K|L)$. We have $U_L \subset \text{Gal}(K|L)$, for each element of U_L fixes L . On the other hand, the image of $\text{Gal}(K|L)$ by the projection $\text{Gal}(K|k) \rightarrow \text{Gal}(M|k)$ is contained in $\text{Gal}(M|L)$, whence the reverse inclusion. Now if $L|k$ is an arbitrary subextension of $K|k$, write it as a union of finite subextensions $L_\alpha|k$. By what we have just proven, each $\text{Gal}(K|L_\alpha)$ is an open subgroup of $\text{Gal}(K|k)$, hence it is also closed by Corollary 4.1.8. Their intersection is precisely $\text{Gal}(K|L)$ which is thus a closed subgroup; its fixed field is exactly L , for K is Galois over L .

Conversely, given a closed subgroup $H \subset G$, it fixes some extension $L|k$ and is thus contained in $\text{Gal}(K|L)$. To show equality, let σ be an element of $\text{Gal}(K|L)$, and pick a fundamental open neighbourhood U_M of the identity in $\text{Gal}(K|L)$, corresponding to a Galois extension $M|L$. Now $H \subset \text{Gal}(K|L)$ surjects onto $\text{Gal}(M|L)$ by the natural projection; indeed, otherwise its image in $\text{Gal}(M|L)$ would fix a subfield of M strictly larger than L according to finite Galois theory, which would contradict our assumption that each element of $M \setminus L$ is moved by some element of H . In particular, some element

of H must map to the same element in $\text{Gal}(M|L)$ as σ . Hence H contains an element of the coset σU_M and, as U_M was chosen arbitrarily, this implies that σ is in the closure of H in $\text{Gal}(K|L)$. But H is closed by assumption, whence the claim. Finally, the assertion about finite extensions follows from the above in view of Corollary 4.1.8. \square

Remark 4.1.11 The group $\text{Gal}(K|k)$ contains many nonclosed subgroups if $K|k$ is an infinite extension. For instance, cyclic subgroups are usually nonclosed; as a concrete example, one may take the cyclic subgroup of $\widehat{\mathbf{Z}}$ generated by 1. In fact, a closed subgroup of a profinite group is itself profinite, but it can be shown that an infinite profinite group is always uncountable. Thus none of the countable subgroups in a profinite group are closed.

4.2 Cohomology of Profinite Groups

Let $G = \varprojlim G_\alpha$ be a profinite group. In this section we attach to G another system of cohomology groups, different from that of the previous chapter for infinite G , which reflects the profiniteness of G and which is more suitable for applications.

By a (*discrete*) *continuous* G -module we shall mean a G -module A such that the stabiliser of each $a \in A$ is open in G . Unless otherwise stated, we shall always regard A as equipped with the discrete topology; continuous G -modules are then precisely the ones for which the action of G (equipped with its profinite topology) is continuous. If $G_\alpha = G/U_\alpha$ is one of the standard quotients of G , the submodule A^{U_α} is naturally a G_α -module. The canonical surjection $\phi_{\alpha\beta} : G_\beta \rightarrow G_\alpha$ between two of the standard quotients induces inflation maps $\text{Inf}_\alpha^\beta : H^i(G_\alpha, A^{U_\alpha}) \rightarrow H^i(G_\beta, A^{U_\beta})$ for all $i \geq 0$. Furthermore, the compatibility condition $\phi_{\alpha\gamma} = \phi_{\alpha\beta} \circ \phi_{\beta\gamma}$ implies that the groups $H^i(G_\alpha, A)$ together with the maps Inf_α^β form a direct system in the following sense.

Construction 4.2.1 A (*filtered*) *direct system* of abelian groups $(B_\alpha, \psi_{\alpha\beta})$ consists of:

- a directed partially ordered set (Λ, \leq) ;
- for each $\alpha \in \Lambda$ an abelian group B_α ;
- for each $\alpha \leq \beta$ a homomorphism $\psi_{\alpha\beta} : B_\alpha \rightarrow B_\beta$ such that we have equalities $\psi_{\alpha\gamma} = \psi_{\beta\gamma} \circ \psi_{\alpha\beta}$ for $\alpha \leq \beta \leq \gamma$.

The *direct limit* of the system is defined as the quotient of the direct sum $\bigoplus_{\alpha \in \Lambda} B_\alpha$ by the subgroup generated by elements of the form $b_\beta - \psi_{\alpha\beta}(b_\alpha)$.

It is denoted by $\varinjlim B_\alpha$. Direct limits of abelian groups with additional structure (e.g. rings or modules) are defined in an analogous way.

Also, given direct systems $(B_\alpha, \psi_{\alpha\beta})$ and $(C_\alpha, \rho_{\alpha\beta})$ indexed by the same directed set Λ , together with maps $\lambda_\alpha : B_\alpha \rightarrow C_\alpha$ satisfying $\lambda_\beta \circ \psi_{\alpha\beta} = \rho_{\alpha\beta} \circ \lambda_\alpha$ for all $\alpha \leq \beta$, we have an induced map $\lambda : \varinjlim B_\alpha \rightarrow \varinjlim C_\alpha$, called the *direct limit of the maps* λ_α .

We can now define:

Definition 4.2.2 Let $G = \varprojlim G_\alpha$ be a profinite group and A a continuous G -module. For all integers $i \geq 0$, we define the *i -th continuous cohomology group* $H_{\text{cont}}^i(G, A)$ as the direct limit of the direct system $(H^i(G_\alpha, A^{U_\alpha}), \text{Inf}_\alpha^\beta)$ constructed above. In the case when $G = \text{Gal}(k_s|k)$ for some separable closure k_s of a field k , we also denote $H_{\text{cont}}^i(G, A)$ by $H^i(k, A)$ and call it the *i -th Galois cohomology group of k with values in A* .

Example 4.2.3 Consider \mathbf{Z} with trivial action by a profinite group G . Then $H_{\text{cont}}^1(G, \mathbf{Z}) = 0$. Indeed, by definition this is the direct limit of the groups $H^1(G/U, \mathbf{Z}) = \text{Hom}(G/U, \mathbf{Z})$ for U open and normal in G , which are trivial, as the G/U are finite and \mathbf{Z} is a torsion free abelian group.

Remark 4.2.4 It follows from the definition that $H_{\text{cont}}^0(G, A) = H^0(G, A)$ for all continuous G -modules A and that $H_{\text{cont}}^i(G, A) = H^i(G, A)$ if G is finite.

However, for $i > 0$ and G infinite the two groups are different in general. Take, for instance, $p = 1$, $G = \widehat{\mathbf{Z}}$ and $A = \mathbf{Q}$ with trivial $\widehat{\mathbf{Z}}$ -action. Then $H_{\text{cont}}^1(\widehat{\mathbf{Z}}, \mathbf{Q}) = \varinjlim \text{Hom}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Q}) = 0$, because \mathbf{Q} is torsion free.

On the other hand, $H^1(\widehat{\mathbf{Z}}, \mathbf{Q})$ is the group of \mathbf{Z} -module homomorphisms $\widehat{\mathbf{Z}} \rightarrow \mathbf{Q}$. But as \mathbf{Q} is a divisible abelian group (i.e. the equation $nx = y$ is solvable in \mathbf{Q} for all $n \in \mathbf{Z}$), one knows that a homomorphism $C \rightarrow \mathbf{Q}$ from a subgroup C of an abelian group B extends to a homomorphism $B \rightarrow \mathbf{Q}$ (see e.g. Weibel [1], p. 39; note that the proof of this fact uses Zorn's lemma). Applying this with $C = \mathbf{Z}$, $B = \widehat{\mathbf{Z}}$ and the natural inclusion $\mathbf{Z} \rightarrow \widehat{\mathbf{Z}}$ we get a nontrivial homomorphism $\widehat{\mathbf{Z}} \rightarrow \mathbf{Q}$.

Convention 4.2.5 From now on, all cohomology groups of a profinite group will be understood to be continuous, and we drop the subscript *cont* from the notation.

We now come to a basic property of the cohomology of profinite groups.

Proposition 4.2.6 For a profinite group G and a continuous G -module A the groups $H^i(G, A)$ are torsion abelian groups for all $i > 0$. Moreover, if G is a *pro- p -group*, then they are *p -primary torsion groups*.

Proof: This follows from the definition together with Corollary 3.3.8. \square

Corollary 4.2.7 *Let V be a \mathbf{Q} -vector space equipped with a continuous action by a profinite group G . Then $H^i(G, V) = 0$ for all $i > 0$.*

Proof: It follows from the construction of cohomology that in this case the groups $H^i(G, V)$ are \mathbf{Q} -vector spaces; since for $i > 0$ they are also torsion groups, they must be trivial. \square

Recall that Corollary 3.3.8 was obtained as a consequence of a statement about restriction and corestriction maps. We now adapt these to the profinite situation.

Construction 4.2.8 Let G be a profinite group, H a *closed* subgroup and A a continuous G -module. Define continuous restriction maps

$$\text{Res} : H^i(G, A) \rightarrow H^i(H, A)$$

as the direct limit of the system of usual restriction maps

$$H^i(G/U_\alpha, A^{U_\alpha}) \rightarrow H^i(H/(H \cap U_\alpha), A^{U_\alpha}),$$

where the U_α are the standard open normal subgroups of G .

In the case when H is *open* in G , one defines continuous corestriction maps $\text{Cor} : H^i(H, A) \rightarrow H^i(G, A)$ in a similar way. Finally, when H is a closed normal subgroup in G , one defines inflation maps

$$\text{Inf} : H^i(G/H, A^H) \rightarrow H^i(G, A)$$

as the direct limit of the system of inflation maps

$$H^i((G/U_\alpha)/(H \cap U_\alpha), A^{H \cap U_\alpha}) \rightarrow H^i(G/U_\alpha, A^{U_\alpha}).$$

Manifestly, in the case of a finite G we get back the previous restriction, corestriction and inflation maps.

Remark 4.2.9 In the above situation, one may define the module $M_H^G(A)$ to be the direct limit $\varinjlim \text{Hom}_{H/(H \cap U_\alpha)}(\mathbf{Z}[G/U_\alpha], A^{U_\alpha})$, where the U_α are the standard open normal subgroups of G . We have a continuous G -action defined by $g(\phi_\alpha(x_\alpha)) = \phi_\alpha(x_\alpha g_\alpha)$, where g_α is the image of g in G/U_α ; one checks that this action is well defined and continuous. (Note that in the spirit of the convention above we employ the notation $M_H^G(A)$ for another G -module as before; the one defined in Chapter 3 is not continuous in general.) Then we

have $M_G^G(A) \cong A$ and the Shapiro isomorphism $H^i(G, M_H^G(A)) \cong H^i(H, A)$ holds with a similar proof as in the non-continuous case. In particular, one has the vanishing of the cohomology $H^i(G, M^G(A))$ of (continuous) co-induced modules for $i > 0$. One may then also define the continuous restriction and corestriction maps using this Shapiro isomorphism, by mimicking the construction of Chapter 3.

As in the non-continuous case, we have:

Proposition 4.2.10 *Let G be a profinite group, H an open subgroup of index n and A a continuous G -module. Then the composite maps*

$$\text{Cor} \circ \text{Res} : H^i(G, A) \rightarrow H^i(G, A)$$

are given by multiplication by n for all $i > 0$. Consequently, the restriction $H^i(G, A) \rightarrow H^i(H, A)$ is injective on the prime-to- n torsion part of $H^i(G, A)$.

Proof: Each element of $H^i(G, A)$ comes from some $H^i(G/U_\alpha, A^{U_\alpha})$, and Proposition 3.3.7 applies. The second statement follows because the multiplication-by- n map is injective on the subgroup of elements of order prime to n . \square

A refined version of the last statement is the following.

Corollary 4.2.11 *Let G be a profinite group, p a prime number and H a closed subgroup such that the image of H in each finite quotient of G has order prime to p . Then for each continuous G -module A the restriction map $H^i(G, A) \rightarrow H^i(H, A)$ is injective on the p -primary torsion part of $H^i(G, A)$.*

Proof: Assume that an element of $H^i(G, A)$ of order prime to p maps to 0 in $H^i(H, A)$. It comes from an element of some $H^i(G_\alpha, A^{U_\alpha})$ of which we may assume, up to replacing U_α by a larger subgroup, that it maps to 0 in $H^i(H/(H \cap U_\alpha), A^{U_\alpha})$. By the proposition (applied to the finite group G/U_α) is must then be 0. \square

The main application of the above corollary will be to *pro- p -Sylow subgroups* of a profinite group G . By definition, these are subgroups of G which are pro- p -groups for some prime number p and whose images in each finite quotient of G are of index prime to p .

Proposition 4.2.12 *A profinite group G possesses pro- p -Sylow subgroups for each prime number p , and any two of these are conjugate in G .*

The proof uses the following well-known lemma.

Lemma 4.2.13 *An inverse limit of nonempty finite sets is nonempty.*

Proof: The proof works more generally for compact topological spaces. Given an inverse system $(X_\alpha, \phi_{\alpha\beta})$ of nonempty compact spaces, consider the subsets $X_{\lambda\mu} \subset \prod X_\alpha$ consisting of the sequences (x_α) satisfying $\phi_{\lambda\mu}(x_\mu) = x_\lambda$ for a fixed pair $\lambda \leq \mu$. These are closed subsets of the product, and their intersection is precisely $\varprojlim X_\alpha$. Furthermore, the directedness of the index set implies that finite intersections of the $X_{\lambda\mu}$ are nonempty. Since $\prod X_\alpha$ is compact by Tikhonov's theorem, it ensues that $\varprojlim X_\alpha$ is nonempty. \square

Proof of Proposition 4.2.12: Write G as an inverse limit of a system of finite groups G_α . For each G_α , denote by S_α the set of its p -Sylow subgroups (for the classical Sylow theorems, see e.g. Lang [3]). These form an inverse system of finite sets, hence by the lemma we may find an element S in the limit $\varprojlim S_\alpha$. This S corresponds to an inverse limit of p -Sylow subgroups of the G_α and hence gives a pro- p -Sylow subgroup of G . If P and Q are two pro- p -Sylow subgroups of G , their images in each G_α are p -Sylow subgroups there and hence are conjugate by some $x_\alpha \in G_\alpha$ by the finite Sylow theorem. Writing X_α for the set of possible x_α 's, we get again an inverse system of finite sets, whose nonempty inverse limit contains an element x with $x^{-1}Px = Q$. \square

Corollary 4.2.11 now implies:

Corollary 4.2.14 *If P is a pro- p -Sylow subgroup of a profinite group G , the restriction maps $\text{Res} : H^i(G, A) \rightarrow H^i(P, A)$ are injective on the p -primary torsion part of $H^i(G, A)$ for all $i > 0$ and continuous G -modules A .*

To conclude this section, we mention another construction from the previous chapter which carries over without considerable difficulty to the profinite case, that of cup-products.

Construction 4.2.15 Given a profinite group G and continuous G -modules A and B , define the tensor product $A \otimes B$ as the tensor product of A and B over \mathbf{Z} equipped with the continuous G -action induced by $\sigma(a \otimes b) = \sigma(a) \otimes \sigma(b)$. In the previous chapter we have constructed for all $i, j \geq 0$ and all open subgroups U of G cup-product maps

$$H^i(G/U, A^U) \times H^j(G/U, B^U) \rightarrow H^{i+j}(G/U, A^U \otimes B^U), \quad (a, b) \mapsto a \cup b$$

satisfying the relation

$$\text{Inf}(a \cup b) = \text{Inf}(a) \cup \text{Inf}(b)$$

for the inflation map arising from the quotient map $G/V \rightarrow G/U$ for an open inclusion $V \subset U$. Note that by the above definition of the G -action we have

a natural map $A^U \otimes B^U \rightarrow (A \otimes B)^U$, so by passing to the limit over all inflation maps of the above type we obtain cup-product maps

$$H^i(G, A) \times H^j(G, B) \rightarrow H^{i+j}(G, A \otimes B), \quad (a, b) \mapsto a \cup b$$

for continuous cohomology.

It follows immediately from the non-continuous case that this cup-product is also associative and graded-commutative, and that moreover it satisfies compatibility formulae with restriction, corestriction and inflation maps as in Proposition 3.4.10. It also satisfies the exactness property of Proposition 3.4.8, but for this we have to establish first the long exact cohomology sequence in the profinite setting. We treat this question in the next section.

4.3 The Cohomology Exact Sequence

We now show that the analogues of exact sequences established for usual cohomology groups also hold for continuous ones. We begin with the long exact cohomology sequence.

Proposition 4.3.1 *Given a profinite group G and a short exact sequence*

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

of continuous G -modules, there is a long exact sequence of abelian groups

$$\dots \rightarrow H^i(G, A) \rightarrow H^i(G, B) \rightarrow H^i(G, C) \rightarrow H^{i+1}(G, A) \rightarrow \dots$$

starting from $H^0(G, A)$.

For the proof we need two formal statements about direct limits.

Lemma 4.3.2 *Let $(A_\alpha, \phi_{\alpha\beta})$, $(B_\alpha, \psi_{\alpha\beta})$ and $(C_\alpha, \rho_{\alpha\beta})$ be three direct systems indexed by the same directed set Λ . Assume moreover given exact sequences*

$$A_\alpha \xrightarrow{\lambda_\alpha} B_\alpha \xrightarrow{\mu_\alpha} C_\alpha$$

for each $\alpha \in \Lambda$ such that the diagrams

$$\begin{array}{ccccc} A_\alpha & \xrightarrow{\lambda_\alpha} & B_\alpha & \xrightarrow{\mu_\alpha} & C_\alpha \\ \phi_{\alpha\beta} \downarrow & & \psi_{\alpha\beta} \downarrow & & \rho_{\alpha\beta} \downarrow \\ A_\beta & \xrightarrow{\lambda_\beta} & B_\beta & \xrightarrow{\mu_\beta} & C_\beta \end{array}$$

commute for all $\alpha \leq \beta$. Then the limit sequence

$$\varinjlim A_\alpha \xrightarrow{\lambda} \varinjlim B_\alpha \xrightarrow{\mu} \varinjlim C_\alpha$$

is exact as well.

Proof: An element of $\ker(\mu)$ is represented by some $b_\alpha \in B_\alpha$ with the property that $\rho_{\alpha\beta}(\mu_\alpha(b_\alpha)) = \mu_\beta(\psi_{\alpha\beta}(b_\alpha)) = 0$ for some $\beta \geq \alpha$. But then there is some $a_\beta \in A_\beta$ with $\lambda_\beta(a_\beta) = \psi_{\alpha\beta}(b_\alpha)$. \square

Lemma 4.3.3 *Consider a profinite group G and a direct system $(A_\alpha, \phi_{\alpha\beta})$ of continuous G -modules (in particular, the $\phi_{\alpha\beta}$ are G -homomorphisms). Then the G -module $\varinjlim A_\alpha$ is also continuous, the groups $H^i(G, A_\alpha)$ with the induced maps form a direct system, and there exist canonical isomorphisms*

$$\varinjlim H^i(G, A_\alpha) \xrightarrow{\sim} H^i(G, \varinjlim A_\alpha)$$

for all $i \geq 0$.

Proof: The first statement follows from the construction of direct limits, which also shows that for each open subgroup U the G/U -module $(\varinjlim A_\alpha)^U$ is the direct limit of the G/U -modules A_α^U . Hence it suffices to show the isomorphism statement for the cohomology of the latter. Taking a projective resolution P^\bullet of the trivial G/U -module \mathbf{Z} , we are reduced to establishing isomorphisms of the form

$$\varinjlim \operatorname{Hom}(P^i, A_\alpha) \xrightarrow{\sim} \operatorname{Hom}(P^i, \varinjlim A_\alpha)$$

compatible with coboundary maps. Such isomorphisms again follow from the construction of direct limits (for instance, one may observe that the canonical isomorphisms $\oplus \operatorname{Hom}(P^i, A_\alpha) \cong \operatorname{Hom}(P^i, \oplus A_\alpha)$ preserve the relations defining the direct limit). \square

Proof of Proposition 4.3.1: The homomorphisms $H^i(G, A) \rightarrow H^i(G, B)$ and $H^i(G, B) \rightarrow H^i(G, C)$ arise from the finite case by passing to the limit. To define the connecting homomorphism $\partial : H^i(G, C) \rightarrow H^{i+1}(G, A)$, consider first an open subgroup U of G and define K_U as the cokernel of the map $B^U \rightarrow C^U$ (this is a nontrivial group in general). As the map $B \rightarrow C$ is surjective, we get that the direct limit of the groups K_U with U running over all open subgroups is trivial. Therefore the last term in the sequence

$$\varinjlim H^i(G/U, (B^U/A^U)) \rightarrow \varinjlim H^i(G/U, C^U) \rightarrow \varinjlim H^i(G/U, K_U)$$

is trivial by Lemma 4.3.3 (note that each K_U is also a G -module via the natural projection). The sequence is exact by Lemma 4.3.2, hence we may always lift an element γ of the middle term, which is none but $H^i(G, C)$,

to an element in some $H^i(G/U, (B^U/A^U))$. The usual long exact sequence coming from the sequence of G/U -modules

$$0 \rightarrow A^U \rightarrow B^U \rightarrow B^U/A^U \rightarrow 0 \quad (1)$$

then yields an element in $H^{i+1}(G/U, A^U)$, and hence in $H^{i+1}(G, A)$, which we define to be $\partial(\gamma)$. This definition manifestly does not depend on the choice of U , and furthermore, the long exact sequence coming from

$$0 \rightarrow B^U/A^U \rightarrow C^U \rightarrow K_U \rightarrow 0$$

shows that any two liftings of γ into $H^i(G/U, (B^U/A^U))$ differ by an element of $H^{i-1}(G/U, K_U)$, which then maps to 0 in $H^{i-1}(G/V, K_V)$ for some $V \subset U$. This shows that the map ∂ is well-defined. Exactness of the sequence at the terms $H^i(G, A)$ and $H^i(G, C)$ now follows from that of the long exact sequence associated with (1) and exactness at the terms $H^i(G, B)$ follows from Lemma 4.3.2. \square

Remarks 4.3.4

1. A more elegant way for establishing the above proposition is by constructing continuous cohomology groups directly as Ext-groups in the category of continuous G -modules; the long exact sequence then becomes a formal consequence, just as in the previous chapter (see e.g. Weibel [1], Section 6.11). We have chosen the above more pedestrian presentation in order to emphasize the viewpoint that all basic facts for the cohomology of profinite groups follow from the finite case by passing to the limit.
2. It is important to note that if the exact sequence

$$0 \rightarrow A \rightarrow B \xrightarrow{p} C \rightarrow 0$$

has a splitting, i.e. a map of G -modules $i : C \rightarrow B$ with $p \circ i = \text{id}_C$, then the induced maps $p_* : H^i(G, B) \rightarrow H^i(G, C)$ and $i_* : H^i(G, C) \rightarrow H^i(G, B)$ also satisfy $p_* \circ i_* = \text{id}$ by the functoriality of cohomology. Therefore the long exact sequence splits up into a collection of (split) short exact sequences

$$0 \rightarrow H^i(G, A) \rightarrow H^i(G, B) \rightarrow H^i(G, C) \rightarrow 0,$$

a fact we shall use many times later.

The inflation-restriction sequences of the last chapter also carry over to the profinite setting:

Corollary 4.3.5 *Let G be a profinite group, H a closed normal subgroup. Then the statements of Propositions 3.3.14 and 3.3.17 remain valid in the continuous cohomology.*

Proof: This follows from *loc. cit.* via Lemma 4.3.2. \square

We conclude this section with a first application of the cohomology of profinite groups which will be invaluable for the sequel.

Proposition 4.3.6 (Kummer Theory) *Let k be a field, and $m > 0$ an integer prime to the characteristic of k . Denote by μ_m the group of m -th roots of unity in a fixed separable closure of k , equipped with its Galois action. There exists a canonical isomorphism*

$$k^\times / k^{\times m} \xrightarrow{\sim} H^1(k, \mu_m)$$

induced by sending an element $a \in k^\times$ to the class of the 1-cocycle $\sigma \mapsto \sigma(\alpha)\alpha^{-1}$, where α is an m -th root of a .

For the proof we need the continuous version of Hilbert's Theorem 90:

Lemma 4.3.7 *The Galois cohomology group $H^1(k, k_s^\times)$ is trivial.*

Proof: This follows from Example 2.3.4 after passing to the limit. \square

Proof of Proposition 4.3.6: Consider the exact sequence of $\text{Gal}(k_s|k)$ -modules

$$1 \rightarrow \mu_m \rightarrow k_s^\times \xrightarrow{m} k_s^\times \rightarrow 1, \quad (2)$$

where the third map is given by raising elements to the m -th power. This map is surjective because the polynomial $x^m - a$ is separable for all $a \in k_s$, in view of the assumption on m . A piece of the associated long exact sequence reads

$$H^0(k, k_s^\times) \rightarrow H^0(k, k_s^\times) \rightarrow H^1(k, \mu_m) \rightarrow H^1(k, k_s^\times),$$

where the last group is trivial by the lemma. Noting that $H^0(k, k_s^\times) = k^\times$ and that the first map is multiplication by m , by construction of cohomology, we obtain the required isomorphism. Its explicit description follows from the construction of the coboundary map in cohomology (see Remark 3.2.4). \square

Remark 4.3.8 Note that it was crucial here to work with k_s and Galois cohomology, for we do not dispose of the analogue of exact sequence (2) at a finite level.

The proposition has the following consequence (which is the original form of Kummer's theorem):

Corollary 4.3.9 *For k and m as above, assume moreover that k contains a primitive m -th root of unity ω . Then every finite Galois extension of k with Galois group isomorphic to $\mathbf{Z}/m\mathbf{Z}$ is of the form $k(\alpha)|k$ with some $\alpha \in k_s^\times$ satisfying $\alpha^m \in k^\times$.*

Proof: The Galois group of an extension as in the corollary is a quotient of $\text{Gal}(k_s|k)$ isomorphic to $\mathbf{Z}/m\mathbf{Z}$, and thus corresponds to a surjection $\chi : \text{Gal}(k_s|k) \rightarrow \mathbf{Z}/m\mathbf{Z}$. But since by assumption $\mu_m \subset k$, we have isomorphisms $\text{Hom}(\text{Gal}(k_s|k), \mathbf{Z}/m\mathbf{Z}) \cong H^1(k, \mathbf{Z}/m\mathbf{Z}) \cong H^1(k, \mu_m)$ (the second one depending on the choice of ω). By the proposition χ corresponds to the class of some $a \in k^\times$ modulo $k^{\times m}$, and moreover the kernel of χ is precisely $\text{Gal}(k(\alpha)|k)$, where α is an m -th root of a . \square

In positive characteristic we have the following complement to Kummer theory.

Proposition 4.3.10 (Artin-Schreier Theory) *Let k be a field of characteristic $p > 0$. Denote by $\wp : k \rightarrow k$ the endomorphism mapping $x \in K$ to $x^p - x$. Then there exists a canonical isomorphism*

$$k/\wp(k) \xrightarrow{\sim} H^1(k, \mathbf{Z}/p\mathbf{Z})$$

induced by mapping $a \in k$ to the cocycle $\sigma \mapsto \sigma(a) - a$, where α is a root of the equation $x^p - x = a$.

The proof is based on the following lemma. It is sometimes called the additive version of Hilbert's Theorem 90, as it concerns the additive group of k_s viewed as a $\text{Gal}(k_s|k)$ -module instead of the multiplicative group.

Lemma 4.3.11 *For an arbitrary field k the groups $H^i(k, k_s)$ are trivial for all $i > 0$.*

Proof: We prove the triviality of $H^i(G, K)$ for all Galois extensions $K|k$ with group G and all $i > 0$. According to the normal basis theorem of Galois theory (see e.g. Lang [3], Chapter VI, Theorem 13.1), we may find an element $x \in K$ such that $\sigma_1(x), \dots, \sigma_n(x)$ form a basis of the k -vector space K , where $1 = \sigma_1, \dots, \sigma_n$ are the elements of G . This means that K is isomorphic to $K \otimes_{\mathbf{Z}} \mathbf{Z}[G]$ as a G -module. The latter is a co-induced G -module by Remark 3.3.4 (3), so its cohomology is trivial by Corollary 3.3.3. \square

Remark 4.3.12 In characteristic 0 the lemma is easy to prove: the coefficient module k_s is a \mathbf{Q} -vector space, hence Corollary 4.2.7 applies. However, we are about to apply the positive characteristic case.

Proof of Proposition 4.3.10: The endomorphism \wp extends to the separable closure k_s with the same definition. Its kernel is the prime field \mathbf{F}_p , which is isomorphic to the trivial $\text{Gal}(k_s|k)$ -module $\mathbf{Z}/p\mathbf{Z}$ as a $\text{Gal}(k_s|k)$ -module.

Moreover, the map $\wp : k_s \rightarrow k_s$ is surjective, because for each $a \in k_s$ the polynomial $x^p - x - a$ is separable. We thus have an exact sequence of $\text{Gal}(k_s|k)$ -modules

$$0 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow k_s \xrightarrow{\wp} k_s \rightarrow 0, \quad (3)$$

from which we conclude as in the proof of Proposition 4.3.6, using Lemma 4.3.11 in place of Hilbert's Theorem 90. \square

Remarks 4.3.13

1. In a similar way as in Corollary 4.3.9 above, one derives from the proposition that every finite Galois extension of k with Galois group $\mathbf{Z}/p\mathbf{Z}$ is generated by a root of some polynomial $x^p - x - a$, with $a \in k$.
2. There is a generalisation of Artin-Schreier theory to powers of the prime p due to Witt. The principle of the proof is the same as above, but instead of the additive group of k_s one has to use so-called Witt vectors (see e.g. Serre [2]).

4.4 The Brauer Group Revisited

The main goal of this section is to identify the Brauer group of a field k with the Galois cohomology group $H^2(k, k_s^\times)$, which is more tractable than the group $H^1(k, \text{PGL}_\infty)$ encountered in Chapter 2. To this aim, we first have to extend the non-commutative cohomology sequence of Proposition 2.7.1.

Proposition 4.4.1 *Let G be a group and*

$$1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$$

an exact sequence of groups equipped with a G -action, such that B and C are not necessarily commutative, but A is commutative and contained in the center of B . Then there is an exact sequence of pointed sets

$$1 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \rightarrow H^2(G, A).$$

Proof: The sequence was constructed until the penultimate term in Proposition 2.7.1. To define the map $\partial : H^1(G, C) \rightarrow H^2(G, A)$, take a 1-cocycle $\sigma \mapsto c_\sigma$ representing a class in $H^1(G, C)$ and lift each c_σ to an element $b_\sigma \in B$. The cocycle relation for $\sigma \mapsto c_\sigma$ implies that for all $\sigma, \tau \in G$ the element $b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$ maps to 1 in C , hence comes from an element $a_{\sigma,\tau} \in A$. The function $(\sigma, \tau) \mapsto a_{\sigma,\tau}$ depends only on the class of $\sigma \mapsto c_\sigma$ in $H^1(G, C)$. Indeed,

if we replace it by an equivalent cocycle $\sigma \mapsto c^{-1}c_\sigma\sigma(c)$, lifting c to $b \in B$ replaces $a_{\sigma\tau}$ by $(b^{-1}b_\sigma\sigma(b))(\sigma(b^{-1})\sigma(b_\tau)\sigma\tau(b))(\sigma\tau(b)^{-1}b_{\sigma,\tau}^{-1}b) = b^{-1}a_{\sigma,\tau}b$, which equals $a_{\sigma,\tau}$ because A is central in B . A straightforward calculation, which we leave to the readers, shows that $(\sigma, \tau) \mapsto a_{\sigma\tau}$ satisfies the 2-cocycle relation $\sigma(a_{\sigma,\tau})a_{\sigma\tau}^{-1}a_{\sigma,\tau\nu}a_{\sigma,\tau\nu}^{-1} = 1$ that we made explicit in Example 3.2.3 (2). Finally, replacing b_σ by another lifting $a_\sigma b_\sigma$ replaces $a_{\sigma,\tau}$ by $a_\sigma b_\sigma \sigma(a_\tau b_\tau) b_{\sigma\tau}^{-1} a_{\sigma\tau}^{-1} = a_\sigma \sigma(a_\tau) a_{\sigma\tau}^{-1} a_{\sigma,\tau}$, which has the same class in $H^2(G, A)$ (notice that we have used again that A is central in B). This defines the map ∂ , and at the same time shows that it is trivial on the image of $H^1(G, B)$.

Finally, in the above notation, a class in $H^1(G, C)$ represented by $\sigma \mapsto c_\sigma$ is in the kernel of ∂ if the 2-cocycle $(\sigma, \tau) \mapsto b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$ equals a 2-coboundary $(\sigma, \tau) \mapsto a_\sigma \sigma(a_\tau) a_{\sigma\tau}^{-1}$. Replacing b_σ by the equivalent lifting $a_\sigma^{-1} b_\sigma$ we may assume $b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1} = 1$, which means that $\sigma \mapsto b_\sigma$ is a 1-cocycle representing a cohomology class in $H^1(G, B)$. \square

Remarks 4.4.2

1. Readers should be warned that the proposition does not hold in the above form when A is not contained in the center of B . Instead, one has to work with twists of A as in Serre [4], §I.5.6.
2. When B and C are commutative, the exact sequence of the proposition is of course part of the long exact sequence for group cohomology. This follows from the cocycle descriptions of Example 3.2.3 and Remark 3.2.4.

Now let $K|k$ be a finite Galois extension of fields with group G , and m a positive integer. Applying the previous proposition to the exact sequence of G -groups

$$1 \rightarrow K^\times \rightarrow \mathrm{GL}_m(K) \rightarrow \mathrm{PGL}_m(K) \rightarrow 1$$

we get an exact sequence of pointed sets

$$H^1(G, \mathrm{GL}_m(K)) \longrightarrow H^1(G, \mathrm{PGL}_m(K)) \xrightarrow{\delta_m} H^2(G, K^\times). \quad (4)$$

Now recall the maps $\lambda_{mn} : H^1(G, \mathrm{PGL}_m(K)) \rightarrow H^1(G, \mathrm{PGL}_{mn}(K))$ introduced in Chapter 2, Section 2.4.

Lemma 4.4.3 *The diagram*

$$\begin{array}{ccc} H^1(G, \mathrm{PGL}_m(K)) & \xrightarrow{\delta_m} & H^2(G, K^\times) \\ \lambda_{mn} \downarrow & & \downarrow \mathrm{id} \\ H^1(G, \mathrm{PGL}_{mn}(K)) & \xrightarrow{\delta_{mn}} & H^2(G, K^\times) \end{array}$$

commutes for all $m, n > 0$.

Proof: A 1-cocycle $\sigma \mapsto c_\sigma$ representing a class in $H^1(G, \mathrm{PGL}_m(K))$ is mapped by δ_m to a 2-cocycle $a_{\sigma,\tau} = b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$ by the construction of the previous proof, where b_σ is given by some invertible matrix M_σ and $a_{\sigma,\tau}$ is the identity matrix I_m multiplied by some scalar $\mu_{\sigma,\tau} \in K^\times$. Performing the same construction for the image of $\sigma \mapsto c_\sigma$ by λ_{mn} means replacing M_σ by the block matrix with m copies of M_σ along the diagonal, which implies that the scalar matrix we obtain by taking the associated 2-cocycle is $\mu_{\sigma,\tau} I_{mn}$. \square

By the lemma, taking the union of the pointed sets $H^1(G, \mathrm{PGL}_m(K))$ with respect to the maps λ_{mn} yields a map

$$\delta_\infty : H^1(G, \mathrm{PGL}_\infty) \rightarrow H^2(G, K^\times).$$

Lemma 4.4.4 *Equip the set $H^1(G, \mathrm{PGL}_\infty)$ with the product operation defined in Chapter 2, Section 2.4. Then the map δ_∞ is a group homomorphism.*

Proof: We have already checked in Chapter 2, Section 2.4 that $H^1(G, \mathrm{PGL}_\infty)$ equipped with the product operation is a group. To show that δ_∞ preserves multiplication, take cohomology classes $c_m \in H^1(G, \mathrm{PGL}_m(K))$ and $c_n \in H^1(G, \mathrm{PGL}_n(K))$. With notations as in the previous proof, the classes $\delta_m(c_m)$ and $\delta_n(c_n)$ are represented by 2-cocycles of the form $(\sigma, \tau) \rightarrow \mu_{\sigma,\tau} I_m$ and $(\sigma, \tau) \rightarrow \nu_{\sigma,\tau} I_n$, respectively. From the fact that the product $c_{mn} \in H^1(G, \mathrm{PGL}_{mn}(K))$ of c_n and c_m is induced by tensor product of linear maps we infer that $\delta_{mn}(c_{mn})$ is represented by a 2-cocycle mapping (σ, τ) to the tensor product of the linear maps given by multiplication by $\mu_{\sigma,\tau}$ and $\nu_{\sigma,\tau}$, respectively. But this tensor product is none but multiplication by $\mu_{\sigma,\tau} \nu_{\sigma,\tau}$, which was to be seen. \square

Now we come to the main result of this section.

Theorem 4.4.5 *The map δ_∞ defined above induces an isomorphism*

$$H^1(G, \mathrm{PGL}_\infty) \xrightarrow{\sim} H^2(G, K^\times)$$

of abelian groups.

Proof: Since δ_∞ is a group homomorphism and $H^1(G, \mathrm{PGL}_\infty)$ is the union of the pointed sets $H^1(G, \mathrm{PGL}_m(K))$, for injectivity it is enough to show that the map δ_m in exact sequence (4) has trivial kernel for all m . This follows from the exact sequence in view of the triviality of $H^1(G, \mathrm{GL}_m(K))$ (Example 2.3.4).

For surjectivity we show much more, namely that the map δ_n is surjective, where n is the order of G . For this, consider $K \otimes_k K$ as a K -vector space.

Multiplication by an invertible element of $K \otimes_k K$ is a K -linear automorphism $K \otimes_k K \rightarrow K \otimes_k K$. In this way we get a group homomorphism $(K \otimes_k K)^\times \rightarrow \mathrm{GL}_n(K)$ which we may insert into a commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & (K \otimes_k K)^\times & \longrightarrow & (K \otimes_k K)^\times / K^\times \longrightarrow 1 \\ & & \mathrm{id} \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & K^\times & \longrightarrow & \mathrm{GL}_n(K) & \longrightarrow & \mathrm{PGL}_n(K) \longrightarrow 1 \end{array}$$

where all maps are compatible with the action of G if we make G act on $K \otimes_k K$ via the right factor and on the other terms by the standard action. Hence by taking cohomology we get a commutative diagram

$$\begin{array}{ccccc} H^1(G, (K \otimes_k K)^\times / K^\times) & \xrightarrow{\alpha} & H^2(G, K^\times) & \longrightarrow & H^2(G, (K \otimes_k K)^\times) \\ \downarrow & & \mathrm{id} \downarrow & & \\ H^1(G, \mathrm{PGL}_n(K)) & \xrightarrow{\delta_n} & H^2(G, K^\times) & & \end{array}$$

where the upper row is exact. Recall now the G -isomorphism $K \otimes_k K \cong \bigoplus K e_i$ explained before the proof of Lemma 2.3.8. In other words, it says that $K \otimes_k K$ is isomorphic as a G -module to $K \otimes_{\mathbf{Z}} \mathbf{Z}[G]$, which implies that $(K \otimes_k K)^\times$ is isomorphic to the G -module $K^\times \otimes_{\mathbf{Z}} \mathbf{Z}[G]$, because the invertible elements in $\bigoplus K e_i$ are exactly those with coefficients in K^\times . Now by Remark 3.3.4 (3) the G -module $K^\times \otimes_{\mathbf{Z}} \mathbf{Z}[G]$ is co-induced, hence the group $H^2(G, (K \otimes_k K)^\times)$ is trivial. This yields the surjectivity of the map α in the diagram, and hence also that of δ_n by commutativity of the diagram. \square

The above proof shows much more than the assertion of the theorem. Namely, the fact that we have at our disposal both the injectivity of δ_m for all m and the surjectivity of δ_n has the following remarkable consequences.

Corollary 4.4.6 *Let $K|k$ be a finite Galois extension of degree n and group G . Then the maps $\lambda_{nm} : H^1(G, \mathrm{PGL}_n(K)) \rightarrow H^1(G, \mathrm{PGL}_{nm}(K))$ are bijective for all m .*

Furthermore, the pointed set $H^1(G, \mathrm{PGL}_n(K))$ is equipped with a group structure via

$$H^1(G, \mathrm{PGL}_n(K)) \times H^1(G, \mathrm{PGL}_n(K)) \rightarrow H^1(G, \mathrm{PGL}_{n^2}(K)) \xrightarrow{\sim} H^1(G, \mathrm{PGL}_n(K))$$

and the map $\delta_n : H^1(G, \mathrm{PGL}_n(K)) \rightarrow H^2(G, K^\times)$ is an isomorphism of abelian groups.

Proof: In the first assertion only surjectivity requires a proof, and this follows from the surjectivity of δ_n together with Lemma 4.4.3. The second assertion then follows from the theorem. \square

Combining the theorem with Proposition 2.4.10 we get:

Theorem 4.4.7 *Let k be a field, $K|k$ a finite Galois extension and k_s a separable closure of k . There exist natural isomorphisms of abelian groups*

$$\mathrm{Br}(K|k) \cong H^2(G, K^\times) \quad \text{and} \quad \mathrm{Br}(k) \cong H^2(k, k_s^\times).$$

The theorem has a number of corollaries. Here is a first one which is quite cumbersome to establish in the context of central simple algebras but is almost trivial once one disposes of cohomological techniques.

Corollary 4.4.8 *Let $K|k$ be a Galois extension of degree n . Then each element of the relative Brauer group $\mathrm{Br}(K|k)$ has order dividing n . Consequently, the Brauer group $\mathrm{Br}(k)$ is a torsion abelian group.*

Proof: This follows from Corollary 3.3.8. \square

One also has the following cohomological interpretation of the m -torsion part ${}_m\mathrm{Br}(k)$ of the Brauer group.

Corollary 4.4.9 *For each positive integer m prime to the characteristic of k we have a canonical isomorphism*

$${}_m\mathrm{Br}(k) \cong H^2(k, \mu_m).$$

Recall that μ_m denotes the group of m -th roots of unity in k_s equipped with its canonical Galois action.

Proof: We again exploit the exact sequence (2). A piece of the associated long exact sequence is

$$H^1(k, k_s^\times) \rightarrow H^2(k, \mu_m) \rightarrow H^2(k, k_s^\times) \rightarrow H^2(k, k_s^\times),$$

where the first group is trivial by Hilbert's Theorem 90 (Lemma 4.3.7). The corollary follows by noting that the last map is multiplication by m . \square

As another corollary, we have a nice description of the relative Brauer group in the case of a cyclic extension.

Corollary 4.4.10 *For a cyclic Galois extension $K|k$ there is a canonical isomorphism*

$$\mathrm{Br}(K|k) \cong k^\times / N_{K|k}(K^\times).$$

Proof: This follows from the theorem in view of the calculation of the cohomology of cyclic groups (Example 3.2.9). \square

Finally, we also record the following inflation-restriction sequence:

Corollary 4.4.11 *For a finite Galois extension $K|k$ there is an exact sequence*

$$0 \rightarrow \text{Br}(K|k) \xrightarrow{\text{Inf}} \text{Br}(k) \xrightarrow{\text{Res}} \text{Br}(K).$$

Proof: This follows from the theorem and Corollary 4.3.5 in degree 2 (which applies to the $\text{Gal}(k_s|k)$ -module k_s^\times in view of Hilbert's Theorem 90). \square

4.5 Index and Period

In this section we use the cohomological theory of the Brauer group to derive basic results of Brauer concerning two important invariants for central simple algebras. We shall assume throughout that the base field k is infinite; indeed, we shall see in Chapter 6 that the Brauer group of a finite field is trivial, so the discussion to follow is vacuous in that case.

The first of the announced invariants is the following.

Definition 4.5.1 Let A be a central simple algebra over a field k . The *index* $\text{ind}_k(A)$ of A over k is defined to be the degree of D over k , where D is the division algebra for which $A \cong M_n(D)$ according to Wedderburn's theorem. We shall drop the subscript k from the notation when clear from the context.

Remarks 4.5.2

1. For a division algebra index and degree are one and the same thing.
2. The index of a central simple k -algebra A depends only on the class of A in the Brauer group $\text{Br}(k)$. Indeed, this class depends only on the division algebra D associated with A by Wedderburn's theorem, and the index is by definition an invariant of D .
3. We have $\text{ind}(A) = 1$ if and only if A is split.

We begin the study of the index with the following elementary proposition which could have figured in Chapter 2.

Proposition 4.5.3 *Let D be a central division algebra over k . If D contains a subfield K which is of degree $\text{ind}(D)$ over k , then D splits over K .*

Proof: Let D° be the opposite algebra to D . We have established during the proof of Proposition 2.4.8 an isomorphism $D \otimes_k D^\circ \cong \text{End}_k(D)$. If K is as above, the inclusion $K \subset D$ induces an inclusion $K \subset D^\circ$ by commutativity of K , whence also an injection $\iota : D \otimes_k K \rightarrow \text{End}_k(D)$. As the endomorphisms of D coming from $D \otimes_k K$ are given by multiplication by elements of K , we see that the image of ι lies in $\text{End}_K(D)$. By definition, we have $\text{End}_K(D) \cong M_n(K)$, where $n = \text{ind}_k(D)$; in particular, it has dimension n^2 over K . On the other hand, we have $\dim_K(D \otimes_k K) = \dim_k(D) = n^2$, so the map $\iota : D \otimes_k K \rightarrow \text{End}_K(D)$ is an isomorphism. \square

We can now prove the following basic fact.

Proposition 4.5.4 *Every central simple k -algebra A is split by a separable extension $K|k$ of degree $\text{ind}(A)$ over k . Moreover, such a K may be found among the k -subalgebras of A .*

The proof is based on the following lemma, which uses the notion of the *reduced characteristic polynomial* $P_a(T)$ of an element $a \in A$. This is defined as the polynomial $\text{Nrd}(T - a) \in k[T]$, where Nrd is the reduced norm map introduced in Construction 2.6.1. Note that if we choose an algebraic closure \bar{k} of k and an isomorphism $A \otimes_k \bar{k} \cong M_n(\bar{k})$, then $P_a(T)$ becomes the characteristic polynomial of the matrix M_a corresponding to a . In particular, its coefficients are polynomials in the entries of M_a .

Lemma 4.5.5 *For A as above, we may find $a \in A$ so that its reduced characteristic polynomial $P_a(T)$ has distinct roots.*

Proof: The polynomial $P_a(T)$ has distinct roots if and only if its discriminant D_a is nonzero. It is known from algebra that D_a is a polynomial in the coefficients of $P_a(T)$. Now choose an isomorphism $A \otimes_k \bar{k} \cong M_n(\bar{k})$ and view the elements $M_n(\bar{k})$ as points of affine n^2 -space over \bar{k} . By the above discussion, the points corresponding to matrices whose characteristic polynomial has nonzero discriminant form a Zariski open subset in $\mathbf{A}_{\bar{k}}^{n^2}$. A k -rational point in this open subset corresponds to an element $a \in A$ with the required property. \square

Proof of Proposition 4.5.4: By Wedderburn's theorem we may assume that A is a division algebra. By the lemma we find $a \in A$ so that $P_a(T)$ has distinct roots. As $P_a(T)$ is the characteristic polynomial of a matrix M_a over \bar{k} , this implies that M_a has distinct eigenvalues, and hence $P_a(T)$ is also its minimal polynomial. In particular, $P_a(T)$ is irreducible over \bar{k} and hence also over k , so the ring $K := k[T]/(P_a(T))$ is a separable field extension

of k . Therefore the homomorphism $k[T] \rightarrow A$ sending T to a embeds K as a subfield in A which is of degree $\deg P_a(T) = \deg_k(A) = \text{ind}_k(A)$ over k (as A is assumed to be a division algebra). We conclude by the previous proposition. \square

To proceed further, we need the following refinement of Theorem 4.4.5.

Proposition 4.5.6 *Let $K|k$ be a separable field extension of degree n . Then the boundary map $\delta_n : H^1(k, \text{PGL}_n(k)) \rightarrow \text{Br}(k)$ induces a bijection*

$$\ker(H^1(k, \text{PGL}_n(k)) \rightarrow H^1(K, \text{PGL}_n(K))) \xrightarrow{\sim} \text{Br}(K|k).$$

The proof uses a lemma from Galois theory.

Lemma 4.5.7 *Let \tilde{K} be the Galois closure of K , and denote the Galois groups $\text{Gal}(\tilde{K}|k)$ and $\text{Gal}(\tilde{K}|K)$ by G and H , respectively. Making G act on the tensor product $K \otimes_k \tilde{K}$ via the second factor, we have an isomorphism of G -modules*

$$(K \otimes_k \tilde{K})^\times \cong M_H^G(\tilde{K}^\times).$$

Proof: According to the theorem of the primitive element, we may write $K = k(\alpha)$ for some $\alpha \in K$ with minimal polynomial $f \in k[x]$, so that \tilde{K} is the splitting field of f . By Galois theory, if $1 = \sigma_1, \dots, \sigma_n$ is a system of left coset representatives for H in G , the roots of f in K are exactly the $\sigma_i(\alpha)$ for $1 \leq i \leq n$. So we get, just like before the proof of Speiser's lemma in Chapter 2, a chain of isomorphisms

$$K \otimes_k \tilde{K} \cong \tilde{K}[x] / \prod_{i=1}^n (x - \sigma_i(\alpha)) \cong \text{Hom}_H(\mathbf{Z}[G], \tilde{K}) = M_H^G(\tilde{K}).$$

The lemma follows by restricting to invertible elements. \square

Proof of Proposition 4.5.6: We have already shown in the proof of Theorem 4.4.5 the injectivity of δ_n (even of δ_∞), so it suffices to see surjectivity. With the notations of the lemma above, consider the short exact sequence of G -modules

$$1 \rightarrow \tilde{K}^\times \rightarrow (K \otimes_k \tilde{K})^\times \rightarrow (K \otimes_k \tilde{K})^\times / \tilde{K}^\times \rightarrow 1,$$

where G acts on $K \otimes_k \tilde{K}$ via the second factor. Part of the associated long exact sequence reads

$$H^1(G, (K \otimes_k \tilde{K})^\times / \tilde{K}^\times) \rightarrow H^2(G, \tilde{K}^\times) \rightarrow H^2(G, (K \otimes_k \tilde{K})^\times). \quad (5)$$

Using the previous lemma, Shapiro's lemma and Theorem 4.4.5, we get a chain of isomorphisms

$$H^2(G, (K \otimes_k \tilde{K})^\times) \cong H^2(G, M_H^G(\tilde{K})) \cong H^2(H, \tilde{K}) \cong \text{Br}(\tilde{K}|K).$$

We also have $H^2(G, \tilde{K}^\times) \cong \text{Br}(\tilde{K}|k)$, so all in all we get from exact sequence (5) a surjection

$$\tilde{\alpha} : H^1(G, (K \otimes_k \tilde{K})^\times / \tilde{K}^\times) \rightarrow \text{Br}(K|k)$$

On the other hand, the choice of a k -basis of \tilde{K} provides an embedding $K \hookrightarrow M_n(k)$, whence a G -equivariant map $K \otimes_k \tilde{K} \rightarrow M_n(\tilde{K})$, and finally a map $(K \otimes_k \tilde{K})^\times \rightarrow \text{GL}_n(\tilde{K})$. Arguing as in the proof of Theorem 4.4.5, we get a commutative diagram:

$$\begin{array}{ccc} H^1(G, (K \otimes_k \tilde{K})^\times / K^\times) & \xrightarrow{\tilde{\alpha}} & H^2(G, \tilde{K}^\times) \\ \downarrow & & \downarrow \text{id} \\ H^1(G, \text{PGL}_n(\tilde{K})) & \xrightarrow{\delta_n} & H^2(G, \tilde{K}^\times) \end{array}$$

Therefore by the surjectivity of $\tilde{\alpha}$ each element of $\text{Br}(K|k) \subset H^2(G, \tilde{K}^\times)$ comes from some element in $H^1(G, \text{PGL}_n(\tilde{K}))$. By the injectivity of δ_n and its obvious compatibility with restriction maps, this element restricts to 1 in $H^1(H, \text{PGL}_n(\tilde{K}))$, as required. \square

We can now prove the following characterisations of the index.

Proposition 4.5.8 *Let A be a central simple k -algebra. The index $\text{ind}(A)$ is the greatest common divisor of the degrees of finite separable field extensions $K|k$ that split A .*

Proof: In view of Proposition 4.5.4 it is enough to show that if a finite separable extension $K|k$ of degree n splits A , then $\text{ind}(A)$ divides n . For such a K , the class of A in $\text{Br}(K|k)$ comes from a class in $H^1(k, \text{PGL}_n(k))$ according to Proposition 4.5.6. By Theorem 2.4.3 this class is also represented by some central simple k -algebra B of degree n , hence of index dividing n . But $\text{ind}(A) = \text{ind}(B)$ by Remark 4.5.2 (2). \square

Combining with Proposition 4.5.4 we get:

Corollary 4.5.9 *The index $\text{ind}(A)$ is the smallest among the degrees of finite separable field extensions $K|k$ that split A .*

Here are some other easy corollaries.

Corollary 4.5.10 *Let A and B be central simple k -algebra that generate the same subgroup in $\text{Br}(k)$. Then $\text{ind}(A) = \text{ind}(B)$.*

Proof: The proposition implies that for all i we have $\text{ind}(A^{\otimes i}) \mid \text{ind}(A)$. But for suitable i and j we have $[A^{\otimes i}] = [B]$ and $[B^{\otimes j}] = [A]$ in $\text{Br}(k)$ by assumption, so the result follows, taking Remark 4.5.2 (2) into account. \square

Corollary 4.5.11 *Let $K|k$ be a finite separable field extension.*

1. *We have the divisibility relations*

$$\text{ind}_K(A \otimes_k K) \mid \text{ind}_k(A) \mid [K : k] \text{ind}_K(A \otimes_k K).$$

2. *If $\text{ind}_k(A)$ is prime to $[K : k]$, then $\text{ind}_k(A) = \text{ind}_K(A \otimes_k K)$. In particular, if A is a division algebra, then so is $A \otimes_k K$.*

Proof: It is enough to prove the first statement. The divisibility relation $\text{ind}_K(A \otimes_k K) \mid \text{ind}_k(A)$ is immediate from the proposition. For the second one, use Proposition 4.5.4 to find a finite separable field extension $K'|K$ splitting $A \otimes_k K$ with $[K' : K] = \text{ind}_K(A \otimes_k K)$. Then K' is also a splitting field of A , so Proposition 4.5.8 shows $\text{ind}_k(A) \mid [K' : k] = \text{ind}_K(A \otimes_k K)[K : k]$. \square

Now we come to the second main invariant.

Definition 4.5.12 The *period* (or *exponent*) of a central simple k -algebra A is the order of its class in $\text{Br}(k)$. We denote it by $\text{per}(A)$.

The basic relations between the period and the index are the following.

Proposition 4.5.13 (Brauer) *Let A be a central simple k -algebra.*

1. *The period $\text{per}(A)$ divides the index $\text{ind}(A)$.*
2. *The period $\text{per}(A)$ and the index $\text{ind}(A)$ have the same prime factors.*

For the proof of the second statement we shall need the following lemma.

Lemma 4.5.14 *Let p be a prime number not dividing $\text{per}(A)$. Then A is split by a finite separable extension $K|k$ of degree prime to p .*

Proof: Let $L|k$ be a finite Galois extension that splits A , let P be a p -Sylow subgroup of $\text{Gal}(L|k)$ and K its fixed field. Then $\text{Br}(L|K) \cong H^2(P, L^\times)$ is a p -primary torsion group by Corollary 4.4.8, so the assumption implies that the image of $[A]$ by the restriction map $\text{Br}(L|k) \rightarrow \text{Br}(L|K)$ is trivial. This means that A is split by K . \square

Proof of Proposition 4.5.13: According to Proposition 4.5.4, the algebra A is split by a separable extension $K|k$ of degree $\text{ind}(A)$ over A . By Proposition 4.5.6, the class $[A]$ of A in $\text{Br}(k)$ is then annihilated by the restriction map $\text{Br}(k) \rightarrow \text{Br}(K)$. Composing with the corestriction $\text{Br}(k) \rightarrow \text{Br}(K)$ and using Proposition 4.2.10, we get that $[A]$ is annihilated by multiplication by $[K : k] = \text{ind}(A)$, whence the first statement. For the second statement, let p be a prime number that does not divide $\text{per}(A)$. By the lemma above, there exists a finite separable splitting field $K|k$ with $[K : k]$ prime to p . Hence by Proposition 4.5.8, the index $\text{ind}(A)$ is also prime to p . \square

Remark 4.5.15 It is an interesting and largely open question to determine the possible values of the integer $\text{ind}(A)/\text{per}(A)$ for central simple algebras over a given field k . For instance, it is conjectured by Michael Artin [1] that for C_2 -fields (see Remark 6.2.2 for this notion) one should always have $\text{per}(A) = \text{ind}(A)$. The conjecture is now known to hold for arithmetic fields (see Corollary 6.3.10 as well as Remarks 6.5.5 and 6.5.6), function fields of complex surfaces (de Jong [1]), and completions of the latter at smooth points (Colliot-Thélène/Ojanguren/Parimala [1]). Another interesting recent result on this topic is that of Saltman [4], who proves that for an algebra A over the function field of a curve over a p -adic field \mathbf{Q}_p the ratio $\text{ind}(A)/\text{per}(A)$ is always at most 2, provided that $\text{per}(A)$ is prime to p .

As an application of the above, we finally prove the following decomposition result.

Proposition 4.5.16 (Brauer) *Let D be a central division algebra over k . Consider the primary decomposition*

$$\text{ind}(D) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}.$$

Then we may find central division algebras D_i ($i = 1, \dots, r$) such that

$$D \cong D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$$

and $\text{ind}(D_i) = p_i^{m_i}$ for $i = 1, \dots, r$. Moreover, the D_i are uniquely determined up to isomorphism.

Proof: The Brauer group is torsion (Corollary 4.4.8), so it splits into p -primary components:

$$\mathrm{Br}(k) = \bigoplus_p \mathrm{Br}(k)\{p\}.$$

In this decomposition the class of D decomposes as a sum

$$[D] = [D_1] + [D_2] + \cdots + [D_r]$$

where the D_i are division algebras with $[D_i] \in \mathrm{Br}(k)\{p_i\}$ for some primes p_i . By Proposition 4.5.13 (2) the index of each D_i is a power of p_i . The tensor product $A = D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$ has degree $\prod_i \mathrm{ind}(D_i)$ over k and its index equals that of D by Remark 4.5.2 (2), so $\mathrm{ind} D$ divides $\prod_i \mathrm{ind}(D_i)$. A repeated application of Proposition 4.5.4 shows that for fixed i one may find a finite separable extension $K_i|k$ of degree prime to p_i that splits all the D_j for $j \neq i$. Then $D \otimes_k K_i$ and $D_i \otimes_k K_i$ have the same class in $\mathrm{Br}(K_i)$, and thus $\mathrm{ind}_{K_i}(D_i \otimes_k K_i) \mid \mathrm{ind}(D)$ by Corollary 4.5.11 (1). The algebras $D_i \otimes_k K_i$ are still division algebras of index $\mathrm{ind}(D_i)$ over K_i by Corollary 4.5.11 (2). To sum up, we have proven that $\mathrm{ind}(D_i)$ divides $\mathrm{ind}(D)$ for all i , so we conclude that $\mathrm{ind}(D) = \prod_i \mathrm{ind}(D_i)$. The k -algebras D and $D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$ thus have the same Brauer class and same dimension, hence they are isomorphic as claimed. The unicity of the D_i holds for the same reason. \square

4.6 The Galois Symbol

It is time to introduce one of the main protagonists of this book, the Galois symbol. To construct it, consider an integer $m > 0$ and a field k of characteristic prime to m . Recall that μ_m denotes the group of m -th roots of unity in a fixed separable closure k_s of k , equipped with its canonical action by $G = \mathrm{Gal}(k_s|k)$. Kummer theory (Proposition 4.3.6) then defines a map

$$\partial : k^\times \rightarrow H^1(k, \mu_m),$$

which is surjective with kernel $k^{\times m}$. On the other hand, for an integer $n > 0$ we may take n copies of $H^1(k, \mu_m)$ and consider the cup-product

$$H^1(k, \mu_m) \otimes \cdots \otimes H^1(k, \mu_m) \rightarrow H^n(k, \mu_m^{\otimes n}),$$

where according to the convention taken in Chapter 3 the G -module $\mu_m^{\otimes n}$ is the tensor product over \mathbf{Z} of n copies of μ_m , equipped with the Galois action defined by $\sigma(\omega_1 \otimes \cdots \otimes \omega_n) = \sigma(\omega_1) \otimes \cdots \otimes \sigma(\omega_n)$.

Putting the two together, we obtain a homomorphism from the n -fold tensor product

$$\partial^n : k^\times \otimes_{\mathbf{Z}} \cdots \otimes_{\mathbf{Z}} k^\times \rightarrow H^n(k, \mu_m^{\otimes n}).$$

We now have the following basic fact due to Tate.

Proposition 4.6.1 *Assume that $a_1, \dots, a_n \in k^\times$ is a sequence of elements such that $a_i + a_j = 1$ for some $1 \leq i < j \leq n$. Then*

$$\partial^i(a_1 \otimes \cdots \otimes a_n) = 0.$$

The proof uses some simple compatibility statements for the Kummer map.

Lemma 4.6.2 *Let $K|k$ be a finite separable field extension. Then the diagrams*

$$\begin{array}{ccc} k^\times & \xrightarrow{\partial_k} & H^1(k, \mu_m) \\ \downarrow & & \downarrow \text{Res} \\ K^\times & \xrightarrow{\partial_K} & H^1(K, \mu_m) \end{array} \quad \text{and} \quad \begin{array}{ccc} K^\times & \xrightarrow{\partial_K} & H^1(K, \mu_m) \\ \downarrow N_{K|k} & & \downarrow \text{Cor} \\ k^\times & \xrightarrow{\partial_k} & H^1(k, \mu_m) \end{array}$$

commute, where in the first diagram the left vertical map is the natural inclusion.

Proof: It follows from the construction of restriction and corestriction maps and Remark 3.1.10 (2) that they are compatible with the boundary maps on cohomology. It therefore remains to see that the maps $\text{Res} : H^0(k, k_s^\times) \rightarrow H^0(K, k_s^\times)$ and $\text{Cor} : H^0(K, k_s^\times) \rightarrow H^0(k, k_s^\times)$ are given by the inclusion $k^\times \rightarrow K^\times$ and the norm $N_{K|k} : K^\times \rightarrow k^\times$, respectively. The first of these statements is obvious, and the second comes from the fact that if we embed $K|k$ into a finite Galois extension $L|k$, the norm of an element $\alpha \in K^\times$ is given by the product $\prod \sigma_i(\alpha)$, where $1 = \sigma_1, \dots, \sigma_l$ is a system of left coset representatives of $\text{Gal}(L|k)$ modulo $\text{Gal}(L|K)$. \square

Proof of Proposition 4.6.1: By graded-commutativity and associativity of the cup-product we may assume $i = 1$ and $j = n = 2$, and use the notation $a_1 = a$, $a_2 = 1 - a$. Take an irreducible factorisation

$$x^m - a = \prod_l f_l$$

in the polynomial ring $k[x]$, for each l let α_l be a root of f_l in k_s and define $K_l = k(\alpha_l)$. We then have

$$1 - a = \prod_l f_l(1) = \prod_l N_{K_l|k}(1 - \alpha_l)$$

by definition of the field norm. Therefore, as ∂^2 is a group homomorphism,

$$\partial^2(a \otimes (1 - a)) = \sum_l \partial^2(a \otimes N_{K_l|k}(1 - \alpha_l)).$$

Here

$$\begin{aligned} \partial^2(a \otimes N_{K_l|k}(1 - \alpha_l)) &= \partial(a) \cup \partial(N_{K_l|k}(1 - \alpha_l)) = \\ &= \partial(a) \cup \text{Cor}_k^{K_l}(\partial(1 - \alpha_l)) = \text{Cor}_k^{K_l}(\text{Res}_k^{K_l}(\partial(a)) \cup \partial(1 - \alpha_l)), \end{aligned}$$

where we have used the definition of ∂^2 , the above lemma and the projection formula (Proposition 3.4.10 (3)), respectively. But (again using the lemma)

$$\text{Res}_k^{K_l}(\partial(a)) = \partial_{K_l}(a) = 0,$$

because by definition we have $a = \alpha_l^m$ in K_l , and so a lies in $K_l^{\times m}$, which is the kernel of ∂_{K_l} . This proves the proposition. \square

The proposition prompts the following definition.

Definition 4.6.3 Let k be a field. For $n > 1$ we define the n -th Milnor K -group $K_n^M(k)$ to be the quotient of the n -fold tensor product $k^\times \otimes_{\mathbf{Z}} \cdots \otimes_{\mathbf{Z}} k^\times$ by the subgroup generated by those elements $a_1 \otimes \cdots \otimes a_n$ with $a_i + a_j = 1$ for some $1 \leq i < j \leq n$. By convention, we put $K_0(k) := \mathbf{Z}$ and $K_1(k) := k^\times$.

For elements $a_1, \dots, a_n \in k^\times$, we denote the class of $a_1 \otimes \cdots \otimes a_n$ in $K_n^M(k)$ by $\{a_1, \dots, a_n\}$. We usually call these classes *symbols*.

By the proposition, the map ∂^n factors through $K_n^M(k)$ and yields a map

$$h_{k,m}^n : K_n^M(k) \rightarrow H^n(k, \mu_m^{\otimes n}),$$

which makes sense even for $n = 0$.

Definition 4.6.4 The above map $h_{k,m}^n$ is called the *Galois symbol*.

We now have the following basic conjecture.

Conjecture 4.6.5 (Bloch-Kato) *The Galois symbol yields an isomorphism*

$$K_n^M(k)/m \xrightarrow{\sim} H^n(k, \mu_m^{\otimes n})$$

for all $n \geq 0$, all fields k and all m prime to the characteristic of k .

The case when m is a power of 2 is usually known as *Milnor's Conjecture*; the attribution of the general case to Bloch and Kato is not sure but generally accepted.

The current status of the conjecture is as follows. For $n = 0$ the statement is trivial, and for $n = 1$ it is none but Kummer theory (Proposition 4.3.6).

The case $n = 2$ is what will occupy us in Chapter 8 of this book.

Theorem 4.6.6 (Merkurjev-Suslin) *The Bloch-Kato conjecture is true for $n = 2$ and all m invertible in k .*

We shall explain in the next section the relation of this statement to the one given in Chapter 2, Section 2.5.

Returning to the general Bloch-Kato conjecture, the case when m is a power of 2 and n is arbitrary was proven by Voevodsky [1]. A proof in the general case has been announced by Rost and Voevodsky, but at the time of writing only parts of this work are available to the mathematical community.

4.7 Cyclic Algebras and Symbols

Continuing the discussion of the previous section, let us now focus on the case $n = 2$. Assume first that k has characteristic prime to m and contains a primitive m -th root of unity ω . The symbol h_k^2 then has as target $H^2(k, \mu_m^{\otimes 2})$, but choosing an isomorphism $\mu_m \cong \mathbf{Z}/m\mathbf{Z}$ by sending ω to 1 we get isomorphisms

$$H^2(k, \mu_m^{\otimes 2}) \cong H^2(k, \mathbf{Z}/m\mathbf{Z}) \cong H^2(k, \mu_m) \cong {}_m\text{Br}(k),$$

the last one by Corollary 4.4.9. We emphasize that this chain of isomorphisms depends on the choice of ω . We then have:

Proposition 4.7.1 *Let $a, b \in k^\times$. Then under the above isomorphisms the element $h_k^2(\{a, b\}) \in H^2(k, \mu_m^{\otimes 2})$ goes to the Brauer class of the cyclic algebra $(a, b)_\omega$ defined in Chapter 2, Section 2.5.*

Remarks 4.7.2

1. The statement makes sense because we have seen in Chapter 2, Section 2.5 that the algebra $(a, b)_\omega$ is split by an extension of degree m , therefore it has period dividing m .
2. The proposition implies that the form of the Merkurjev-Suslin theorem stated in Theorem 2.5.7 is equivalent to the surjectivity of h_k^2 under the assumption $\omega \in k$. Henceforth, by 'Merkurjev-Suslin theorem' we shall mean this most general form, i.e. Theorem 4.6.6.

Before embarking on the proof, recall from the construction of the Kummer map $\partial : k^\times \rightarrow H^1(k, \mu_m)$ that under the identification

$$H^1(k, \mu_m) \cong H^1(k, \mathbf{Z}/m\mathbf{Z}) = \text{Hom}(\text{Gal}(k_s|k), \mathbf{Z}/m\mathbf{Z})$$

induced by sending ω to 1 the element $\partial(a)$ is mapped to the character sending the automorphism $\sigma : \sqrt[m]{a} \mapsto \omega \sqrt[m]{a}$ to 1, where $\sqrt[m]{a}$ is an m -th root of a in k_s . The kernel of this character fixes the cyclic Galois extension $K = k(\sqrt[m]{a})$ of k , whence an isomorphism $\chi : \text{Gal}(K|k) \rightarrow \mathbf{Z}/m\mathbf{Z}$. In Corollary 2.5.5 we have shown that $(a, b)_\omega$ is isomorphic to the more general cyclic algebra (χ, b) introduced in Construction 2.5.1 of *loc. cit.*, the isomorphism depending, as always, on the choice of ω .

We shall derive Proposition 4.7.1 from the following more general one which is valid without assuming m prime to the characteristic of k .

Proposition 4.7.3 *Let k be a field and $m > 0$ an integer. Assume given a degree m cyclic Galois extension $K|k$ with group G , and let $\chi : G \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z}$ be an isomorphism. Take a lifting $\tilde{\chi}$ of χ to a character $\text{Gal}(k_s|k) \rightarrow \mathbf{Z}/m\mathbf{Z}$, and fix an element $b \in k^\times$. Denoting by δ the coboundary map $H^1(k, \mathbf{Z}/m\mathbf{Z}) \rightarrow H^2(k, \mathbf{Z})$ coming from the exact sequence $0 \rightarrow \mathbf{Z} \xrightarrow{m} \mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \rightarrow 0$, the cup-product map*

$$H^2(k, \mathbf{Z}) \times H^0(k, k_s^\times) \rightarrow H^2(k, k_s^\times) \cong \text{Br}(k).$$

sends the element $\delta(\tilde{\chi}) \cup b$ to the Brauer class of the cyclic algebra (χ, b) .

Proof: Recall from Chapter 2, Section 2.5 that we have constructed the algebra (χ, b) via Galois descent, by twisting the standard Galois action on the matrix algebra $M_m(k)$ by the 1-cocycle $z(b) : G \rightarrow \text{PGL}_m(K)$ given by applying first χ and then sending 1 to the class $F(b)$ of the invertible matrix

$$\tilde{F}(b) = \begin{bmatrix} 0 & 0 & \cdots & 0 & b \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

in $\text{PGL}_m(K)$. Recall also that $\tilde{F}(b)^m = b \cdot I_m$.

Consider now the commutative diagram of G -groups

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathbf{Z} & \xrightarrow{m} & \mathbf{Z} & \longrightarrow & \mathbf{Z}/m\mathbf{Z} \longrightarrow 1 \\ & & b \downarrow & & \tilde{F}(b) \downarrow & & F(b) \downarrow \\ 1 & \longrightarrow & K^\times & \longrightarrow & \text{GL}_m(K) & \longrightarrow & \text{PGL}_m(K) \longrightarrow 1, \end{array}$$

where the maps denoted by $b, F(b), \tilde{F}(b)$ mean the map induced by sending 1 to the corresponding element. The commutativity of the left square follows from the equality $\tilde{F}(b)^m = b \cdot I_m$, and that of the right one is straightforward. Taking cohomology we obtain the commutative diagram

$$\begin{array}{ccc} H^1(G, \mathbf{Z}/m\mathbf{Z}) & \xrightarrow{\delta} & H^2(G, \mathbf{Z}) \\ (F(b))_* \downarrow & & b_* \downarrow \\ H^1(G, \mathrm{PGL}_m(K)) & \xrightarrow{\delta_m} & H^2(G, K^\times), \end{array}$$

where the horizontal arrows are boundary maps. The character χ is naturally an element of $\mathrm{Hom}(G, \mathbf{Z}/m\mathbf{Z}) = H^1(G, \mathbf{Z}/m\mathbf{Z})$ and, as explained above, it is mapped by $F(b)_*$ to the class of the 1-cocycle $z(b)$. By definition, we have therefore $\delta_m((F(b))_*\chi) = [(\chi, b)]$, so by commutativity of the diagram $[(\chi, b)] = b_*(\delta(\chi))$. But one checks from the definition of cup-products that the map b_* is given by cup-product with the class of b in $H^0(G, K^\times)$, so we get $[(\chi, b)] = \delta(\chi) \cup b$. Moreover, we defined the character $\tilde{\chi}$ as the image of χ by the inflation map $H^1(G, \mathbf{Z}/m\mathbf{Z}) \rightarrow H^1(k, \mathbf{Z}/m\mathbf{Z})$, and the inflation map $H^0(G, K^\times) \rightarrow H^0(k, k_s^\times)$ is obviously the identity. We finally get $[(\chi, b)] = \delta(\tilde{\chi}) \cup b$ by compatibility of the cup-product with inflations. \square

Before moving on to the proof of Proposition 4.7.1, we note some interesting consequences.

Corollary 4.7.4 *For $K|k$, G and χ as above, the isomorphism*

$$H^2(G, K^\times) \cong k^\times / N_{K|k}(K^\times) \quad (6)$$

of Corollary 4.4.10 is induced by the map $k^\times \rightarrow H^2(G, K^\times)$ sending an element $b \in k^\times$ to the class of the cyclic algebra (χ, b) .

Proof: By Proposition 3.4.11, the isomorphism (6) is induced (from right to left) by cup-product with $\delta(\chi)$, as it is a generator of the group $H^2(G, \mathbf{Z}) \cong \mathbf{Z}/m\mathbf{Z}$. On the other hand, the previous proposition implies that $\delta(\chi) \cup b$ is exactly the class of (χ, b) in $\mathrm{Br}(K|k) \cong H^2(G, K^\times)$. \square

This immediately yields the following criterion for the splitting of cyclic algebras, which will be used many times in the sequel.

Corollary 4.7.5 *The class of the cyclic algebra (χ, b) in $\mathrm{Br}(K|k)$ is trivial if and only if b is a norm from the extension $K|k$.*

Another consequence is the following characterisation of cyclic algebras.

Corollary 4.7.6 *Let $K|k$, m and G be as above, and let A be a central simple k -algebra split by K .*

1. *There exist an isomorphism $\chi : G \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z}$ and an element $b \in k$ such that the cyclic algebra (χ, b) is Brauer equivalent to A .*
2. *If moreover A has degree m , then we have actually $(\chi, b) \cong A$.*

Proof: The first statement is an immediate consequence of Corollary 4.7.4. The second follows from the first, since we are then dealing with Brauer equivalent algebras of the same degree. \square

We now finally prove Proposition 4.7.1.

Proof of Proposition 4.7.1: In view of Proposition 4.7.3 and the discussion preceding it, all that remains to be seen is the equality

$$\delta(\tilde{\chi}) \cup b = \tilde{\chi} \cup \partial(b),$$

where $\delta(\tilde{\chi}) \cup b \in H^2(k, k_s^\times)$ is the element considered in Proposition 4.7.3, the map $\partial : k^\times \rightarrow H^1(k, \mu_m)$ is the Kummer coboundary and the cup-product on the left is that between $H^1(k, \mathbf{Z}/m\mathbf{Z})$ and $H^1(k, \mu_m)$. This follows from (the profinite version of) of Proposition 3.4.9, with the exact sequences

$$0 \rightarrow \mathbf{Z} \xrightarrow{m} \mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \rightarrow 0, \quad 1 \rightarrow \mu_m \rightarrow k_s^\times \rightarrow k_s^\times \rightarrow 1,$$

the pairing $\mathbf{Z} \times k_s^\times \rightarrow k_s^\times$ (which is trivial on $m\mathbf{Z} \times \mu_m$), and the elements $\tilde{\chi} \in H^1(k, \mathbf{Z})$ and $b \in H^0(k, k_s^\times)$. \square

Putting together Proposition 4.7.1 and Corollary 4.7.5 we get:

Corollary 4.7.7 *Assume k contains a primitive m -th root of unity ω , and let $a, b \in k^\times$. Then the following statements are equivalent.*

1. *The symbol $h_k^2(\{a, b\})$ is trivial.*
2. *The cyclic algebra $(a, b)_\omega$ is split.*
3. *The element b is a norm from the extension $k(\sqrt[m]{a})|k$.*

Note that the equivalence (2) \Leftrightarrow (3) generalises the equivalence (1) \Leftrightarrow (4) in Proposition 1.1.7.

Remark 4.7.8 Since the first two conditions of the corollary are symmetric in a and b , we get that b is a norm from the extension $k(\sqrt[m]{a})|k$ if and only if a is a norm from the extension $k(\sqrt[m]{b})|k$. This type of statement is usually called a *reciprocity law* in arithmetic.

EXERCISES

1. Show that in the correspondence of Theorem 4.1.10 Galois extensions $L|k$ contained in K correspond to closed normal subgroups of $\text{Gal}(K|k)$.
2. (Continuous cochains) Let G be a profinite group and A a continuous G -module. Define the group $C_{\text{cont}}^i(G, A)$ of *continuous i -cochains* as the subgroup of those maps in $\text{Hom}_G(\mathbf{Z}[G^{i+1}], A)$ whose restriction to G^{i+1} is continuous when G^{i+1} is equipped with the product topology. Show that the boundary maps δ^{i*} of the complex $C^\bullet(G, A)$ introduced in Construction 3.2.1 map $C_{\text{cont}}^i(G, A)$ into $C_{\text{cont}}^{i+1}(G, A)$, and that the cohomology groups of the arising complex $C_{\text{cont}}^\bullet(G, A)$ are isomorphic to the continuous cohomology groups $H_{\text{cont}}^i(G, A)$.
3. Let $m > 0$ be an integer, and k a field containing a primitive m -th root of unity ω . Consider a degree m cyclic extension $K = k(\sqrt[m]{a})|k$ with Galois group G .

- (a) Show that the group $(K^\times/K^{\times m})^G$ is generated by k^\times and $\sqrt[m]{a}$. [*Hint*: Use Proposition 3.3.14].
- (b) Determine explicitly the cokernel of the map

$$k^\times/k^{\times m} \rightarrow (K^\times/K^{\times m})^G.$$

4. Give a new proof of Lemma 2.7.4 based on the injectivity of the group homomorphism $\delta_\infty : H^1(G, \text{PGL}_\infty) \rightarrow H^2(G, K^\times)$.
5. (Theorem of Frobenius) Prove that $\text{Br}(\mathbf{R}) \cong \mathbf{Z}/2\mathbf{Z}$, the nontrivial class being that of the Hamilton quaternions.
6. Let k be a field of characteristic 0 such that $\text{Gal}(\bar{k}|k) \cong \mathbf{Z}/p\mathbf{Z}$ for some prime number p .
 - (a) Show that $\text{Br}(k) \cong \text{Br}(k)/p \text{Br}(k) \cong k^\times/k^{\times p}$. [*Hint*: Use the Kummer sequence and the periodicity of the cohomology of cyclic groups.]
 - (b) By computing $\text{Br}(k)$ in a different way, show that $N_{\bar{k}|k}(\bar{k}^\times) = k^{\times p}$.
 - (c) Conclude that the above is only possible for $p = 2$ and $\bar{k} = k(\sqrt{-1})$.
 - (d) Show that moreover in the above case k may be equipped with an ordered field structure. [*Hint*: Declare the squares to be the positive elements.]
7. Using the previous exercise, prove the following theorem of E. Artin and O. Schreier: If k is a field of characteristic 0 whose absolute Galois group is a nontrivial finite group, then $\bar{k} = k(\sqrt{-1})$ and k has an ordered field

structure. [*Hint*: Begin by taking a p -Sylow subgroup in the Galois group and recall that p -groups are solvable.]

[*Remark*: In fact, Artin and Schreier also showed that in positive characteristic the absolute Galois group is either trivial or infinite.]

8. Let k be a field of characteristic 0, and A a central simple algebra over k of degree n . Denote by $[A]$ the class of A in $H^2(k, \mu_n) \cong {}_n\text{Br}(k)$, and consider the map $H^1(k, \mu_n) \rightarrow H^3(k, \mu_n^{\otimes 2})$ given by cup-product with $[A]$.
- (a) If $x \in \text{Nrd}(A^\times)$, show that $\delta(x) \cup [A] = 0$ in $H^3(k, \mu_n^{\otimes 2})$, where δ is the Kummer coboundary map. [*Hint*: Use Exercise 10 of Chapter 2.]
- (b) Give an example of k , A and $x \in k^\times$ such that $\delta(x) \cup [A] \neq 0$.
9. (Wang's theorem in the general case) Let D be a central division algebra over k .

- (a) Consider the primary decomposition

$$D \cong D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$$

of Proposition 4.5.16. Show that

$$SK_1(D) \cong \bigoplus_{i=1}^r SK_1(D_i).$$

- (b) Assume that $\text{ind}(D)$ is squarefree, i.e. a product of distinct primes. Show that $SK_1(D) = 0$. [*Hint*: Reduce to Theorem 2.8.12.]
10. (a) Verify the relations $(\chi, b_1) \otimes (\chi, b_2) \cong (\chi, b_1 b_2)$ and $(\chi, b)^{\text{op}} \cong (\chi, b^{-1})$ for cyclic algebras.
- (b) Deduce that the cyclic algebras (χ, b_1) and (χ, b_2) are isomorphic if and only if $b_1 b_2^{-1}$ is a norm from the cyclic extension of the base field determined by χ .
11. Let n be a positive integer, and let k be a field containing a primitive n -th root of unity ω . Consider a purely transcendental extension $k(x, y)$ of dimension 2. Given integers i, j prime to n , show that the cyclic $k(x, y)$ -algebras $(x, y)_{\omega^i}$ and $(x, y)_{\omega^j}$ are isomorphic if and only if $i - j$ is divisible by n .

Chapter 5

Severi-Brauer varieties

In Chapter 1 we associated with each quaternion algebra a conic with the property that the conic has a k -point if and only if the algebra splits over k . We now generalise this correspondence to arbitrary dimension: with each central simple algebra A of degree n over an arbitrary field k we associate a projective k -variety X of dimension $n - 1$ which has a k -point if and only if A splits. Both objects will correspond to a class in $H^1(G, \mathrm{PGL}_n(K))$, where K is a Galois splitting field for A with group G . The varieties X arising in this way are called Severi-Brauer varieties; they are characterised by the property that they become isomorphic to some projective space over the algebraic closure. This interpretation will enable us to give another, geometric construction of the Brauer group. Another central result of this chapter is a theorem of Amitsur which states that for a Severi-Brauer variety X with function field X the kernel of the natural map $\mathrm{Br}(k) \rightarrow \mathrm{Br}(k(X))$ is a cyclic group generated by the class of X . This seemingly technical statement (which generalises Witt's theorem proven in Chapter 1) has very fruitful algebraic applications. At the end of the chapter we shall present one such application, due to Saltman, which shows that all central simple algebras of fixed degree n over a field k containing the n -th roots of unity can be made cyclic via base change to some large field extension of k .

Severi-Brauer varieties were introduced in the pioneering paper of Châtelet [1], under the name 'variétés de Brauer'. Practically all results in the first half of the present chapter stem from this work. The term 'Severi-Brauer variety' was coined by Beniamino Segre in his note [1], who expressed his discontent that Châtelet had ignored previous work by Severi in the area. Indeed, in the paper of Severi [1] Severi-Brauer varieties are studied in a classical geometric context, and what is known today as Châtelet's theorem is proven in some cases. As an amusing feature, we may mention that Severi calls the varieties in question 'varietà di Segre', but beware, this does not refer to Beniamino but to his second uncle Corrado Segre. The groundbreak-

ing paper by Amitsur [1] was the first to emphasize the importance of the birational viewpoint on Severi-Brauer varieties in the study of central simple algebras. This observation was a milestone on the road leading to the proof of the Merkurjev-Suslin theorem.

5.1 Basic Properties

In Chapter 2 we have seen that as a consequence of Wedderburn's theorem one may define a central simple algebra over a field k as a finite dimensional k -algebra that becomes isomorphic to some full matrix algebra $M_n(K)$ over a finite extension $K|k$ of the base field. As a consequence of descent theory, we have seen that when $K|k$ is Galois, the central simple k -algebras split by K can be described by means of the automorphism group $\mathrm{PGL}_n(K)$ of $M_n(K)$. But $\mathrm{PGL}_n(K)$ is also the automorphism group of projective $(n - 1)$ -space \mathbf{P}_K^{n-1} (considered as an algebraic variety), which motivates the following definition.

Definition 5.1.1 A Severi-Brauer variety over a field k is a projective algebraic variety X over k such that the base extension $X_K := X \times_k K$ becomes isomorphic to \mathbf{P}_K^{n-1} for some finite field extension $K|k$. The field K is called a *splitting field* for X .

Remarks 5.1.2

1. A k -variety X is a Severi-Brauer variety if and only if $X_{\bar{k}} \cong \mathbf{P}_{\bar{k}}^{n-1}$ for an algebraic closure \bar{k} of k . Indeed, necessity is obvious and sufficiency follows from the fact that the coefficients of the finitely many polynomials defining an isomorphism $X_{\bar{k}} \cong \mathbf{P}_{\bar{k}}^{n-1}$ are all contained in a finite extension of k .
2. It follows from general considerations in algebraic geometry that a Severi-Brauer variety is necessarily smooth. Also, the assumption that X be projective is also superfluous: it can be shown that an algebraic variety (i.e. separated scheme of finite type) over k that becomes isomorphic to a projective variety over a finite extension of k is itself projective.

As examples of Severi-Brauer varieties we may cite the projective plane conics encountered in Chapter 1. The next section will describe a general method for constructing examples.

We now come to the fundamental result about Severi-Brauer varieties. Before stating it, let us introduce some (non-standard) terminology: we say

that a closed subvariety $Y \rightarrow X$ defined over k is a *twisted-linear* subvariety of X if Y is a Severi-Brauer variety and moreover over \bar{k} the inclusion $Y_{\bar{k}} \subset X_{\bar{k}}$ becomes isomorphic to the inclusion of a linear subvariety of $\mathbf{P}_{\bar{k}}^{n-1}$.

Theorem 5.1.3 (Châtelet) *Let X be a Severi-Brauer variety of dimension $n - 1$ over the field k . The following are equivalent:*

1. X is isomorphic to projective space \mathbf{P}_k^{n-1} over k .
2. X is birationally isomorphic to projective space \mathbf{P}_k^{n-1} over k .
3. X has a k -rational point.
4. X contains a twisted-linear subvariety D of codimension 1.

It is usually the equivalence of statements (1) and (3) that is referred to as Châtelet's theorem. The only implication which is not straightforward to establish is (3) \Rightarrow (4); we owe the beautiful proof given below to Endre Szabó. This proof uses some elementary notions from algebraic geometry; however, for the less geometrically minded, we note that in Section 5.3 another proof will be given, under the assumption that X has a Galois splitting field. We shall see in Corollary 5.1.5 below that this condition is always satisfied.

Proof: The implication (1) \Rightarrow (2) is obvious. If (2) holds, then X and \mathbf{P}_k^{n-1} have k -isomorphic Zariski open subsets, but a Zariski open subset of \mathbf{P}_k^{n-1} contains a k -rational point, whence (3). Next we prove (4) \Rightarrow (1). The subvariety D whose existence is postulated by (4) is a divisor, so we may consider the associated complete linear system $|D|$ (see the Appendix) which defines a rational map ϕ_D into some projective space. Over \bar{k} the divisor D becomes a hyperplane by assumption, so the rational map it defines is in fact an isomorphism with projective $(n - 1)$ -space $\mathbf{P}_{\bar{k}}^{n-1}$. Hence the target of ϕ_D must be \mathbf{P}_k^{n-1} and it must be an everywhere defined isomorphism.

It remains to prove the implication (3) \Rightarrow (4). Let P be a k -rational point and denote by $\pi : Y \rightarrow X$ the blow-up of X at P (see Appendix, Example A.2.3). As X (and in particular P) is smooth, the exceptional divisor E is isomorphic to \mathbf{P}_k^{n-2} . Pick a hyperplane $L \subset E$. Over the algebraic closure \bar{k} our $Y_{\bar{k}}$ is isomorphic to the blow-up of $\mathbf{P}_{\bar{k}}^{n-1}$ in P , hence it is a subvariety of $\mathbf{P}_{\bar{k}}^{n-1} \times \mathbf{P}_{\bar{k}}^{n-2}$. The second projection induces a morphism $\psi_{\bar{k}} : Y_{\bar{k}} \rightarrow \mathbf{P}_{\bar{k}}^{n-2}$, mapping $E_{\bar{k}}$ isomorphically onto $\mathbf{P}_{\bar{k}}^{n-2}$. As the fibres of $\psi_{\bar{k}}$ are projective lines and $\pi_{\bar{k}}$ is an isomorphism outside P , we see that the subvariety $D_{\bar{k}} := \pi_{\bar{k}}(\psi_{\bar{k}}^{-1}(\psi_{\bar{k}}(L_{\bar{k}}))) \subset X_{\bar{k}}$ is a hyperplane in $\mathbf{P}_{\bar{k}}^{n-1}$. We want

to define this structure over k , i.e. we are looking for a morphism $\psi : Y \rightarrow Z$ defined over k which becomes $\psi_{\bar{k}}$ after base extension to \bar{k} .

Let $A \subset X$ be an ample divisor, and let d denote the degree of $A_{\bar{k}}$ in the projective space $X_{\bar{k}} \cong \mathbf{P}_{\bar{k}}^{n-1}$. The divisor $(\pi^*A - dE)_{\bar{k}}$ has degree 0 on the fibres of $\psi_{\bar{k}}$ and has degree d on $E_{\bar{k}}$. Hence the morphism $Y_{\bar{k}} \rightarrow \mathbf{P}_{\bar{k}}^N$ associated with the corresponding linear system factors as the composite

$$Y_{\bar{k}} \xrightarrow{\psi_{\bar{k}}} Z_{\bar{k}} \xrightarrow{\phi_d} \mathbf{P}_{\bar{k}}^N,$$

where ϕ_d is the d -uple embedding. The linear system $|\pi^*A - dE|$ defines (over k) a rational map $\psi : Y \rightarrow \mathbf{P}_k^N$. By construction this ψ becomes the above $\psi_{\bar{k}}$ after base extension to \bar{k} , hence it is actually an everywhere defined morphism $Y \rightarrow Z$, where $Z := \psi(Y)$. Then the subvariety $D := \pi(\psi^{-1}(\psi(L))) \subset X$ is defined over k , and becomes $D_{\bar{k}}$ after extension to \bar{k} . This is the D we were looking for. \square

Corollary 5.1.4 *A Severi-Brauer variety X always splits over a finite separable extension of the base field k .*

Proof: By a now familiar argument, it is enough to show that X becomes isomorphic to projective space over a separable closure k_s of k . This follows from the theorem, for X_{k_s} always has a rational point over k_s (see Appendix, Proposition A.1.1). \square

By embedding a separable splitting field into its Galois closure, we get:

Corollary 5.1.5 *A Severi-Brauer variety X always splits over a finite Galois extension of the base field k .*

5.2 Classification by Galois cohomology

Let X be a Severi-Brauer variety of dimension $n - 1$ over a field k , and let $K|k$ be a finite Galois extension with group G which is a splitting field of X . We now associate with X a 1-cohomology class of G with values in $\mathrm{PGL}_n(K)$ by a construction analogous to that in the theory of central simple algebras.

First some conventions. Given quasi-projective varieties Y, Z over k , denote by Y_K, Z_K the varieties obtained by base extension to K , and make G act on the set of morphisms $Y_K \rightarrow Z_K$ by $\phi \mapsto \sigma(\phi) := \phi \circ \sigma^{-1}$. In particular, for $Y = Z$ we obtain a left action of G on the K -automorphism group $\mathrm{Aut}_K(Y)$.

Given a K -isomorphism $\phi : \mathbf{P}_K^{n-1} \xrightarrow{\sim} X_K$, define for each element $\sigma \in G$ a K -automorphism $a_\sigma \in \text{Aut}_K(\mathbf{P}_K^{n-1})$ by

$$a_\sigma := \phi^{-1} \circ \sigma(\phi).$$

Exactly the same computations as in Chapter 2, Section 2.3 show that the map $\sigma \mapsto a_\sigma$ is a 1-cocycle of G with values in $\text{Aut}_K(\mathbf{P}_K^{n-1})$, and that changing ϕ amounts to changing a_σ by a 1-coboundary. Therefore we have assigned to X a class $[a_\sigma]$ in $H^1(G, \text{Aut}_K(\mathbf{P}_K^{n-1}))$. Fixing an isomorphism $\text{Aut}_K(\mathbf{P}_K^{n-1}) \cong \text{PGL}_n(K)$ (see Appendix, Example A.2.2), we may consider it as a class in $H^1(G, \text{PGL}_n(K))$. Using the boundary map $H^1(G, \text{PGL}_n(K)) \rightarrow \text{Br}(K|k)$ we can also assign to X a class $[X]$ in $\text{Br}(K|k)$.

Denote by $SB_n(k)$ the pointed set of isomorphism classes of Severi-Brauer varieties of dimension $n - 1$ over k , the base point being the class of \mathbf{P}_k^{n-1} .

Theorem 5.2.1 *The map $SB_n(k) \rightarrow H^1(k, \text{PGL}_n)$ given by $X \mapsto [a_\sigma]$ is a base point preserving bijection.*

Combining the theorem with Theorem 2.4.3 we thus get a base point preserving bijection

$$CSA_n(k) \leftrightarrow SB_n(k).$$

Given a central simple k -algebra A of degree n , we shall call (somewhat abusively) a Severi-Brauer variety X whose isomorphism class corresponds to that of A by the bijection above a *Severi-Brauer variety associated with A* .

We now prove Theorem 5.2.1 using a construction due to Kang [1]. The proof will at the same time yield the following important property.

Theorem 5.2.2 *Let X be a Severi-Brauer variety of dimension $n - 1$ over k , and let d be the period of X , i.e. the order of $[X]$ in the Brauer group $\text{Br}(K|k)$. Then there exists a projective embedding*

$$\rho : X \hookrightarrow \mathbf{P}_k^{N-1}, \quad N = \binom{n+d-1}{d}$$

such that $\rho_K : X_K \hookrightarrow \mathbf{P}_K^{N-1}$ is isomorphic to the d -uple embedding ϕ_d .

Proof of Theorems 5.2.1 and 5.2.2 : We begin by proving the injectivity of the map $SB_n(k) \rightarrow H^1(k, \text{PGL}_n)$. Let X and Y be Severi-Brauer varieties split by K and having the same class in $H^1(G, \text{PGL}_n)$. Take trivialisation isomorphisms $\phi : \mathbf{P}_K^{n-1} \xrightarrow{\sim} X_K$ and $\psi : \mathbf{P}_K^{n-1} \xrightarrow{\sim} Y_K$. Our assumption that the

cocycles $\phi^{-1} \circ \sigma(\phi)$ and $\psi^{-1} \circ \sigma(\psi)$ have the same class in $H^1(G, \mathrm{PGL}_n(K))$ means that there exists $h \in \mathrm{PGL}_n(K)$ such that

$$\phi^{-1} \circ \sigma(\phi) = h^{-1} \circ \psi^{-1} \circ \sigma(\psi) \circ \sigma(h)$$

for all $\sigma \in G$. We then have

$$\psi \circ h \circ \phi^{-1} = \sigma(\psi \circ h \circ \phi^{-1}) \in \mathrm{Hom}_K(X_K, Y_K),$$

so the K -isomorphism $\psi \circ h \circ \phi^{-1} : X_K \rightarrow Y_K$ is G -equivariant. It follows that $\psi \circ h \circ \phi^{-1}$ is defined over k , and hence yields a k -isomorphism between X and Y .

Let now $\alpha = [a_\sigma]$ be a class in $H^1(G, \mathrm{PGL}_n(K))$. We show that α can be realised as the cohomology class of a Severi-Brauer variety of dimension $n - 1$ which becomes isomorphic over K to $\phi_d(\mathbf{P}_K^{n-1})$. This will prove the surjectivity statement in Theorem 5.2.1 and at the same time Theorem 5.2.2.

Consider the boundary map $\delta : H^1(G, \mathrm{PGL}_n(K)) \rightarrow H^2(G, K^\times)$. By definition, a 2-cocycle representing $\delta(\alpha)$ is obtained by lifting the elements $a_\sigma \in \mathrm{PGL}_n(K)$ to elements $\tilde{a}_\sigma \in \mathrm{GL}_n(K)$ and setting

$$b_{\sigma,\tau} = \tilde{a}_\sigma \sigma(\tilde{a}_\tau) \tilde{a}_{\sigma\tau}^{-1}. \quad (1)$$

Let d be the order of $\delta(\alpha)$ in $\mathrm{Br}(K|k)$ (which is a torsion group by Corollary 4.4.8). In terms of the cocycle $b_{\sigma,\tau}$ this means that $(b_{\sigma,\tau})^d$ is a 2-coboundary, i.e. there is a 1-cochain $\sigma \mapsto c_\sigma$ with values in K^\times such that

$$(b_{\sigma,\tau})^d = c_\sigma \sigma(c_\tau) c_{\sigma\tau}^{-1}. \quad (2)$$

Now consider the natural left action of the group $\mathrm{GL}_n(K)$ on $V := K^n$ which is compatible with that of G in the sense of Construction 2.3.6. This action extends to the tensor powers $V_i := V^{\otimes i}$ by setting

$$\tilde{a}(v_1 \otimes \cdots \otimes v_i) = \tilde{a}(v_1) \otimes \cdots \otimes \tilde{a}(v_i).$$

Note that V_i is none but the space of homogeneous polynomials of degree i over K . We extend the action of G to the V_i in a similar way. Now consider the case $i = d$, and for each $\sigma \in G$ define an element $\nu_\sigma \in \mathrm{Aut}_K(V_d)$ by

$$\nu_\sigma := c_\sigma^{-1} \tilde{a}_\sigma,$$

where c_σ^{-1} acts as constant multiplication and \tilde{a}_σ via the action of $\mathrm{GL}_n(K)$ on V_d described above. We contend that the map $\sigma \rightarrow \nu_\sigma$ is a 1-cocycle. Indeed, for $\sigma, \tau \in G$, we compute using (1)

$$\nu_{\sigma\tau} = c_{\sigma\tau}^{-1} \tilde{a}_{\sigma\tau} = c_{\sigma\tau}^{-1} (b_{\sigma,\tau}^{-1} \tilde{a}_\sigma \sigma(\tilde{a}_\tau)) = (c_{\sigma\tau}^{-1} b_{\sigma,\tau}^{-d}) (\tilde{a}_\sigma \sigma(\tilde{a}_\tau)),$$

where in the second step we considered $b_{\sigma\tau}$ as a scalar matrix in $\mathrm{GL}_n(K)$ and in the third just as a scalar. Hence using (2) we get

$$\nu_{\sigma\tau} = c_{\sigma\tau}^{-1}(c_{\sigma\tau}\sigma(c_\tau)^{-1}c_\sigma^{-1})(\tilde{a}_\sigma\sigma(\tilde{a}_\tau)) = (c_\sigma\sigma(c_\tau))^{-1}\tilde{a}_\sigma\sigma(\tilde{a}_\tau) = \nu_\sigma\sigma(\nu_\tau),$$

so that we have indeed defined a 1-cocycle.

Now equip V_d with the twisted G -action defined by ν_σ (see Construction 2.3.6 for the definition). Let $W := ({}_\nu V_d)^G$ be the invariant subspace under this twisted action. By Speiser's lemma (Lemma 2.3.8), this is a k -vector space such that $W \otimes_k K \cong V_d$. Let $k[X]$ be the graded k -subalgebra of $K[x_0, \dots, x_{n-1}] \cong \bigoplus_i V_i$ generated by W . Choosing a k -basis v_0, \dots, v_{N-1} of W we get a natural surjection of graded k -algebras $k[x_0, \dots, x_{N-1}] \rightarrow k[X]$ induced by sending x_i to v_i . The kernel of this surjection is a homogeneous ideal in $k[x_1, \dots, x_{N-1}]$ defining a closed subset $X \subset \mathbf{P}_k^{N-1}$. Moreover, the isomorphism $W \otimes_k K \cong V_d$ implies that $k[X] \otimes_k K$ becomes isomorphic to the graded K -subalgebra of $K[x_1, \dots, x_{n-1}]$ generated by V_d . But this is none but the homogeneous coordinate ring of $\phi_d(\mathbf{P}_K^{n-1})$ (see Appendix, Example A.2.1), hence $X \otimes_k K \cong \phi_d(\mathbf{P}_K^{n-1})$. This shows that X is a Severi-Brauer variety, and at the same time that Theorem 5.2.2 holds. By construction the class in $H^1(G, \mathrm{PGL}_n(K))$ associated with X is indeed α . \square

Remark 5.2.3 It should be noted that the embedding $X \hookrightarrow \mathbf{P}_k^{N-1}$ constructed in the above proof is not canonical, but depends on the choice of the cocycle $\sigma \mapsto c_\sigma$.

Example 5.2.4 Theorem 5.2.1 shows that the 1-dimensional Severi-Brauer varieties are exactly the smooth projective conics. Indeed, such a variety X defines a class in $H^1(k, \mathrm{PGL}_2)$ which also corresponds to a central simple algebra of degree 2 by Theorem 2.4.3. By the results of Chapter 1, this must be a quaternion algebra (a, b) , whose class has always order 2 in the Brauer group. By Theorem 5.2.2, we can embed X as a smooth subvariety in \mathbf{P}_k^2 which is isomorphic to the conic $x_1^2 = x_0x_2$ over the algebraic closure. It is a well-known fact from algebraic geometry that then X itself is a conic. In Section 5.4 we shall prove that X is in fact the conic $C(a, b)$ associated with the quaternion algebra (a, b) in Chapter 1.

Remark 5.2.5 In the literature one finds other approaches to the construction of Severi-Brauer varieties. The classical approach, going back to Châtelet, is to construct the Severi-Brauer variety associated with a degree n algebra A as the variety of left ideals of dimension n in A , by embedding it as a closed subvariety into the Grassmannian $Gr(n, n^2)$ (see e.g. Saltman [3] or Knus-Merkurjev-Rost-Tignol [1]). This construction has the advantage

of being canonical, but the projective embedding it gives is far from being the most ‘economical’ one. For instance, Severi-Brauer varieties of dimension 1 are realised not as plane conics, but as curves in \mathbf{P}^5 defined by 31 (non-independent) equations; see Jacobson [3], p. 113. Another approach is that of Grothendieck, which is based on general techniques in descent theory. It has similar advantages and disadvantages: it is more conceptual than the one above and works in a much more general situation, but it does not give explicit information on the projective embedding. See Jahnel [1] for a very detailed exposition of Grothendieck’s construction.

5.3 Geometric Brauer Equivalence

In the previous section we have shown that isomorphism classes of Severi-Brauer varieties of dimension $n - 1$ correspond bijectively to elements in the pointed set $H^1(k, \mathrm{PGL}_n)$. They therefore have a class in $\mathrm{Br}(k)$. Defining this class involves, however, the consideration of an equivalence relation on the disjoint union of the sets $H^1(k, \mathrm{PGL}_n)$ for all n , which corresponds to Brauer equivalence on central simple algebras. We now show that Brauer equivalence is quite easy to define geometrically on Severi-Brauer varieties, using closed embeddings of twisted-linear subvarieties.

The first step in this direction is:

Proposition 5.3.1 *Let X be a Severi-Brauer variety and Y a twisted-linear subvariety of X . Then X and Y have the same class in $\mathrm{Br}(k)$.*

Proof: Let $n - 1$ be the dimension of X , and $d - 1$ that of Y . Let $V_d \subset k^n$ be the linear subspace generated by the first d standard basis vectors, and $\tilde{P}_d(k)$ the subgroup of $\mathrm{GL}_n(k)$ consisting of elements leaving $V_d \subset k^n$ invariant. In other words, $\tilde{P}_d(k)$ is the subgroup

$$\left[\begin{array}{cc} \mathrm{GL}_d(k) & * \\ 0 & \mathrm{GL}_{n-d}(k) \end{array} \right] \subset \mathrm{GL}_n(k).$$

We denote by $P_d(k)$ its image in $\mathrm{PGL}_n(k)$. Note that restriction to the subspace V_d yields a natural map $\tilde{P}_d(k) \rightarrow \mathrm{GL}_d(k)$, and hence a map $P_d(k) \rightarrow \mathrm{PGL}_d(k)$.

Now by definition of a twisted-linear subvariety (taking Corollary 5.1.5 into account), there exists a finite Galois extension $K|k$ of group G and a

commutative diagram of trivialisations

$$\begin{array}{ccc} X \times_k K & \xleftarrow[\sim]{\phi} & \mathbf{P}^{n-1} \times_k K \\ \uparrow & & \uparrow \\ Y \times_k K & \xleftarrow[\sim]{\psi} & \mathbf{P}^{d-1} \times_k K, \end{array}$$

where the right vertical map is the inclusion of a projective linear subspace. Since $\mathrm{PGL}_n(k)$ acts transitively on the $(d-1)$ -dimensional projective linear subspaces of \mathbf{P}_k^{n-1} , we may assume that this map actually is the projectivisation of the inclusion map $V_d \otimes_k K \rightarrow K^n$. Therefore the cocycle $a_\sigma : \sigma \mapsto \psi \circ \sigma(\psi^{-1})$ defining the class of Y in $H^1(G, \mathrm{PGL}_n(K))$ takes its values in the subgroup $P_d(K) \subset \mathrm{PGL}_n(K)$. In other words, the class of $[Y]$ is in the image of the map $H^1(G, P_d(K)) \rightarrow H^1(G, \mathrm{PGL}_d(K))$. The commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & \mathrm{GL}_n(K) & \longrightarrow & \mathrm{PGL}_n(K) \longrightarrow 1 \\ & & \mathrm{id} \uparrow & & \uparrow & & \uparrow \\ 1 & \longrightarrow & K^\times & \longrightarrow & \tilde{P}_d(K) & \longrightarrow & P_d(K) \longrightarrow 1 \\ & & \mathrm{id} \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & K^\times & \longrightarrow & \mathrm{GL}_d(K) & \longrightarrow & \mathrm{PGL}_d(K) \longrightarrow 1 \end{array}$$

yields the commutative diagram of boundary maps

$$\begin{array}{ccc} [X] \in H^1(G, \mathrm{PGL}_n(K)) & \longrightarrow & H^2(G, K^\times) \\ & \uparrow & \mathrm{id} \uparrow \\ [a_\sigma] \in H^1(G, P_d(K)) & \longrightarrow & H^2(G, K^\times) \\ & \downarrow & \mathrm{id} \downarrow \\ [Y] \in H^1(G, \mathrm{PGL}_d(K)) & \longrightarrow & H^2(G, K^\times). \end{array} \quad (3)$$

Here the commutativity of the upper square is obvious and that of the lower one is proven by an argument similar to that of Lemma 4.4.3. We conclude that $[Y] = [X] \in \mathrm{Br}(k)$. \square

Proposition 5.3.2 *Let B be a central simple algebra, and let $A = M_r(B)$ for some $r > 0$. Denote by X and Y the Severi-Brauer varieties associated with A and B , respectively. Then Y can be embedded as a twisted-linear subvariety into X .*

The proof below is due to Michael Artin.

Proof: We keep the notations from the proof of Proposition 5.3.1; in particular, let d be the degree of B , and $n = rd$ that of A . It will be enough to show that the class of B in $H^1(G, \mathrm{PGL}_d(K))$ lies in the image of the natural map

$$H^1(G, P_d(K)) \rightarrow H^1(G, \mathrm{PGL}_d(K)).$$

Indeed, then diagram (3) shows that $[X]$ and $[Y]$ are both images of the same class in $H^1(G, P_d(K))$, and the construction of Severi-Brauer varieties out of 1-cocycles given in the previous chapter implies that Y embeds as a twisted-linear subvariety into X . To see this, consider the natural projection $\pi_d : K^n \rightarrow K^d$ given by mapping the last $n-d$ basis elements to 0. In the construction of the varieties X and Y we twisted the G -action on a tensor power of these vector spaces by the action of PGL_n , resp. PGL_d . These twisted actions are compatible with each other under the maps $\mathrm{PGL}_n \leftarrow P_d \rightarrow \mathrm{PGL}_d$. The induced map on G -invariants is surjective, because so is the map given by base change to K , which is just the above π_d by Speiser's lemma. The construction of X and Y then shows that this surjection of k -vector spaces induces a surjection of homogeneous coordinate rings $k[X] \rightarrow k[Y]$, which corresponds to a closed embedding of Y into X as a twisted-linear subvariety.

Now to prove our claim about the class $[B]$, consider the commutative diagram with exact rows and columns

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \\
 1 \rightarrow K^\times & \xrightarrow{\Delta} & K^\times \times K^\times & \xrightarrow{(+,-)} & K^\times & \rightarrow & 1 \\
 \mathrm{id} \downarrow & & \downarrow & & \downarrow & & \\
 1 \rightarrow K^\times & \longrightarrow & \mathrm{GL}_d(K) \times \mathrm{GL}_{n-d}(K) & \longrightarrow & (\mathrm{GL}_d(K) \times \mathrm{GL}_{n-d}(K)) / K^\times & \rightarrow & 1 \\
 & & \downarrow & & \downarrow & & \\
 & & \mathrm{PGL}_d(K) \times \mathrm{PGL}_{n-d}(K) & \xrightarrow{\mathrm{id}} & \mathrm{PGL}_d(K) \times \mathrm{PGL}_{n-d}(K) & & \\
 & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & &
 \end{array}$$

where Δ is the diagonal map, and $(+, -)$ is the map $(a, b) \mapsto a - b$. This is a diagram of groups equipped with a G -action, so by taking cohomology we

get a commutative diagram of pointed sets with exact columns

$$\begin{array}{ccc}
H^1(G, \mathrm{PGL}_d(K)) \times H^1(G, \mathrm{PGL}_{n-d}(K)) & \rightarrow & H^1(G, (\mathrm{GL}_d(K) \times \mathrm{GL}_{n-d}(K))/K^\times) \\
\downarrow & & \downarrow \\
H^1(G, \mathrm{PGL}_d(K)) \times H^1(G, \mathrm{PGL}_{n-d}(K)) & \xrightarrow{\mathrm{id}} & H^1(G, \mathrm{PGL}_d(K)) \times H^1(G, \mathrm{PGL}_{n-d}(K)) \\
\downarrow & & \downarrow \\
H^2(G, K^\times) \times H^2(G, K^\times) & \xrightarrow{(+,-)} & H^2(G, K^\times).
\end{array}$$

We have $n-d = (r-1)d$, so $M_{(r-1)d}(B)$ is a central simple algebra of degree $n-d$ satisfying

$$[M_r(B)] - [M_{(r-1)d}(B)] = [B] - [B] = 0 \in H^2(G, K^\times).$$

The diagram then shows that the pair $([M_r(B)], [M_{(r-1)d}(B)])$ defines an element of $H^1(G, \mathrm{PGL}_d(K)) \times H^1(G, \mathrm{PGL}_{n-d}(K))$ which is in the image of the map

$$H^1(G, (\mathrm{GL}_d(K) \times \mathrm{GL}_{n-d}(K))/K^\times) \rightarrow H^1(G, \mathrm{PGL}_d(K)) \times H^1(G, \mathrm{PGL}_{n-d}(K)).$$

In particular, the class $[B]$ is in the image of the map

$$\lambda : H^1(G, (\mathrm{GL}_d(K) \times \mathrm{GL}_{n-d}(K))/K^\times) \rightarrow H^1(G, \mathrm{PGL}_d(K))$$

obtained from the previous one by composing with the natural projection. Now observe that the natural surjection

$$\alpha : P_d(K) \rightarrow (\mathrm{GL}_d(K) \times \mathrm{GL}_{n-d}(K))/K^\times$$

induced by the mapping

$$\begin{bmatrix} \mathrm{GL}_d(K) & * \\ 0 & \mathrm{GL}_{n-d}(K) \end{bmatrix} \longrightarrow \begin{bmatrix} \mathrm{GL}_d(K) & 0 \\ 0 & \mathrm{GL}_{n-d}(K) \end{bmatrix}$$

has a section $\beta : (\mathrm{GL}_d(K) \times \mathrm{GL}_{n-d}(K))/K^\times \rightarrow P_d(K)$ satisfying $\alpha \circ \beta = \mathrm{id}$, which is induced by the obvious map in the reverse direction. Consequently, the natural map

$$H^1(G, P_d(K)) \xrightarrow{\alpha_*} H^1(G, (\mathrm{GL}_d(K) \times \mathrm{GL}_{n-d}(K))/K^\times)$$

induced on cohomology is surjective, so we conclude that the class $[B]$ lies in the image of the composite map

$$\lambda \circ \alpha_* : H^1(G, P_d(K)) \rightarrow H^1(G, \mathrm{PGL}_d(K)),$$

as was to be shown. \square

We can sum up the two previous propositions in the following statement.

Theorem 5.3.3 (Châtelet) *Two Severi-Brauer varieties X and Y over k have the same class in $\text{Br}(k)$ if and only if there exists a Severi-Brauer variety Z over k into which both X and Y can be embedded as twisted-linear subvarieties.*

Remark 5.3.4 Châtelet formulated this statement in a different but equivalent way: he stated that two Severi-Brauer varieties are Brauer equivalent if and only if they have isomorphic twisted-linear subvarieties (indeed, the corresponding central simple algebras are then matrix algebras over the same division algebra, by Wedderburn's theorem).

The theorem has several interesting consequences. First some terminology: we call a Severi-Brauer variety *minimal* if it has no proper twisted-linear subvarieties.

Corollary 5.3.5 *A central simple algebra A is a division algebra if and only if the associated Severi-Brauer variety is minimal.*

Proof: This follows from the theorem and the fact that division algebras are the central simple algebras of lowest dimension in their Brauer class. \square

Next recall that we have defined the index of a central simple algebra A to be the degree of the division algebra D for which $A \cong M_r(D)$ according to Wedderburn's theorem. In other words, the index $\text{ind}(A)$ is the degree of the unique division algebra in the Brauer class of A . Hence:

Corollary 5.3.6 (Châtelet) *Let A be a central simple algebra, and let X be the Severi-Brauer variety associated with A . Then all minimal twisted-linear subvarieties of X have the same dimension d , satisfying the equality*

$$d = \text{ind}(A) - 1.$$

We thus get a geometric definition of the index.

Remarks 5.3.7

1. Recall that A is split if and only if it has index 1. According to the proposition, this happens if and only if the minimal twisted-linear subvarieties have dimension 0. The subvarieties of dimension 0 defined over k are precisely the k -rational points, and conversely these are trivially twisted-linear subvarieties (if they exist). We thus get another proof of Châtelet's theorem (assuming the existence of a separable splitting field, which was used in the proof of Theorem 5.3.3).

2. One can construct the correspondence between central simple algebras and Severi-Brauer varieties in a purely geometric way. This makes it possible to obtain the results in this section without the use of cohomology. It is also feasible to introduce geometrical operations on Severi-Brauer varieties which correspond to multiplication and the inverse map in the Brauer group; they are, however, more complicated to define than the operations on central simple algebras. For all these constructions we refer to the paper of Endre Szabó [1].

5.4 Amitsur's Theorem

Let V be a variety over a field k . The natural inclusion $k \subset k(V)$ induces a map

$$r_V : \text{Br}(k) \rightarrow \text{Br}(k(V))$$

given by mapping the class of a Severi-Brauer variety X over k to the class of the variety $X_{k(V)}$ obtained by base extension. In particular, this applies to $V = X$. In this case, the base extension $X_{k(X)}$ has a $k(X)$ -rational point coming from the generic point of X . Hence by Châtelet's theorem the class of X in $\text{Br}(k)$ lies in the kernel of the map r_X . The following famous theorem shows that this construction already describes the kernel.

Theorem 5.4.1 (Amitsur) *Let X be a Severi-Brauer variety defined over a field k . Then the kernel of the restriction map $r_X : \text{Br}(k) \rightarrow \text{Br}(k(X))$ is a cyclic group generated by the class of X in $\text{Br}(k)$.*

An immediate corollary is:

Corollary 5.4.2 *Let X and Y be Severi-Brauer varieties that are birational over k . Then their classes $[X]$ and $[Y]$ generate the same subgroup in $\text{Br}(k)$.*

Remark 5.4.3 *Amitsur's conjecture predicts that the converse to the above corollary should be true: if $[X]$ and $[Y]$ generate the same subgroup in $\text{Br}(k)$, then X should be birational to Y over k . See Roquette [1] and Tregub [1] for partial results in this direction.*

Note, however, that a weaker result is quite easy to prove: *If $[X]$ and $[Y]$ generate the same subgroup in $\text{Br}(k)$, then X and Y are stably birational over k , i.e. there exist positive integers m, n such $X \times_k \mathbf{P}^m$ is birational to $Y \times_k \mathbf{P}^n$ over k .* Indeed, the assumption implies that $X \times_k k(Y)$ and $Y \times_k k(Y)$ generate the same subgroup in $\text{Br}(k(Y))$. But $Y \times_k k(Y)$ has a $k(Y)$ -rational point (coming from the generic point of Y), so by Châtelet's theorem its class in $\text{Br}(k(Y))$ is trivial. Hence so is that of $X \times_k k(Y)$, which

means that $X \times_k k(Y) \cong \mathbf{P}^n \times_k k(Y)$. In particular, these varieties have the same function field, which by definition equals $k(X \times_k Y)$ for the left hand side and $k(\mathbf{P}^n \times_k Y)$ for the right hand side. Thus $X \times_k Y$ is birational to $\mathbf{P}^n \times_k Y$, and the claim follows by symmetry.

The main ingredient in the proof of Amitsur's theorem is the following proposition. Before stating it, we recall from Proposition A.4.4 (2) of the Appendix that the Picard group of projective space \mathbf{P}_K^n over a field K is isomorphic to \mathbf{Z} , generated by the class of a K -rational hyperplane. We call the map realizing the isomorphism $\text{Pic}(\mathbf{P}_K^n) \cong \mathbf{Z}$ the *degree map*, and define the degree of a divisor on \mathbf{P}_K^n to be the image of its class by the degree map. This map is not to be confused with the degree map defined for curves.

Proposition 5.4.4 *Let $K|k$ be a finite Galois extension with group G that is a splitting field for X . There is an exact sequence*

$$0 \rightarrow \text{Pic}(X) \xrightarrow{\text{deg}} \mathbf{Z} \xrightarrow{\delta} H^2(G, K^\times) \rightarrow H^2(G, K(X)^\times),$$

where the map deg is given by composing the natural map $\text{Pic}(X) \rightarrow \text{Pic}(X_K)$ with the degree map.

Proof: By definition of the Picard group, we have an exact sequence of G -modules

$$0 \rightarrow K(X)^\times / K^\times \rightarrow \text{Div}(X_K) \rightarrow \text{Pic}(X_K) \rightarrow 0. \quad (4)$$

The beginning of the associated long exact cohomology sequence reads

$$\begin{aligned} 0 \rightarrow (K(X)^\times / K^\times)^G \rightarrow \text{Div}(X_K)^G \rightarrow \text{Pic}(X_K)^G \rightarrow \\ \rightarrow H^1(G, K(X)^\times / K^\times) \rightarrow H^1(G, \text{Div}(X_K)). \end{aligned}$$

The group G acts by permutation on $\text{Div}(X_K)$, hence this G -module is none but the *co-induced* G -module coming from $\text{Div}(X)$. Corollary 3.3.3 therefore implies $H^1(G, \text{Div}(X_K)) = 0$.

Next, a piece of the long exact sequence coming from the sequence of G -modules

$$0 \rightarrow K^\times \rightarrow K(X)^\times \rightarrow K(X)^\times / K^\times \rightarrow 0 \quad (5)$$

reads

$$H^1(G, K(X)^\times) \rightarrow H^1(G, K(X)^\times / K^\times) \rightarrow H^2(G, K^\times) \rightarrow H^2(G, K(X)^\times).$$

Here the group $H^1(G, K(X)^\times)$ is trivial by Hilbert's Theorem 90 (applied to the extension $K(X)|k(X)$). Therefore by splicing the two long exact sequences together we get

$$\begin{aligned} 0 \rightarrow (K(X)^\times/K^\times)^G \rightarrow \text{Div}(X_K)^G \rightarrow \text{Pic}(X_K)^G \rightarrow \\ \rightarrow H^2(G, K^\times) \rightarrow H^2(G, K(X)^\times). \end{aligned}$$

To identify this sequence with that of the proposition we make the following observations. First, we have $(\text{Div}(X_K))^G = \text{Div}(X)$ (again because $\text{Div}(X_K)$ is the co-induced module associated with $\text{Div}(X)$). Next, the beginning of the long exact sequence associated with (5) and the vanishing of $H^1(G, K^\times)$ (again by Hilbert's Theorem 90) yields the isomorphism $k(X)^\times/k^\times \cong (K(X)^\times/K^\times)^G$. So we may replace the first two terms in the sequence above by $\text{Pic}(X)$.

Finally, we have $X_K \cong \mathbf{P}_K^{n-1}$, whence an isomorphism $\text{Pic}(X_K) \cong \mathbf{Z}$ given by the degree map. To finish the proof, we have to show that $\text{Pic}(X_K)$ is a *trivial* G -module. Indeed, the group G can only act on \mathbf{Z} by sending 1 to 1 or -1 . This action, however, comes from the action of G on line bundles on \mathbf{P}_K^{n-1} and the line bundles in the class of -1 have no global sections, whereas those in the class of 1 do. (In terms of linear systems, the complete linear system associated with the class of 1 is that of hyperplanes in \mathbf{P}_K^{n-1} , whereas that associated with the class of -1 is empty.) This implies that 1 can only be fixed by G . \square

Now it is easy to derive the following basic exact sequence.

Theorem 5.4.5 *There is an exact sequence*

$$0 \rightarrow \text{Pic}(X) \xrightarrow{\text{deg}} \mathbf{Z} \xrightarrow{\delta} \text{Br}(k) \rightarrow \text{Br}(k(X)),$$

with $\text{deg} : \text{Pic}(X) \rightarrow \mathbf{Z}$ the same map as above.

For the proof of the theorem we need the following lemma.

Lemma 5.4.6 *Let V be a k -variety having a smooth k -rational point. Then the restriction map $\text{Br}(k) \rightarrow \text{Br}(k(V))$ is injective.*

Proof: If P is a smooth k -point on V , the local ring $\mathcal{O}_{X,P}$ embeds into the formal power series ring $k[[t_1, \dots, t_n]]$, where n is the dimension of V (see Appendix, Theorem A.5.4). Passing to quotient fields we get an injection $k(V) \subset k((t_1, \dots, t_n))$. This field in turn can be embedded into the iterated Laurent series field $k((t_1))((t_2)) \dots ((t_n))$. All in all, we have an induced map

$\text{Br}(k(V)) \rightarrow \text{Br}(k((t_1)) \dots ((t_n)))$. We show injectivity of the composite map $r : \text{Br}(k) \rightarrow \text{Br}(k((t_1)) \dots ((t_n)))$. For this it will be enough to treat the case $n = 1$, i.e. the injectivity of $r : \text{Br}(k) \rightarrow \text{Br}(k((t)))$, as the general case then follows by a straightforward induction.

Represent a class in the kernel of r by a Severi-Brauer variety X defined over k . Regarding it as a variety defined over $k((t))$, Châtelet's theorem implies that it has a $k((t))$ -rational point. If X is embedded into projective space \mathbf{P}^N , this point has homogeneous coordinates (x_0, \dots, x_N) . Viewing $k((t))$ as the quotient field of the ring $k[[t]]$, we may assume that each x_i lies in $k[[t]]$ and not all of them are divisible by t . Setting $t = 0$ then defines a rational point of X over k , and we conclude by Châtelet's theorem that the class of X in $\text{Br}(k)$ is trivial. \square

Proof of Theorem 5.4.5: By Theorem 4.4.7 we have isomorphisms

$$H^2(G, K^\times) \cong \text{Br}(K|k) \quad \text{and} \quad H^2(G, K(X)^\times) \cong \text{Br}(K(X)|k(X)).$$

Now the inflation-restriction sequence for Brauer groups (Corollary 4.4.11) gives a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Br}(K|k) & \longrightarrow & \text{Br}(k) & \longrightarrow & \text{Br}(K) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Br}(K(X)|k(X)) & \longrightarrow & \text{Br}(k(X)) & \longrightarrow & \text{Br}(K(X)) \end{array}$$

Here the third vertical map is injective by the lemma above. Hence the snake lemma gives an isomorphism

$$\ker(\text{Br}(K|k) \rightarrow \text{Br}(K(X)|k(X))) \cong \ker(\text{Br}(k) \rightarrow \text{Br}(k(X))),$$

and the theorem results from the previous proposition. \square

Remark 5.4.7 The exact sequence of the theorem is easy to establish using the *Hochschild-Serre spectral sequence* in étale cohomology (see e.g. Milne [2]).

We can now prove Amitsur's theorem.

Proof of Theorem 5.4.1: The exact sequence of the theorem shows that the kernel of the map $r_X : \text{Br}(k) \rightarrow \text{Br}(k(X))$ is cyclic, so it is a finite cyclic group, because $\text{Br}(k)$ is a torsion group. By the remarks at the beginning of this section, the class of X is contained in $\ker(r_X)$, so if d denotes the order of this class, we see that $\ker(r_X)$ has order divisible by d . On the other hand, by the exact sequence of the theorem the group $\ker(r_X)$ is the quotient of \mathbf{Z} by the image of the map $\text{deg} : \text{Pic}(X) \rightarrow \mathbf{Z}$. Theorem 5.2.2 implies

that there is a divisor class on X which becomes the d -th power of the class of a hyperplane over the algebraic closure. This means that $\text{Im}(\text{deg}) \subset \mathbf{Z}$ contains d , therefore $\ker(r_X)$ must have exact order d and the class of X must be a generator. \square

Our next goal is to show that Witt's theorem (Theorem 1.4.2) follows from that of Amitsur. First a corollary already announced before:

Corollary 5.4.8 *Assume that the base field k is not of characteristic 2. Let (a, b) a quaternion algebra over k . Then the Severi-Brauer variety associated with (a, b) is the conic $C(a, b)$ introduced in Chapter 1.*

Proof: The conic $C := C(a, b)$ is a Severi-Brauer variety of dimension 1, so it defines a class $[C]$ in $\text{Br}(k)$. The conic has a point over some quadratic extension $L|k$, so by Châtelet's theorem $[C]$ restricts to the trivial class in $\text{Br}(L)$. By the restriction-corestriction formula (Corollary 4.2.10) $[C]$ therefore lies in the 2-torsion of $\text{Br}(k)$. By Amitsur's theorem, this 2-torsion class generates the kernel of the map $\text{Br}(k) \rightarrow \text{Br}(k(C))$. On the other hand, by Proposition 1.3.2 the algebra $(a, b) \otimes_k k(C)$ splits, so $[(a, b)] = [C]$ or $[(a, b)] = 0$. If (a, b) is split, C has a k -point by *loc. cit.* and Châtelet's theorem implies that $[C] = 0$ as required. In the other case, $[(a, b)]$ must be the nontrivial element in the kernel which is $[C]$, and we are done again. \square

Remarks 5.4.9

1. Now we see how Witt's Theorem follows from Amitsur's theorem above: by the above proof, for a quaternion algebra (a, b) the only nontrivial class in the kernel of the map $\text{Br}(k) \rightarrow \text{Br}(k(C))$ is that of (a, b) . But if two division algebras of the same degree have the same Brauer class, they are isomorphic by Wedderburn's theorem.
2. The corollary also holds in characteristic 2, for the quaternion algebras (a, b) and the associated conics defined in Exercise 4 of Chapter 1.

We conclude this section by the following refinement of Theorem 5.4.5 which incorporates most of the results obtained so far.

Theorem 5.4.10 (Lichtenbaum) *Let X be a Severi-Brauer variety over a field k . In the exact sequence*

$$0 \rightarrow \text{Pic}(X) \rightarrow \mathbf{Z} \xrightarrow{\delta} \text{Br}(k) \rightarrow \text{Br}(k(X))$$

the map δ is given by sending 1 to the class of X in $\text{Br}(k)$.

Proof: Let $K|k$ be a Galois extension splitting X . By the proof of Proposition 5.4.4, the map δ arises as the composition of the coboundary maps

$$\mathrm{Pic}(X_K)^G \rightarrow H^1(G, K(X)^\times/K^\times) \quad \text{and} \quad H^1(G, K(X)^\times/K^\times) \rightarrow H^2(G, K^\times)$$

coming from the short exact sequences (4) and (5), respectively. In view of the construction of these coboundary maps (see the proofs of Proposition 2.7.1 and Proposition 4.4.1), we can therefore describe $\delta(1)$ as follows. One takes first a divisor D representing the divisor class $1 \in \mathbf{Z} \cong \mathrm{Pic}(X_K)$. Here the divisor D is not G -invariant in general but its class is (see the end of the proof of Proposition 5.4.4), so one finds a function f_σ with $\mathrm{div}(f_\sigma) = \sigma(D) - D$. The $K(X)^\times$ -valued map $\sigma \mapsto f_\sigma$ is the lifting of a 1-cocycle with values in $K(X)^\times/K^\times$, and the image of this cocycle by the second coboundary map is by definition the 2-cocycle $(\sigma, \tau) \mapsto f_\sigma \sigma(f_\tau) f_{\sigma\tau}^{-1}$. This is the 2-cocycle representing $\delta(1)$.

Now since D is of degree 1, the linear system $|D|$ defines an isomorphism $X_K \cong \mathbf{P}_K^{n-1}$, where $n = \dim X$. This isomorphism arises by taking the associated projective space to an isomorphism of vector spaces $L(D) \cong K^n$. Let g_0, \dots, g_{n-1} be a basis of the left hand side mapping to the standard basis e_0, \dots, e_{n-1} of K^n . Denote by λ the inverse isomorphism sending e_i to g_i . In terms of linear systems, the map λ sends e_i to the positive divisor $(g_i) + D$. So for $\sigma \in G$, the isomorphism $\sigma(\lambda)$ sends e_i to the divisor $(\sigma(g_i)) + \sigma(D) = (\sigma(g_i)) + (f_\sigma) + D = (f_\sigma \sigma(g_i)) + D$. This last divisor is also an element of $|D|$, therefore $f_\sigma \sigma(g_i) \in L(D)$. We may therefore write

$$f_\sigma \sigma(g_i) = \sum a_{ij\sigma} g_i \tag{6}$$

with some $a_{ij\sigma} \in K$. The matrix $A_\sigma := [a_{ij\sigma}]$ is therefore the matrix of the K -automorphism $\sigma(\lambda) \circ \lambda^{-1}$. Comparing with the definition at the beginning of Section 5.2, we see that this is exactly the matrix defining the class of X in $H^1(G, \mathrm{PGL}_n(K))$, and the class in $\mathrm{Br}(k)$ is therefore given by the 2-cocycle $(\sigma, \tau) \mapsto A_\sigma \sigma(A_\tau) A_{\sigma\tau}^{-1}$.

To compare these two 2-cocycles, we perform the following computation in the function field $K(X)$:

$$\begin{aligned} \sigma\tau(g_i) &= \sigma(\tau(g_i)) = \sigma(f_\tau^{-1} A_\tau g_i) = \sigma(f_\tau^{-1}) \sigma(A_\tau) \sigma(g_i) = \\ &= \sigma(f_\tau^{-1}) \sigma(A_\tau) (f_\sigma^{-1} A_\sigma g_i) = \sigma(f_\tau^{-1}) f_\sigma^{-1} \sigma(A_\tau) A_\sigma g_i. \end{aligned}$$

Comparing with equation (6) applied to $\sigma\tau$ gives

$$g_i = f_{\sigma\tau} \sigma(f_\tau^{-1}) f_\sigma^{-1} A_{\sigma\tau}^{-1} \sigma(A_\tau) A_\sigma g_i$$

for all i , and therefore

$$f_\sigma \sigma(f_\tau) f_{\sigma\tau}^{-1} = (A_\sigma^{-1} \sigma(A_\tau^{-1}) A_{\sigma\tau})^{-1}.$$

It remains to observe that the 2-cocycle $(\sigma, \tau) \mapsto (A_\sigma^{-1} \sigma(A_\tau^{-1}) A_{\sigma\tau})$ represents the class $-[X]$ in $\text{Br}(k)$. \square

Remarks 5.4.11

1. Lichtenbaum's theorem immediately implies Amitsur's, and therefore yields a proof which does not use the results of Section 2, just the construction of the Brauer class associated with X .
2. We also get a second (less explicit) proof of Theorem 5.2.2: if the class of X has order d in the Brauer group, then there exists a divisor class of degree d on X . The associated linear system defines the d -uple embedding over a splitting field K .

5.5 An Application: Making Central Simple Algebras Cyclic

We give now the following nice application of Amitsur's theorem, whose statement is purely algebraic and apparently does not involve Severi-Brauer varieties.

Theorem 5.5.1 (Saltman) *Assume that k contains a primitive n -th root of unity ω , and let A be a central simple algebra of degree n over k . There exists a field extension $F|k$ such that*

- *the algebra $A \otimes_k F$ is isomorphic to a cyclic algebra;*
- *the restriction map $\text{Br}(k) \rightarrow \text{Br}(F)$ is injective.*

Saltman himself did not publish this result (but see Berhuy-Frings [1], Theorem 4 for a slightly more general statement).

Remark 5.5.2 An iterated application of the theorem (possibly infinitely many times) shows that there exists a field extension $K|k$ such that the map $\text{Br}(k) \rightarrow \text{Br}(K)$ is injective, and *all* central simple k -algebras of degree n become cyclic over K .

For the proof of Saltman's theorem we need the following lemma.

Lemma 5.5.3 *Consider a purely transcendental extension $k(x, y)|k$ generated by the independent variables x and y . The degree n cyclic algebra $(x, y)_\omega$ over $k(x, y)$ has period n .*

Proof: We prove slightly more than required, namely that the algebra $(x, y)_\omega \otimes_{k(x, y)} K$ has period n , where K denotes the field $k((x))(y)$. The extension $L := K(\sqrt[n]{y})$ is cyclic of degree n and splits $(x, y)_\omega \otimes_{k(x, y)} K$. By Corollary 4.7.4, the isomorphism $K^\times / N_{L|K}(L^\times) \cong \text{Br}(L|K)$ is given by mapping $a \in K^\times$ to the class of the cyclic algebra $(a, y)_\omega$ over K , therefore the period of the K -algebra $(x, y)_\omega$ equals the order of $x \in K^\times$ in the group $K^\times / N_{L|K}(L^\times)$.

Denoting this order by e , we thus have by definition some $z \in L^\times$ with $x^e = N_{L|K}(z)$. By the general theory of formal power series, L is the formal Laurent series ring in one variable $\sqrt[n]{y}$ over $k((x))$. If z viewed as a Laurent series in $\sqrt[n]{y}$ had a nonzero term of negative degree, the same would be true of x^e viewed as a (constant) Laurent series in the variable y , which is not the case. Therefore $z \in k((x))[[\sqrt[n]{y}]]$, and taking its image by the natural map $k((x))[[\sqrt[n]{y}]] \rightarrow k((x))$ sending $\sqrt[n]{y}$ to 0 we get an element $\bar{z} \in k((x))$ satisfying $x^e = (\bar{z})^n$. Writing \bar{z} as a power series in x , we see that n must divide e . On the other hand, e divides n , because quite generally the period divides the degree (even the index; see Proposition 4.5.13 (1)). Therefore $e = n$, and the lemma is proven. \square

Proof of Theorem 5.5.1 : Define the field F to be the function field of a Severi-Brauer variety associated to the central simple algebra

$$B := (A \otimes_k k(x, y)) \otimes_{k(x, y)} (x, y)_\omega$$

defined over the field $k(x, y)$. By Châtelet's theorem (see the discussion before Theorem 5.4.1), the algebra

$$B \otimes_{k(x, y)} F \cong (A \otimes_k F) \otimes_F ((x, y)_\omega \otimes_{k(x, y)} F)$$

splits. This implies that $A \otimes_k F$ and the opposite algebra of $(x, y)_\omega \otimes_k F$ have the same class in $\text{Br}(F)$. As they both have degree n , they must be isomorphic. But the latter algebra is isomorphic to the F -algebra $(x, y^{-1})_\omega$, as one sees from their presentation. We conclude that $A \otimes_k F$ is isomorphic to a cyclic algebra.

We now show that $\text{Br}(k)$ injects into $\text{Br}(F)$. Let α be an element in the kernel of the map $\text{Br}(k) \rightarrow \text{Br}(F)$. For a field K containing k , we denote by α_K the image of α in $\text{Br}(K)$. According to Amitsur's theorem, the group $\ker(\text{Br}(k(x, y)) \rightarrow \text{Br}(F))$ is the cyclic subgroup generated by the class of B , so there exists an integer $m > 0$ for which the equality

$$\alpha_{k(x, y)} = m [A \otimes_k k(x, y)] + m [(x, y)_\omega] \tag{7}$$

holds in $\text{Br}(k(x, y))$. By passing to the field $k_s(x, y)$ we obtain

$$0 = \alpha_{k_s(x, y)} = m [(x, y)_\omega] \in \text{Br}(k_s(x, y)),$$

because A and α split over k_s . By Lemma 5.5.3, the $k_s(x, y)$ -algebra $(x, y)_\omega$ has period n , so n divides m . But since both A and $(x, y)_\omega$ have degree n and the period divides the degree, we have $n[A] = 0$ in $\text{Br}(k)$ and $n[(x, y)_\omega] = 0$ in $\text{Br}(k(x, y))$. Therefore we get from the identity (7) that $\alpha_{k(x, y)} = 0$, whence $\alpha = 0$ by Lemma 5.4.6, as desired. \square

EXERCISES

- Let k be a field containing a primitive n -th root ω of unity, and let $K = k(\sqrt[n]{a})$ be a cyclic extension of degree n . Given $b \in k^\times$, consider the closed subvariety Y_b of \mathbf{A}_k^{n+1} defined by the equation

$$bx = N_{K/k} \left(\sum_{i=0}^{n-1} (\sqrt[n]{a})^i y_i \right),$$

where we denoted the coordinates by $(x, y_0, y_1, \dots, y_{n-1})$.

- Verify that $Y_b(k) \neq \emptyset$ if and only if the cyclic algebra $(a, b)_\omega$ is split.
 - If $Y_b(k) \neq \emptyset$, show that Y is a k -rational variety.
 - Show that Y_b is *stably birational* to the Severi-Brauer variety associated to the cyclic algebra $(a, b)_\omega$. [*Hint*: Argue as in Remark 5.4.3.]
- (Heuser) Let A be a central simple algebra of degree n over k , and let e_1, \dots, e_{n^2} be a k -basis of A . Consider the reduced characteristic polynomial $\text{Nrd}_A(x - \sum e_i x_i)$ as a polynomial in the variables x, x_1, \dots, x_{n^2} , and let $X \subset \mathbf{A}_k^{n^2+1}$ be the associated affine hypersurface. Moreover, let $Y \subset \mathbf{P}_k^{n^2-1}$ be the projective hypersurface associated to the homogeneous polynomial $\text{Nrd}_A(\sum e_i x_i)$; it is called the *norm hypersurface* of A .
 - Show that the function field $k(X)$ of X is a splitting field of A . [*Hint*: Observe that $k(X)$ is a degree n extension of $k(x_1, \dots, x_{n^2})$ that may be embedded into $A \otimes_k k(x_1, \dots, x_{n^2})$.]
 - Show that the function field $k(Y)$ of Y is a splitting field of A . [*Hint*: Let $\tilde{Y} \subset \mathbf{A}^{n^2}$ be the affine cone over Y , i.e. the affine hypersurface defined by $\text{Nrd}_A(\sum e_i x_i) = 0$. Show that $k(X)|k(\tilde{Y})$ and $k(\tilde{Y})|k(Y)$ are purely transcendental extensions, and specialise.]
 - Let k be a field, and let A_1, A_2 be central simple algebras over k . Denote by X_1 , resp. X_2 the associated Severi-Brauer varieties. Compute the kernel of the natural map $\text{Br}(k) \rightarrow \text{Br}(k(X_1 \times X_2))$.

[*Hint:* Mimic the proof of Amitsur's theorem, and use the isomorphism $\text{Pic}(\mathbf{P}^n \times \mathbf{P}^m) \cong \mathbf{Z} \oplus \mathbf{Z}$ (Shafarevich [2], III.1.1, Example 3).]

4. Let k be a field of characteristic different from 2, and let C be a projective conic over k without k -rational points. Construct a field $F \supset k$ and a central simple algebra A over F such that $1 < \text{ind}_{F(C)}(A \otimes_F F(C)) < \text{ind}_F(A)$.
5. Let $\phi : C_1 \rightarrow C_2$ be a nonconstant morphism of projective conics defined over a field k . Denote by d the degree of ϕ , i.e. the degree of the induced extension $k(C_1)|\phi^*k(C_2)$ of function fields.

(a) Show that ϕ induces a commutative diagram

$$\begin{array}{ccc} \text{Pic}(\overline{C}_2)^G & \xrightarrow{\delta} & \text{Br}(k) \\ d \downarrow & & \downarrow \text{id} \\ \text{Pic}(\overline{C}_1)^G & \xrightarrow{\delta} & \text{Br}(k), \end{array}$$

where G is the absolute Galois group of k , and δ is the map of Theorem 5.4.5.

- (b) Conclude that if d is even, then C_2 has a k -rational point. [*Hint:* Use Lichtenbaum's theorem.]
6. Let k be a field of characteristic 0, A a central simple algebra over k and X the associated Severi-Brauer variety. Denote by $N_X(k) \subset k^\times$ the subgroup of k^\times generated by the subgroups $N_{K/k}(K^\times) \subset k^\times$ for those finite field extensions $K|k$ for which $X(K) \neq \emptyset$. Prove that $\text{Nrd}(A^\times) = N_X(k)$.

[*Remark:* The group $N_X(k)$ is called the *norm group* of X .]

Chapter 6

Residue Maps

Residue maps constitute a fundamental technical tool for the study of the cohomological symbol. Their definition is not particularly enlightening at a first glance, but the reader will see that they emerge naturally during the computation of Brauer groups of function fields or power series fields. When one determines these, a natural idea is to pass to a field extension having trivial Brauer group, so one needs some sufficient condition that ensures this property. The C_1 condition introduced by Emil Artin and baptised by Serge Lang furnishes such a sufficient condition via the vanishing of low-degree polynomials. There are three famous classes of C_1 -fields: finite fields, function fields of curves and Laurent series fields, the latter two over an algebraically closed base field. Once we know that the Brauer groups of these fields vanish, we are able to compute the Brauer groups of function fields and Laurent series fields over an arbitrary perfect field. The central result here is Faddeev's exact sequence for the Brauer group of a rational function field. We give two important applications of this theory: one to the class field theory of curves over finite fields, the other to constructing counterexamples to the rationality of the field of invariants of a finite group acting on some linear space. Following this ample motivation, we finally attack residue maps with finite coefficients, thereby preparing the ground for the next two chapters.

Residue maps for the Brauer group first appeared in the work of the German school on class field theory; the names of Artin, Hasse and F. K. Schmidt are the most important to be mentioned here. It was apparently Witt who first noticed the significance of residue maps over arbitrary discretely valued fields. Residue maps with finite coefficients came into the foreground in the 1960's in the context of étale cohomology; another source for their emergence in Galois cohomology is work by Arason [1] on quadratic forms.

6.1 Cohomological Dimension

Before embarking on the study of fields with vanishing Brauer group it is convenient to discuss the relevant cohomological background: this is the theory of cohomological dimension for profinite groups, introduced by Tate.

Recall that for an abelian group B and a prime number p , the notation $B\{p\}$ stands for the p -primary torsion subgroup of B , i.e. the subgroup of elements of p -power order.

Definition 6.1.1 Let G be a profinite group, p a prime number. We say that G has p -cohomological dimension $\leq n$ if $H^i(G, A)\{p\} = 0$ for all $i > n$ and all continuous torsion G -modules A . We define the p -cohomological dimension $\text{cd}_p(G)$ to be the smallest positive integer n for which G has cohomological dimension $\leq n$ if such an n exists, and set $\text{cd}_p(G) = \infty$ otherwise.

One may wonder why we restrict to torsion G -modules in the definition and why not take all G -modules. This is solely for technical convenience; the analogous notion defined using all G -modules is called the *strict* p -cohomological dimension of G in the literature. In fact, there is not much difference between the two concepts, as the following proposition shows.

Proposition 6.1.2 *Assume that $\text{cd}_p(G) \leq n$. Then $H^i(G, A)\{p\} = 0$ for all $i > n + 1$ and all continuous G -modules A .*

Proof: Let A be a continuous G -module, and consider the multiplication-by- p map $p : A \rightarrow A$. Its kernel ${}_pA$ and cokernel A/pA are torsion G -modules fitting into the exact sequence

$$0 \rightarrow {}_pA \rightarrow A \xrightarrow{p} A \rightarrow A/pA \rightarrow 0,$$

which may be split into two short exact sequences

$$0 \rightarrow {}_pA \rightarrow A \xrightarrow{p} C \rightarrow 0 \quad \text{and} \quad 0 \rightarrow C \rightarrow A \rightarrow A/pA \rightarrow 0,$$

with $C := \text{Im}(p)$. By assumption, the groups $H^i(G, {}_pA)$ and $H^i(G, A/pA)$ vanish for $i > n$, so the associated long exact sequences induce isomorphisms

$$H^i(G, A) \cong H^i(G, C) \quad \text{and} \quad H^{i+1}(G, C) \cong H^{i+1}(G, A)$$

for $i > n$. Thus for $i > n + 1$ the induced map $p_* : H^i(G, A) \rightarrow H^i(G, A)$ is an isomorphism. But by the construction of cohomology, the map p_* is also given by multiplication by p , so if it is an isomorphism, then the group $H^i(G, A)$ cannot have p -primary torsion. The claim follows. \square

As a first example, we have:

Proposition 6.1.3 *We have $\text{cd}_p(\hat{\mathbf{Z}}) = 1$ for all primes p .*

Proof: Note first that $\text{cd}_p(\hat{\mathbf{Z}}) \neq 0$, because

$$H^1(\hat{\mathbf{Z}}, \mathbf{Z}/p\mathbf{Z}) = \varinjlim \text{Hom}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/p\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}.$$

Next we show the vanishing of $H^2(\hat{\mathbf{Z}}, A)$ for all torsion $\hat{\mathbf{Z}}$ -modules A . By definition, this group is the direct limit of the groups $H^2(\mathbf{Z}/n\mathbf{Z}, A)$ via the inflation maps $\text{Inf} : H^2(\mathbf{Z}/n\mathbf{Z}, A) \rightarrow H^2(\mathbf{Z}/mn\mathbf{Z}, A)$, which by construction are induced by the natural map between the projective resolutions of \mathbf{Z} considered as a trivial $(\mathbf{Z}/mn\mathbf{Z})$ - and $(\mathbf{Z}/n\mathbf{Z})$ -module, respectively. On the special projective resolution of Example 3.2.9 all of whose terms equal $\mathbf{Z}[\mathbf{Z}/mn\mathbf{Z}]$ and $\mathbf{Z}[\mathbf{Z}/n\mathbf{Z}]$, respectively, this map is given by mapping a generator σ of $\mathbf{Z}/mn\mathbf{Z}$ to the generator $m\sigma$ of $\mathbf{Z}/n\mathbf{Z}$. Hence the above inflation map is nothing but multiplication by m . In particular, it annihilates all m -torsion elements of $H^2(\mathbf{Z}/n\mathbf{Z}, A)$, which implies the claim because m was arbitrary here.

Finally, we prove the vanishing of $H^i(\hat{\mathbf{Z}}, A)$ for $i > 2$ by dimension shifting as follows. Given a continuous torsion $\hat{\mathbf{Z}}$ -module A , we may embed it to the co-induced module $M^G(A)$ which is torsion by construction (see Remark 4.2.9). Hence so is the quotient $M^G(A)/A$, and so Corollary 4.3.1 gives $H^i(\hat{\mathbf{Z}}, M^G(A)/A) \cong H^{i+1}(\hat{\mathbf{Z}}, A)$, which is trivial for $i > 1$ by induction, starting from the case $i = 2$ treated above. \square

Next a general lemma about cohomological dimension.

Lemma 6.1.4 *Let G and p be as above, and let H be a closed subgroup of G . Then $\text{cd}_p(H) \leq \text{cd}_p(G)$. Here equality holds in the case when the image of H in all finite quotients of G has index prime to p . In particular, $\text{cd}_p(G) = \text{cd}_p(G_p)$ for a pro- p -Sylow subgroup G_p of G .*

Proof: Let B be a continuous torsion H -module. Then the continuous G -module $M_H^G(B)$ introduced in Remark 4.2.9 is also torsion and satisfies $H^i(H, B) = H^i(G, M_H^G(B))$ for all $i \geq 0$ by Shapiro's lemma, whence the inequality $\text{cd}_p(H) \leq \text{cd}_p(G)$. The opposite inequality in the case when H satisfies the prime-to- p condition of the lemma follows from Corollary 4.2.11. \square

In the case of pro- p -groups there is a very useful criterion for determining the p -cohomological dimension.

Proposition 6.1.5 *Let G be a pro- p -group for some prime number p . Then $\text{cd}_p(G) \leq n$ if and only if $H^{n+1}(G, \mathbf{Z}/p\mathbf{Z}) = 0$.*

For the proof we need the following lemma from module theory.

Lemma 6.1.6 *If G is a finite p -group, the only simple G -module of p -power order is $\mathbf{Z}/p\mathbf{Z}$ with trivial action.*

Proof: If A is a finite G -module of p -power order, then A^G must be a nontrivial G -submodule. Indeed, the complement $A \setminus A^G$ is the disjoint union of G -orbits each of which has p -power order and thus A^G cannot consist of the unit element only. Now if moreover we assume A to be simple, we must have $A = A^G$, i.e. triviality of the G -action. But then A must be $\mathbf{Z}/p\mathbf{Z}$, because a subgroup of a trivial G -module is a G -submodule. \square

Proof of Proposition 6.1.5: Necessity of the condition is obvious. For sufficiency, note first that $H^j(G, A\{p\}) = H^j(G, A)$ for all $j > 0$; indeed, decomposing A into the direct sum of its p -primary components, we see that for a prime $\ell \neq p$ the group $H^j(G, A\{\ell\})$ is both ℓ -primary torsion (by definition of cohomology) and p -primary torsion (by Proposition 4.2.6), hence trivial. Thus we may restrict to p -primary torsion modules. Next observe that it is enough to prove $H^{i+1}(G, A) = 0$ for all p -primary torsion G -modules A , by a similar dimension shifting argument as at the end of the proof of Proposition 6.1.3. By the definition of continuous cohomology we may assume that G is finite. Writing A as the direct limit of its finitely generated G -submodules, we may assume using Lemma 4.3.3 that A is finitely generated, hence finite of p -power order. Then by general module theory A has a composition series whose successive quotients are simple G -modules. The long exact cohomology sequence and induction on the length of the composition series implies that it is enough to consider these. We have arrived at the situation of the above lemma, and may conclude from the assumption. \square

Now we come to the cohomological dimension of fields.

Definition 6.1.7 The p -cohomological dimension $\text{cd}_p(k)$ of a field k is the p -cohomological dimension of the absolute Galois group $\text{Gal}(k_s|k)$ for some separable closure k_s . Its cohomological dimension $\text{cd}(k)$ is defined as the supremum of the $\text{cd}_p(k)$ for all primes p .

For us the most interesting case is that of fields of p -cohomological dimension 1, for this is a property that can be characterised using the Brauer group.

Theorem 6.1.8 *Let k be a field and p a prime number different from the characteristic of k . Then the following statements are equivalent:*

1. *The p -cohomological dimension of k is ≤ 1 .*

2. For all separable algebraic extensions $K|k$ we have $\text{Br}(K)\{p\} = 0$.
3. The norm map $N_{L|K} : L^\times \rightarrow K^\times$ is surjective for all separable algebraic extensions $K|k$ and all Galois extensions $L|K$ with $\text{Gal}(L|K) \cong \mathbf{Z}/p\mathbf{Z}$.

Proof: For the implication (1) \Rightarrow (2), choose a separable closure k_s of k containing K . Then $\text{Gal}(k_s|K)$ identifies with a closed subgroup of $\text{Gal}(k_s|k)$, and hence we have $\text{cd}_p(K) \leq \text{cd}_p(k) \leq 1$ using Lemma 6.1.4. In particular, the group $H^2(K, \mu_{p^i})$ is trivial for all $i > 0$, but this group is none but the p^i -torsion part of $\text{Br}(K)$ according to Corollary 4.4.9. For (2) \Rightarrow (3), note first that for $L|K$ as in (3) we have $\text{Br}(L|K) \cong K^\times/N_{L|K}(L^\times)$ thanks to Corollary 4.4.10. But $\text{Gal}(L|K) \cong \mathbf{Z}/p\mathbf{Z}$ also implies that $\text{Br}(L|K)$ is annihilated by p , so $\text{Br}(L|K) \subset \text{Br}(K)\{p\} = 0$, whence the claim.

Finally, for (3) \Rightarrow (1) let G_p be a pro- p -Sylow subgroup of $\text{Gal}(k_s|k)$. Lemma 6.1.4 implies that it is enough to prove $\text{cd}_p(G_p) \leq 1$, and moreover for this it is enough to show $H^2(G_p, \mathbf{Z}/p\mathbf{Z}) = 0$ by Proposition 6.1.5. As the extension $k(\mu_p)|k$ has degree $p - 1$, the fixed field k_p of G_p contains the p -th roots of unity, hence we have a chain of isomorphisms $H^2(G_p, \mathbf{Z}/p\mathbf{Z}) \cong H^2(k_p, \mu_p) \cong {}_p\text{Br}(k_p)$. Let $K_p|k_p$ be a finite extension contained in k_s and denote by P the Galois group $\text{Gal}(K_p|k_p)$. As $\text{Br}(K_p|k_p)$ injects into $\text{Br}(k_p)$, we are reduced to showing ${}_p\text{Br}(K_p|k_p) = 0$. The group P , being a finite p -group, is solvable, i.e. there exists a finite chain

$$P = P_0 \supset P_1 \supset \cdots \supset P_n = \{1\}$$

of normal subgroups such that $P_i/P_{i+1} \cong \mathbf{Z}/p\mathbf{Z}$. These subgroups correspond to field extensions

$$k_p = K_0 \subset K_1 \subset \cdots \subset K_n = K$$

such that $\text{Gal}(K_i|k_p) \cong P/P_i$. We now show ${}_p\text{Br}(K_i|k_p) = 0$ by induction on i , the case $i = 0$ being trivial. Assuming the statement for $i - 1$, consider the exact sequence

$$0 \rightarrow H^2(P/P_{i-1}, K_{i-1}^\times) \rightarrow H^2(P/P_i, K_i^\times) \rightarrow H^2(P_{i-1}/P_i, K_i^\times)$$

coming from Proposition 3.3.17 applied with $G = P/P_i$, $H = P_{i-1}/P_i$ and $A = K_i^\times$, noting that $H^1(P_i/P_{i-1}, K_i^\times) = 0$ thanks to Hilbert's Theorem 90. Restricting to p -torsion subgroups, we get

$$0 \rightarrow {}_p\text{Br}(K_{i-1}|k_p) \rightarrow {}_p\text{Br}(K_i|k_p) \rightarrow {}_p\text{Br}(K_i|K_{i-1}).$$

Here the right hand side group is trivial by (3) applied with $K = K_{i-1}$ and $L = K_i$ (and noting Corollary 4.4.10 again), and the left hand side group is

trivial by induction. Hence so is the middle one, which completes the proof of the inductive step. \square

We have the following complement:

Proposition 6.1.9 *Let k be a field of characteristic $p > 0$. Then $\text{cd}_p(k) \leq 1$.*

Proof: By Lemma 6.1.4, we may replace k by the fixed field of some pro- p -Sylow subgroup of $\text{Gal}(k_s|k)$. Hence we may assume that k is a field of characteristic p whose absolute Galois group is a pro- p -group. By Proposition 6.1.5, it suffices therefore to establish the vanishing of $H^2(k, \mathbf{Z}/p\mathbf{Z})$. For this, recall the exact sequence

$$0 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow k_s \xrightarrow{\wp} k_s \rightarrow 0$$

from the proof of Proposition 4.3.10, where $\wp : k_s \rightarrow k_s$ is given by $\wp(x) = x^p - x$. Part of the associated long exact sequence reads

$$H^1(k, k_s) \rightarrow H^2(k, \mathbf{Z}/p\mathbf{Z}) \rightarrow H^2(k, k_s),$$

from which we get the required vanishing, the two extremal terms being trivial by Lemma 4.3.11. \square

Remark 6.1.10 According to the proposition, the higher Galois cohomology groups with p -torsion coefficients are trivial invariants for fields of characteristic $p > 0$. In the study of these other cohomology theories have been helpful. One approach, proposed by Milne [1] and Kato [2], is to use the modules $\nu(n)$ of logarithmic differentials that we shall discuss later in Section 9.5, and consider the groups $H_p^{n+1}(k) := H^1(k, \nu(n)_{k_s})$ for $n \geq 1$. As we shall see in Section 9.2, for $n = 1$ one has $H_p^2(k) \cong {}_p\text{Br}(k)$, which is a nontrivial group in general for non-perfect k , in contrast to the situation of Theorem 6.1.8.

This phenomenon is related to the problem of defining the ‘right’ notion of p -cohomological dimension for fields of characteristic p . In Serre [2], §II.3 such a field k is defined to be of p -dimension ≤ 1 if ${}_p\text{Br}(K) = 0$ for all finite extensions $K|k$. In Kato [2] and Kato-Kuzumaki [1] a generalisation of this condition is proposed: k is said to be of p -dimension n if n is the smallest integer with $[k : k^p] \leq p^n$ and $H_p^{n+1}(K) = 0$ for all finite extensions $K|k$.

We conclude this chapter by two examples of fields of cohomological dimension 1. For the moment, we have at our disposal only the ones with absolute Galois group $\hat{\mathbf{Z}}$; we shall see more examples in the next section.

Examples 6.1.11 Finite fields and Laurent series fields over an algebraically closed field of characteristic 0 have absolute Galois group isomorphic to $\hat{\mathbf{Z}}$, by Examples 4.1.5 and 4.1.6, respectively. They therefore have cohomological dimension 1 by Proposition 6.1.3.

6.2 C_1 -Fields

The pertinence of the following condition to our subject matter has been first observed by Emil Artin.

Definition 6.2.1 A field k is said to satisfy condition C_1 if every homogeneous polynomial $f \in k[x_1, \dots, x_n]$ of degree $d < n$ has a nontrivial zero in k^n .

We briefly call such fields C_1 -fields.

Remarks 6.2.2

1. More generally, a field k satisfies condition C_r for an integer $r > 0$ if every homogeneous polynomial $f \in k[x_1, \dots, x_n]$ of degree d with $d^r < n$ has a nontrivial zero in k^n . This condition was introduced and first studied by Lang [1].
2. Even more generally, a field k is said to satisfy condition C'_r for some integer $r > 0$ if each finite system $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ of homogeneous polynomials of respective degrees d_1, \dots, d_m has a nontrivial common zero in k^n , provided that $d_1^r + \dots + d_m^r < n$. For more on this property, see the book of Pfister [1].

Artin himself called C_1 -fields quasi-algebraically closed, because they have the property that there is no nontrivial finite dimensional central division algebra over them. In fact, one has:

Proposition 6.2.3 *Let k be a C_1 -field. Then $\text{cd}(k) \leq 1$, and $\text{Br}(L) = 0$ for every finite extension $L|k$.*

Note that the extension $L|k$ is not assumed to be separable. We prove first the following lemma which will be also useful later.

Lemma 6.2.4 *If K is a C_1 -field, then so is every finite extension $L|K$.*

Proof: Let $f \in L[x_1, \dots, x_n]$ be a homogeneous polynomial of degree $d < n$, and let v_1, \dots, v_m be a basis of the K -vector space L . Introduce new variables x_{ij} ($1 \leq i \leq n, 1 \leq j \leq m$) satisfying $x_{i1}v_1 + \dots + x_{im}v_m = x_i$, and consider the equation $N_{L|K}(f(x_1, \dots, x_n)) = 0$. This is then a homogeneous equation over K of degree md in the mn variables x_{ij} , so by assumption it has a nontrivial zero $(\alpha_{11}, \dots, \alpha_{mn})$ in K^{mn} , since $md < mn$. Whence a nontrivial element $(\alpha_1, \dots, \alpha_n) \in L^n$ satisfying $N_{L|K}(f(\alpha_1, \dots, \alpha_n)) = 0$, which holds if and only if $f(\alpha_1, \dots, \alpha_n) = 0$. \square

Proof of Proposition 6.2.3: If our C_1 -field k has positive characteristic p , we have $\text{cd}_p(k) \leq 1$ by the general Proposition 6.1.9. So as far as cohomological dimension is concerned, we may concentrate on the other primes and conclude from Theorem 6.1.8 and Lemma 6.2.4 that it is enough to show the second statement in the case $L = k$, i.e. that a C_1 -field has trivial Brauer group.

So consider a division algebra D of degree n over a C_1 -field k , and denote by $\text{Nrd} : D \rightarrow k$ the associated reduced norm. Choosing a k -basis v_1, \dots, v_{n^2} of D considered as a k -vector space, we see from the construction of Nrd in Chapter 2 that $f(x_1, \dots, x_{n^2}) := \text{Nrd}(x_1v_1 + \dots + x_{n^2}v_{n^2})$ is a homogeneous polynomial of degree n in the n^2 variables x_1, \dots, x_{n^2} . If here $n > 1$, then by the C_1 property f has a nontrivial zero in k^n . But this contradicts the assumption that D is a division algebra, by Proposition 2.6.2. Therefore $n = 1$, and $D = k$ is the trivial division algebra over k . \square

Remark 6.2.5 The question arises whether the converse of the proposition holds true. The answer is no: Ax [1] has constructed a field of cohomological dimension 1 (and of characteristic 0) which is not a C_1 -field. See also the book of Shatz [1] for details.

Here are the first nontrivial examples of C_1 -fields.

Theorem 6.2.6 (Chevalley) *Finite fields satisfy the C_1 property.*

Proof: Let \mathbf{F}_q be the field with q elements, where q is some power of a prime number p . Following Warning, we prove more, namely that the number of solutions in \mathbf{F}_q^n of a polynomial equation $f(x_1, \dots, x_n) = 0$ of degree $d < n$ is divisible by p . If f is moreover homogeneous, it already has the trivial solution, whence the claim.

For a polynomial $g \in k[x_1, \dots, x_n]$ denote by $N(g)$ the number of its zeros in \mathbf{F}_q^n , and introduce the notation

$$\Sigma(g) := \sum_{(\alpha_1, \dots, \alpha_n) \in \mathbf{F}_q^n} (g(\alpha_1, \dots, \alpha_n))^{q-1}.$$

As $\alpha^{q-1} = 1$ for each nonzero $\alpha \in \mathbf{F}_q$, we see that the element $\Sigma(g) \in \mathbf{F}_q$ actually lies in $\mathbf{F}_p \subset \mathbf{F}_q$, and moreover

$$q^n - \Sigma(g) = \sum_{(\alpha_1, \dots, \alpha_n) \in \mathbf{F}_q^n} (1 - (g(\alpha_1, \dots, \alpha_n))^{q-1}) \equiv N(g) \pmod{p}.$$

Therefore it is enough to show that $\Sigma(f) = 0$ in \mathbf{F}_q for our particular f above. For this, write $f(x_1, \dots, x_n)^{q-1}$ as a linear combination of monomials $x_1^{r_1} \dots x_n^{r_n}$. We show that $\Sigma(x_1^{r_1} \dots x_n^{r_n}) = 0$ in \mathbf{F}_q for all occurring monomials $x_1^{r_1} \dots x_n^{r_n}$. This is obvious if one of the r_i is 0, so we may assume this is not the case. Then, as f has degree less than n by assumption, we may assume that one of the r_i , say r_1 , is smaller than $q - 1$. Then fixing $(\alpha_2, \dots, \alpha_n) \in \mathbf{F}_q^{n-1}$ and taking a generator ω of the cyclic group \mathbf{F}_q^\times we get

$$\sum_{\alpha \in \mathbf{F}_q} \alpha^{r_1} \alpha_2^{r_2} \dots \alpha_n^{r_n} = \alpha_2^{r_2} \dots \alpha_n^{r_n} \sum_{i=0}^{q-2} \omega^{ir_1} = (\alpha_2^{r_2} \dots \alpha_n^{r_n}) \frac{(\omega^{r_1})^{q-1} - 1}{\omega^{r_1} - 1},$$

which equals 0 in \mathbf{F}_q . We conclude by making $(\alpha_2, \dots, \alpha_n)$ run over \mathbf{F}_q^{n-1} . \square

Remark 6.2.7 Together with the previous proposition, the theorem gives another proof of the fact that finite fields have cohomological dimension 1. Moreover, we also get that finite fields have trivial Brauer group (up to now, we only knew that the prime-to- p part is trivial, by Theorem 6.1.8). In other words, we have proven another famous theorem due to Wedderburn: *A finite dimensional division algebra over a finite field is a field.*

Other classic examples of C_1 -fields are given by the following theorem.

Theorem 6.2.8 (Tsen) *Let k be an algebraically closed field, and let K be the function field of an algebraic curve over k . Then K is a C_1 -field.*

Proof: Using Lemma 6.2.4 we may assume K is a simple transcendental extension $k(t)$ of k . Given a homogeneous polynomial $f \in k(t)[x_1, \dots, x_n]$ of degree $d < n$, we may also assume the coefficients to be in $k[t]$, and we may look for solutions in $k[t]^n$. Choose an integer $N > 0$ and look for the x_i in the form

$$x_i = \sum_{j=0}^N a_{ij} t^j,$$

with the $a_{ij} \in k$ to be determined. Plugging this expression into f and regrouping according to powers of t , we get a decomposition

$$0 = f(x_1, \dots, x_n) = \sum_{l=0}^{dN+r} f_l(a_{10}, \dots, a_{nN}) t^l,$$

where r is the maximal degree of the coefficients of f and the f_l are homogeneous polynomials in the a_{ij} all of which should equal 0. Since $d < n$ by assumption, for N sufficiently large the number $dN + r + 1$ of the polynomials f_l is smaller than the number $n(N + 1)$ of the indeterminates a_{ij} , so they define a nonempty Zariski closed subset in projective $(nN + n - 1)$ -space \mathbf{P}^{nN+n-1} (see Appendix, Corollary A.3.3). As k is algebraically closed, this closed set has a point in $\mathbf{P}^{nN+n-1}(k)$, whence the a_{ij} we were looking for. \square

Remarks 6.2.9

1. The theorems of Chevalley and Tsen can be sharpened in the sense that finite fields as well as function fields of curves over algebraically closed fields (or even C_1 -fields) satisfy the C'_1 property of Remark 6.2.2 (2). The proofs are similar to the ones given above and are left as an exercise.
2. Tsen's theorem has the following geometric interpretation. Let C be a smooth projective curve with function field K . The homogeneous polynomial $f \in K[x_1, \dots, x_n]$ defines an $(n - 1)$ -dimensional projective variety equipped with a surjective morphism $X \rightarrow C$. A nontrivial solution of $f(x_1, \dots, x_n) = 0$ in K^n defines a *section* of p , i.e. a morphism $s : C \rightarrow X$ with $p \circ s = \text{id}_C$. In particular, $s(C) \subset X$ is a closed subvariety of dimension 1 mapped isomorphically onto C by p .

As a particular example, consider a degree 2 homogeneous polynomial in 3 variables with coefficients in $k[t]$. It defines a surface fibred in conics over the projective line. By Tsen's theorem, there is a curve on the surface intersecting each fibre in exactly one point. For remarkable recent generalisations of this fact, see Graber-Harris-Starr [1] and de Jong-Starr [1].

Before moving over to other classes of C_1 -fields, we point out the following interesting corollary to Tsen's theorem.

Corollary 6.2.10 *Let C be a smooth projective geometrically connected curve over a finite field \mathbf{F} . Every central simple algebra over the function field $\mathbf{F}(C)$ is split by a cyclic field extension, and hence it is Brauer equivalent to a cyclic algebra.*

Proof: Let $\overline{\mathbf{F}}$ be an algebraic closure of \mathbf{F} . We have $\text{Br}(\overline{\mathbf{F}}(C)) = 0$ by Tsen's theorem, so every central simple algebra over $\mathbf{F}(C)$ is split by $\mathbf{F}'(C)$ for some finite extension $\mathbf{F}'|\mathbf{F}$. This is necessarily a cyclic extension as \mathbf{F} is finite. The second statement follows from Proposition 4.7.6. \square

The third famous class of C_1 -fields is that of fields complete with respect to a discrete valuation with algebraically closed residue field. The C_1 property for these was established by Serge Lang in his thesis (Lang [1]). In this book we shall only need the equal characteristic case, which reads as follows. For a field k consider the field of formal Laurent series $k((t))$, and denote by $k((t))_{nr}$ the composite of the separable closure k_s of k with $k((t))$ inside a fixed separable closure of the latter. This field is the maximal unramified extension of the discretely valued field $k((t))$. It is the union of the fields $k'((t))$ for all finite extensions $k'|k$ inside k_s .

Theorem 6.2.11 (Lang) *For a perfect field k the field $k((t))_{nr}$ is a C_1 -field. In particular, if k is algebraically closed, then $k((t))$ itself is a C_1 -field.*

We shall deduce the theorem above from Tsen's theorem using an approximation method taken from Greenberg [1]. The crucial statement is:

Theorem 6.2.12 (Greenberg) *Let k be a perfect field, and let moreover $S = \{f_1, \dots, f_m\}$ be a system of polynomials in $k[[t]][x_1, \dots, x_n]$. There is an integer $N_0(S) > 0$, depending on S , such that for all $N > N_0(S)$ the existence of a common solution $(a_1^{(N)}, \dots, a_n^{(N)})$ of the congruences*

$$f_i(x_1, \dots, x_n) = 0 \pmod{t^N}, \quad i = 1, \dots, m$$

implies the existence of a common zero $(a_1, \dots, a_n) \in k[[t]]^n$ of the $f_i \in S$.

We first show that *Theorem 6.2.12 implies Theorem 6.2.11*. Consider a homogeneous polynomial $f \in k((t))_{nr}[x_1, \dots, x_n]$ of degree $d < n$. To prove that f has a zero in $k((t))_{nr}^n$, after multiplying with a common denominator we may assume that f has coefficients in $k'[[t]]$ for a finite extension $k'|k$. Since the rings $k'[[t]]/(t^N)$ and $k'[t]/(t^N)$ are isomorphic for all $N > 0$, we may find for each N a degree d homogeneous polynomial $f^{(N)} \in k'[t][x_1, \dots, x_n]$ with $f^{(N)} = f \pmod{t^N}$. By Tsen's theorem, after replacing k' by a finite extension we see that $f^{(N)}$ has a zero $(a_1^{(N)}, \dots, a_n^{(N)}) \in k'(t)^n$, where we may assume the $a_j^{(N)}$ to lie in $k'[t]$ by homogeneity of $f^{(N)}$. Reducing modulo (t^N) thus yields a zero of f modulo (t^N) , and so for N sufficiently large the case $m = 1$ of Theorem 6.2.12 applies. \square

Proof of Theorem 6.2.12: Consider the affine closed subset $V \subset \mathbf{A}^n$ defined as the locus of common zeroes of the $f_i \in S$. We prove the theorem by induction on the dimension d of V , starting from the obvious case $d = -1$, i.e. $V = \emptyset$.

We first make a reduction to the case when V is a closed subvariety of \mathbf{A}^n . For this, let J be the ideal in $k((t))[x_1, \dots, x_n]$ generated by the $f_i \in S$. Let g be a polynomial with $g \notin J$ but $g^r \in J$ for some $r > 1$. Then if $(a_1, \dots, a_n) \in k[[t]]^n$ satisfies $f_i(a_1, \dots, a_n) = 0 \pmod{t^N}$ for all i , we conclude the same for g^r , and hence we get $g(a_1, \dots, a_n) = 0 \pmod{t^\nu}$ for all integers $0 < \nu \leq N/r$. Applying this to a system of generators $T = \{g_1, \dots, g_M\}$ of the radical of J , we see that if the theorem holds for the system T with some constant $N_0(T)$, it also holds for the system S with a sufficiently high multiple $N_0(S)$ of $N_0(T)$. So we may assume J equals its own radical, and hence is an intersection of finitely many prime ideals P_1, \dots, P_r . Now if $g_j \in P_j$ are such that $g_1 \dots g_r \in J$, we see as above that $f_i(a_1, \dots, a_n) = 0 \pmod{t^N}$ for all i implies that there is some j with $g_j(a_1, \dots, a_n) = 0 \pmod{t^\nu}$ for all $0 < \nu \leq N/r$. Reasoning as above, we therefore conclude that it is enough to prove the theorem for the P_j , i.e. we may assume V is a variety.

Now for each subset $I \subset \{1, \dots, m\}$ of cardinality $n - d$ consider the closed subset V_I defined in \mathbf{A}^n by the system $S_I = \{f_i \in S : i \in I\}$, and let $V_I^+ \subset V_I$ be the union of the d -dimensional $k((t))$ -irreducible components different from V . The sets V_I^+ are defined as the locus of zeroes of some finite system $S_I^+ \supset S_I$ of polynomials. Consider also the singular locus $W \subset V$ of V . Propositions A.3.4 and A.3.7 of the Appendix imply that it is a proper closed subset of V , and as such has dimension $< d$. Furthermore, it is defined by a system S_W of polynomials obtained by adding some equations (namely the $(n - d) \times (n - d)$ minors of the Jacobian of the f_i) to S . Finally, let $P = (a_1, \dots, a_n) \in k[[t]]^n$ be a point satisfying $f_i(a_1, \dots, a_n) = 0 \pmod{t^N}$ for all $f_i \in S$, with some N to be determined later. If P also happens to satisfy all the other equations in S_W modulo (t^N) , and if $N > N_0(S_W)$, we conclude by the inductive hypothesis that there is some point in $W \subset V$ congruent to P modulo (t^N) , and we are finished. Similarly, if P also satisfies the equations in some S_I^+ modulo (t^N) , then by the inductive hypothesis applied to the proper closed subset $V \cap V_I^+$ we get a point in $V \cap V_I^+$ congruent to P , provided $N > N_0(S \cup S_I^+)$. So we may choose N greater than both $N_0(S_W)$ and the $N_0(S \cup S_I^+)$, and assume we are not in the above cases. Then if P is congruent to a $k[[t]]$ -valued point of V modulo (t^N) , it must be a smooth point not contained in any of the other components of the V_I , so it will be enough to assure that P is congruent to some smooth point in V_I .

We may assume $I = \{1, \dots, n - d\}$, and we may enlarge the system S_I by adding the linear polynomials $x_{n-d+1} - a_{n-d+1}, \dots, x_n - a_n$. For ease of notation we denote this new system again by S . Let J_S be the Jacobian matrix of the system S , and let h be its determinant evaluated at P . Observe that since the j -th partial derivatives of the $x_i - a_i$ equal 0 for $i \neq j$ and 1 for $i = j$, the subdeterminant formed by the first $n - d$ columns in the

Jacobian of the system S_I at P also equals h . Hence h is nontrivial modulo (t^N) by assumption; denote by ν the highest power of t dividing h , and take N so large that $N > 2\nu$. Under this assumption a refined form of Hensel's lemma (cf. Appendix, Proposition A.5.6) implies that there is a point of V_I over $k[[t]]$ congruent to P modulo $(t^{N-\nu})$, and we are done. \square

Remarks 6.2.13

1. An examination of the above proof shows that even if we only need the case $m = 1$ for the application to Lang's Theorem, in order to prove this special case we still have to consider systems of polynomials to make the induction work. Thus working with several polynomials is often more advantageous than with a single one; in particular, the C'_1 property can be more handy than just C_1 . In fact, assuming the C'_1 analogue of Tsen's theorem (Remark 6.2.9 (1)), we get from the above proof that the fields $k((t))_{nr}$ are actually C'_1 -fields.
2. Greenberg's theorem is more general than the form proven above, and is very useful for many applications. It states that given a discrete valuation ring R for which Hensel's lemma holds and a system of equations with coefficients in R , then under a separability assumption one may approximate solutions over the completion \widehat{R} by solutions over R arbitrary closely in the topology of \widehat{R} . For example, this more general statement works for the subring $R \subset k[[t]]$ formed by power series algebraic over $k(t)$. In the characteristic 0 case there is also a constructive method for finding a good approximation (Kneser [1]).

6.3 Cohomology of Laurent Series Fields

In the next section we shall apply Tsen's theorem to study the cohomology of function fields of curves. It will be convenient to look a local situation first. Namely, the completion of a local ring at a smooth closed point P of a curve C over a field k is isomorphic to the formal power series ring $\kappa(P)[[t]]$ (see Appendix, Proposition A.5.3). Assume that the residue field $\kappa(P)$ is separable over k , and take a separable closure k_s of $\kappa(P)$. Then the completions of the local rings of the curve $C \times_k k_s$ at the points lying above P are isomorphic to $k_s[[t]]$. This ring is equipped with a natural action by the Galois group $G := \text{Gal}(k_s|k)$.

Consider the valuation homomorphism

$$v : k_s((t))^\times \rightarrow \mathbf{Z}$$

sending a Laurent series over k_s to the degree of the least nonzero term. This map is G -equivariant if \mathbf{Z} carries the trivial action, and restricts to a G -equivariant map on the field $k((t))_{nr}$ of the previous section. Denoting by U_{nr} the multiplicative group of invertible power series contained in $k((t))_{nr}$ we get an exact sequence of G -modules

$$0 \rightarrow U_{nr} \rightarrow k((t))_{nr}^\times \rightarrow \mathbf{Z} \rightarrow 0 \quad (1)$$

which is split by the map $\mathbf{Z} \rightarrow k((t))_{nr}^\times$ sending 1 to t . Hence for each $i \geq 0$ we have a split exact sequence of cohomology groups

$$0 \rightarrow H^i(G, U_{nr}) \rightarrow H^i(G, k((t))_{nr}^\times) \rightarrow H^i(G, \mathbf{Z}) \rightarrow 0$$

by Remark 4.3.4 (2). For $i = 0$ this is just the analogue of exact sequence (1) for k instead of k_s , and for $i = 1$ it is uninteresting because of Hilbert's Theorem 90. For $i \geq 2$, we may use the exact sequence

$$0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Q} \rightarrow \mathbf{Q}/\mathbf{Z} \rightarrow 0$$

to obtain isomorphisms $H^i(G, \mathbf{Z}) \cong H^{i-1}(G, \mathbf{Q}/\mathbf{Z})$, as $H^i(G, \mathbf{Q}) = 0$ for $i > 0$ by Corollary 4.2.7. Hence we may rewrite the above sequence as

$$0 \rightarrow H^i(G, U_{nr}) \rightarrow H^i(G, k((t))_{nr}^\times) \xrightarrow{r_v} H^{i-1}(G, \mathbf{Q}/\mathbf{Z}) \rightarrow 0.$$

The map r_v is called the *residue map* associated to v .

As regards the kernel of the residue map, we have:

Proposition 6.3.1 *The natural map $U_{nr} \rightarrow k_s^\times$ sending a power series to its constant term induces isomorphisms*

$$H^i(G, U_{nr}) \cong H^i(G, k_s^\times)$$

for all $i > 0$. Therefore we have split exact sequences

$$0 \rightarrow H^i(G, k_s^\times) \rightarrow H^i(G, k((t))_{nr}^\times) \xrightarrow{r_v} H^{i-1}(G, \mathbf{Q}/\mathbf{Z}) \rightarrow 0.$$

For the proof we need a formal lemma.

Lemma 6.3.2 *Let G be a finite group, and $(A_\alpha)_{\alpha \in \mathbf{Z}_+}$ be an inverse system of continuous G -modules indexed by the directed set \mathbf{Z}_+ of positive integers. Assume that $i > 0$ is an integer such that $H^i(G, A_\alpha) = 0$ for all $\alpha \in \mathbf{Z}_+$. Then $H^i(G, \varprojlim A_\alpha) = 0$.*

Here the inverse limit is equipped, as before, with the discrete topology.

Proof: Choose a projective resolution P^\bullet of \mathbf{Z} , and represent an element of $H^i(G, \varprojlim A_\alpha)$ by an element $\phi \in \text{Hom}(P^i, A)$ annihilated by the coboundary map δ_*^i . Now ϕ is a collection of homomorphisms $\phi_\alpha : P^i \rightarrow A_\alpha$ each of which are mapped to 0 by δ_*^i , hence are of the form $\delta_*^{i-1}(\psi_\alpha)$ by assumption. The maps $\psi_\alpha : P^{i-1} \rightarrow A_\alpha$ may not be compatible with the maps in the inverse system, but for a fixed pair $\lambda < \mu$ the image of ψ_μ by the map $\rho_{\lambda\mu} : \text{Hom}(P^{i-1}, A_\mu) \rightarrow \text{Hom}(P^{i-1}, A_\lambda)$ differs from ψ_λ by an element $\tau_\lambda \in \ker(\delta_*^{i-1})$. Hence if for fixed μ we replace ϕ_λ by $\phi_\lambda + \tau_\lambda$ for all $\lambda < \mu$, we get by induction on μ an element $\psi \in \text{Hom}(P^{i-1}, \varprojlim A_\alpha)$ with $\delta_*^{i-1}(\psi) = \phi$. \square

Proof of Proposition 6.3.1: In view of the discussion preceding the proposition it will be enough to prove the first statement. For this it will be enough to establish isomorphisms $H^i(\text{Gal}(k'|k), k'[[t]]^\times) \cong H^i(\text{Gal}(k'|k), k'^\times)$, by definition of Galois cohomology. Consider for all $j > 0$ the multiplicative subgroups

$$U^j := 1 + t^j k'[[t]]$$

of $k'[[t]]^\times$. Sending t to 0 yields a natural exact sequence

$$1 \rightarrow U^1 \rightarrow k'[[t]]^\times \rightarrow k'^\times \rightarrow 1$$

whose associated long exact sequence shows that the proposition follows if we show $H^i(\text{Gal}(k'|k), U^1) = 0$ for all $i > 0$. For this, consider the exact sequences

$$1 \rightarrow U^{j+1} \rightarrow U^j \rightarrow k' \rightarrow 0$$

obtained by sending a power series in U^j to the coefficient of t^j . Here we have $H^i(\text{Gal}(k'|k), k') = 0$ for $i > 0$ by Lemma 4.3.11, so $H^i(\text{Gal}(k'|k), U^j/U^{j+1}) = 0$ for $i, j > 0$. By induction on j using the exact sequences

$$1 \rightarrow U^j/U^{j+1} \rightarrow U^1/U^{j+1} \rightarrow U^1/U^j \rightarrow 1$$

we obtain $H^i(\text{Gal}(k'|k), U^1/U^j) = 0$ for all $i > 0$ and $j > 0$. As U^1 is the inverse limit of the U^1/U^j , we conclude using the lemma above. \square

Remark 6.3.3 For k of characteristic 0 one can give a simpler proof of the proposition by remarking that U^1 is a divisible abelian group, and hence a \mathbf{Q} -vector space. This fact can be proven using Hensel's lemma (see Appendix, Proposition A.5.5). In characteristic $p > 0$, the group U^1 is only divisible by integers prime to p .

For $i = 2$ we get the Brauer group of k as the left term in the exact sequence of the proposition. In fact, in this case the middle term of the

sequence is none but the Brauer group of $k((t))$, if we assume moreover that k is perfect. To show this, let K_s be a separable closure of $k((t))$. There is a natural surjection $\text{Gal}(K_s|k((t))) \rightarrow G$ giving rise to inflation maps.

Proposition 6.3.4 *Assume moreover that k is perfect. Then the inflation maps*

$$\text{Inf} : H^i(G, k((t))_{nr}^\times) \rightarrow H^i(k((t)), K_s^\times)$$

are isomorphisms for all $i > 0$.

The key to the proof of the proposition is the following lemma.

Lemma 6.3.5 *Under the above assumptions the groups $H^i(k((t))_{nr}, K_s^\times)$ are trivial for $i > 0$. In particular, the Brauer group of $k((t))_{nr}$ vanishes.*

Proof: Since $k((t))_{nr}$ is a C_1 -field by Lang's theorem (Theorem 6.2.11), the lemma is a consequence of Propositions 6.2.3 and 6.1.2 for $i > 1$, and of Hilbert's Theorem 90 for $i = 1$. \square

Remarks 6.3.6

1. In characteristic 0 there is an easier proof of the lemma, because $\text{Gal}(K_s|k((t))_{nr}) \cong \widehat{\mathbf{Z}}$ by the same argument as in Example 4.1.6.
2. For two other proofs for the vanishing of $\text{Br}(k((t))_{nr})$, more traditional than the one given above, consult Serre [2], Chapter XII, §§1, 2.

Proof of Proposition 6.3.4: By the lemma, the condition for the exactness of the inflation-restriction sequence (Proposition 3.3.17 completed by Corollary 4.3.5) is satisfied, so we have for each $i > 0$ an exact sequence

$$0 \rightarrow H^i(G, k((t))_{nr}^\times) \xrightarrow{\text{Inf}} H^i(k((t)), K_s^\times) \xrightarrow{\text{Res}} H^i(k((t))_{nr}, K_s^\times).$$

Again by the lemma, the last group vanishes for $i > 0$, and the proposition follows. \square

Thus in the exact sequence of Proposition 6.3.1 we may replace the middle term by $H^i(k((t)), K_s^\times)$. As already indicated, the most important case is when $i = 2$, and we record it separately.

Corollary 6.3.7 (Witt) *For a perfect field k there is a split exact sequence*

$$0 \rightarrow \text{Br}(k) \rightarrow \text{Br}(k((t))) \rightarrow \text{Hom}_{\text{cont}}(G, \mathbf{Q}/\mathbf{Z}) \rightarrow 0 \quad (2)$$

induced by the residue map $r_v : \text{Br}(k((t))) \rightarrow \text{Hom}(G, \mathbf{Q}/\mathbf{Z})$.

Proof: The identification with Brauer groups follows from Theorem 4.4.7, and the isomorphism $H^1(G, \mathbf{Q}/\mathbf{Z}) \cong \text{Hom}_{\text{cont}}(G, \mathbf{Q}/\mathbf{Z})$ follows from Example 3.2.3 (1) by passing to the limit. \square

Remark 6.3.8 In terms of central simple algebras, the last corollary may be restated as follows: *Every central simple algebra over $k((t))$ is Brauer equivalent to a tensor product of the form $(A \otimes_k k((t))) \otimes_{k((t))} (\chi, t)$, where A is a central simple algebra over k , and (χ, t) is a cyclic algebra over $k((t))$ for some character $\chi : G \rightarrow \mathbf{Q}/\mathbf{Z}$.* This statement follows from the corollary above and the observation that the section of exact sequence (2) coming from the splitting $\mathbf{Z} \rightarrow k((t))_{nr}^\times, 1 \mapsto t$ of the valuation map is given by $\chi \mapsto (\chi, t)$. We leave the easy verification to the readers.

We now focus on the important special case of a finite base field.

Proposition 6.3.9 (Hasse) *Let \mathbf{F} be a finite field. Then we have a canonical isomorphism*

$$\text{Br}(\mathbf{F}((t))) \cong \mathbf{Q}/\mathbf{Z}.$$

Moreover, for a finite separable extension $L|\mathbf{F}((t))$ we have commutative diagrams

$$\begin{array}{ccc} \text{Br}(L) & \xrightarrow{\cong} & \mathbf{Q}/\mathbf{Z} & & \text{Br}(\mathbf{F}((t))) & \xrightarrow{\cong} & \mathbf{Q}/\mathbf{Z} \\ \text{Cor} \downarrow & & \downarrow \text{id} & \text{and} & \text{Res} \downarrow & & \downarrow [L:\mathbf{F}((t))] \\ \text{Br}(\mathbf{F}((t))) & \xrightarrow{\cong} & \mathbf{Q}/\mathbf{Z} & & \text{Br}(L) & \xrightarrow{\cong} & \mathbf{Q}/\mathbf{Z}, \end{array}$$

where the right vertical map in the second diagram is multiplication by the degree $[L : \mathbf{F}((t))]$.

The map inducing the isomorphism $\text{Br}(\mathbf{F}((t))) \cong \mathbf{Q}/\mathbf{Z}$ is classically called the *Hasse invariant map*.

Proof: The first statement results from Corollary 6.3.7, taking into account that $\text{Br}(\mathbf{F}) = 0$ (Example 6.1.11) and $\text{Hom}_{\text{cont}}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) \cong \mathbf{Q}/\mathbf{Z}$. For the second statement, note first that it is enough to verify the commutativity of the second diagram, in view of the formula $\text{Cor} \circ \text{Res} = [L : \mathbf{F}((t))]$ (Proposition 4.2.10). Next, observe that we may write L in the form $L = \mathbf{F}'((u))$ with some finite extension $\mathbf{F}'|\mathbf{F}$ and parameter u . It will then be enough to treat the case of the extensions $\mathbf{F}'((t))|\mathbf{F}((t))$ and $\mathbf{F}'((u))|\mathbf{F}'((t))$ separately. This follows from the fact that the composition of restriction (resp. corestriction) maps is again a restriction (resp. corestriction) map, as one sees directly

from the definition. For the extension $\mathbf{F}'((t))|\mathbf{F}((t))$, the commutativity of the second diagram follows from that of the diagram

$$\begin{array}{ccc} H^1(\mathbf{F}', \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\cong} & \mathbf{Q}/\mathbf{Z} \\ \text{Cor} \downarrow & & \downarrow \text{id} \\ H^1(\mathbf{F}, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\cong} & \mathbf{Q}/\mathbf{Z} \end{array}$$

whose commutativity results from the definition of corestriction maps. In the case of the extension $\mathbf{F}'((u))|\mathbf{F}'((t))$, the corestriction map on Brauer groups induces the identity on $H^1(\mathbf{F}', \mathbf{Q}/\mathbf{Z})$, whence the required commutativity is obvious. \square

We finally describe central simple algebras over $\mathbf{F}((t))$.

Proposition 6.3.10 *Every central simple algebra over $\mathbf{F}((t))$ is isomorphic to a cyclic algebra, and its period equals its index.*

Proof: Let A be a central simple algebra of degree n over $\mathbf{F}((t))$. By Remark 6.3.8 and the triviality of $\text{Br}(F)$ it is Brauer equivalent to the cyclic algebra (χ, t) , where $\chi \in \text{Hom}(\widehat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) \cong \mathbf{Q}/\mathbf{Z}$ is the character defining the Hasse invariant of A . The order d of χ in \mathbf{Q}/\mathbf{Z} is the period of A , and the fixed field \mathbf{F}_χ of $\ker(\chi)$ is a degree d extension of \mathbf{F} such that $\mathbf{F}_\chi((t))$ splits (χ, t) and *a fortiori* A . Thus by Proposition 4.5.8 the index of A divides d , so it must be actually equal to d by Proposition 4.5.13 (1), whence the second statement. The first statement then follows from Proposition 4.7.6, for A is split by $\mathbf{F}'((t))$, where $\mathbf{F}' \supset \mathbf{F}$ is a degree n cyclic extension containing \mathbf{F}_χ . \square

Remark 6.3.11 The results of this section (with basically the same proofs) are valid more generally for complete discrete valuation fields with perfect residue field. See Serre [2], Chapter XII, §3.

6.4 Cohomology of Function Fields of Curves

Let k again be a *perfect* field and C a smooth projective curve over k with function field K . We choose an algebraic closure \bar{k} of k , and denote by G the Galois group $\text{Gal}(\bar{k}|k)$. We denote the curve $C \times_k \bar{k}$ (which is assumed to be connected) by \bar{C} ; its function field is by definition the composite $K\bar{k}$.

We shall investigate the cohomology of G with values in the multiplicative group $(K\bar{k})^\times$. As in Chapter 5, Section 5.4, the key tool for this will be the exact

sequence of G -modules

$$0 \rightarrow \bar{k}^\times \rightarrow (K\bar{k})^\times \xrightarrow{\text{div}} \text{Div}(\bar{C}) \rightarrow \text{Pic}(\bar{C}) \rightarrow 0, \quad (3)$$

but we shall go further in the associated long exact sequences this time. There is a similar exact sequence over k :

$$0 \rightarrow k^\times \rightarrow K^\times \xrightarrow{\text{div}} \text{Div}(C) \rightarrow \text{Pic}(C) \rightarrow 0. \quad (4)$$

This sequence exists in arbitrary dimension, but our assumption that C is a curve makes it possible to define a *degree map*

$$\text{deg} : \text{Div}(C) \rightarrow \mathbf{Z}$$

associating to a divisor $\sum_P m_P P$ the integer $\sum_P m_P [\kappa(P) : k]$ (not to be confused with the degree map used in Chapter 5, Section 5.4). It is a fundamental fact (see Appendix, Proposition A.4.6) that the image of the divisor map $\text{div} : K^\times \rightarrow \text{Div}(C)$ is contained in the kernel $\text{Div}^0(C)$ of the degree map, so we have an induced map $\text{deg} : \text{Pic}(C) \rightarrow \mathbf{Z}$. We denote its kernel by $\text{Pic}^0(C)$.

One can decompose the group $\text{Div}(\bar{C})$ into G -orbits as follows. For each closed point P , the group G permutes the closed points lying over P (Appendix, Proposition A.6.3 (1) and Example A.6.2). Therefore we get a direct sum decomposition

$$\text{Div}(\bar{C}) = \bigoplus_{P \in C_0} \left(\bigoplus_{Q \mapsto P} \mathbf{Z} \right), \quad (5)$$

where C_0 denotes the set of closed points of C , and the notation $Q \mapsto P$ stands for the closed points Q of \bar{C} lying over P .

Hence for each $i \geq 0$ the divisor map induces maps

$$H^i(G, (K\bar{k})^\times) \rightarrow H^i(G, \text{Div}(\bar{C})) \xrightarrow{\sim} \bigoplus_{P \in C_0} H^i\left(G, \bigoplus_{Q \mapsto P} \mathbf{Z}\right), \quad (6)$$

as cohomology commutes with direct sums (more generally, with direct limits; see Lemma 4.3.3 and its proof).

To proceed further, we need a lemma. Fix a preimage Q_0 of P in \bar{C} and denote by G_P the stabilizer of Q_0 in G ; it is an open subgroup of G depending on Q_0 only up to conjugation.

Lemma 6.4.1 *We have an isomorphism of G -modules $M_{G_P}^G(\mathbf{Z}) \cong \bigoplus_{Q \mapsto P} \mathbf{Z}$.*

Proof: By definition of $M_{G_P}^G(\mathbf{Z})$, we have to construct an isomorphism

$$\mathrm{Hom}_{G_P}(\mathbf{Z}[G], \mathbf{Z}) \xrightarrow{\sim} \bigoplus_{Q \mapsto P} \mathbf{Z}.$$

For this, choose a system of left coset representatives $1 = \sigma_1, \dots, \sigma_r$ of G modulo G_P . The map $\phi \mapsto \phi(\sigma_1), \dots, \phi(\sigma_r)$ induces an isomorphism

$$\mathrm{Hom}_{G_P}(\mathbf{Z}[G], \mathbf{Z}) \xrightarrow{\sim} \bigoplus_{i=1}^r \mathbf{Z},$$

which does not depend on the choice of the system $\{\sigma_1, \dots, \sigma_r\}$, as ϕ is a G_P -homomorphism. So it will be enough to identify the right hand side with the sum indexed by the set $\{Q \mapsto P\}$ of points of \overline{C} lying above P . But as G acts transitively on $\{Q \mapsto P\}$ (see Appendix, Proposition A.6.3 (1) and Example A.6.2), and G_P is the stabilizer of Q_0 , the map $\sigma_i \mapsto \sigma_i(Q)$ is a bijection between the sets $\{\sigma_1, \dots, \sigma_r\}$ and $\{Q \mapsto P\}$. \square

By Shapiro's lemma (Remark 4.2.9) and the lemma above, we may rewrite the maps (6) as

$$H^i(G, (K\bar{k})^\times) \rightarrow \bigoplus_{P \in C_0} H^i(G_P, \mathbf{Z}).$$

Furthermore, the exact sequence $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Q} \rightarrow \mathbf{Q}/\mathbf{Z} \rightarrow 0$ induces isomorphisms $H^i(G_P, \mathbf{Z}) \cong H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z})$ for $i \geq 2$, as in the previous section. So finally we get for each $i \geq 2$ and $P \in C_0$ a map

$$r_P : H^i(G, (K\bar{k})^\times) \rightarrow H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z}),$$

called the *residue map associated with P* . By construction, for fixed i these maps are trivial for all but finitely many P . In order to get honest maps, we still have to prove:

Lemma 6.4.2 *The maps r_P depend only on P , and not on the closed point Q_0 lying above P used in the previous lemma.*

Proof: As G acts transitively on the set $\{Q \mapsto P\}$, if we work with another point Q' instead of Q_0 , we may find an element $\tau \in G$ with $Q' = \tau(Q_0)$. The stabilizer of Q' then will be $\tau G_P \tau^{-1}$. So an inspection of the previous construction reveals that is enough to see that the maps $H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z}) \rightarrow H^{i-1}(\tau G_P \tau^{-1}, \mathbf{Q}/\mathbf{Z})$ induced by the natural map $\mathbf{Z}[G_P] \rightarrow \mathbf{Z}[\tau G_P \tau^{-1}]$ on cohomology became identity maps after identification of G_P with $\tau G_P \tau^{-1}$,

which in turn is an immediate consequence of the construction of group cohomology. \square

The relation of the above residue maps with those of the previous section is as follows. As C is a smooth curve, the completion of the local ring of C at P is isomorphic to a formal power series ring $\kappa(P)[[t]]$ (see Appendix, Proposition A.5.3). By our assumption that k is perfect, here \bar{k} is a separable closure of $\kappa(P)$, with $\text{Gal}(\bar{k}|\kappa(P)) \cong G_P$. The construction of the previous section therefore yields residue maps $r_v : H^i(G_P, \kappa(P)((t))_{nr}^\times) \rightarrow H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z})$.

Proposition 6.4.3 *The diagram*

$$\begin{array}{ccc} H^i(G, (K\bar{k})^\times) & \xrightarrow{r_P} & H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z}) \\ \text{Res} \downarrow & & \uparrow r_v \\ H^i(G_P, (K\bar{k})^\times) & \longrightarrow & H^i(G_P, \kappa(P)((t))_{nr}^\times) \end{array}$$

commutes, where the bottom map is induced by the inclusion $K\bar{k} \hookrightarrow \bar{k}((t))$ coming from completing the local ring of a point of \bar{C} above P .

Proof: By Shapiro's lemma and Lemma 6.4.1, we have a chain of isomorphisms

$$H^i(G_P, (K\bar{k})^\times) \cong H^i(G, M_{G_P}^G(K\bar{k})^\times) \cong \bigoplus_{Q \mapsto P} H^i(G, (K\bar{k})^\times),$$

and the restriction map in the diagram is induced by taking a component of the direct sum corresponding to a point above P , say Q_0 . The component of the divisor map associated with Q_0 is none but the discrete valuation $v_{Q_0} : (K\bar{k})^\times \rightarrow \mathbf{Z}$ corresponding to the local ring $\mathcal{O}_{\bar{C}, Q_0}$ of Q_0 . The Proposition now follows from the isomorphism $G_P \cong \text{Gal}(\bar{k}|\kappa(P))$ and the obvious fact that the discrete valuation induced on the completion $\bar{k}[[t]]$ of $\mathcal{O}_{\bar{C}, Q}$ is none but the usual valuation v of the power series ring. \square

The basic fact concerning residue maps is:

Theorem 6.4.4 (Residue Theorem) *With notations as above, consider the corestriction maps*

$$\text{Cor}_P : H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z}) \rightarrow H^{i-1}(G, \mathbf{Q}/\mathbf{Z})$$

for each closed point P . The sequence of morphisms

$$H^i(G, (K\bar{k})^\times) \xrightarrow{\oplus r_P} \bigoplus_{P \in C_0} H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\Sigma \text{Cor}_P} H^{i-1}(G, \mathbf{Q}/\mathbf{Z})$$

is a complex for all $i \geq 1$.

Proof: The long exact sequence associated with the exact sequence of G -modules

$$0 \rightarrow (K\bar{k})^\times / \bar{k}^\times \rightarrow \text{Div}(\bar{C}) \rightarrow \text{Pic}(\bar{C}) \rightarrow 0 \quad (7)$$

yields exact sequences

$$H^i(G, (K\bar{k})^\times / \bar{k}^\times) \rightarrow H^i(G, \text{Div}(\bar{C})) \rightarrow H^i(G, \text{Pic}(\bar{C}))$$

for each i . By construction, the direct sum of the maps r_P is obtained by composing the natural map $H^i(G, (K\bar{k})^\times) \rightarrow H^i(G, (K\bar{k})^\times / \bar{k}^\times)$ with the first map in the above sequence, and then applying the chain of isomorphisms

$$H^i(G, \text{Div}(\bar{C})) \cong \bigoplus_{P \in C_0} H^i(G_P, \mathbf{Z}) \cong \bigoplus_{P \in C_0} H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z}).$$

On the other hand, the degree map $\text{deg} : \text{Pic}(\bar{C}) \rightarrow \mathbf{Z}$ induces a map $H^i(G, \text{Pic}(\bar{C})) \rightarrow H^i(G, \mathbf{Z})$. Therefore the theorem follows if we prove that the diagram

$$\begin{array}{ccc} H^i(G, \text{Div}(\bar{C})) & \longrightarrow & H^i(G, \text{Pic}(\bar{C})) \\ \cong \downarrow & & \downarrow \\ \bigoplus_{P \in C_0} H^i(G_P, \mathbf{Z}) & \xrightarrow{\Sigma \text{Cor}_P} & H^i(G, \mathbf{Z}) \end{array}$$

commutes. As the degree map $\text{Div}(\bar{C}) \rightarrow \mathbf{Z}$ factors through $\text{Pic}(\bar{C})$, it will be enough to show that the composite

$$H^i(G, \text{Div}(\bar{C})) \xrightarrow{\sim} \bigoplus_{P \in C_0} H^i(G_P, \mathbf{Z}) \xrightarrow{\Sigma \text{Cor}_P} H^i(G, \mathbf{Z})$$

equals the map induced by $\text{deg} : \text{Div}(\bar{C}) \rightarrow \mathbf{Z}$, or else, by decomposing $\text{Div}(\bar{C})$ as in (5), that the composite

$$H^i\left(G, \bigoplus_{Q \rightarrow P} \mathbf{Z}\right) \xrightarrow{\sim} H^i(G_P, \mathbf{Z}) \xrightarrow{\text{Cor}_P} H^i(G, \mathbf{Z})$$

equals the map induced by $(m_1, \dots, m_r) \mapsto \sum m_i$. But by Lemma 6.4.1 we may rewrite the above composite map as

$$H^i(G, M_{G_P}^G(\mathbf{Z})) \rightarrow H^i(G, \mathbf{Z}),$$

the map being induced by summation according to the definition of corestriction maps. This finishes the verification of commutativity. \square

In special cases we can say more. The most important of these is when C is the projective line. Then K is a rational function field $k(t)$, and we have the following stronger statement.

Theorem 6.4.5 (Faddeev) *Assume that C is the projective line. Then for each $i \geq 1$ the sequence*

$$0 \rightarrow H^i(G, \bar{k}^\times) \rightarrow H^i(G, (K\bar{k})^\times) \xrightarrow{\oplus_{rP}} \bigoplus_{P \in \mathbf{P}_0^1} H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\Sigma \text{Cor}_P} H^{i-1}(G, \mathbf{Q}/\mathbf{Z}) \rightarrow 0$$

is exact.

Proof: For $\bar{C} = \mathbf{P}^1$ the degree map $\text{deg} : \text{Pic}(\bar{C}) \rightarrow \mathbf{Z}$ is an isomorphism, hence exact sequence (7) takes the form

$$0 \rightarrow (K\bar{k})^\times / \bar{k}^\times \rightarrow \text{Div}(\bar{C}) \rightarrow \mathbf{Z} \rightarrow 0.$$

Moreover, the choice of a rational point of C (say 0) defines a G -equivariant splitting $\mathbf{Z} \rightarrow \text{Div}(\bar{C})$ of the above exact sequence, so that the sequence

$$0 \rightarrow H^i(G, (K\bar{k})^\times / \bar{k}^\times) \rightarrow H^i(G, \text{Div}(\bar{C})) \xrightarrow{\text{deg}_*} H^i(G, \mathbf{Z}) \rightarrow 0 \quad (8)$$

is (split) exact for all i (see Remark 4.3.4 (2)). We have seen in the proof of Theorem 6.4.4 that here for $i \geq 1$ the map deg_* can be identified with the map

$$\bigoplus_{P \in C_0} H^{i-1}(G_P, \mathbf{Q}/\mathbf{Z}) \rightarrow H^{i-1}(G, \mathbf{Q}/\mathbf{Z})$$

given by the sum of corestrictions. Hence to conclude the proof it will be enough to establish exact sequences

$$0 \rightarrow H^i(G, \bar{k}^\times) \rightarrow H^i(G, (K\bar{k})^\times) \rightarrow H^i(G, (K\bar{k})^\times / \bar{k}^\times) \rightarrow 0 \quad (9)$$

for all $i \geq 1$. For this, consider the exact sequence

$$0 \rightarrow \bar{k}^\times \rightarrow (K\bar{k})^\times \rightarrow (K\bar{k})^\times / \bar{k}^\times \rightarrow 0$$

of G -modules. We claim that in the associated long exact sequence

$$\dots \rightarrow H^i(G, \bar{k}^\times) \xrightarrow{\alpha_i} H^i(G, (K\bar{k})^\times) \rightarrow H^i(G, (K\bar{k})^\times / \bar{k}^\times) \rightarrow H^{i+1}(G, \bar{k}^\times) \rightarrow \dots \quad (10)$$

the maps $\alpha_i : H^i(G, \bar{k}^\times) \rightarrow H^i(G, (K\bar{k})^\times)$ are injective for $i \geq 1$. Indeed, the completion of the local ring at a k -rational point of \mathbf{P}_k^1 (say 0) is isomorphic to $\bar{k}[[t]]$ as a G -module, whence a sequence of G -equivariant embeddings $\bar{k}^\times \rightarrow K\bar{k}^\times \rightarrow \bar{k}((t))^\times$, the second one factoring through $k((t))_{nr}^\times$. The composite of the induced maps

$$H^i(G, \bar{k}^\times) \xrightarrow{\alpha_i} H^i(G, K\bar{k}^\times) \rightarrow H^i(G, k((t))_{nr}^\times)$$

is injective by Proposition 6.3.1, hence so is the map α_i . By this injectivity property the long exact sequence splits up into a collection of short exact sequences (9), as desired. \square

The case $i = 2$ is of particular importance because of the relation with the Brauer group.

Corollary 6.4.6 (Faddeev) *The sequence*

$$0 \rightarrow \mathrm{Br}(k) \rightarrow \mathrm{Br}(K) \xrightarrow{\oplus r_P} \bigoplus_{P \in \mathbf{P}_0^1} H^1(G_P, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\Sigma \mathrm{Cor}_P} H^1(G, \mathbf{Q}/\mathbf{Z}) \rightarrow 0$$

is exact.

Proof: The corollary follows from the case $i = 2$ of the theorem, once we show that $H^2(G, (K\bar{k})^\times) \cong \mathrm{Br}(K)$. This is established in the same way as the isomorphism $H^2(G, k((t))_{nr}^\times) \cong \mathrm{Br}(k((t)))$ in Proposition 6.3.4, except that we use Tsen's theorem instead of Lemma 6.3.5. \square

Remark 6.4.7 One may also derive Faddeev's exact sequence using methods of étale cohomology. See Milne [2], Example 2.22.

6.5 Application to Class Field Theory

We now investigate the particular case when the base field is finite, and combine the techniques of the last section with some nontrivial facts from algebraic geometry in order to derive the main results in the class field theory of function fields over finite fields, first obtained by Hasse using a different method.

Throughout this section, \mathbf{F} will denote a finite field, $G \cong \mathrm{Gal}(\bar{\mathbf{F}}|\mathbf{F})$ its absolute Galois group, and K the function field of a smooth projective curve C over \mathbf{F} . We shall continue to use some notations from the previous section.

Theorem 6.5.1 *The complex*

$$0 \rightarrow \mathrm{Br}(K) \xrightarrow{\oplus r_P} \bigoplus_{P \in C_0} H^1(G_P, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\Sigma \mathrm{Cor}_P} H^1(G, \mathbf{Q}/\mathbf{Z}) \rightarrow 0$$

coming from Theorem 6.4.4 is exact. Furthermore, we have $H^i(G, (K\bar{\mathbf{F}})^\times) = 0$ for $i \geq 3$.

Facts 6.5.2 The proof will use the following facts about curves over finite fields which we quote from the literature:

For a smooth projective curve C over a finite field \mathbf{F} , the group $\text{Pic}^0(\overline{C})$ is a torsion abelian group and the group $H^1(\mathbf{F}, \text{Pic}^0(\overline{C}))$ vanishes.

The first claim follows from the fact that $\text{Pic}^0(\overline{C})$ can be identified with the group $J(\overline{\mathbf{F}})$ of $\overline{\mathbf{F}}$ -points of an abelian variety J defined over \mathbf{F} , the *Jacobian* of C (see e.g. Milne [4]). Being a projective variety, J has only a finite number of points over each finite extension $\mathbf{F}'|\mathbf{F}$ of the finite field \mathbf{F} , and the group $J(\overline{\mathbf{F}})$ is the union of the $J(\mathbf{F}')$, so it is a torsion abelian group. The second fact is a theorem of Lang [2]: for an abelian variety A (in fact, for any connected algebraic group) over a finite field \mathbf{F} the group $H^1(\mathbf{F}, A(\overline{\mathbf{F}}))$ vanishes. This holds in particular for J .

As a first step towards the proof of the theorem, we derive the following classical lemma.

Lemma 6.5.3 (F. K. Schmidt) *Let C be a smooth projective curve over a finite field \mathbf{F} . Then the degree map $\text{deg} : \text{Div}(C) \rightarrow \mathbf{Z}$ is surjective.*

Proof: As the degree map factors through $\text{Pic}(C)$, it will be enough to consider the induced map $\text{Pic}(C) \rightarrow \mathbf{Z}$. The sequence

$$0 \rightarrow \text{Pic}^0(\overline{C}) \longrightarrow \text{Pic}(\overline{C}) \xrightarrow{\text{deg}} \mathbf{Z} \rightarrow 0 \quad (11)$$

is an exact sequence of G -modules. In the piece

$$\text{Pic}(\overline{C})^G \xrightarrow{\text{deg}} \mathbf{Z} \rightarrow H^1(G, \text{Pic}^0(\overline{C}))$$

of the corresponding long exact sequence the last term vanishes by Lang's theorem recalled above, so it remains to identify the group $\text{Pic}(\overline{C})^G$ with $\text{Pic}(C)$. For this, consider the long exact sequence

$$0 \rightarrow ((K\overline{\mathbf{F}})^\times / \overline{\mathbf{F}}^\times)^G \rightarrow \text{Div}(\overline{C})^G \rightarrow \text{Pic}(\overline{C})^G \rightarrow H^1(G, (K\overline{\mathbf{F}})^\times / \overline{\mathbf{F}}^\times)$$

coming from (7) applied with $k = \mathbf{F}$. In the long exact sequence (10) (again with $k = \mathbf{F}$) the terms vanish for $i > 1$ since $\text{cd}(\mathbf{F}) = 1$, and so do the the terms $H^1(G, \overline{\mathbf{F}}^\times)$ and $H^1(G, (K\overline{\mathbf{F}})^\times)$, by Hilbert's Theorem 90. Therefore the map $K^\times \rightarrow ((K\overline{\mathbf{F}})^\times / \overline{\mathbf{F}}^\times)^G$ is surjective and the group $H^1(G, (K\overline{\mathbf{F}})^\times / \overline{\mathbf{F}}^\times)$ is trivial, so $\text{Pic}(\overline{C})^G$ gets identified with the quotient $\text{Div}(\overline{C})^G / K^\times$. Now Lemma 6.4.1 gives $\text{Div}(\overline{C}) \cong M^G(\text{Div}(C))$, from which

the equality $\text{Div}(\overline{C})^G = \text{Div}(C)$ follows by the case $i = 0$ of Shapiro's lemma. \square

Proof of Theorem 6.5.1: As $\text{cd}(\mathbf{F}) = 1$, the second statement follows from Proposition 6.1.2. Granted the Facts 6.5.2 above, the proof of the case $i = 2$ is very similar to that of Theorem 6.4.5. The point is that the groups $H^i(G, \text{Pic}^0(\overline{C}))$ are trivial for $i > 0$; for $i = 1$ this is just Lang's theorem, and for $i > 1$ it results from the fact that $\text{Pic}^0(\overline{C})$ is torsion, in view of $\text{cd}(k) \leq 1$. Now in the piece

$$H^i(G, \text{Pic}^0(\overline{C})) \rightarrow H^i(G, \text{Pic}(\overline{C})) \rightarrow H^i(G, \mathbf{Z}) \rightarrow H^{i+1}(G, \text{Pic}^0(\overline{C}))$$

of the long exact sequence associated with (11) the first and last groups are trivial for $i > 0$. Hence in the piece

$$\begin{aligned} H^1(G, \text{Div}(\overline{C})) &\xrightarrow{\beta_1} H^1(G, \text{Pic}(\overline{C})) \rightarrow H^2(G, (K\overline{\mathbf{F}})^\times / \overline{\mathbf{F}}^\times) \rightarrow \\ &\longrightarrow H^2(G, \text{Div}(\overline{C})) \xrightarrow{\beta_2} H^2(G, \text{Pic}(\overline{C})) \rightarrow 0 \end{aligned}$$

of the long exact sequence associated with (7) we may replace the groups $H^i(G, \text{Pic}(\overline{C}))$ by $H^i(G, \mathbf{Z})$ for $i = 1, 2$. By Lemma 6.5.3 the degree map $\text{Div}(\overline{C}) \rightarrow \mathbf{Z}$ has a G -equivariant section, so the map $H^1(G, \text{Div}(\overline{C})) \rightarrow H^1(G, \mathbf{Z})$ is a split surjection. We conclude that β_1 is surjective, and obtain an exact sequence

$$0 \rightarrow H^2(G, (K\overline{\mathbf{F}})^\times / \overline{\mathbf{F}}^\times) \longrightarrow H^2(G, \text{Div}(\overline{C})) \xrightarrow{\beta_2} H^2(G, \mathbf{Z}) \rightarrow 0.$$

As $H^i(G, \overline{\mathbf{F}}^\times) = 0$ for $i > 0$, the long exact sequence (10) yields an isomorphism $H^2(G, (K\overline{\mathbf{F}})^\times) \cong H^2(G, (K\overline{\mathbf{F}})^\times / \overline{\mathbf{F}}^\times)$, so we may replace $(K\overline{\mathbf{F}})^\times / \overline{\mathbf{F}}^\times$ by $(K\overline{\mathbf{F}})^\times$ in the left hand side group. Hence we arrive at the Brauer group of K as in Corollary 6.4.6. To conclude the proof, one identifies the map β_2 with the sum of corestrictions $\bigoplus H^1(G_P, \mathbf{Q}/\mathbf{Z}) \rightarrow H^1(G, \mathbf{Q}/\mathbf{Z})$, in the same way as in the proof of the Residue Theorem. \square

One can obtain a more classical formulation of the theorem as follows. Take the completion of the local ring of C at a closed point P and denote by K_P its fraction field. It is a Laurent series field over the residue field $\kappa(P)$, so Proposition 6.3.9 yields an isomorphism $\text{Br}(K_P) \cong \mathbf{Q}/\mathbf{Z}$ induced by the Hasse invariant map, which we denote here by inv_P . The theorem then implies the following statement, which can be regarded as the main theorem in the class field theory of curves over finite fields.

Corollary 6.5.4 (Hasse) *With assumptions and notations as above, we have an exact sequence*

$$0 \rightarrow \mathrm{Br}(K) \rightarrow \bigoplus_{P \in C_0} \mathrm{Br}(K_P) \xrightarrow{\Sigma \mathrm{inv}_P} \mathbf{Q}/\mathbf{Z} \rightarrow 0.$$

Proof: This follows from the theorem and the discussion above, noting the compatibility of Proposition 6.4.3 and the second commutative diagram of Proposition 6.3.9. \square

Remark 6.5.5 Using the above corollary and the function field analogue of the so-called Grunwald-Wang theorem, one proves, following Hasse, that a central simple algebra A over K is cyclic and its period equals its index (see Weil [3]). Note a subtle point here: though we know by Corollary 6.2.10 that A is split by a cyclic extension of the base field \mathbf{F} , in general the degree of such an extension is larger than the degree n of A . But in order to apply Proposition 4.7.6 one needs a cyclic splitting field of degree n . Therefore in general the required cyclic extension does not come from the base field, and our method based on Tsen's theorem does not apply.

Remark 6.5.6 According to the celebrated theorem of Albert, Brauer, Hasse and Noether, there is an exact sequence like the one in Corollary 6.5.4 above also in the case when K is a *number field*, i.e. a finite extension of \mathbf{Q} . Here the fields K_P run over all completions of K with respect to its (inequivalent) valuations. As opposed to the geometric case discussed above, these may be of two types. Either they are discrete valuations coming from some prime ideal in the ring of integers; in these cases an invariant map for the Brauer group similar to that in Proposition 6.3.9 can be constructed according to a theorem of Hasse. But there also exist so-called archimedean valuations, for which the completion is isomorphic to \mathbf{R} or \mathbf{C} . The Brauer groups of these fields are respectively $\mathbf{Z}/2\mathbf{Z}$ and 0 , and thus may be viewed as subgroups of \mathbf{Q}/\mathbf{Z} , yielding the 'archimedean invariant maps' in the sequence. The proof of this theorem is different from the one given above, and uses the main results of class field theory for number fields. See e.g. Tate [2] or Neukirch-Schmidt-Wingberg [1]. Using this result, Brauer, Hasse and Noether also proved that over a number field every central simple algebra is cyclic, and its period equals its index. See Kersten [1], Pierce [1] or Roquette [4] for recent accounts of the proof.

These famous theorems were found a few years earlier than the geometric statements we have discussed above, but from today's viewpoint the latter are easier to establish thanks to the geometric techniques which are unavailable in the arithmetic case.

6.6 Application to the Rationality Problem: The Method

In this section we show how an application of Faddeev's exact sequence yields a simple answer to a long-standing problem in algebraic geometry. The question may be stated in purely algebraic terms as follows.

Problem 6.6.1 *Let k be a field, and $k(t_1, \dots, t_n)$ a purely transcendental extension of k . Let $k \subset K \subset k(t_1, \dots, t_n)$ be a subfield such that $k(t_1, \dots, t_n)|K$ is a finite extension. Is it true that $K|k$ is a purely transcendental extension?*

Remarks 6.6.2

1. In the language of algebraic geometry, the problem may be rephrased as follows. A k -variety X of dimension n is called *rational (over k)* if it is birational over k to projective n -space \mathbf{P}_k^n ; it is *unirational* if there exists a dominant rational map $\mathbf{P}_k^n \rightarrow X$ over k . So the question is: *is every unirational k -variety rational?*
2. *Positive results.* When $n = 1$, the answer is yes, by a classical theorem due to Lüroth (see e.g. van der Waerden [1], §73). For this reason, the problem is sometimes called the Lüroth problem in the literature. In the case $n = 2$ counterexamples can be given if the ground field k is not assumed to be algebraically closed (see the Exercises). However, when k is algebraically closed of characteristic 0, it follows from a famous theorem of Castelnuovo in the classification of surfaces (see e.g. Beauville [1], Chapter V) that the answer is positive. Zariski showed that the answer is also positive for k algebraically closed of characteristic $p > 0$ if one assumes the extension $K|K_0$ to be separable.
3. *Negative results.* Castelnuovo's theorem dates back to 1894. However, after some false starts by Fano and Roth, the first counterexamples showing that the answer may be negative over $k = \mathbf{C}$ in dimension 3 have only been found around 1970, by Clemens-Griffiths [1] and Iskovskih-Manin [1], independently. Immediately afterwards, Artin and Mumford [1] found counterexamples which could be explained by the nonvanishing of a certain *birational invariant* (i.e. an element of some group associated functorially to varieties and depending only on the birational isomorphism class of the variety) which is trivial for projective space. The group in question was the torsion part of the cohomology group $H^3(X, \mathbf{Z})$.

Still, even the counterexamples cited above did not rule out the possibility that the answer to the following weaker question might be positive. Observe

that a purely transcendental field extension $k(t_1, \dots, t_n)$ of k may be identified with the field of rational functions on an n -dimensional k -vector space V (by looking at V as affine n -space \mathbf{A}^n over k , or by passing to the tensor algebra of V). If a finite group G acts k -linearly on V , there is an induced action on the field $k(V)$. The action is called *faithful* if the homomorphism $G \rightarrow \mathrm{GL}(V)$ is injective. In this case the field extension $k(V)|k(V)^G$ is Galois with group G .

Problem 6.6.3 *Let k be an algebraically closed field of characteristic 0 and let V be a finite dimensional vector space over k . Assume that a finite group G acts k -linearly and faithfully on V . Is it true that the field of invariants $k(V)^G$ is a purely transcendental extension of k ?*

In his 1984 paper [2] Saltman showed that the answer to even this weaker question is negative in general. His approach, which was inspired by that of Artin and Mumford, but much more elementary, was developed further in works of Bogomolov ([1] and [2]). Our account below has been influenced by the notes of Colliot-Thélène and Sansuc [1].

The starting point for the construction of the counterexample is the consideration of the following invariant. Let $K|k$ be an extension of fields of characteristic 0, and $A \supset k$ a discrete valuation ring with fraction field K . The completion of K is isomorphic to a Laurent series field $\kappa((t))$, where κ is the residue field of A (see Appendix, Proposition A.5.3). Note that if the transcendence degree of $K|k$ is at least 2, then the extension $\kappa|k$ is transcendental. Let $\bar{\kappa}$ be an algebraic closure of κ . As in Section 6.3, we have a residue map

$$r_A : H^2(\mathrm{Gal}(\bar{\kappa}|\kappa), \kappa((t))_{nr}^\times) \rightarrow H^1(\kappa, \mathbf{Q}/\mathbf{Z})$$

induced by the valuation associated with A . As $\mathrm{Br}(\kappa((t))_{nr})$ is trivial, the inflation-restriction sequence shows as in the proof of Proposition 6.3.4 that we may identify the Brauer group of $\kappa((t))$ with $H^2(\mathrm{Gal}(\bar{\kappa}|\kappa), \kappa((t))_{nr}^\times)$, so we get a composite map

$$\mathrm{Br}(K) \rightarrow \mathrm{Br}(\kappa((t))) \rightarrow H^1(\kappa, \mathbf{Q}/\mathbf{Z})$$

which we also denote by r_A .

Definition 6.6.4 The intersection $\bigcap \ker(r_A) \subset \mathrm{Br}(K)$ of the groups $\ker(r_A)$ for all discrete valuation rings of $K|k$ is called the *unramified Brauer group* of $K|k$ and denoted by $\mathrm{Br}_{nr}(K)$.

Though not reflected in the notation, one should bear in mind that $\mathrm{Br}_{nr}(K)$ is an invariant which is relative to k . Of course, an analogous

definition can be made for the higher cohomology groups of \bar{k}^\times ; the proofs of the basic properties established below carry over without change.

In the case when K is the function field of a variety X defined over k , we may view $\text{Br}_{\text{nr}}(K)$ as an invariant attached to X . As it depends only on K , it is a *birational invariant* in the sense explained above. We now have the following functorial property.

Lemma 6.6.5 *Given a field extension $L|K$, the natural map $\text{Br}(K) \rightarrow \text{Br}(L)$ sends the subgroup $\text{Br}_{\text{nr}}(K)$ into $\text{Br}_{\text{nr}}(L)$.*

Proof: Let B be a discrete valuation ring of $L|k$, with residue field κ_B . Its completion is isomorphic to $\kappa_B((t))$. If B contains K as a subfield, then we must have $K \subset \kappa_B$ in $\kappa_B((t))$ since the elements of K are units, and thus $K \subset \ker(r_B)$ by Corollary 6.3.7. Otherwise the intersection $A := B \cap K$ is a discrete valuation ring of $K|k$. Denoting by κ_A its residue field, we have a natural inclusion $\kappa_A \subset \kappa_B$. The associated valuations satisfy an equality $v_A = e \cdot v_B$ with some integer $e \geq 1$, for if t_A generates the maximal ideal of A , we have $t_A = ut^e$ for some unit u in B . The construction of residue maps then implies the commutativity of the diagram

$$\begin{array}{ccc} \text{Br}(\kappa_B((t))) & \xrightarrow{r_B} & H^1(\kappa_B, \mathbf{Q}/\mathbf{Z}) \\ \text{Res} \uparrow & & \uparrow e \cdot \text{Res} \\ \text{Br}(\kappa_A((t_A))) & \xrightarrow{r_A} & H^1(\kappa_A, \mathbf{Q}/\mathbf{Z}), \end{array}$$

whence $\ker(r_A) \subset \ker(r_B)$, and the lemma follows. \square

The following crucial proposition implies that purely transcendental extensions have trivial unramified Brauer group.

Proposition 6.6.6 *Let K be as above, and let $K(t)|K$ be a purely transcendental extension. Then the natural map $\text{Br}_{\text{nr}}(K) \rightarrow \text{Br}_{\text{nr}}(K(t))$ given by the previous lemma is an isomorphism.*

Proof: The map $\text{Br}(K) \rightarrow \text{Br}(K(t))$ is injective by Corollary 6.4.6, hence so is the map $\text{Br}_{\text{nr}}(K) \rightarrow \text{Br}_{\text{nr}}(K(t))$ by the previous lemma. Therefore it is enough to check surjectivity. For this take an $\alpha \in \text{Br}_{\text{nr}}(K(t))$. As α is in the kernel of all residue maps coming from valuations trivial on K , we have $\alpha \in \text{Br}(K)$, again by Corollary 6.4.6. It therefore remains to be seen that $r_A(\alpha) = 0$ for each discrete valuation ring A of $K|k$. But for such an A one may find a discrete valuation ring B of $K(t)|k$ with $B \cap K = A$, by continuing the discrete valuation v_A to a discrete valuation v_B on $K(t)$ via

setting $v_B(t) = 0$ (see Appendix, Proposition A.6.11). For the associated discrete valuations one has $e = 1$, and hence $\ker(r_B) \cap K \subset \ker(r_A)$ by the diagram of the previous proof. Since $\alpha \in \ker(r_B)$ by assumption, the claim follows. \square

We get by induction starting from the case $n = 1$ (Faddeev's theorem):

Corollary 6.6.7 *For a purely transcendental extension $k(t_1, \dots, t_m)$ of k one has*

$$\mathrm{Br}_{\mathrm{nr}} k(t_1, \dots, t_m) \cong \mathrm{Br}(k).$$

In particular, if k is algebraically closed, then $\mathrm{Br}_{\mathrm{nr}} k(t_1, \dots, t_m) = 0$.

We now turn to the construction of Bogomolov and Saltman. *In the rest of this section we assume that the base field is algebraically closed of characteristic 0.*

As an appetizer, we prove the following classical result of Fischer [1] which shows that in the counterexample to Problem 6.6.3 G must be noncommutative.

Theorem 6.6.8 (Fischer) *Assume that a finite abelian group A acts k -linearly and faithfully on a finite-dimensional k -vector space V . Then the field of invariants $k(V)^A$ is a purely transcendental extension of k .*

Proof: As we are in characteristic 0, the A -representation on V is semi-simple, i.e. the $k[A]$ -module V decomposes as a direct sum of 1-dimensional sub- $k[A]$ -modules V_i , such that on V_i the A -action is given by $\sigma(v) = \chi_i(\sigma)v$ for some character $\chi_i : A \rightarrow k^\times$. Let v_i be a nonzero vector in V_i for each i and let X be the subgroup of $k(V)^\times$ generated by the v_i . As the v_i are linearly independent, X is a free abelian group. Now let $\widehat{A} = \mathrm{Hom}(A, k^\times)$ be the character group of A and consider the homomorphism $\phi : X \rightarrow \widehat{A}$ given by $v_i \mapsto \chi_i$. By construction, we have $\sigma(x) = (\phi(x)(\sigma))x$ for $x \in X$ and $\sigma \in A$. In particular, with the notation $Y := \ker(\phi)$ we get $Y \subset k(V)^A$. On the other hand, the index of Y in X is at most $|\widehat{A}| = |A|$, so the field index $[k(V) : k(Y)]$ is at most $|A|$. But $[k(V) : k(V)^A] = |A|$, as this extension is Galois with group A . Thus we conclude $k(Y) = k(V)^A$. Now Y is a free abelian group, being a subgroup of X , and therefore we have $k(Y) = k(y_1, \dots, y_m)$ for a basis y_1, \dots, y_m of Y . This proves the theorem. \square

Remark 6.6.9 An examination of the above proof reveals that the theorem is valid more generally for an arbitrary finite abelian group A of exponent e and any ground field F of characteristic prime to e and containing the e -th

roots of unity. In the case of arbitrary F the field $F(V)^A$ will be the function field of an algebraic torus, not necessarily rational over F (see Voskresensky [2], §7.2).

This being said, Corollary 6.6.7 shows that in order to find a counterexample to Problem 6.6.3 it suffices to find a faithful representation V of a finite group G with $\text{Br}_{\text{nr}}(k(V)^G) \neq 0$. The key to this will be the following basic theorem characterising the unramified Brauer group of invariant fields.

Theorem 6.6.10 (Bogomolov) *Let V be a finite dimensional k -vector space, and let G be a finite group acting k -linearly and faithfully on V . Then*

$$\text{Br}_{\text{nr}}(k(V)^G) = \ker \left(\text{Br}(k(V)^G) \rightarrow \prod_{H \in \mathcal{B}} \text{Br}(k(V)^H) \right),$$

where \mathcal{B} denotes the set of bicyclic subgroups of G .

Recall that a bicyclic group is just a direct product of two cyclic groups.

Proof: By Lemma 6.6.5 the image of $\text{Br}_{\text{nr}}(k(V)^G)$ by each restriction map $\text{Br}(k(V)^G) \rightarrow \text{Br}(k(V)^H)$ lies in $\text{Br}_{\text{nr}}(k(V)^H)$. But since bicyclic groups are abelian, we have $\text{Br}_{\text{nr}}(k(V)^H) = 0$ by Fischer's theorem (Theorem 6.6.8) and Corollary 6.6.7. So we conclude that the left hand side is contained in the right hand side.

For the reverse inclusion, take an element $\alpha \in \text{Br}(k(V)^G)$ with $r_A(\alpha) \neq 0$ for some discrete valuation ring A of $k(V)^G|k$. Let B be one of the finitely many discrete valuation rings of $k(V)|k$ lying above A , let $D \subset G$ be the stabilizer of B under the action of G , and let κ_B and κ_A be the respective residue fields of B and A . As the finite extension $k(V)|k(V)^G$ is Galois, it is known (cf. Appendix, Proposition A.6.3 (2)) that the extension $\kappa_B|\kappa_A$ is a finite Galois extension as well, and there is a natural surjection $D \rightarrow \text{Gal}(\kappa_B|\kappa_A)$. Denote by I the kernel of this map. As κ_A is algebraically closed of characteristic 0, it is also known (see Appendix, Corollary A.6.10) that I is a central cyclic subgroup in D . If the image of α by the restriction map $\text{Res}_I : \text{Br}(k(V)^G) \rightarrow \text{Br}(k(V)^I)$ is nonzero, then so is its image by the map $\text{Br}(k(V)^G) \rightarrow \text{Br}(k(V)^H)$ for a bicyclic subgroup H containing the cyclic subgroup I , and we are done. So we may assume $\text{Res}_I(\alpha) = 0$. Now consider the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Br}(k(V)^I|k(V)^G) & \xrightarrow{\text{Inf}} & \text{Br}(k(V)^G) & \xrightarrow{\text{Res}} & \text{Br}(k(V)^I) \\ & & \downarrow & & \downarrow r_A & & \downarrow r_C \\ 0 & \longrightarrow & H^1(\text{Gal}(\kappa_B|\kappa_A), \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\text{Inf}} & H^1(\kappa_A, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\text{Res}} & H^1(\kappa_B, \mathbf{Q}/\mathbf{Z}) \end{array}$$

in which the rows are restriction-inflation sequences (Corollary 4.3.5), and the map r_C is the residue map associated with the discrete valuation ring $C := B \cap k(V)^I$ which has the same residue field κ_B as B . The diagram shows that α comes from an element of $\text{Br}(k(V)^I|k(V)^G)$ and $r_A(\alpha)$ may be identified with a homomorphism $\phi_\alpha : D/I \rightarrow \mathbf{Q}/\mathbf{Z}$. Let $g \in D$ be an element whose image \bar{g} in $\text{Gal}(\kappa_B|\kappa_A) \cong D/I$ satisfies $\phi_\alpha(\bar{g}) \neq 0$. As I is a central cyclic subgroup in D , the subgroup $H^g \subset D$ generated by g and I is bicyclic. We now show that the image of α by the restriction map $\text{Res}_{H^g} : \text{Br}(k(V)^G) \rightarrow \text{Br}(k(V)^{H^g})$ is nontrivial. Indeed, if we denote by B^g the discrete valuation ring $B \cap k(V)^{H^g}$, then the same argument as above with B^g in place of A shows that the image of $\text{Res}_{H^g}(\alpha)$ by the associated residue map r_{B^g} is some homomorphism $H^g/I \rightarrow \mathbf{Q}/\mathbf{Z}$. By construction, this homomorphism is none but the restriction of ϕ_α to the group H^g/I , and hence is nonzero. So $\text{Res}_{H^g}(\alpha)$ itself is nonzero, as required. \square

Remark 6.6.11 The above proof (together with Fischer's theorem) shows that instead of \mathcal{B} one could take the set of all *abelian* subgroups of G .

As a consequence of the preceding theorem, Bogomolov and Saltman were able to give a purely group-theoretic characterisation of $\text{Br}_{\text{nr}}(k(V)^G)$.

Theorem 6.6.12 *Let $k(V)$, G and \mathcal{B} be as in the theorem above.*

The group $\text{Br}_{\text{nr}}(k(V)^G)$ is canonically isomorphic to the group

$$H_{\mathcal{B}}^2(G) := \ker \left(H^2(G, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\text{Res}} \prod_{H \in \mathcal{B}} H^2(H, \mathbf{Q}/\mathbf{Z}) \right).$$

Proof: The proof is in three steps.

Step 1. We first establish an isomorphism

$$\text{Br}_{\text{nr}}(k(V)^G) = \ker \left(H^2(G, k(V)^\times) \rightarrow \prod_{H \in \mathcal{B}} H^2(H, k(V)^\times) \right).$$

For this, consider the inflation-restriction sequence

$$0 \rightarrow \text{Br}(k(V)|k(V)^G) \xrightarrow{\text{Inf}} \text{Br}(k(V)^G) \xrightarrow{\text{Res}} \text{Br}(k(V)).$$

of Corollary 4.4.11. As $\text{Br}_{\text{nr}}(k(V)) = 0$ by Corollary 6.6.7, we see using Lemma 6.6.5 that each element of $\text{Br}_{\text{nr}}(k(V)^G)$ comes from $\text{Br}(k(V)|k(V)^G)$. Using the fact that the composite map $\text{Br}(k(V)|k(V)^G) \rightarrow \text{Br}(k(V)^G) \rightarrow \text{Br}(k(V)^H)$ factors through $\text{Br}(k(V)|k(V)^H)$ and noting the isomorphism

$\text{Br}(k(V)|k(V)^G) \cong H^2(G, k(V)^\times)$, we may rewrite the formula of the previous theorem as stated above.

Step 2. We next show that we may replace the coefficient module $k(V)^\times$ by k^\times , i.e. we have an isomorphism

$$\text{Br}_{\text{nr}}(k(V)^G) = \ker \left(H^2(G, k^\times) \rightarrow \prod_{H \in \mathcal{B}} H^2(H, k^\times) \right).$$

For this we view $k(V)$ as the function field of affine n -space \mathbf{A}_k^n . As the Picard group of \mathbf{A}_k^n is trivial (cf. Appendix, Proposition A.4.4 (1)), we have an exact sequence of G -modules

$$0 \rightarrow k^\times \rightarrow k(V)^\times \rightarrow \text{Div}(\mathbf{A}_k^n) \rightarrow 0. \quad (12)$$

Denote by W the affine variety with coordinate ring $k[t_1, \dots, t_n]^G$. By exactly the same argument as in Lemma 6.4.1, we have a direct sum decomposition

$$\text{Div}(\mathbf{A}_k^n) \cong \bigoplus_{P \in W^1} M_{G_P}^G(\mathbf{Z}),$$

where W^1 denotes the set of codimension 1 irreducible subvarieties of W and G_P is the stabilizer of an irreducible component lying over the codimension 1 subvariety P . Therefore using Shapiro's lemma we get from sequence (12) an exact sequence

$$\bigoplus_{P \in W^1} H^1(G_P, \mathbf{Z}) \rightarrow H^2(G, k^\times) \xrightarrow{\pi} H^2(G, k(V)^\times) \xrightarrow{\rho} \bigoplus_{P \in W^1} H^2(G_P, \mathbf{Z}).$$

Here the groups $H^1(G_P, \mathbf{Z}) = \text{Hom}(G_P, \mathbf{Z})$ are trivial because the G_P are finite, so the map π is injective.

As for the groups $H^2(G_P, \mathbf{Z}) \cong H^1(G_P, \mathbf{Q}/\mathbf{Z}) = \text{Hom}(G_P, \mathbf{Q}/\mathbf{Z})$, we obviously have injections $\iota_P : \text{Hom}(G_P, \mathbf{Q}/\mathbf{Z}) \hookrightarrow \bigoplus \text{Hom}(\langle g \rangle, \mathbf{Q}/\mathbf{Z})$, where the sum is over all cyclic subgroups $\langle g \rangle$ of G_P . Now if the restrictions of an element $\alpha \in H^2(G, k(V)^\times)$ to all bicyclic subgroups are trivial, the same must be true for all restrictions to cyclic subgroups, so all components of $\rho(\alpha) \in \bigoplus \text{Hom}(G_P, \mathbf{Q}/\mathbf{Z})$ are sent to 0 by the various ι_P . Therefore $\rho(\alpha) = 0$ and α comes from $H^2(G, k^\times)$. The claim follows by noting that the maps $H^2(G, k^\times) \rightarrow H^2(H, k(V)^\times)$ factor through $H^2(H, k^\times)$.

Step 3. In view of the previous step, to prove the proposition it is enough to establish isomorphisms

$$H^2(G, k^\times) \cong H^2(G, \mathbf{Q}/\mathbf{Z}) \quad \text{and} \quad H^2(H, k^\times) \cong H^2(H, \mathbf{Q}/\mathbf{Z})$$

for all H . Now as k is algebraically closed of characteristic 0, the group k^\times is divisible and its torsion subgroup (i.e. the group of roots of unity in k) is isomorphic to \mathbf{Q}/\mathbf{Z} . Therefore the quotient $k^\times/(\mathbf{Q}/\mathbf{Z})$ is a \mathbf{Q} -vector space, so the long exact sequence coming from the exact sequence

$$0 \rightarrow \mathbf{Q}/\mathbf{Z} \rightarrow k^\times \rightarrow k^\times/(\mathbf{Q}/\mathbf{Z}) \rightarrow 0$$

of trivial G -modules yields the required isomorphisms in view of Corollary 4.2.7. \square

6.7 Application to the Rationality Problem: The Example

Keeping the assumptions and the notations of the previous section, we show at last:

Theorem 6.7.1 *There exists a finite group G for which $H_{\mathbb{R}}^2(G) \neq 0$. Therefore G yields a counterexample to Problem 6.6.3 over k .*

The proof below is based on an idea of Shafarevich [1]. The following lemma from the theory of group extensions will be a basic tool.

Lemma 6.7.2 *Let A, B be two abelian groups. Regard A as a B -module with trivial action.*

1. *There is a homomorphism*

$$\rho_A : H^2(B, A) \rightarrow \text{Hom}(\Lambda^2 B, A),$$

functorial in A , sending the class of an extension

$$0 \rightarrow A \rightarrow E \rightarrow B \rightarrow 0$$

to the map $\phi_E : b_1 \wedge b_2 \rightarrow [\tilde{b}_1, \tilde{b}_2]$, where the \tilde{b}_i are arbitrary liftings of the b_i to E , and $[\tilde{b}_1, \tilde{b}_2]$ denotes their commutator. The kernel of ρ_A consists of extension classes with E commutative.

2. *In terms of cocycles, the map ρ_A sends the class of a normalised 2-cocycle c_{b_1, b_2} to the alternating map $b_1 \wedge b_2 \mapsto c_{b_1, b_2} - c_{b_2, b_1}$.*
3. *Assume moreover that A and B are finite dimensional \mathbf{F}_p -vector spaces for a prime number $p > 2$. Then ρ_A has a canonical splitting.*

Here $\Lambda^2 B$ denotes the quotient of $B \otimes_{\mathbf{Z}} B$ by the subgroup generated by the elements $b \otimes b$ for all $b \in B$. Part (1) of the lemma can be proven using the universal coefficient sequence for cohomology (Weibel [1], Theorem 3.6.5); we give here a direct argument.

Proof: For (1), note first that since B acts trivially on A , the extension E is central, and therefore in the above definition $\phi_E(b_1, b_2) = [\tilde{b}_1, \tilde{b}_2]$ does not depend of the choice of the liftings \tilde{b}_1, \tilde{b}_2 . Moreover, ϕ_E satisfies $\phi_E(b, b) = 0$ for all $b \in B$; let us check that it is also bilinear. For this, let $s : B \rightarrow E$ be a (set-theoretic) section of the projection $E \rightarrow B$ satisfying $s(1) = 1$. As in Example 3.2.6 this yields the normalised 2-cocycle $c_{b_1, b_2} = s(b_1)s(b_2)s(b_1 + b_2)^{-1}$ of B with values in A . Recall also the formula $[g_1g_2, g_3] = g_1[g_2, g_3]g_1^{-1}[g_1, g_3]$ which holds in any group. Since A is central in E , we have

$$\begin{aligned} \phi_E(b_1 + b_2, b_3) &= [s(b_1 + b_2), s(b_3)] = [c_{b_1, b_2}^{-1}s(b_1)s(b_2), s(b_3)] = [s(b_1)s(b_2), s(b_3)] \\ &= s(b_1)[s(b_2), s(b_3)]s(b_1)^{-1}[s(b_1), s(b_3)] = \phi_E(b_2, b_3) + \phi_E(b_1, b_3). \end{aligned}$$

Similarly, $\phi_E(b_1, b_2 + b_3) = \phi_E(b_1, b_2) + \phi_E(b_1, b_3)$, so ϕ_E is a well-defined alternating bilinear map. To finish the proof of (1), it remains to check that ρ_A is a group homomorphism, because the second statement in (1) is then immediate from the definition of ρ_A . For this it is enough to establish (2), because the map $c_{b_1, b_2} \mapsto c_{b_1, b_2} - c_{b_2, b_1}$ is manifestly a homomorphism from the group of normalised 2-cocycles of B with values in A to the group $\text{Hom}(\Lambda^2 B, A)$. But for the 2-cocycle c_{b_1, b_2} associated with E above we have

$$\phi_E(b_1, b_2) = s(b_1)s(b_2)s(b_1)^{-1}s(b_2)^{-1} = c_{b_1, b_2}s(b_1 + b_2)s(b_2 + b_1)^{-1}c_{b_2, b_1}^{-1},$$

which is indeed $c_{b_1, b_2} - c_{b_2, b_1}$ in the additive notation.

We finally turn to (3). It will be enough to construct a splitting in the case $A = \mathbf{F}_p$. Recall from linear algebra that the space of bilinear forms splits as the direct sum of the spaces of symmetric and alternating forms via the map $\lambda \mapsto (\lambda + \lambda^\tau, \lambda - \lambda^\tau)$, where λ^τ is the bilinear form obtained from λ by switching the entries. Thus given an alternating bilinear form $\phi : \Lambda^2 B \rightarrow \mathbf{F}_p$, there exists a bilinear form $\gamma : B \times B \rightarrow \mathbf{F}_p$ such that

$$\phi(b_1 \wedge b_2) = \gamma(b_1, b_2) - \gamma(b_2, b_1).$$

Notice that the map $(b_1, b_2) \mapsto \gamma(b_1, b_2)$ is a normalised 2-cocycle, as we have $\gamma(0, b) = \gamma(b, 0) = 0$ for all $b \in B$, and the cocycle relation holds by the calculation

$$\gamma(b_2, b_3) - \gamma(b_1 + b_2, b_3) + \gamma(b_1, b_2 + b_3) - \gamma(b_1, b_2) = -\gamma(b_1, b_3) + \gamma(b_1, b_3) = 0.$$

The difference of two choices of γ is a symmetric bilinear form. But if γ is symmetric, then since $p > 2$, we may write

$$\gamma(b_1, b_2) = \frac{1}{2} \left(\gamma(b_1 + b_2, b_1 + b_2) - \gamma(b_1, b_1) - \gamma(b_2, b_2) \right) = (df)(b_1, b_2),$$

where f is the 1-cocycle $b \mapsto (1/2)\gamma(b, b)$ of B with values in the trivial B -module \mathbf{F}_p . Therefore the class $[\gamma]$ of the 2-cocycle $(b_1, b_2) \mapsto \gamma(b_1, b_2)$ in $H^2(B, \mathbf{F}_p)$ only depends on the alternating form ϕ , and we may define the map $\xi : \text{Hom}(\Lambda^2 B, \mathbf{F}_p) \rightarrow H^2(B, \mathbf{F}_p)$ by sending ϕ to $[\gamma]$. By (2), the map ξ satisfies $\rho_{\mathbf{F}_p} \circ \xi = \text{id}_{\mathbf{F}_p}$. \square

The lemma enables us to construct important examples of nilpotent groups.

Example 6.7.3 Let $p > 2$ be a prime number, and let V be an n -dimensional \mathbf{F}_p -vector space. Applying the canonical splitting constructed in part (3) of the above lemma for $B = V$, $A = \Lambda^2 V$, we get that the identity map of $\Lambda^2 V$ gives rise to an extension \overline{G}_n of V by $\Lambda^2 V$. Here $\Lambda^2 V$ is both the center and the commutator subgroup of the group \overline{G}_n , which is in particular nilpotent of class 2. It is the *universal nilpotent group of class 2 and exponent p on n generators*. Its elements can be written in the form $\prod_i a_i^{\alpha_i} \prod_{i < j} [a_i, a_j]^{\beta_{ij}}$, where a_1, \dots, a_n are liftings of a basis of V to G and $\alpha_i, \beta_{ij} \in \mathbf{F}_p$.

Proof of Theorem 6.7.1: Let $p > 2$ be a prime number, and consider the group \overline{G}_n of the above example for $n \geq 4$. Let a_1, \dots, a_n be a system of generators as above, and look at the element $z = [a_1, a_2][a_3, a_4]$. Note that z lies in the center $\Lambda^2 V$ of \overline{G}_n , and it has the property that the powers $z^r = [a_1, a_2]^r [a_3, a_4]^r$ cannot be expressed as commutators $[b_1, b_2]$ of elements $b_1, b_2 \in \overline{G}_n$ whose images in V are linearly independent over \mathbf{F}_p . Indeed, in $\Lambda^2 V$ the z^r correspond to bivectors of the form $r(v_1 \wedge v_2) + r(v_1 \wedge v_3)$, which are either trivial or indecomposable bivectors, i.e. not of the form $w_1 \wedge w_2$ for independent w_i .

Now define G as the quotient of \overline{G}_n by the central cyclic subgroup $\langle z \rangle$ generated by z . The conjugation action of G on $\langle z \rangle$ is trivial, hence it is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ as a G -module. The extension

$$1 \rightarrow \langle z \rangle \rightarrow \overline{G}_n \rightarrow G \rightarrow 1 \quad (13)$$

therefore defines a class $c(\overline{G}_n) \in H^2(G, \mathbf{Z}/p\mathbf{Z})$ by Example 3.2.6. We may send it to a class in $H^2(G, \mathbf{Q}/\mathbf{Z})$ via the map $\iota_* : H^2(G, \mathbf{Z}/p\mathbf{Z}) \rightarrow H^2(G, \mathbf{Q}/\mathbf{Z})$ induced by the inclusion $\iota : \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Q}/\mathbf{Z}$ sending 1 to $1/p$. Let us now show that $\iota_*(c(\overline{G}_n))$ lies in $H_{\mathbf{B}}^2(G)$. For this it will be enough to see that the images of $c(\overline{G}_n)$ by the restriction maps $H^2(G, \mathbf{Z}/p\mathbf{Z}) \rightarrow H^2(H, \mathbf{Z}/p\mathbf{Z})$ are trivial for each bicyclic subgroup $H \subset G$. Such a subgroup necessarily meets the center $Z(G)$ of G . Indeed, write $H = \langle h_1 \rangle \times \langle h_2 \rangle$ with some generators h_1, h_2 . As the h_i commute, we have $[h_1, h_2] = 1$ in G and so $[b_1, b_2] = z^k$ in \overline{G}_n for some $k \in \mathbf{F}_p$ and liftings b_i of the h_i in \overline{G}_n . By the choice of z made

above, the images of the b_i should be linearly dependent in $V \cong G/Z(G)$, which means precisely that $H \cap Z(G) \neq \{1\}$. Now as $Z(G)$ is the image of $\Lambda^2 V$ in G , this implies that the inverse image \overline{H} of H in \overline{G}_n is cyclic modulo $\overline{H} \cap (\Lambda^2 V)$, and thus it is a commutative subgroup. Moreover, it is an \mathbf{F}_p -vector space, because \overline{G}_n is of exponent p . But then the extension $1 \rightarrow \langle z \rangle \rightarrow \overline{H} \rightarrow H \rightarrow 1$ is an extension of \mathbf{F}_p -vector spaces and therefore a split extension. On the other hand, its class in $H^2(H, \mathbf{Z}/p\mathbf{Z})$ is precisely the image of $c(\overline{G}_n) \in H^2(G, \mathbf{Z}/p\mathbf{Z})$ by the restriction map to H , and we are done.

It remains to see that $i_*(c(\overline{G}_n))$ is a nontrivial class. For this, observe first that the extension (13) is nonsplit. Indeed, if it were, then since it is a central extension, we would get a direct product decomposition $\overline{G}_n \cong \langle z \rangle \times G$, which is impossible (e.g. because then z would not lie in the commutator subgroup of \overline{G}_n). Next we show that $c(\overline{G}_n)$ is the image of a class $c \in H^2(V, \mathbf{Z}/p\mathbf{Z})$ by the inflation map $\text{Inf} : H^2(V, \mathbf{Z}/p\mathbf{Z}) \rightarrow H^2(G, \mathbf{Z}/p\mathbf{Z})$. For this, decompose $\Lambda^2 V$ as a direct sum $\Lambda^2 V \cong \langle z \rangle \oplus W$, and define c as the class of the extension

$$1 \rightarrow \langle z \rangle \rightarrow G_z \rightarrow V \rightarrow 1 \quad (14)$$

obtained by pushforward from the extension $1 \rightarrow \Lambda^2 V \rightarrow \overline{G}_n \rightarrow V \rightarrow 1$ via the map $\Lambda^2 V \rightarrow \langle z \rangle$ sending W to 0 and z to itself. We leave it to the readers to check that the pullback of the extension (14) by the surjection $G \rightarrow V$ is indeed (13).

Now consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}(W, \mathbf{Z}/p\mathbf{Z}) & \longrightarrow & H^2(V, \mathbf{Z}/p\mathbf{Z}) & \xrightarrow{\text{Inf}} & H^2(G, \mathbf{Z}/p\mathbf{Z}) \\ & & \cong \downarrow & & \iota_* \downarrow & & \iota_* \downarrow \\ 0 & \longrightarrow & \text{Hom}(W, \mathbf{Q}/\mathbf{Z}) & \longrightarrow & H^2(V, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\text{Inf}} & H^2(G, \mathbf{Q}/\mathbf{Z}) \end{array}$$

whose exact rows come from Proposition 3.3.14 (noting the identifications $H^1(W, A)^V \cong \text{Hom}(W, A)$ for G -modules A with trivial action). Here the left vertical map is an isomorphism, since W is an \mathbf{F}_p -vector space. Therefore if we assume $\iota_*(c(\overline{G}_n)) = 0$, a diagram chase shows that we may replace c by a class c' still mapping to $c(\overline{G}_n)$ in $H^2(G, \mathbf{Z}/p\mathbf{Z})$, but with $\iota_*(c') = 0$. Now using Lemma 6.7.2 (1) we conclude that c' must be the class of a commutative group extension. Indeed, one has $\text{Hom}(\Lambda^2 V, \mathbf{Z}/p\mathbf{Z}) \cong \text{Hom}(\Lambda^2 V, \mathbf{Q}/\mathbf{Z})$ because V is an \mathbf{F}_p -vector space, so we must have $\rho_{\mathbf{Z}/p\mathbf{Z}}(c') = 0$ in the notation of the lemma. Here c' cannot be 0, as it maps to a nonzero class in $H^2(G, \mathbf{Z}/p\mathbf{Z})$, and so it must come from an abelian group E which has elements of order p^2 . But then \overline{G}_n cannot be obtained by pullback from E , for it has no elements of order p^2 in its abelian quotients. This contradiction concludes the proof.

□

Remarks 6.7.4

1. For $n = 4$ the group G considered above is one of the first examples of Saltman [2]. Bogomolov has given a classification of all finite p -groups G of nilpotence class 2 and $G/Z(G) \cong \mathbf{F}_p^4$ with $H_B^2(G) \neq 0$. He has also made a thorough study of the unramified Brauer group of invariant fields under actions of reductive algebraic groups, a topic which has interesting connections with geometric invariant theory. Besides the original papers (Bogomolov [1], [2]) one may profitably consult the survey of Colliot-Thélène and Sansuc [1].
2. One may ask whether the vanishing of the unramified Brauer group is a sufficient condition for the rationality of a variety. This is not the case: Colliot-Thélène and Ojanguren [1] gave examples of unirational but nonrational varieties with trivial unramified Brauer group. Moreover, Peyre [1] found a finite group G acting faithfully on a \mathbf{C} -vector space V with $\text{Br}_{\text{nr}}(\mathbf{C}(V)^G) = 0$, but $\mathbf{C}(V)^G$ not purely transcendental over \mathbf{C} . In these examples, nonrationality is explained by the nonvanishing of an unramified cohomology group of degree 3.
3. A question closely related to the above is the famous *Noether problem*. The issue is the same as in Problem 6.6.3, except that the ground field is $k = \mathbf{Q}$. Emmy Noether's interest in the problem stemmed from its connection with the inverse Galois problem. Namely, it is a consequence of Hilbert's irreducibility theorem (see e.g. Serre [3], §10.1) that a positive answer to the problem for a given group G would yield an infinite family of Galois extensions of \mathbf{Q} with group G obtained via specializations $t_i \mapsto a_i$. However, as opposed to the case of an algebraically closed ground field, the answer here may be negative even for cyclic G . Swan [1] and Voskresensky [1] found independently the first counterexample with $G = \mathbf{Z}/47\mathbf{Z}$; this is the smallest group of prime order yielding a counterexample. Later, Lenstra [1] found a counterexample with $G = \mathbf{Z}/8\mathbf{Z}$ and gave a necessary and sufficient condition for the answer to be positive in the case of a general commutative G . Saltman [1] found a new approach to the counterexample $G = \mathbf{Z}/8\mathbf{Z}$ by relating it to Wang's counterexample to the so-called Grunwald theorem in class field theory. See Swan [2] or Kersten [2] for nice surveys of the area including an account of Saltman's work. See also Garibaldi-Merkurjev-Serre [1] for a discussion from the point of view of cohomological invariants. Theorem 33.16 of this reference explains Saltman's approach by showing that in his counterexample a

certain element in $\text{Br}_{\text{nr}}(\mathbf{Q}(V)^G)$ does not come from $\text{Br}(\mathbf{Q})$, and hence $\mathbf{Q}(V)^G$ cannot be purely transcendental by Corollary 6.6.7.

6.8 Residue Maps with Finite Coefficients

This section and the next are of a technical nature; their results will be needed for our study of the cohomological symbol. Our purpose here is to define and study residue maps of the form

$$\partial_v^i : H^i(K, \mu_m^{\otimes j}) \rightarrow H^{i-1}(\kappa(v), \mu_m^{\otimes(j-1)}),$$

where K is a field equipped with a discrete valuation v with residue field $\kappa(v)$, m is an integer invertible in $\kappa(v)$ and i, j are positive integers. This is a finite coefficient analogue of the residue map studied earlier, because for $j = 1$ we get maps $H^i(K, \mu_m) \rightarrow H^{i-1}(\kappa(v), \mathbf{Z}/m\mathbf{Z})$, i.e. instead of the multiplicative group we work with its m -torsion part. We shall only need the case when K and $\kappa(v)$ have the same characteristic, so we conduct our study under this restrictive assumption, but the arguments work more generally.

The basis for our labours is the following construction in homological algebra.

Construction 6.8.1 Let G be a profinite group, and let H be a closed normal subgroup in G with $\text{cd}(H) \leq 1$. We construct maps

$$\partial_i : H^i(G, A) \rightarrow H^{i-1}(G/H, H^1(H, A))$$

for all torsion G -modules A and all integers $i > 0$ as follows. Embed A into the co-induced module $M^G(A)$, and let C be the G -module fitting into the exact sequence

$$0 \rightarrow A \rightarrow M^G(A) \rightarrow C \rightarrow 0. \quad (15)$$

Observe that here $H^j(H, C) = 0$ for all $j \geq 1$. Indeed, by Lemma 3.3.15 we have $H^j(H, M^G(A)) = 0$ for all $j \geq 1$, so that the long exact sequence in H -cohomology associated with (15) yields isomorphisms $H^j(H, C) \cong H^{j+1}(H, A)$ for all $j \geq 1$, but the latter groups are all trivial by assumption.

This shows that for $i > 2$ the assumptions of Proposition 3.3.17 (completed by Corollary 4.3.5) are satisfied, and therefore the inflation maps

$$\text{Inf} : H^{i-1}(G/H, C^H) \rightarrow H^{i-1}(G, C)$$

are isomorphisms. We draw a similar conclusion for $i = 2$ from Proposition 3.3.14 of *loc. cit.* On the other hand, for $i \geq 2$ we get from the long

exact sequence associated with (15) isomorphisms $H^{i-1}(G, C) \cong H^i(G, A)$, so finally isomorphisms

$$H^i(G, A) \cong H^{i-1}(G/H, C^H). \quad (16)$$

But from the long exact sequence in H -cohomology coming from (15) we also obtain a map $C^H \rightarrow H^1(H, A)$, which is a morphism of G/H -modules by Lemma 3.3.13. Hence there are induced maps

$$H^{i-1}(G/H, C^H) \rightarrow H^{i-1}(G/H, H^1(H, A))$$

for all $i \geq 1$. Composing with the isomorphism (16) we thus obtain a construction of the maps ∂_i for $i > 1$. The case $i = 1$ was treated in Proposition 3.3.14 (in fact, it is just a restriction map).

If p is a fixed prime, and we only assume $\text{cd}_\ell(H) \leq 1$ for $\ell \neq p$, then the same construction works for prime-to- p torsion G -modules A .

A fundamental property of the maps ∂_i is the following.

Proposition 6.8.2 *The maps ∂_i fit into a functorial long exact sequence*

$$\dots \rightarrow H^i(G/H, A^H) \xrightarrow{\text{Inf}} H^i(G, A) \xrightarrow{\partial_i} H^{i-1}(G/H, H^1(H, A)) \rightarrow H^{i+1}(G/H, A^H) \rightarrow \dots$$

starting from $H^1(G, A)$.

Proof: The beginning of the long exact sequence in H -cohomology coming from exact sequence (15) above reads

$$0 \rightarrow A^H \rightarrow M^G(A)^H \rightarrow C^H \rightarrow H^1(H, A) \rightarrow 0.$$

We may split this up into two short exact sequences

$$0 \rightarrow A^H \rightarrow M^G(A)^H \rightarrow T \rightarrow 0, \quad (17)$$

$$0 \rightarrow T \rightarrow C^H \rightarrow H^1(H, A) \rightarrow 0. \quad (18)$$

The long exact sequence in G/H -cohomology associated with (18) reads

$$\dots \rightarrow H^{i-1}(G/H, T) \rightarrow H^{i-1}(G/H, C^H) \rightarrow H^{i-1}(G/H, H^1(H, A)) \rightarrow H^i(G, T) \rightarrow \dots$$

Using Lemma 3.3.15 we see that $H^i(G/H, M^G(A)^H) = 0$ for all $i > 0$, hence the long exact sequence associated with (17) yields isomorphisms $H^i(G/H, A^H) \cong H^{i-1}(G/H, T)$ for all $i > 1$. Taking isomorphism (16) into account we may therefore identify the above long exact sequence with that of the proposition. The fact that the maps $H^i(G/H, A^H) \rightarrow H^i(G, A)$ are indeed the usual inflation maps follows from an easy compatibility between inflations and boundary maps in long exact sequences, which readers may check for themselves. \square

Remark 6.8.3 In the literature the maps ∂_i are usually obtained as edge morphisms of the Hochschild-Serre spectral sequence for group extensions, and the exact sequence of the above proposition results from the degeneration of the spectral sequence. It can be shown that the two constructions yield the same map.

The maps ∂_i enjoy the following compatibility property with respect to cup-products.

Lemma 6.8.4 *In the situation above let A, B be continuous G -modules. Assume that exact sequence (15) remains exact when tensored over \mathbf{Z} by B . Then the diagram*

$$\begin{array}{ccccc} H^p(G, A) & \times & H^q(G, B) & \xrightarrow{\cup} & H^{p+q}(G, A \otimes B) \\ \downarrow \partial_p & & \uparrow \text{Inf} & & \downarrow \partial_{p+q} \\ H^{p-1}(G/H, H^1(H, A)) \times H^q(G/H, H^0(H, B)) & \xrightarrow{\cup} & H^{p+q-1}(G/H, H^1(H, A \otimes B)) & & \end{array}$$

commutes. In other words, for $a \in H^p(G, A)$ and $b \in H^q(G/H, H^0(H, B))$ we have

$$\partial_{p+q}(a \cup \text{Inf}(b)) = \partial_p(a) \cup b.$$

Proof: Observe first that we have $M^G(A) \otimes_{\mathbf{Z}} B \cong M^G(A \otimes B)$. To establish this isomorphism, we may assume G finite, by compatibility of tensor products with direct limits. Then given $\phi : \mathbf{Z}[G] \rightarrow A$ sending $g_i \in G$ to $a_i \in A$, we may define for each $b \in B$ a map $\phi_b : \mathbf{Z}[G] \rightarrow A \otimes B$ by sending g_i to $a_i \otimes b$. This construction is bilinear, and defines the required isomorphism. Now the assumption of the lemma implies exactness of the sequence

$$0 \rightarrow A \otimes B \rightarrow M^G(A \otimes B) \rightarrow C \otimes B \rightarrow 0,$$

which we may use to construct the map ∂_{p+q} on the right as in Construction 6.8.1. The compatibility of cup-products with boundary maps (Proposition 3.4.8) and inflations (Proposition 3.4.10 (2)) gives then rise to the commutative diagram

$$\begin{array}{ccccc} H^p(G, A) & \times & H^q(G, B) & \xrightarrow{\cup} & H^{p+q}(G, A \otimes B) \\ \uparrow \cong & & \uparrow \text{Inf} & & \uparrow \cong \\ H^{p-1}(G/H, C^H) & \times & H^q(G/H, B^H) & \xrightarrow{\cup} & H^{p+q-1}(G/H, (C \otimes B)^H) \end{array}$$

where the two unnamed vertical maps come from the isomorphism (16), itself defined as the composite of a boundary map and an inflation. The lemma now follows from the commutative diagram

$$\begin{array}{ccccc}
H^{p-1}(G/H, C^H) & \times & H^q(G/H, B^H) & \xrightarrow{\cup} & H^{p+q-1}(G/H, (C \otimes B)^H) \\
\downarrow & & \downarrow \text{id} & & \downarrow \\
H^{p-1}(G/H, H^1(H, A)) & \times & H^q(G/H, H^0(H, B)) & \xrightarrow{\cup} & H^{p+q-1}(G/H, H^1(H, A \otimes B))
\end{array}$$

resulting from the functoriality of cup-products. \square

We now turn to the promised construction of residue maps.

Construction 6.8.5 Let k be a field, and $k((t))$ the Laurent series field over k . Choose a separable closure K_s of $k((t))$, and write G and H for the Galois groups $\text{Gal}(K_s|k((t)))$ and $\text{Gal}(K_s|k((t))_{nr})$, respectively, where $k((t))_{nr}$ is the maximal unramified extension as in Section 6.2. Note that the ℓ -Sylow subgroups of H are isomorphic to \mathbf{Z}_ℓ for ℓ prime to $\text{char}(k)$ by Proposition A.6.9 of the Appendix. Therefore $\text{cd}_\ell(H) \leq 1$ for such ℓ by Proposition 6.1.3 and Lemma 6.1.4, so for m prime to $\text{char}(k)$ Construction 6.8.1 applied with $A = \mu_m^{\otimes j}$ and the above G and H yields maps

$$H^i(k((t)), \mu_m^{\otimes j}) \rightarrow H^{i-1}(k, H^1(k((t))_{nr}, \mu_m^{\otimes j}))$$

for all $i, j > 0$. As H acts trivially on μ_m , we see that there is an isomorphism of G/H -modules

$$H^1(k((t))_{nr}, \mu_m^{\otimes j}) \cong H^1(k((t))_{nr}, \mu_m) \otimes \mu_m^{\otimes(j-1)}.$$

Now Kummer theory gives an isomorphism

$$H^1(k((t))_{nr}, \mu_m) \cong k((t))_{nr}^\times / k((t))_{nr}^{\times m},$$

which is also G/H -equivariant according to Lemma 3.3.13. This may be composed with the (equally G/H -equivariant) valuation map

$$k((t))_{nr}^\times / k((t))_{nr}^{\times m} \rightarrow \mathbf{Z}/m\mathbf{Z}$$

sending t to 1. Putting the above together, we get a map

$$H^i(k((t)), \mu_m^{\otimes j}) \rightarrow H^{i-1}(k, \mu_m^{\otimes(j-1)}),$$

as required.

For a general field K equipped with a discrete valuation v whose residue field $\kappa(v)$ has characteristic equal to that of K , we first pass to the completion

which is isomorphic to the Laurent series field $\kappa(v)((t))$ (Appendix, Proposition A.5.3). Then we may apply the above construction with $k = \kappa(v)$ to obtain a map

$$\partial_v^i : H^i(K, \mu_m^{\otimes j}) \rightarrow H^{i-1}(\kappa(v), \mu_m^{\otimes(j-1)})$$

as at the beginning of this section. This is the *residue map* with $\mu_m^{\otimes j}$ -coefficients associated with v .

By means of the residue map we may define another useful map in Galois cohomology.

Construction 6.8.6 (Specialisation maps) Consider first the Laurent series field $k((t))$ as above with its standard valuation v . Denote by $(-t)$ the image of $-t$ by the Kummer map $k((t))^\times \rightarrow H^1(k((t)), \mu_m)$. Using the cup-product we may associate with each $a \in H^i(k((t)), \mu_m^{\otimes j})$ the element $\partial_v^{i+1}((-t) \cup a)$ lying in $H^i(k, \mu_m^{\otimes j})$. The choice of the minus sign may have an air of mystery at the moment, but will be justified in the next chapter (Remark 7.1.6 (1) and Corollary 7.5.3).

In this way we obtain a map

$$H^i(k((t)), \mu_m^{\otimes j}) \rightarrow H^i(k, \mu_m^{\otimes j}).$$

As above, given a general discretely valued field K of equal characteristic, we may embed it into its completion $\kappa(v)((t))$ to obtain a map

$$s_t^i : H^i(K, \mu_m^{\otimes j}) \rightarrow H^i(\kappa(v), \mu_m^{\otimes j}).$$

This is the i -th *specialisation map* associated with t . It depends on the choice of the parameter t .

For Laurent series fields $k((t))$ the specialisation map enjoys the following crucial property.

Proposition 6.8.7 *The composite maps*

$$H^i(k, \mu_m^{\otimes j}) \xrightarrow{\text{Inf}} H^i(k((t)), \mu_m^{\otimes j}) \xrightarrow{s_t^i} H^i(k, \mu_m^{\otimes j})$$

are identity maps for all $i, j > 0$.

Proof: Apply Lemma 6.8.4 with G and H as in Construction 6.8.5, $A = \mu_m$, $B = \mu_m^{\otimes j}$, $p = 1$ and $q = i$. The condition of the lemma is obviously satisfied, as on the level of abelian groups we are just tensoring $\mathbf{Z}/n\mathbf{Z}$ -modules by $\mathbf{Z}/n\mathbf{Z}$. For $b \in H^i(k, \mu_m^{\otimes j})$ and $a = (-t)$ the lemma then yields

$$s_t^i(\text{Inf}(a)) = \partial_v^1((-t)) \cup b.$$

But $\partial_v^1((-t)) = 1$, because ∂_v^1 becomes the mod m valuation map via the Kummer isomorphism and $-t$ has valuation 1. Hence cup-product with $\partial_v^1((-t))$ is the identity, and the proposition is proven. \square

Corollary 6.8.8 *The sequences*

$$0 \rightarrow H^i(k, \mu_m^{\otimes j}) \xrightarrow{\text{Inf}} H^i(k((t)), \mu_m^{\otimes j}) \xrightarrow{\partial^i} H^{i-1}(k, \mu_m^{\otimes(j-1)}) \rightarrow 0$$

are exact for all $i, j > 0$.

Proof: Apply Proposition 6.8.2 with G, H and A as in Construction 6.8.5. By the proposition, the maps s_t^i split up the resulting long exact sequence into a collection of short exact sequences as in the corollary. \square

6.9 The Faddeev Sequence with Finite Coefficients

We now come to the main result concerning our freshly constructed residue maps, namely the analogue of Faddeev's theorem with finite coefficients.

Theorem 6.9.1 *Let k be a field, \mathbf{P}^1 the projective line over k and K its function field. For each $i, j > 0$ and m invertible in k the sequence*

$$0 \rightarrow H^i(k, \mu_m^{\otimes j}) \xrightarrow{\text{Inf}} H^i(K, \mu_m^{\otimes j}) \xrightarrow{\oplus \partial_P^i} \bigoplus_{P \in \mathbf{P}_0^1} H^{i-1}(\kappa(P), \mu_m^{\otimes(j-1)}) \xrightarrow{\Sigma \text{Cor}_P} H^{i-1}(k, \mu_m^{\otimes(j-1)}) \rightarrow 0$$

is exact.

Remark 6.9.2 Note that in contrast to Theorem 6.4.5 we did not assume here that k is perfect. Therefore we have to explain what we mean by the corestriction maps Cor_P in characteristic $p > 0$. For a finite separable extension $F'|F$ of fields, we define the associated corestriction map as before, using Galois theory. For a purely inseparable extension $F''|F$ of degree p^r we define the corestriction map to be multiplication by p^r . In the case of a general finite extension $F''|F$, we let $F'|F$ be the maximal separable subextension and define the corestriction to be the composite of the above two maps. This

definition works for Galois cohomology with coefficients in torsion modules having no nontrivial elements of order p . In the presence of p -torsion much more sophisticated constructions should be used (or one should work with a different cohomology theory; compare Remark 6.1.10).

Proof of Theorem 6.9.1: Assume first that k is a perfect field. In this case the proof follows a pattern similar to that of Theorem 6.4.5, with some local differences. First, using the isomorphism $\text{Pic}(\mathbf{P}_k^1) \cong \mathbf{Z}$ we consider the exact sequence of G -modules

$$0 \rightarrow (K\bar{k})^\times / \bar{k}^\times \rightarrow \text{Div}(\mathbf{P}_{\bar{k}}^1) \rightarrow \mathbf{Z} \rightarrow 0,$$

which has a G -equivariant splitting coming from a k -rational point of \mathbf{P}^1 . Therefore after tensoring with $\mu_m^{\otimes(j-1)}$ we still get a split exact sequence

$$0 \rightarrow ((K\bar{k})^\times / \bar{k}^\times) \otimes \mu_m^{\otimes(j-1)} \rightarrow \text{Div}(\mathbf{P}_{\bar{k}}^1) \otimes \mu_m^{\otimes(j-1)} \rightarrow \mu_m^{\otimes(j-1)} \rightarrow 0.$$

For each $i > 0$ this induces short exact sequences

$$\begin{aligned} 0 &\rightarrow H^{i-1}(k, ((K\bar{k})^\times / \bar{k}^\times) \otimes \mu_m^{\otimes(j-1)}) \rightarrow \\ &\rightarrow H^{i-1}(k, \text{Div}(\mathbf{P}_{\bar{k}}^1) \otimes \mu_m^{\otimes(j-1)}) \xrightarrow{\alpha} H^{i-1}(k, \mu_m^{\otimes(j-1)}) \rightarrow 0. \end{aligned}$$

Now exactly in the same way as in the proof of Theorem 6.4.4 we identify the map α to the map ΣCor_P of the theorem. Furthermore, since \bar{k}^\times is an m -divisible group, the tensor product $\bar{k}^\times \otimes \mu_m^{\otimes(j-1)}$ vanishes, so that tensoring the exact sequence

$$0 \rightarrow \bar{k}^\times \rightarrow (K\bar{k})^\times \rightarrow (K\bar{k})^\times / \bar{k}^\times \rightarrow 0$$

by $\mu_m^{\otimes(j-1)}$ yields an isomorphism

$$(K\bar{k})^\times \otimes \mu_m^{\otimes(j-1)} \cong ((K\bar{k})^\times / \bar{k}^\times) \otimes \mu_m^{\otimes(j-1)}.$$

We may therefore make this replacement in the exact sequence above and thus reduce to identifying the group $H^{i-1}(k, (K\bar{k})^\times \otimes \mu_m^{\otimes(j-1)})$ with the co-kernel of the inflation map

$$\text{Inf} : H^i(k, \mu_m^{\otimes j}) \rightarrow H^i(K, \mu_m^{\otimes j}). \quad (19)$$

To this end, we use the long exact sequence of Proposition 6.8.2 with $G = \text{Gal}(\bar{K}|K)$, $H = \text{Gal}(\bar{K}|\bar{k})$ and $A = \mu_m^{\otimes j}$. Here $\text{cd}(H) \leq 1$ by Tsen's theorem, so the proposition applies and yields a long exact sequence

$$\dots \rightarrow H^i(k, \mu_m^{\otimes j}) \xrightarrow{\text{Inf}} H^i(K, \mu_m^{\otimes j}) \rightarrow H^{i-1}(k, (K\bar{k})^\times \otimes \mu_m^{\otimes(j-1)}) \rightarrow \dots$$

after making the identification $H^1(K\bar{k}, \mu_m^{\otimes j}) \cong (K\bar{k})^\times \otimes \mu_m^{\otimes(j-1)}$ as in Construction 6.8.5 above. Now just like in the proof of Theorem 6.4.5, the point is that the inflation maps (19) are injective for all $i > 0$. To see this, it is enough to show injectivity of the composite maps $H^i(k, \mu_m^{\otimes j}) \rightarrow H^i(k((t)), \mu_m^{\otimes j})$ obtained via the embedding $K \hookrightarrow k((t))$. But these maps are injective, because the specialisation map yields a section for them by virtue of Proposition 6.8.7. Finally, the identification of the resulting maps

$$H^i(K, \mu_m^{\otimes j}) \rightarrow \bigoplus_{P \in \mathbf{P}_0^1} H^{i-1}(\kappa(P), \mu_m^{\otimes(j-1)})$$

with a direct sum of residue maps follows by an argument similar to that in Proposition 6.4.3.

It remains to reduce the case of a general base field k of characteristic $p > 0$ to the perfect case. To do so, consider the *perfect closure* k_{p^∞} of k (recall that this is the perfect field obtained by adjoining all p -power roots of elements in k). Given a separable closure k_s of k , the composite $k_{p^\infty}k_s$ is a separable closure of k_{p^∞} , as the extension $k_{p^\infty}|k$ is purely inseparable. In this way we may identify the absolute Galois group of k with that of k_{p^∞} , and similar considerations apply to the absolute Galois groups of $k(t)$ and $k_{p^\infty}(t)$. As $\mu_m \subset k_s$ for m prime to p , the action of these groups on the modules $\mu_m^{\otimes j}$ is the same, so we get natural isomorphisms on the corresponding Galois cohomology groups. Whence the isomorphic vertical maps in the commutative diagram

$$\begin{array}{ccc} H^i(k, \mu_m^{\otimes j}) & \xrightarrow{\text{Inf}} & H^i(K, \mu_m^{\otimes j}) \\ \cong \downarrow & & \downarrow \cong \\ H^i(k_{p^\infty}, \mu_m^{\otimes j}) & \xrightarrow{\text{Inf}} & H^i(Kk_{p^\infty}, \mu_m^{\otimes j}). \end{array}$$

Next, consider a closed point P of $\mathbf{P}_k^1 \setminus \{\infty\}$. It corresponds to an irreducible polynomial $f \in k[t]$, which becomes the p^r -th power of an irreducible polynomial in $k_{p^\infty}[t]$, where p^r is the inseparability degree of the extension $\kappa(P)|k$. This shows that there is a unique closed point P' of $\mathbf{P}_{k_{p^\infty}}^1$ lying above P , with

$$[\kappa(P') : k_{p^\infty}] = p^{-r}[\kappa(P) : k]. \quad (20)$$

Therefore we have a commutative diagram with isomorphic vertical maps

$$\begin{array}{ccccc}
H^i(K, \mu_m^{\otimes j}) & \xrightarrow{\oplus \partial_P^i} & \bigoplus_{P \in \mathbf{P}_{k,0}^1} H^{i-1}(\kappa(P), \mu_m^{\otimes(j-1)}) & \xrightarrow{\Sigma \text{Cor}_P} & H^{i-1}(k, \mu_m^{\otimes(j-1)}) \\
\cong \downarrow & & \cong \downarrow & & \cong \downarrow \\
H^i(Kk_{p^\infty}, \mu_m^{\otimes j}) & \xrightarrow{\oplus \partial_P^i} & \bigoplus_{P \in \mathbf{P}_{k_{p^\infty},0}^1} H^{i-1}(\kappa(P'), \mu_m^{\otimes(j-1)}) & \xrightarrow{\Sigma \text{Cor}_P} & H^{i-1}(k_{p^\infty}, \mu_m^{\otimes(j-1)}).
\end{array}$$

Here the left square commutes by the construction of residue maps and our remarks on the Galois groups of K and Kk_{p^∞} . Commutativity of the right square follows from our definition of corestriction maps in Remark 6.9.2 and the formula (20). This completes the identification of the exact sequence over k with that over k_{p^∞} . \square

Observe that for the point at infinity ∞ of \mathbf{P}_k^1 we have $\kappa(\infty) = k$, and the corestriction map $\text{Cor}_\infty : H^{i-1}(\kappa(\infty), \mu_m^{\otimes j}) \rightarrow H^{i-1}(k, \mu_m^{\otimes j})$ is the identity map. Hence we get:

Corollary 6.9.3 *In the situation of the theorem there is an exact sequence*

$$0 \rightarrow H^i(k, \mu_m^{\otimes j}) \xrightarrow{\text{Inf}} H^i(K, \mu_m^{\otimes j}) \xrightarrow{\oplus \partial_P^i} \bigoplus_{P \in \mathbf{P}_0^1 \setminus \{\infty\}} H^{i-1}(\kappa(P), \mu_m^{\otimes(j-1)}) \rightarrow 0$$

split by the specialisation map $s_{t^{-1}}^i : H^i(K, \mu_m^{\otimes j}) \rightarrow H^i(k, \mu_m^{\otimes j})$ associated with the local parameter t^{-1} at ∞ .

Proof: The exact sequence results from that of the theorem, and the statement about the splitting from Proposition 6.8.7 (after embedding K into the Laurent series field $k((t^{-1}))$). \square

The split exact sequence of the corollary allows us to define maps

$$\psi_P^i : H^{i-1}(\kappa(P), \mu_m^{\otimes(j-1)}) \rightarrow H^i(K, \mu_m^{\otimes j})$$

satisfying $\partial_P^i \circ \psi_P^i = \text{id}$ for each closed point P of \mathbf{P}_k^1 , which we may call *coresidue maps*. We then get the following useful description of corestrictions.

Corollary 6.9.4 *The corestriction maps*

$$\text{Cor}_P : H^{i-1}(\kappa(P), \mu_m^{\otimes(j-1)}) \rightarrow H^{i-1}(k, \mu_m^{\otimes(j-1)})$$

satisfy the formula

$$\text{Cor}_P = -\partial_\infty^i \circ \psi_P^i,$$

where ∂_∞^i is the residue map associated with the point ∞ .

Proof: Let α be an element of $H^{i-1}(\kappa(P), \mu_m^{\otimes(j-1)})$. In the exact sequence of Theorem 6.9.1, consider the element of $\bigoplus H^{i-1}(\kappa(P), \mu_m^{\otimes(j-1)})$ given by α in the component indexed by P , $-\text{Cor}_P(\alpha)$ in the component indexed by ∞ , and 0 elsewhere. Since Cor_∞ is the identity map, this element maps to 0 in $H^{i-1}(k, \mu_m^{\otimes(j-1)})$ by the sum of corestriction maps, hence it is the residue of some element in $H^i(\kappa(P), \mu_m^{\otimes j})$, which is none but $\psi_P^i(\alpha)$. This proves the corollary. \square

Remarks 6.9.5

1. The results of this section generalise in a straightforward way to the case of an arbitrary $\mathbf{Z}/m\mathbf{Z}$ -module A equipped with a $\text{Gal}(k_s|k)$ -action instead of $\mu_m^{\otimes j}$ (still assuming m prime to the characteristic). The role of the $\text{Gal}(k_s|k)$ -modules $\mu_m^{\otimes(j-1)}$ is then played by the groups $\text{Hom}(\mu_m, A)$ equipped with the usual Galois action.
2. It is again possible to obtain the results of this section via methods of étale cohomology, namely using the localisation theory and the so-called purity isomorphisms (see Milne [2]). But it is not obvious to check that the residue maps in the two theories are the same up to a sign.

EXERCISES

1. Let G be a profinite group of finite cohomological dimension, and let H be an open subgroup of G . Prove that $\text{cd}_p(G) = \text{cd}_p(H)$ for all primes p .
[Hint: Show that the corestriction map $\text{Cor} : H^n(H, A) \rightarrow H^n(G, A)$ is surjective for $n = \text{cd}(G)$ and a torsion G -module A .]
2. Let G be a finite group. Show that $\text{cd}_p(G) = \infty$ if p divides the order of G , and $\text{cd}_p(G) = 0$ otherwise. *[Hint: Use the previous exercise.]*
3. (Kato, Kuzumaki) Let k be a perfect field such that the absolute Galois group $\Gamma = \text{Gal}(k_s|k)$ has no nontrivial elements of finite order, and let X be a Severi-Brauer variety over k . Prove that for all primes p not dividing $\text{char}(k)$ the product of restriction maps

$$H^1(k, \mathbf{Z}/p\mathbf{Z}) \rightarrow \prod_{P \in X_0} H^1(\kappa(P), \mathbf{Z}/p\mathbf{Z})$$

is injective, where the sum is over all closed points of X . *[Hint: By the assumption on Γ , the subgroup topologically generated by an element $\sigma \in \Gamma$ is isomorphic to $\hat{\mathbf{Z}}$, and hence its fixed field has trivial Brauer group.]*

[Remark: The condition on Γ is not very restrictive, for by Chapter 4, Exercise 7 fields of characteristic 0 having no ordered field structure enjoy this property.]

4. (a) Show that finite fields satisfy the C'_1 property (Remark 6.2.2 (2)).
 (b) Same question for the function field of a curve over an algebraically closed field.
5. Let $L|K$ be a purely inseparable extension of fields of characteristic $p > 0$. Prove that the natural map $\text{Br}(K) \rightarrow \text{Br}(L)$ is surjective, and its kernel is a p -primary torsion group. *[Hint: Take a separable closure K_s of K , exploit the exact sequence $1 \rightarrow K_s^\times \rightarrow (LK_s)^\times \rightarrow (LK_s)^\times / K_s^\times \rightarrow 1$ and use $\text{cd}_p(K) \leq 1$.]*
6. Let k be a field and p a prime invertible in k . Let $\chi \in H^1(k, \mathbf{Z}/p\mathbf{Z})$ be a surjective character, and $K|k$ the associated cyclic extension. Let $A|k$ be a central simple algebra. Over the rational function field $k(t)$ consider the $k(t)$ -algebra $A_{k(t)} := A \otimes_k k(t)$ and the cyclic $k(t)$ -algebra (χ, t) . Finally, define $B := A_{k(t)} \otimes_{k(t)} (\chi, t)$ and $\widehat{B} := B \otimes_{k(t)} k((t))$.
 (a) Show that $\text{ind}_{k((t))}(\widehat{B})$ divides $p \text{ind}_K(A \otimes_k K)$. *[Hint: use Corollary 4.5.11.]*

- (b) Let $L|k$ be a field extension such that $L((t))|k((t))$ splits \widehat{B} . Show that L contains K . [*Hint*: Use Corollary 6.3.7.]
- (c) Show that $\text{ind}_{k((t))}(\widehat{B}) = p \text{ind}_K(A \otimes_k K)$ and $\text{ind}_{k(t)}(B) = \text{ind}_K(A \otimes_k K)$.
- (d) Conclude that $A \otimes_k K$ is a division algebra if and only if B is a division algebra.
7. (suggested by Colliot-Thélène) Let $F = k(x, y)$ be the rational function field in the two indeterminates x, y , and let a, b be elements of k^\times .

Prove that the biquaternion algebra $(a, x) \otimes_F (b, y)$ over F is a division algebra if and only if the images of the elements a and b in the \mathbf{F}_2 -vector space $k^\times/k^{\times 2}$ are linearly independent. [*Hint*: Use the previous exercise.]

[*Remark*: Generalising the technique of this exercise one may construct algebras of period 2 and index 2^d over the purely transcendental extension $\mathbf{Q}(x_1, \dots, x_d)$ for all $d > 1$.]

8. Let C be a projective conic over a perfect field k with $C(k) = \emptyset$. Show that there is an exact sequence

$$0 \rightarrow \mathbf{Z}/2\mathbf{Z} \rightarrow \text{Br}(k) \rightarrow \text{Br}(k(C)) \xrightarrow{\oplus r_P} \bigoplus_{P \in C_0} H^1(\kappa(P), \mathbf{Q}/\mathbf{Z}) \xrightarrow{\Sigma \text{Cor}_P} H^1(k, \mathbf{Q}/\mathbf{Z}).$$

What can you say about the cokernel of the last map?

9. Let K be the function field of a smooth projective curve over a perfect field k . Let (χ, b) be a cyclic algebra over K , where $b \in K$ and χ defines a degree m cyclic Galois extension of k with group G . We view χ as an element of $H^1(G, \mathbf{Z}/m\mathbf{Z})$.

- (a) For a closed point P of C , show that the residue map r_P is given by

$$r_P((\chi, b)) = \text{Res}_{G_P}^G(\chi) \cup v_P(b) \in H^1(G_P, \mathbf{Z}/m\mathbf{Z}),$$

where G_P is the stabilizer of P in G , and $v_P(b)$ is viewed as an element of $H^0(G_P, \mathbf{Z})$.

- (b) Assuming moreover that k is finite, deduce a formula of Hasse:

$$r_P((\chi, b)) = \frac{[\kappa(P) : k] v_P(b)}{m} \in \mathbf{Q}/\mathbf{Z}.$$

- (c) Still assuming k finite, show that the Residue Theorem for (χ, b) is equivalent to the formula $\text{deg}(\text{div}(b)) = 0$.

[*Remark*: This exercise gives some hint about the origin of the name of the Residue Theorem, because the formula $\text{deg}(\text{div}(f)) = 0$ for an algebraic function f is equivalent (in characteristic 0) to the fact that the sum of the residues of the logarithmic differential form $f^{-1}df$ equals 0.]

10. Consider the affine surface X of equation $x^3 - x = y^2 + z^2$ over the field \mathbf{R} of real numbers.
- (a) Show that X unirational over \mathbf{R} . [*Hint*: Find an extension $\mathbf{R}(z)|\mathbf{R}(x)$ which splits the quaternion algebra $(-1, x^3 - x)$ over $\mathbf{R}(x)$, and use Proposition 1.3.2.]
 - (b) Show that X is not rational by examining $\text{Br}_{\text{nr}}(k(X))$. [*Hint*: Consider the class of the quaternion algebra $(-1, x)$.]
11. ('No-name lemma' for finite groups) Let G be a finite group, and let V and W be vector spaces over a field k , of dimensions n and m , respectively.
- (a) Prove that $k(V \oplus W)^G \cong k(V)^G(t_1, \dots, t_m)$ for some independent variables t_i . [*Hint*: Apply Speiser's lemma to the extension $k(V)|k(V)^G$ and the vector space $W \otimes_k k(V)$.]
 - (b) Conclude that $k(V)^G(t_1, \dots, t_m) \cong k(W)^G(u_1, \dots, u_n)$ for some independent variables t_i and u_j , and hence $\text{Br}_{\text{nr}}(k(V)^G) \cong \text{Br}_{\text{nr}}(k(W)^G)$.

[*Remark*: This exercise shows that the answer to Problem 6.6.3 depends only on the group G , and not on the representation V .]

12. This exercise gives a new proof of the Steinberg relation for Galois cohomology by using Theorem 6.9.1. Let k be a field, m an integer invertible in k , and $k(t)$ the rational function field.
- (a) Verify the relation $(t) \cup (1 - t) = 0$ in $H^2(k(t), \mu_m^{\otimes 2})$ by calculating the residues of both sides and specialising at 0.
 - (b) Given $a \in k^\times$, $a \neq 0, 1$, deduce by specialisation that $(a) \cup (1 - a) = 0$ in $H^2(k, \mu_m^{\otimes 2})$.

Chapter 7

Milnor K-Theory

In this chapter we study the Milnor K-groups introduced in Chapter 4. There are two basic constructions in the theory: that of *tame symbols*, which are analogues of the residue maps in cohomology, and *norm maps* that generalise the field norm $N_{K|k} : K^\times \rightarrow k^\times$ for a finite extension $K|k$ to higher K-groups. Of these the first is relatively easy to construct, but showing the well-definedness of second involves some rather intricate checking. This foreshadows that the chapter will be quite technical, but nevertheless it contains a number of interesting results. Among these, we mention Weil's reciprocity law for the tame symbol over the function field of a curve, a reciprocity law of Rosset and Tate, and considerations of Bloch and Tate about the Bloch-Kato conjecture.

Most of the material in this chapter stems from the three classic papers of Milnor [1], Bass-Tate [1] and Tate [4]. Kato's theorem on the well-definedness of the norm map appears in the second part of his treatise on the class field theory of higher dimensional local fields (Kato [1]), with a sketch of the proof.

7.1 The Tame Symbol

Recall that we have defined the Milnor K-groups $K_n^M(k)$ attached to a field k as the quotient of the n -th tensor power $(k^\times)^{\otimes n}$ of the multiplicative group of k by the subgroup generated by those elements $a_1 \otimes \cdots \otimes a_n$ for which $a_i + a_j = 1$ for some $1 \leq i < j \leq n$. Thus $K_0^M(k) = \mathbf{Z}$ and $K_1^M(k) = k^\times$. Elements of $K_n^M(k)$ are called *symbols*; we write $\{a_1, \dots, a_n\}$ for the image of $a_1 \otimes \cdots \otimes a_n$ in $K_n^M(k)$. The relation $a_i + a_j = 1$ will be often referred to as the *Steinberg relation*.

Milnor K-groups are functorial with respect to field extensions: given an inclusion $\phi : k \subset K$, there is a natural map $i_{K|k} : K_n^M(k) \rightarrow K_n^M(K)$ induced by ϕ . Given $\alpha \in K_n^M(K)$, we shall often abbreviate $i_{K|k}(\alpha)$ by α_K .

There is also a natural product structure

$$K_n^M(k) \times K_m^M(k) \rightarrow K_{n+m}^M(k), \quad (\alpha, \beta) \mapsto \{\alpha, \beta\} \quad (1)$$

coming from the tensor product pairing $(k^\times)^{\otimes n} \times (k^\times)^{\otimes m} \rightarrow (k^\times)^{\otimes n+m}$ which obviously preserves the Steinberg relation. This product operation equips the direct sum

$$K_*^M(k) = \bigoplus_{n \geq 0} K_n^M(k)$$

with the structure of a graded ring indexed by the nonnegative integers. The ring $K_*^M(k)$ is commutative in the graded sense:

Proposition 7.1.1 *The product operation (1) is graded-commutative, i.e. it satisfies*

$$\{\alpha, \beta\} = (-1)^{mn} \{\beta, \alpha\}$$

for $\alpha \in K_n^M(k)$, $\beta \in K_m^M(k)$.

For the proof we first establish an easy lemma:

Lemma 7.1.2 *The group $K_2^M(k)$ satisfies the relations*

$$\{x, -x\} = 0 \quad \text{and} \quad \{x, x\} = \{x, -1\}.$$

Proof: For the first relation, we compute in $K_2^M(k)$

$$\{x, -x\} + \{x, -(1-x)x^{-1}\} = \{x, 1-x\} = 0,$$

and so

$$\{x, -x\} = -\{x, -(1-x)x^{-1}\} = -\{x, 1-x^{-1}\} = \{x^{-1}, 1-x^{-1}\} = 0.$$

The second one follows by bilinearity. \square

Proof of Proposition 7.1.1: By the previous lemma, in $K_2^M(k)$ we have the equalities

$$0 = \{xy, -xy\} = \{x, -x\} + \{x, y\} + \{y, x\} + \{y, -y\} = \{x, y\} + \{y, x\},$$

which takes care of the case $n = m = 1$. The proposition follows from this by a straightforward induction. \square

These basic facts are already sufficient for calculating the following example.

Example 7.1.3 For a finite field \mathbf{F} the groups $K_n^M(\mathbf{F})$ are trivial for all $n > 1$.

To see this it is enough to treat the case $n = 2$. Writing ω for a generator of the cyclic group \mathbf{F}^\times , we see from bilinearity of symbols that it suffices to show $\{\omega, \omega\} = 0$. By Lemma 7.1.2 this element equals $\{\omega, -1\}$ and hence it has order at most 2. We show that it is also annihilated by an odd integer, which will prove the claim. If \mathbf{F} has order 2^m for some m , we have $0 = \{1, \omega\} = \{\omega^{2^m-1}, \omega\} = (2^m - 1)\{\omega, \omega\}$, and we are done. If \mathbf{F} has odd order, then the same counting argument as in Example 1.3.6 shows that we may find elements $a, b \in \mathbf{F}^\times$ that are *not* squares in \mathbf{F} which satisfy $a + b = 1$. But then $a = \omega^k$, $b = \omega^l$ for some odd integers k, l and hence $0 = \{a, b\} = kl\{\omega, \omega\}$, so we are done again.

As we have seen in Chapter 6, a fundamental tool for studying the Galois cohomology of discrete valuation fields is furnished by the residue maps. We now construct their analogue for Milnor K-theory; the construction will at the same time yield specialisation maps for K-groups.

Let K be a field equipped with a discrete valuation $v : K^\times \rightarrow \mathbf{Z}$. Denote by A the associated discrete valuation ring and by κ its residue field. Once a local parameter π (i.e. an element with $v(\pi) = 1$) is fixed, each element $x \in K^\times$ can be uniquely written as a product $u\pi^i$ for some unit u of A and integer i . From this it follows by bilinearity and graded-commutativity of symbols that the groups $K_n^M(K)$ are generated by symbols of the form $\{\pi, u_2, \dots, u_n\}$ and $\{u_1, \dots, u_n\}$, where the u_i are units in A .

Proposition 7.1.4 *For each $n \geq 1$ there exists a unique homomorphism*

$$\partial^M : K_n^M(K) \rightarrow K_{n-1}^M(\kappa)$$

satisfying

$$\partial^M(\{\pi, u_2, \dots, u_n\}) = \{\bar{u}_2, \dots, \bar{u}_n\} \quad (2)$$

for all local parameters π and all $(n-1)$ -tuples (u_2, \dots, u_n) of units of A , where \bar{u}_i denotes the image of u_i in κ .

Moreover, once a local parameter π is fixed, there is a unique homomorphism

$$s_\pi^M : K_n^M(K) \rightarrow K_n^M(\kappa)$$

with the property

$$s_\pi^M(\{\pi^{i_1}u_1, \dots, \pi^{i_n}u_n\}) = \{\bar{u}_1 \cdots \bar{u}_n\} \quad (3)$$

for all n -tuples of integers (i_1, \dots, i_n) and units (u_1, \dots, u_n) of A .

The map ∂^M is called the *tame symbol* or the *residue map* for Milnor K-theory; the maps s_π^M are called *specialisation maps*. We stress the fact that the s_π^M depend on the choice of π , whereas ∂^M does not, as seen from its definition.

Proof: Unicity for s_π^M is obvious, and that of ∂^M follows from the above remark on generators of $K_n^M(K)$, in view of the fact that a symbol of the form $\{u_1, \dots, u_n\}$ can be written as a difference $\{\pi u_1, u_2, \dots, u_n\} - \{\pi, u_2, \dots, u_n\}$ with local parameters π and πu_1 , and hence it must be annihilated by ∂^M .

We prove existence simultaneously for ∂^M and the s_π^M via a construction due to Serre. Consider the free graded-commutative $K_*^M(\kappa)$ -algebra $K_*^M(\kappa)[x]$ on one generator x of degree 1. By definition, its elements can be identified with polynomials with coefficients in $K_*^M(\kappa)$, but the multiplication is determined by $\alpha x = -x\alpha$ for $\alpha \in K_*^M(\kappa)$. Now take the quotient $K_*^M(\kappa)[\xi]$ of $K_*^M(\kappa)[x]$ by the ideal $(x^2 - \{-1\}x)$ where $\{-1\}$ is regarded as a symbol in $K_1(\kappa)$. The image ξ of x in the quotient satisfies $\xi^2 = \{-1\}\xi$. The ring $K_*^M(\kappa)[\xi]$ has a natural grading in which ξ has degree 1: one has

$$K_*^M(\kappa)[\xi] = \bigoplus_{n \geq 0} L_n,$$

where $L_n = K_n^M(\kappa) \oplus K_{n-1}(\kappa)\xi$ for $n > 0$ and $L_0 = K_0^M(\kappa) = \mathbf{Z}$.

Now fix a local parameter π and consider the group homomorphism

$$d_\pi : K^\times \rightarrow L_1 = \kappa^\times \oplus \mathbf{Z}\xi$$

given by $\pi^i u \mapsto (\bar{u}, i\xi)$. Taking tensor powers and using the product structure in $K_*^M(\kappa)[\xi]$, we get maps

$$d_\pi^{\otimes n} : (K^\times)^{\otimes n} \rightarrow L_n = K_n^M(\kappa) \oplus K_{n-1}(\kappa)\xi.$$

Denoting by $\pi_1 : L_n \rightarrow K_n^M(\kappa)$ and $\pi_2 : L_n \rightarrow K_{n-1}(\kappa)$ the natural projections, put

$$\partial^M := \pi_2 \circ d_\pi^{\otimes n} \quad \text{and} \quad s_\pi^M := \pi_1 \circ d_\pi^{\otimes n}.$$

One sees immediately that these maps satisfy the properties (2) and (3). Therefore the construction will be complete if we show that $d_\pi^{\otimes n}$ factors through $K_n^M(K)$, for then so do ∂^M and s_π^M .

Concerning our claim about $d_\pi^{\otimes n}$, it is enough to establish the Steinberg relation $d_\pi(x)d_\pi(1-x) = 0$ in L_2 . To do so, note first that the multiplication map $L_1 \times L_1 \rightarrow L_2$ is given by

$$(x, i\xi)(y, j\xi) = (\{x, y\}, \{(-1)^{ij}x^j y^i\}\xi), \quad (4)$$

where apart from the definition of the L_i we have used the fact that the multiplication map $K_0(\kappa) \times K_1(\kappa) \rightarrow K_1(\kappa)$ is given by $(i, x) \mapsto x^i$.

Now take $x = \pi^i u$. If $i > 0$, the element $1 - x$ is a unit, hence $d_\pi(1 - x) = 0$ and the Steinberg relation holds trivially. If $i < 0$, then $1 - x = (-u + \pi^{-i})\pi^i$ and $d_\pi(1 - x) = (-\bar{u}, i\xi)$. It follows from (4) that

$$d_\pi(x)d_\pi(1 - x) = (\bar{u}, i\xi)(-\bar{u}, i\xi) = (\{\bar{u}, -\bar{u}\}, \{(-1)^{-i^2}\bar{u}^i(-\bar{u})^{-i}\}\xi),$$

which is 0 in L_2 . It remains to treat the case $i = 0$. If $v(1 - x) \neq 0$, then replacing x by $1 - x$ we arrive at one of the above cases. If $v(1 - x) = 0$, i.e. x and $1 - x$ are both units, then $d_\pi(x)d_\pi(1 - x) = (\{\bar{u}, 1 - \bar{u}\}, 0 \cdot \xi) = 0$, and the proof is complete. \square

Example 7.1.5 The tame symbol $\partial^M : K_1(K) \rightarrow K_0(\kappa)$ is none but the valuation map $v : K^\times \rightarrow \mathbf{Z}$. The tame symbol $\partial^M : K_2(K) \rightarrow K_1(\kappa)$ is given by the formula

$$\partial^M(\{a, b\}) = (-1)^{v(a)v(b)} \overline{a^{v(b)}b^{-v(a)}},$$

where the line denotes the image in κ as usual. One checks this using the definition of ∂^M and the second statement of Lemma 7.1.2.

This is the classical formula for the tame symbol in number theory; it has its origin in the theory of the Hilbert symbol.

Remarks 7.1.6

1. The reader may have rightly suspected that tame symbols and specialisation maps are not unrelated. In fact, for $\{a_1, \dots, a_n\} \in K_n^M(K)$ one has the formula

$$s_\pi^M(\{a_1, \dots, a_n\}) = \partial^M(\{-\pi, a_1, \dots, a_n\})$$

for all local parameters π .

Indeed, if $a_1 = \pi^i u_1$ for some unit u_1 and integer i , one has

$$\{-\pi, a_1, \dots, a_n\} = i\{-\pi, \pi, a_2, \dots, a_n\} + \{-\pi, u_1, a_2, \dots, a_n\},$$

where the first term on the right is trivial by the first statement in Lemma 7.1.2. Continuing this process, we may eventually assume that all the a_i are units, in which case the formula follows from the definitions.

2. The behaviour of tame symbols under field extensions can be described as follows. Let $L|K$ be a field extension and v_L a discrete valuation of L extending v with residue field κ_L and ramification index e . Denoting the associated tame symbol by ∂_L^M , one has for all $\alpha \in K_n^M(K)$

$$\partial_L^M(\alpha_L) = e \partial^M(\alpha).$$

To see this, write a local parameter π for v as $\pi = \pi_L^e u_L$ for some local parameter π_L and unit u_L for v_L . Then for all $(n-1)$ -tuples (u_2, \dots, u_n) of units for v one gets

$$\{\pi, u_2, \dots, u_n\}_L = e \{\pi_L, u_2, \dots, u_n\} + \{u_L, u_2, \dots, u_n\},$$

where the second term is annihilated by ∂_L^M . The formula follows.

We close this section with the determination of the kernel and the cokernel of the tame symbol.

Proposition 7.1.7 *We have exact sequences*

$$0 \rightarrow U_n \rightarrow K_n^M(K) \xrightarrow{\partial^M} K_{n-1}^M(\kappa) \rightarrow 0$$

and

$$0 \rightarrow U_n^1 \rightarrow K_n^M(K) \xrightarrow{(s_\pi^M, \partial^M)} K_n^M(\kappa) \oplus K_{n-1}^M(\kappa) \rightarrow 0,$$

where U_n is the subgroup of $K_n^M(K)$ generated by those symbols $\{u_1, \dots, u_n\}$ where all the u_i are units in A , and $U_n^1 \subset K_n^M(K)$ is the subgroup generated by symbols $\{x_1, \dots, x_n\}$ with x_1 a unit in A satisfying $\bar{x}_1 = 1$.

The original proof of the exactness of the first sequence in Bass-Tate [1] contained a gap. It is filled in by the following lemma, whose elegant proof is taken from Dennis-Stein [1].

Lemma 7.1.8 *With notations as in the proposition, the subgroup U_n^1 is contained in U_n .*

Proof: By writing elements of K^\times as $x = u\pi^i$ with some unit u and prime element π one easily reduces the general case to the case $n = 2$ using bilinearity and the relation $\{\pi, -\pi\} = 0$. Then it suffices to show that symbols of the form $\{1 + a\pi, \pi\}$ with some $a \in A$ are contained in U_2 .

Case 1: a is a unit in A . Then

$$\{1 + a\pi, \pi\} = \{1 + a\pi, -a\pi\} + \{1 + a\pi, -a^{-1}\} = \{1 + a\pi, -a^{-1}\}$$

by the Steinberg relation, and the last symbol lies in U_n .

Case 2: a lies in the maximal ideal of A . Then

$$\{1 + a\pi, \pi\} = \left\{1 + \frac{1+a}{1-\pi}\pi, \pi\right\} + \{1 - \pi, \pi\} = \left\{1 + \frac{1+a}{1-\pi}\pi, \pi\right\}.$$

Since here the element $(1+a)(1-\pi)^{-1}$ is a unit in A , we conclude by the first case. \square

Proof of Proposition 7.1.7: It follows from the definitions that ∂^M and s_π^M are surjective, and that the two sequences are complexes. By the lemma, for the exactness of the first sequence it is enough to check that each element in $\ker(\partial^M)$ is a sum of elements from U_n and U_n^1 . Consider the map

$$\psi : K_{n-1}^M(\kappa) \rightarrow K_n^M(K)/U_n^1$$

defined by $\{\bar{u}_1, \dots, \bar{u}_{n-1}\} \mapsto \{\pi, u_2, \dots, u_{n-1}\} \bmod U_n^1$, where the u_i are arbitrary liftings of the \bar{u}_i . This is a well-defined map, because replacing some u_i by another lifting u'_i modifies $\{\pi, u_2, \dots, u_{n-1}\}$ by an element in U_n^1 . Now for $\alpha \in U_n$ we have $(\psi \circ \partial^M)(\alpha) = 0$, and for an element in $\ker(\partial^M)$ of the form $\beta = \{\pi, u_2, \dots, u_n\}$ with the u_i units we have $0 = (\psi \circ \partial^M)(\beta) = \beta \bmod U_n^1$, i.e. $\beta \in U_n^1$. Since the β of this form generate $\ker(\partial^M)$ together with U_n , we are done.

We now turn to the second sequence. Define a map $K_n^M(\kappa) \rightarrow U_n/U_n^1$ by sending $\{\bar{u}_1, \dots, \bar{u}_n\}$ to $\{u_1, \dots, u_n\} \bmod U_n^1$, again with some liftings u_i of the \bar{u}_i . We see as above that this map is well-defined, and moreover it is an inverse to the map induced by the restriction of s_π^M to U_n (which is of course trivial on U_n^1). \square

Remark 7.1.9 It follows from the first sequence above (and was implicitly used in the second part of the proof) that the restriction of s_π^M to $\ker(\partial^M)$ is independent of the choice of π .

Corollary 7.1.10 *Assume moreover that K is complete with respect to v , and let $m > 0$ be an integer invertible in κ . Then the pair (s_π, ∂^M) induces an isomorphism*

$$K_n^M(K)/mK_n^m(K) \xrightarrow{\sim} K_n^M(\kappa)/mK_n^M(\kappa) \oplus K_{n-1}^M(\kappa)/mK_{n-1}^M(\kappa).$$

Proof: By virtue of the second exact sequence of the proposition it is enough to see that in this case $mU_n^1 = U_n^1$, which in turn needs only to be checked for $n = 1$ by multilinearity of symbols. But since m is invertible in κ , for each unit $u \in U_1^1$ Hensel's lemma (cf. Appendix, Proposition A.5.5) applied to the polynomial $x^m - u$ shows that $u \in mU_1^1$. \square

7.2 Milnor's Exact Sequence and the Bass-Tate Lemma

We now describe the Milnor K -theory of the rational function field $k(t)$ and establish an analogue of Faddeev's exact sequence due to Milnor.

Recall that the discrete valuations of $k(t)$ trivial on k correspond to the local rings of closed points P on the projective line \mathbf{P}_k^1 . As before, we denote by $\kappa(P)$ their residue fields and by v_P the associated valuations. At each closed point $P \neq \infty$ a local parameter is furnished by a monic irreducible polynomial $\pi_P \in k[t]$; at $P = \infty$ one may take $\pi_P = t^{-1}$. The degree of the field extension $[\kappa(P) : k]$ is called the degree of the closed point P ; it equals the degree of the polynomial π_P .

By the theory of the previous section we obtain tame symbols

$$\partial_P^M : K_n^M(k(t)) \rightarrow K_{n-1}^M(\kappa(P))$$

and specialisation maps

$$s_{\pi_P}^M : K_n^M(k(t)) \rightarrow K_n^M(\kappa(P)).$$

Note that since each element in $k(t)^\times$ is a unit for all but finitely many valuations v_P , the image of the product map

$$\partial^M := (\partial_P^M) : K_n^M(k(t)) \rightarrow \prod_{P \in \mathbf{P}_0^1 \setminus \{\infty\}} K_{n-1}^M(\kappa(P))$$

lies in the direct sum.

Theorem 7.2.1 (Milnor) *The sequence*

$$0 \rightarrow K_n^M(k) \rightarrow K_n^M(k(t)) \xrightarrow{\partial^M} \bigoplus_{P \in \mathbf{P}_0^1 \setminus \{\infty\}} K_{n-1}^M(\kappa(P)) \rightarrow 0$$

is exact and split by the specialisation map $s_{t^{-1}}^M$ at ∞ .

Note that for $i = 1$ we get the sequence

$$1 \rightarrow k^\times \rightarrow k(t)^\times \xrightarrow{\partial^M} \bigoplus_{\pi} \mathbf{Z} \rightarrow 0$$

which is equivalent to the decomposition of a rational function into a product of irreducible factors.

The proof exploits the filtration on $K_n^M(k(t))$

$$K_n^M(k) = L_0 \subset L_1 \subset \cdots \subset L_d \subset \cdots \quad (5)$$

where L_d is the subgroup of $K_n^M(k(t))$ generated by those symbols $\{f_1, \dots, f_n\}$ where the f_i are polynomials in $k[t]$ of degree $\leq d$.

The key statement is the following.

Lemma 7.2.2 *For each $d > 0$ consider the homomorphism*

$$\partial_d^M : K_n^M(k(t)) \rightarrow \bigoplus_{\deg(P)=d} K_{n-1}^M(\kappa(P))$$

defined as the direct sum of the maps ∂_P^M for all closed points P of degree d . Its restriction to L_d induces an isomorphism

$$\bar{\partial}_d^M : L_d/L_{d-1} \xrightarrow{\sim} \bigoplus_{\deg(P)=d} K_{n-1}^M(\kappa(P)).$$

Proof: If P is a closed point of degree d , the maps ∂_P^M are trivial on the elements of L_{d-1} , hence the map $\bar{\partial}_d^M$ exists. To complete the proof we construct an inverse for $\bar{\partial}_d^M$.

Let P be a closed point of degree d . For each element $\bar{a} \in \kappa(P)$, there exists a unique polynomial $a \in k[t]$ of degree $\leq d-1$ whose image in $\kappa(P)$ is \bar{a} . Define maps

$$h_P : K_{n-1}^M(\kappa(P)) \rightarrow L_d/L_{d-1}$$

by the assignment

$$h_P(\{\bar{a}_2, \dots, \bar{a}_n\}) = \{\pi_P, a_2, \dots, a_n\} \pmod{L_{d-1}}.$$

The maps h_P obviously satisfy the Steinberg relation, for $\bar{a}_i + \bar{a}_j = 1$ implies $a_i + a_j = 1$. So if we show that they are linear in each variable, we get that each h_P is a homomorphism, and then by construction the direct sum $\bigoplus h_P$ yields an inverse for $\bar{\partial}_d^M$.

We check linearity in the case $n = 2$, the general case being similar. For $\bar{a}_2 = \bar{b}_2\bar{c}_2$, we compare the polynomials a_2 and b_2c_2 . If they are equal, the claim is obvious. If not, we perform Euclidean division of b_2c_2 by π_P to get $b_2c_2 = a_2 - \pi_P f$ with some polynomial $f \in k[t]$ of degree $\leq d-1$ (note that the rest of the division must be a_2 by uniqueness). Therefore

$$\frac{\pi_P f}{a_2} = 1 - \frac{b_2c_2}{a_2}, \tag{6}$$

and so in $K_2^M(k(t))$ we have the equalities

$$\{\pi_P, b_2c_2\} - \{\pi_P, a_2\} = \left\{ \pi_P, \frac{b_2c_2}{a_2} \right\} = - \left\{ \frac{f}{a_2}, \frac{b_2c_2}{a_2} \right\} + \left\{ \frac{\pi_P f}{a_2}, \frac{b_2c_2}{a_2} \right\} = - \left\{ \frac{f}{a_2}, \frac{b_2c_2}{a_2} \right\},$$

where we used the equality (6) in the last step. The last symbol lies in L_{d-1} , and the claim follows. \square

Proof of Theorem 7.2.1: Using induction on d , we derive from the previous lemma exact sequences

$$0 \rightarrow L_0 \rightarrow L_d \rightarrow \bigoplus_{\deg(P) \leq d} K_{n-1}^M(\kappa(P)) \rightarrow 0$$

for each $d > 0$. These exact sequences form a natural direct system with respect to the inclusions coming from the filtration (5). As $L_0 = K_n^M(k)$ and $\bigcup L_d = K_n^M(k(t))$, we obtain the exact sequence of the theorem by passing to the limit. The statement about s_{t-1}^M is straightforward. \square

Note that Milnor's exact sequence bears a close resemblance to Faddeev's exact sequence in the form of Corollary 6.9.3. As in that chapter, the fact that the sequence splits allows us to define *coresidue* maps

$$\psi_P^M : K_{n-1}^M(\kappa(P)) \rightarrow K_n^M(k(t))$$

for all closed points $P \neq \infty$, enjoying the properties $\partial_P^M \circ \psi_P^M = \text{id}_{\kappa(P)}$ and $\partial_P^M \circ \psi_Q^M = 0$ for $P \neq Q$. We thus obtain the following formula useful in calculations.

Corollary 7.2.3 *For all closed points P of \mathbf{A}_k^1 , let a_P be a generator of the extension $\kappa(P)|k$. Then we have the equality*

$$\alpha = s_{t-1}(\alpha)_{k(t)} + \sum_{P \in \mathbf{A}_0^1} (\psi_P^M \circ \partial_P)(\alpha)$$

for all $n > 0$ and all $\alpha \in K_n^M(k(t))$.

For all $P \neq \infty$ we define *norm maps* $N_P : K_n^M(\kappa(P)) \rightarrow K_n^M(k)$ by the formula

$$N_P := -\partial_\infty^M \circ \psi_P^M$$

for all $n \geq 0$. For $P = \infty$ we define N_P to be the identity map of $K_n^M(k)$.

With the above notations, Milnor's exact sequence implies

Corollary 7.2.4 (Weil reciprocity law) *For all $\alpha \in K_n^M(k(t))$ we have*

$$\sum_{P \in \mathbf{P}_0^1} (N_P \circ \partial_P^M)(\alpha) = 0.$$

Proof: For $P \neq \infty$ we have from the defining property of the maps ψ_P

$$\partial_P \left(\alpha - \sum_{P \neq \infty} (\psi_P \circ \partial_P)(\alpha) \right) = \partial_P(\alpha) - \partial_P(\alpha) = 0,$$

so by Milnor's exact sequence

$$\alpha - \sum_{P \neq \infty} (\psi_P \circ \partial_P)(\alpha) = \beta$$

for some β coming from $K_n^M(k)$. We have $\partial_\infty(\beta) = 0$, so the corollary follows by applying $-\partial_\infty$ to both sides. \square

Weil's original reciprocity law concerned the case $n = 2$ and had the form

$$\sum_{P \in \mathbf{P}_0^1} (N_{\kappa(P)|k} \circ \partial_P^M)(\alpha) = 0.$$

Note that in this case the tame symbols ∂_P^M have an explicit description by Example 7.1.5. To relate this form to the previous corollary, it suffices to use the second statement of the following proposition.

Proposition 7.2.5 *For $n = 0$ the map $N_P : K_0^M(\kappa(P)) \rightarrow K_0^M(k)$ is given by multiplication with $[\kappa(P) : k]$, and for $n = 1$ it coincides with the field norm $N_{\kappa(P)|k} : \kappa(P)^\times \rightarrow k^\times$.*

The proof relies on the following behaviour of the norm map under extensions of the base field.

Lemma 7.2.6 *Let $K|k$ be a field extension, and P a closed point of \mathbf{P}_k^1 . Then the diagram*

$$\begin{array}{ccc} K_n^M(\kappa(P)) & \xrightarrow{N_P} & K_n^M(k) \\ \oplus_{i_{\kappa(Q)|\kappa(P)}} \downarrow & & \downarrow i_{K|k} \\ \bigoplus_{Q \mapsto P} K_n^M(\kappa(Q)) & \xrightarrow{\sum e_Q N_Q} & K_n^M(K) \end{array}$$

commutes, where the notation $Q \mapsto P$ stands for the closed points of \mathbf{P}_K^1 lying above P , and e_Q is the ramification index of the valuation v_Q extending v_P to $K(t)$.

Proof: According to Remark 7.1.6 (2), the diagram

$$\begin{array}{ccc} K_{n+1}^M(k(t)) & \xrightarrow{\partial_P^M} & K_n^M(\kappa(P)) \\ i_{K(t)|k(t)} \downarrow & & \downarrow \oplus i_{\kappa(Q)|\kappa(P)} \\ K_{n+1}^M(K(t)) & \xrightarrow{\oplus e_Q \partial_Q^M} & \bigoplus_{Q \rightarrow P} K_n^M(\kappa(Q)) \end{array}$$

commutes. Hence so does the diagram

$$\begin{array}{ccc} K_{n+1}^M(k(t)) & \xleftarrow{\psi_P^M} & K_n^M(\kappa(P)) \\ i_{K(t)|k(t)} \downarrow & & \downarrow \oplus i_{\kappa(Q)|\kappa(P)} \\ K_{n+1}^M(K(t)) & \xleftarrow{\Sigma e_Q \psi_Q^M} & \bigoplus_{Q \rightarrow P} K_n^M(\kappa(Q)) \end{array}$$

whence the compatibility of the lemma in view of the definition of the norm maps N_P . \square

Proof of Proposition 7.2.5: Apply the above lemma with K an algebraic closure of k . In this case the points Q have degree 1 over K , so the maps N_Q are identity maps. Moreover, the vertical maps are injective for $n = 0, 1$. The statement for $n = 0$ then follows from the formula $\sum e_Q = [\kappa(P) : k]$ (a particular case of Proposition A.6.7 of the Appendix), and for $n = 1$ from the definition of the field norm $N_{\kappa(P)|k}(\alpha)$ as the product of the roots in K (considered with multiplicity) of the minimal polynomial of α . \square

Remark 7.2.7 For later use, let us note that the norm maps N_P satisfy the *projection formula*: for $\alpha \in K_n^M(k)$ and $\beta \in K_m^M(\kappa(P))$ one has

$$N_P(\{\alpha_{\kappa(P)}, \beta\}) = \{\alpha, N_P(\beta)\}.$$

This is an immediate consequence of the definitions.

We conclude this section by a very useful technical statement which is not a consequence of Milnor's exact sequence itself, but is proven in a similar vein. Observe that if $K|k$ is a field extension, the graded ring $K_*^M(K)$ becomes a (left) $K_*^M(k)$ -module via the change-of-fields map $K_*^M(k) \rightarrow K_*^M(K)$ and the product structure.

Proposition 7.2.8 (Bass-Tate Lemma) *Let $K = k(a)$ be a field extension obtained by adjoining a single element a of degree d to k . Then $K_*^M(K)$ is generated as a left $K_*^M(k)$ -module by elements of the form*

$$\{\pi_1(a), \pi_2(a), \dots, \pi_m(a)\},$$

where the π_i are monic irreducible polynomials in $k[t]$ satisfying $\deg(\pi_1) < \deg(\pi_2) < \dots < \deg(\pi_m) \leq d - 1$.

The proof is based on the following property of the subgroups L_d introduced in Lemma 7.2.2.

Lemma 7.2.9 *The subgroup $L_d \subset K_n^M(k(t))$ is generated by symbols of the shape*

$$\{a_1, \dots, a_m, \pi_{m+1}, \pi_{m+2}, \dots, \pi_n\}, \quad (7)$$

where the a_i belong to k^\times and the π_i are monic irreducible polynomials in $k[t]$ satisfying $\deg(\pi_{m+1}) < \deg(\pi_{m+2}) < \dots < \deg(\pi_n) \leq d$.

Proof: By factoring polynomials into irreducible terms and using bilinearity and graded-commutativity of symbols, we obtain generators for the group L_d of the shape (7), except that the π_i a priori only satisfy $\deg(\pi_{m+1}) \leq \dots \leq \deg(\pi_n) \leq d$. The point is to show that the inequalities may be chosen to be strict, which we do in the case $n = 2$ for polynomials π_1, π_2 of the same degree, the general case being similar. We use induction on d starting from the case $d = 0$ where we get constants $\pi_1 = a_1, \pi_2 = a_2$. So assume $d > 0$. If $\deg(\pi_1) = \deg(\pi_2) < d$, we are done by induction. It remains the case $\deg(\pi_1) = \deg(\pi_2) = d$, where we perform Euclidean division to get $\pi_2 = \pi_1 + f$ with some f of degree $\leq d - 1$. So $1 = \pi_1/\pi_2 + f/\pi_2$ and therefore $\{\pi_1/\pi_2, f/\pi_2\} = 0$ in $K_2^M(k(t))$. Using Lemma 7.1.2 we may write

$$\{\pi_1, \pi_2\} = \{\pi_1/\pi_2, \pi_2\} + \{\pi_2, -1\} = -\{\pi_1/\pi_2, f/\pi_2\} + \{\pi_1/\pi_2, f\} + \{\pi_2, -1\},$$

which equals $-(\{f, \pi_1\} + \{-f, \pi_2\})$ by bilinearity and graded-commutativity. We conclude by decomposing the polynomial f into irreducible factors. \square

Proof of Proposition 7.2.8: Let π_P be the minimal polynomial of a over k ; it defines a closed point P of degree d on \mathbf{P}_k^1 . It follows from Lemma 7.2.2 that the tame symbol ∂_P^M induces a surjection of L_d onto $K_n^M(\kappa(P))$. Applying the previous lemma, we conclude that $K_n^M(\kappa(P))$ is generated by symbols of the form

$$\partial_P^M \{a_1, \dots, a_m, \pi_{m+1}, \pi_{m+2}, \dots, \pi_n\},$$

where the a_i belong to k^\times and the π_i are monic irreducible polynomials satisfying $\deg(\pi_1) < \deg(\pi_2) < \cdots < \deg(\pi_n) \leq d$. If $\pi_n \neq \pi_P$, all the π_i satisfy $v_\pi(\pi_i) = 0$ and the above symbols are zero. For $\pi_n = \pi_P$, they equal $\{a_1, \cdots, a_m, \pi_{m+1}(a), \pi_{m+2}(a), \cdots, \pi_{n-1}(a)\}$ up to a sign by the defining property of ∂_P^M , and the proposition follows. \square

In the sequel we shall use the Bass-Tate lemma several times via the following corollary.

Corollary 7.2.10 *Let $K|k$ be a finite field extension. Assume one of the following holds:*

- $K|k$ is a quadratic extension,
- $K|k$ is of prime degree p and k has no nontrivial finite extensions of degree prime to p .

Then $K_^M(K)$ is generated as a left $K_*^M(k)$ -module by $K_1^M(K) = K^\times$. In other words, the product maps $K_{n-1}^M(k) \otimes K^\times \rightarrow K_n^M(K)$ are surjective.*

Proof: In both cases, K is obtained by adjoining a single element a to k , and the only monic irreducible polynomials in $k[t]$ of degree strictly smaller than $[K : k]$ are the linear polynomials $x - a$. We conclude by applying the proposition. \square

Remark 7.2.11 A typical case when the second condition of the corollary is satisfied is when k is a *maximal prime to p extension* of some field $k_0 \subset k$. This is an algebraic extension $k|k_0$ such that all finite subextensions have degree prime to p and which is maximal with respect to this property. If k_0 is perfect or has characteristic p , we can construct such an extension k by taking the subfield of a separable closure k_s of k_0 fixed by a pro- p Sylow subgroup of $\text{Gal}(k_s|k_0)$. If k_0 is none of the above, we may take k to be a maximal prime to p extension of a perfect closure of k_0 .

7.3 The Norm Map

Let $K|k$ be a finite field extension. In this section we construct norm maps $N_{K|k} : K_n^M(K) \rightarrow K_n^M(k)$ for all $n \geq 0$ satisfying the following properties:

1. The map $N_{K|k} : K_0^M(K) \rightarrow K_0^M(k)$ is multiplication by $[K : k]$.
2. The map $N_{K|k} : K_1^M(K) \rightarrow K_1^M(k)$ is the field norm $N_{K|k} : K^\times \rightarrow k^\times$.

3. (Projection formula) Given $\alpha \in K_n^M(k)$ and $\beta \in K_m^M(K)$, one has

$$N_{K|k}(\{\alpha_K, \beta\}) = \{\alpha, N_{K|k}(\beta)\}.$$

4. (Composition) Given a tower of field extensions $K'|K|k$, one has

$$N_{K'|k} = N_{K|k} \circ N_{K'|K}.$$

Furthermore, a reasonable norm map should be compatible (for finite separable extensions) with the corestriction maps on cohomology via the Galois symbol. This issue will be discussed in the next section.

Remark 7.3.1 For any norm map satisfying the above properties (1)–(3) the composite maps $N_{K|k} \circ i_{K|k} : K_n^M(k) \rightarrow K_n^M(k)$ are given by multiplication with the degree $[K : k]$ for all n . This is obvious for $n = 0, 1$, and the case $n > 1$ follows from the case $n = 1$ by an easy induction using the projection formula.

In the case when $K = k(a)$ is a simple field extension, the minimal polynomial of a defines a closed point P on \mathbf{P}_k^1 for which $K \cong \kappa(P)$. The norm map N_P of the previous section satisfies properties (1) and (2) by virtue of Proposition 7.2.5, as well as property (3) by Remark 7.2.7, so it is a natural candidate for $N_{K|k}$. But even in this case one has to check that the definition depends only on K and not on the choice of P .

Changing the notation slightly, for a simple finite field extension $K = k(a)$ define $N_{a|k} : K_n^M(k(a)) \rightarrow K_n^M(k)$ by $N_{a|k} := N_P$, where P is the closed point of \mathbf{P}_k^1 considered above. Given an arbitrary finite field extension $K|k$, write $K = k(a_1, \dots, a_r)$ for some generators a_1, \dots, a_r and consider the chain of subfields

$$k \subset k(a_1) \subset k(a_1, a_2) \subset \cdots \subset k(a_1, \dots, a_r) = K.$$

Now put

$$N_{a_1, \dots, a_r|k} := N_{a_r|k(a_1, \dots, a_{r-1})} \circ \cdots \circ N_{a_2|k(a_1)} \circ N_{a_1|k}.$$

Note that by the preceding discussion the maps $N_{a_1, \dots, a_r|k}$ satisfy properties (1)–(4) above, and also the formula $N_{a_1, \dots, a_r|k} \circ i_{K|k} = [K : k]$, by virtue of Remark 7.3.1.

Theorem 7.3.2 (Kato) *The maps $N_{a_1, \dots, a_r|k} : K_n^M(K) \rightarrow K_n^M(k)$ do not depend on the choice of the generating system (a_1, \dots, a_r) .*

The theorem allows us to define without ambiguity

$$N_{K|k} := N_{a_1, \dots, a_r|k} : K_n^M(K) \rightarrow K_n^M(k)$$

for all $n \geq 0$. We have the following immediate corollary:

Corollary 7.3.3 *For a k -automorphism $\sigma : K \rightarrow K$ one has $N_{K|k} \circ \sigma = N_{K|k}$.*

Proof: Indeed, according to the theorem $N_{a_1, \dots, a_r|k} = N_{\sigma(a_1), \dots, \sigma(a_r)|k}$ for every system of generators (a_1, \dots, a_r) . \square

The rest of this section will be devoted to the proof of Kato's theorem. A major step in the proof is the following reduction statement, essentially due to Bass and Tate.

Proposition 7.3.4 *Assume that Theorem 7.3.2 holds for all fields k that have no nontrivial finite extension of degree prime to p for some prime number p . Then the theorem holds for arbitrary k .*

For the proof we need some auxiliary statements.

Lemma 7.3.5 *For an algebraic extension $K|k$ the kernel of the change-of-fields map $i_{K|k} : K_n^M(k) \rightarrow K_n^M(K)$ is a torsion group. It is annihilated by the degree $[K : k]$ in the case of a finite extension.*

Proof: Considering $K_n^M(K)$ as the direct limit of the groups $K_n^M(K_i)$ for all finite subextensions $k \subset K_i \subset K$ we see that it suffices to prove the second statement. Write $K = k(a_1, \dots, a_r)$ for some generators a_i . As noted above, the norm map $N_{a_1, \dots, a_r|k}$ satisfies the formula $N_{a_1, \dots, a_r|k} \circ i_{K|k} = [K : k]$, whence the claim. \square

Before stating the next lemma, recall the following well-known facts from algebra (see e.g. Atiyah-Macdonald [1], Chapter 8). Given a finite field extension $K|k$ and an arbitrary field extension $L|k$, the tensor product $K \otimes_k L$ is a finite dimensional (hence Artinian) L -algebra, and as such decomposes as a finite direct sum of local L -algebras R_j in which the maximal ideal M_j is nilpotent. Let e_j be the smallest positive integer with $M_j^{e_j} = 0$. In the case when $K = k(a)$ is a simple field extension, the e_j correspond to the multiplicities of the irreducible factors in the decomposition of the minimal polynomial $f \in k[t]$ of a over L . In particular, for $K|k$ separable all the e_j are equal to 1.

Lemma 7.3.6 *In the above situation, write $K = k(a_1, \dots, a_r)$ with suitable $a_i \in K$. Denote by L_j the residue field R_j/M_j and by $p_j : L \otimes_k K \rightarrow L_j$ the natural projections. Then the diagram*

$$\begin{array}{ccc} K_n^M(K) & \xrightarrow{N_{a_1, \dots, a_r|k}} & K_n^M(k) \\ \oplus i_{L_j|K} \downarrow & & \downarrow i_{L|k} \\ \bigoplus_{j=1}^m K_n^M(L_j) & \xrightarrow{\sum e_j N_{p_j(a_1), \dots, p_j(a_r)|L}} & K_n^M(L) \end{array}$$

commutes.

Proof: By the discussion above, for $r = 1$ we are in the situation of Lemma 7.2.6 and thus the statement has been already proven (modulo a straightforward identification of the e_i with the ramification indices of the corresponding valuations on $k(t)$). We prove the general case by induction on r . Write $k(a_1) \otimes_k L \cong \oplus R_j$ for some local L -algebras R_j , and decompose the finite dimensional L -algebra $K \otimes_{k(a_1)} R_j$ as $K \otimes_{k(a_1)} R_j = \oplus R_{ij}$ for some R_{ij} . Note that $K \otimes_k L \cong \oplus_{i,j} R_{ij}$. Write L_j (resp. L_{ij}) for the residue fields of the L -algebras R_j (resp. R_{ij}), and similarly e_j and e_{ij} for the corresponding nilpotence indices. In the diagram

$$\begin{array}{ccccc}
 K_n^M(K) & \xrightarrow{N_{a_2, \dots, a_r | k(a_1)}} & K_n^M(k(a_1)) & \xrightarrow{N_{a_1 | k}} & K_n^M(k) \\
 \oplus i_{L_{ij} | K} \downarrow & & \oplus i_{L_j | k(a_1)} \downarrow & & \downarrow i_{L | k} \\
 \bigoplus_{i,j} K_n^M(L_{ij}) & \xrightarrow{\bigoplus_j \sum_i (e_{ij} e_j^{-1}) N_{p_{ij}(a_2), \dots, p_{ij}(a_r) | L_j}} & \bigoplus_j K_n^M(L_j) & \xrightarrow{\sum e_j N_{p_j(a_1) | L}} & K_n^M(L)
 \end{array}$$

both squares commute by the inductive hypothesis. The lemma follows. \square

Proof of Proposition 7.3.4: Write $K = k(a_1, \dots, a_r) = k(b_1, \dots, b_s)$ in two different ways. Let $\Delta \subset K_n^M(K)$ be the subgroup generated by elements of the form $N_{a_1, \dots, a_r | k}(\alpha) - N_{b_1, \dots, b_s | k}(\alpha)$ for some $\alpha \in K_n^M(K)$. Our job is to prove $\Delta = 0$. Consider the diagram of the previous lemma with $L = \bar{k}$, an algebraic closure of k . Then $L_j \cong L$ for all j and in the bottom row we have a sum of identity maps. Considering the similar diagram for $N_{b_s, \dots, b_s | k}$ we get an equality $i_{\bar{k} | k} \circ N_{a_1, \dots, a_r | k} = i_{\bar{k} | k} \circ N_{b_1, \dots, b_s | k}$, whence $\Delta \subset \ker(i_{\bar{k} | k})$. We thus conclude from Lemma 7.3.5 that Δ is a torsion group. Denoting by Δ_p its p -primary component it is therefore enough to show that $\Delta_p = 0$ for all prime numbers p . Fix a prime p and let L be a maximal prime to p extension of k (cf. Remark 7.2.11). As all finite subextensions of $L | k$ have degree prime to p , an application of Lemma 7.3.5 shows that the restriction of $i_{L | k}$ to Δ_p is injective. On the other hand, the assumption of the proposition applies to L and hence the map $\sum N_{p_j(a_1), \dots, p_j(a_r) | L}$ of Lemma 7.3.6 does not depend on the a_i . Therefore $i_{L | k}(\Delta_p) = 0$, which concludes the proof. \square

For the rest of this section p will be a fixed prime number, and k will always denote a field having no nontrivial finite extensions of degree prime to p .

Concerning such fields, the following easy lemma will be helpful.

Lemma 7.3.7 *Let $K | k$ be a finite extension.*

1. *The field K inherits the property of having no nontrivial finite extension of degree prime to p .*

2. If $K \neq k$, there exists a subfield $k \subset K_1 \subset K$ such that $K_1|k$ is a normal extension of degree p .

Proof: For the first statement let $L|K$ be a finite extension of degree prime to p . If $L|k$ is separable, take a Galois closure \tilde{L} . By our assumption on k , the fixed field of a p -Sylow subgroup in $\text{Gal}(\tilde{L}|k)$ must equal k , so that $L = K$. If $K|k$ is purely inseparable, then $L|K$ must be separable, so $L|k$ has a subfield $L_0 \neq k$ separable over k unless $L = K$. Finally, if $K|k$ is separable but $L|K$ is not, we may assume the latter to be purely inseparable. Taking a normal closure \tilde{L} , the fixed field of $\text{Aut}_k(\tilde{L})$ defines a nontrivial prime to p extension of k unless $L = K$.

The second statement is straightforward in the case when the extension $K|k$ is purely inseparable, so by replacing K with the maximal separable subextension of $K|k$ we may assume that $K|k$ is a separable extension. Consider the Galois closure \tilde{K} of K . The first statement implies that the Galois group $G := \text{Gal}(\tilde{K}|k)$ is a p -group. Now let H be a maximal subgroup of G containing $\text{Gal}(\tilde{K}|K)$. By the theory of finite p -groups (see e.g. Suzuki [1], Corollary of Theorem 1.6), it is a normal subgroup of index p in G , so we may take K_1 to be its fixed field. \square

We now start the proof of Theorem 7.3.2 with the case of a degree p extension, still due to Bass and Tate.

Proposition 7.3.8 *Assume that $[K : k] = p$, and write $K = k(a)$ for some $a \in K$. The norm maps $N_{a|k} : K_n^M(k(a)) \rightarrow K_n^M(k)$ do not depend on the choice of a .*

Proof: Let P be the closed point of \mathbf{P}_k^1 defined by the minimal polynomial of a . According to Corollary 7.2.10, the group $K_n^M(K)$ is generated by symbols of the form $\{\alpha_K, b\}$, with $\alpha \in K_{n-1}^M(k)$ and $b \in K^\times$. We compute using the projection formula for N_P (Remark 7.2.7) and Proposition 7.2.5:

$$N_{a|k}(\{\alpha_K, b\}) = N_P(\{\alpha_K, b\}) = \{\alpha, N_P(b)\} = \{\alpha, N_{K|k}(b)\}.$$

Here the right hand side does not depend on a , as was to be shown. \square

Henceforth the notation $N_{L|K} : K_n^M(L) \rightarrow K_n^M(K)$ will be legitimately used for extensions of degree p (and for those of degree 1).

Next we need the following compatibility statement with the tame symbol (which does not concern k , so there is no assumption on the fields involved). For a generalisation, see Proposition 7.4.1 in the next section.

Proposition 7.3.9 *Let K be a field complete with respect to a discrete valuation v with residue field κ , and $K'|K$ a normal extension of degree p . Denote by κ' the residue field of the unique extension v' of v to K' . Then for all $n > 0$ the diagram*

$$\begin{array}{ccc} K_n^M(K') & \xrightarrow{\partial_{K'}^M} & K_{n-1}^M(\kappa') \\ N_{K'|K} \downarrow & & \downarrow N_{\kappa'|\kappa} \\ K_n^M(K) & \xrightarrow{\partial_K^M} & K_{n-1}^M(\kappa) \end{array}$$

commutes.

The notes of Sridharan [1] have been helpful to us in writing up the following proof. We begin with a special case.

Lemma 7.3.10 *The compatibility of the proposition holds for symbols of the form $\alpha = \{a', a_2, \dots, a_n\} \in K_n^M(K')$, with $a' \in K'^{\times}$ and $a_i \in K^{\times}$.*

Proof: Using Lemma 7.1.2, multilinearity and graded-commutativity we may assume that $v(a_i) = 0$ for $i > 2$ and $0 \leq v(a'), v(a_2) \leq 1$. Setting $f := [\kappa' : \kappa]$ and denoting by e the ramification index of $v'|v$ we have the formula

$$f \cdot v' = v \circ N_{K'|K} \quad (8)$$

(see Appendix, Proposition A.6.8 (2)). Now there are four cases to consider.

Case 1: $v'(a') = v(a_2) = 0$. Then $v(N_{K'|K}(a')) = 0$, so using the projection formula we obtain $\partial_K^M(N_{K'|K}(\alpha)) = 0$, and likewise $\partial_{K'}^M(\alpha) = 0$.

Case 2: $v'(a') = 1, v(a_2) = 0$. In this case Remark 7.3.1 implies that with the usual notations $N_{\kappa'|\kappa}(\partial_{K'}^M(\alpha)) = f\{\bar{a}_2, \dots, \bar{a}_n\}$. On the other hand, from (8) we infer that $N_{K'|K}(a') = u\pi^f$ for some unit u and local parameter π for v . So using the projection formula and the multilinearity of symbols we get $N_{K'|K}(\alpha) = f\{\pi, a_2, \dots, a_n\} + \{u, a_2, \dots, a_n\}$. This element has residue $f\{\bar{a}_2, \dots, \bar{a}_n\}$ as well.

Case 3: $v'(a') = 0, v(a_2) = 1$. Then $a_2 = u'\pi'^e$ for some unit u' and local parameter π' for v' , so using graded-commutativity and multilinearity of symbols we obtain $\partial_{K'}^M(\alpha) = -e\{\bar{a}', \bar{a}_3, \dots, \bar{a}_n\}$. This element has norm $-e\{N_{\kappa'|\kappa}(\bar{a}'), \bar{a}_3, \dots, \bar{a}_n\}$ by the projection formula. On the other hand, $\partial_K^M(N_{K'|K}(\alpha)) = -\{N_{K'|K}(a'), \bar{a}_3, \dots, \bar{a}_n\}$. The claim now follows from the equality $N_{K'|K}(a') = N_{\kappa'|\kappa}(\bar{a}')^e$, which is easily verified in both the unramified and the totally ramified case.

Case 4: $v'(a') = v(a_2) = 1$. Write $a' = \pi'$, $a_2 = \pi$, $\pi = u'\pi'^e$, $N_{K'|K}(\pi') = u\pi^f$ as above. Then using multilinearity and Lemma 7.1.2 we get

$$\partial_{K'}^M(\alpha) = \partial_{K'}^M(\{\pi', u', a_3, \dots, a_n\} + e\{\pi', -1, a_3, \dots, a_n\}) = \{(-1)^e \bar{u}', \bar{a}_3, \dots, \bar{a}_n\},$$

which has norm $\{(-1)^{ef} N_{\kappa'|\kappa}(\bar{u}'), \bar{a}_3, \dots, \bar{a}_n\}$. On the other hand, using the projection formula we obtain as above

$$\begin{aligned} \partial_K^M(N_{K'|K}(\alpha)) &= \partial_K^M(\{u\pi^f, \pi, a_3, \dots, a_n\}) = \\ &= \partial_K^M(-\{\pi, u, a_3, \dots, a_n\} + f\{\pi, -1, a_3, \dots, a_n\}) = \{(-1)^f \bar{u}^{-1}, \bar{a}_3, \dots, \bar{a}_n\}. \end{aligned}$$

So it is enough to see $(-1)^{ef} N_{\kappa'|\kappa}(\bar{u}') = (-1)^f \bar{u}^{-1}$. Notice that in the above computations we are free to modify π and π' by units. In particular, in the case when $e = 1$ and $f = p$ we may take $\pi = \pi'$, so that $u' = u = 1$ and the equality is obvious. In the case $e = p$, $f = 1$ the element π' is a root of an Eisenstein polynomial $x^p + a_{p-1}x^{p-1} + \dots + a_0$ and we may take $\pi = a_0$. Then $u = (-1)^p$ and $\bar{u}' = -1$, so we are done again. \square

Proof of Proposition 7.3.9: Let α be an element of $K_n^M(K')$, and set $\delta := \partial_K^M(N_{K'|K}(\alpha)) - N_{\kappa'|\kappa}(\partial_{K'}^M(\alpha))$. We prove $\delta = 0$ by showing that δ is annihilated both by some power of p and by some integer prime to p .

By Corollary 7.2.10, if $K^{(p)}$ denotes a maximal prime to p extension of K , the image of α in $K_n^M(K'K^{(p)})$ is a sum of symbols of the shape as in Lemma 7.3.10 above (for the extension $KK^{(p)}|K^{(p)}$). These symbols are all defined at a finite level, so the lemma enables us to find some extension $L|K$ of degree prime to p so that

$$\delta^L := \partial_L^M(N_{LK'|L}(i_{LK'|K'}(\alpha))) - N_{\kappa'_L|\kappa_L}(\partial_{LK'}^M(i_{LK'|K'}(\alpha))) = 0.$$

Now since $K'|K$ has degree p , we have $LK' \cong L \otimes_K K'$. This implies that the valuations $v'|v$ and their unique extensions $v'_L|v_L$ have the same ramification index e , and hence by Remark 7.1.6 (2) the tame symbol $\partial_{LK'}^M$ is the e -th multiple of ∂_L^M on symbols coming from $K_n^M(L)$, just like the tame symbol $\partial_{K'}^M$ is the e -th multiple of ∂_K^M on $i_{K'|K}(K_n^M(K))$. On the other hand, by Lemma 7.3.6 the norm map $N_{LK'|L}$ is the base change of $N_{K'|K}$ to $K_n^M(LK')$. It follows from these remarks that we have $i_{L|K}(\delta) = \delta^L$, and hence $i_{L|K}(\delta) = 0$. Thus $[L : K]\delta = 0$ by Lemma 7.3.5.

To see that δ is annihilated by some power of p , we look at the base change $K' \otimes_K K'$. Assume first that $K'|K$ is separable. Then it is Galois by assumption, so $K' \otimes_K K'$ splits as a product of p copies of K' . Therefore it is obvious that the required compatibility holds for α after base change to K' .

But now there is a difference between the unramified and the ramified case. In the unramified case the residue fields in the copies of K' all equal κ , so the compatibilities of Remark 7.1.6 (2) and Lemma 7.3.6 apply with all ramification indices equal to 1, and we conclude as above that $i_{K'|K}(\delta) = 0$, hence $p\delta = 0$. In the ramified case the said compatibilities apply with ramification indices equal to p on the level of residue fields, so we conclude $pi_{K'|K}(\delta) = 0$ and $p^2\delta = 0$. Finally, in the case when $K'|K$ is purely inseparable, the tensor product $K' \otimes_K K'$ is a local ring with residue field κ' and nilpotent maximal ideal of length p . After base change to K' we therefore arrive at a diagram where both norm maps are identity maps, so the required compatibility is a tautology. Remark 7.1.6 (2) and Lemma 7.3.6 again apply with ramification indices equal to p , so we conclude as in the previous case that $p^2\delta = 0$. \square

Corollary 7.3.11 *Let $L|k$ be a normal extension of degree p , and let P be a closed point of the projective line \mathbf{P}_k^1 . Then the diagram*

$$\begin{array}{ccc} K_n^m(L(t)) & \xrightarrow{\oplus \partial_Q} & \bigoplus_{Q \rightarrow P} K_{n-1}^M(\kappa(Q)) \\ N_{L(t)|k(t)} \downarrow & & \downarrow \Sigma N_{\kappa(Q)|\kappa(P)} \\ K_n^m(k(t)) & \xrightarrow{\partial_P} & K_{n-1}^M(\kappa(P)) \end{array}$$

commutes for all $n > 0$.

Proof: Denote by \widehat{K}_P (resp. \widehat{L}_Q) the completions of $k(t)$ (resp. $L(t)$) with respect to the valuations defined by P and Q . In the diagram

$$\begin{array}{ccccc} K_n^M(L(t)) & \longrightarrow & \bigoplus_{Q \rightarrow P} K_n^M(\widehat{L}_Q) & \xrightarrow{\oplus \partial_Q} & \bigoplus_{Q \rightarrow P} K_{n-1}^M(\kappa(Q)) \\ N_{L(t)|k(t)} \downarrow & & \downarrow \Sigma N_{\widehat{L}_Q|\widehat{K}_P} & & \downarrow \Sigma N_{\kappa(Q)|\kappa(P)} \\ K_n^M(k(t)) & \longrightarrow & K_n^M(\widehat{K}_P) & \xrightarrow{\partial_P} & K_{n-1}^M(\kappa(P)) \end{array} \quad (9)$$

the right square commutes by the above proposition. Commutativity of the left square follows from Lemma 7.2.6 (or Lemma 7.3.6), noting that $L(t) \otimes_{k(t)} \widehat{K}_P$ is a direct product of fields according to Proposition A.6.4 (1) of the Appendix (and the remark following it). The corollary follows. \square

Now comes the crucial step in the proof of Theorem 7.3.2.

Lemma 7.3.12 *Let $L|k$ be a normal extension of degree p , and let $k(a)|k$ be a simple finite field extension. Assume that L and $k(a)$ are both subfields of*

some algebraic extension of k , and denote by $L(a)$ their composite. Then for all $n \geq 0$ the diagram

$$\begin{array}{ccc} K_n^M(L(a)) & \xrightarrow{N_{a|L}} & K_n^M(L) \\ N_{L(a)|k(a)} \downarrow & & \downarrow N_{L|k} \\ K_n^M(k(a)) & \xrightarrow{N_{a|k}} & K_n^M(k) \end{array}$$

commutes.

Proof: Let P (resp. Q_0) be the closed point of \mathbf{P}_k^1 (resp. \mathbf{P}_L^1) defined by the minimal polynomial of a over k (resp. L). Given $\alpha \in K_n^M(L(a))$, we have $N_{a|L}(\alpha) = -\partial_\infty^M(\beta)$ for some $\beta \in K_{n+1}^M(L(t))$ satisfying $\partial_{Q_0}^M(\beta) = \alpha$ and $\partial_Q^M(\beta) = 0$ for $Q \neq Q_0$. Corollary 7.3.11 yields

$$\partial_P^M(N_{L(t)|k(t)}(\beta)) = \sum_{Q \rightarrow P} N_{\kappa(Q)|\kappa(P)}(\partial_Q^M(\beta)) = N_{\kappa(Q_0)|\kappa(P)}(\alpha),$$

and, by a similar argument, $\partial_{P'}^M(N_{L(t)|k(t)}(\beta)) = 0$ for $P \neq P'$. Hence by definition of $N_{a|k}$ we get

$$N_{a|k}(N_{L(a)|k(a)}(\alpha)) = -\partial_\infty^M(N_{L(t)|k(t)}(\beta)).$$

On the other hand, since the only point of \mathbf{P}_L^1 above ∞ is ∞ , another application of Corollary 7.3.11 gives

$$\partial_\infty^M(N_{L(t)|k(t)}(\beta)) = N_{L|k}(\partial_\infty^M(\beta)).$$

Hence finally

$$N_{a|k}(N_{L(a)|k(a)}(\alpha)) = -N_{L|k}(\partial_\infty^M(\beta)) = N_{L|k}(N_{a|L}(\alpha)).$$

□

At last, we come to:

Proof of Theorem 7.3.2: As noted before, it is enough to treat the case when k has no nontrivial extension of degree prime to p for a fixed prime p . Let p^m the degree of the extension $K|k$. We use induction on m , the case $m = 1$ being Proposition 7.3.8. Write $K = k(a_1, \dots, a_r) = k(b_1, \dots, b_s)$ in two different ways. By Lemma 7.3.7 (2) the extension $k(a_1)|k$ contains a normal subfield $k(\bar{a}_1)$ of degree p over k . Applying Lemma 7.3.12 with $a = a_1$ and $L = k(\bar{a}_1)$ yields $N_{a_1|k} = N_{\bar{a}_1|k} \circ N_{a_1|k(\bar{a}_1)}$. So by inserting \bar{a}_1 in the system

of the a_i and reindexing we may assume that $[k(a_1) : k] = p$, and similarly $[k(b_1) : k] = p$. Write K_0 for the composite of $k(a_1)$ and $k(b_1)$ in K , and choose elements c_i with $K = K_0(c_1, \dots, c_t)$. Note that by Lemma 7.3.7 (1) the fields $k(a_1)$ and $k(b_1)$ have no nontrivial prime to p extensions, so we may apply induction to conclude that

$$N_{a_2, \dots, a_r | k(a_1)} = N_{K_0 | k(a_1)} \circ N_{c_1, \dots, c_t | K_0} \quad \text{and} \quad N_{b_2, \dots, b_s | k(b_1)} = N_{K_0 | k(b_1)} \circ N_{c_1, \dots, c_t | K_0}.$$

On the other hand, Lemma 7.3.12 for $a = a_1$ and $L = k(b_1)$ implies

$$N_{a_1 | k} \circ N_{K_0 | k(a_1)} = N_{b_1 | k} \circ N_{K_0 | k(b_1)}.$$

The above equalities imply $N_{a_1, \dots, a_r | k} = N_{b_1, \dots, b_s | k}$, as desired. \square

7.4 Reciprocity Laws

As an application of the existence of norm maps, we now prove two theorems which both go under the name ‘reciprocity law’, though they are quite different. The first one will be the general form of the Weil reciprocity law. For its proof we need a compatibility between the tame symbol and the norm map (generalising Proposition 7.3.9) which we explain first.

Proposition 7.4.1 *Let K be a field complete with respect to a discrete valuation v with residue field κ . Let $K' | K$ be a finite extension, and denote by κ' the residue field of the unique extension v' of v to K' . Then for all $n > 0$ the diagram*

$$\begin{array}{ccc} K_n^M(K') & \xrightarrow{\partial_{K'}^M} & K_{n-1}^M(\kappa') \\ N_{K' | K} \downarrow & & \downarrow N_{\kappa' | \kappa} \\ K_n^M(K) & \xrightarrow{\partial_K^M} & K_{n-1}^M(\kappa) \end{array}$$

commutes.

Proof: We may split up $K' | K$ into a separable and a purely inseparable extension. The latter can be written as the union of a tower of radical extensions of degree equal to the characteristic of K . By applying Proposition 7.3.9 to each of these extensions we reduce to the case when $K' | K$ is a separable extension.

We next fix a prime number p , and let $K^{(p)}$ denote a maximal prime to p extension of K . Then $K^{(p)} \otimes_K K'$ splits up into a product of finite separable extensions $K_i | K^{(p)}$ with $[K_i : K^{(p)}]$ a power of p . Using Lemma

7.3.7 inductively, we may write $K_i|K^{(p)}$ as the union of a tower of normal extensions of degree p . A repeated application of Proposition 7.3.9 therefore implies the claim for $K_i|K^{(p)}$. Arguing as in the proof of that proposition, we obtain that for each $\alpha \in K_n^M(K')$ the element $\delta = \partial_K^M(N_{K'|K}(\alpha)) - N_{\kappa'|\kappa}(\partial_{K'}^M(\alpha))$ is annihilated by some integer prime to p . As p was arbitrary here, the proof is complete. \square

Corollary 7.4.2 *Assume moreover that there exist local parameters π and π' for v and v' , respectively, satisfying $(-\pi')^e = -\pi$, where e is the ramification index. Then for all $n > 0$ the diagram*

$$\begin{array}{ccc} K_n^M(K') & \xrightarrow{s_{\pi'}^M} & K_n^M(\kappa') \\ N_{K'|K} \downarrow & & \downarrow e N_{\kappa'|\kappa} \\ K_n^M(K) & \xrightarrow{s_{\pi}^M} & K_n^M(\kappa) \end{array}$$

commutes.

Note that the assumption of the corollary is satisfied in the cases when the ramification is tame (see Appendix, Proposition A.6.8 (4)) or the extension is purely inseparable.

Proof: By Remark 7.1.6 (1) and the projection formula we have

$$s_{\pi}^M(N_{K'|K}(\alpha)) = \partial_K^M(\{-\pi, N_{K'|K}(\alpha)\}) = \partial_K^M(N_{K'|K}(\{-\pi, \alpha\}))$$

for all $\alpha \in K_n^M(K')$. By our assumption on π and Proposition 7.4.1, the last term here equals $e N_{\kappa'|\kappa}(\partial_{K'}^M(\{-\pi', \alpha\})) = e N_{\kappa'|\kappa}(s_{\pi'}^M(\alpha))$, as desired. \square

The proposition has the following globalisation.

Corollary 7.4.3 *Let K be a field equipped with a discrete valuation v with residue field $\kappa(v)$, and let $K'|K$ be a finite extension. Assume that the integral closure of the valuation ring A of v in K' is a finite A -module, and for an extension w of v to K' denote by $\kappa(w)$ the corresponding residue field. Then for all $n > 0$ the diagram*

$$\begin{array}{ccc} K_n^M(K') & \xrightarrow{\oplus_{w|v} \partial_w^M} & \bigoplus_{w|v} K_{n-1}^M(\kappa(w)) \\ N_{K'|K} \downarrow & & \downarrow \Sigma N_{\kappa(w)|\kappa(v)} \\ K_n^M(K) & \xrightarrow{\partial_K^M} & K_{n-1}^M(\kappa(v)) \end{array}$$

commutes, where the sum is over the finitely many extensions w of v .

Proof: This is proven by exactly the same argument as Corollary 7.3.11: one has a diagram analogous to diagram (9) considered there, whose right square commutes by Proposition 7.4.1, and the left square by Proposition 7.3.6. \square

We may now extend the Weil reciprocity law to the case of curves.

Proposition 7.4.4 (Weil reciprocity law for a curve) *Let C be a smooth projective curve over k . For a closed point P let $\partial_P^M : K_n^M(k(C)) \rightarrow K_{n-1}^M(\kappa(P))$ be the tame symbol coming from the valuation on $k(C)$ defined by P . Then for all $\alpha \in K_n^M(k(C))$ we have*

$$\sum_{P \in C_0} (N_{\kappa(P)|k} \circ \partial_P^M)(\alpha) = 0.$$

Proof: Take a finite morphism $\phi : C \rightarrow \mathbf{P}^1$ defined over k . It induces a diagram

$$\begin{array}{ccccc} K_n^M(k(C)) & \xrightarrow{\oplus \partial_Q^M} & \bigoplus_{Q \in C_0} K_{n-1}^M(\kappa(Q)) & \xrightarrow{\Sigma N_{\kappa(Q)|k}} & K_{n-1}^M(k) \\ N_{k(C)|k(t)} \downarrow & & \downarrow \bigoplus_{P \in \mathbf{P}_0^1} \Sigma N_{\kappa(Q)|\kappa(P)} & & \downarrow \text{id} \\ K_n^M(k(t)) & \xrightarrow{\oplus \partial_P^M} & \bigoplus_{P \in \mathbf{P}_0^1} K_{n-1}^M(\kappa(P)) & \xrightarrow{\Sigma N_{\kappa(P)|k}} & K_{n-1}^M(k), \end{array}$$

where commutativity of the left square follows from Corollary 7.4.3 (applicable in view of Remark A.6.5 of the Appendix), and that of the right square from property (4) of the norm map. According to Corollary 7.2.4, the lower row is a complex, hence so is the upper row by commutativity of the diagram. \square

Remark 7.4.5 A special case of Weil’s reciprocity law often occurs in the following form. For a divisor $D = \sum n_P P \in \text{Div}(C)$ and a rational function $f \in k(C)$ such that $n_P = 0$ at all poles of f put

$$f(D) := \prod_P N_{\kappa(P)|k}(f(P))^{n_P},$$

where $f(P)$ is defined as the image of f in $\kappa(P)$.

Now suppose f and g are rational functions on C such that $\text{div}(f)$ and $\text{div}(g)$ have disjoint support, i.e. no closed point of C has a nonzero coefficient in both $\text{div}(f)$ and $\text{div}(g)$. Then by applying the case $n = 2$ of the Weil

reciprocity law to the symbol $\{f, g\}$ and using the explicit description of Example 7.1.5 one obtains the simple formula

$$f(\operatorname{div}(g)) = g(\operatorname{div}(f)).$$

The second reciprocity law we discuss in this section is due to Rosset and Tate, and only concerns K_2 . Let $f, g \in k[t]$ be nonzero relatively prime polynomials. Define the *Rosset-Tate symbol* $(f|g) \in K_2^M(k)$ by

$$(f|g) := s_t \left(\sum_{\{P: g(P)=0\}} (\psi_P^M \circ \partial_P^M)(\{g, f\}) \right), \quad (10)$$

where s_t is a specialisation map at 0 and ψ_P^M is the coresidue map introduced before Corollary 7.2.3. For g constant we set $(f|g) := 0$.

The symbol is additive in both variables, in the sense that $(f|g_1g_2) = (f|g_1) + (f|g_2)$ and $(f_1f_2|g) = (f_1|g) + (f_2|g)$. The following lemma describes it explicitly.

Lemma 7.4.6 *The Rosset-Tate symbol has the following properties.*

1. *If g is constant or $g = t$, then $(f|g) = 0$.*
2. *If g is a nonconstant irreducible polynomial different from t and a is a root of g in some algebraic closure of k , then*

$$(f|g) = N_{k(a)|k}(\{-a, f(a)\}).$$

Proof: In statement (1) we only have to treat the case $g = t$. In this case the sum in (10) defining $(f|g)$ has only one term coming from $P = 0$. Applying Corollary 7.2.3 with $\alpha = \{t, f\}$ yields $\{t, f\} = (\psi_0^M \circ \partial_0^M)(\{t, f\})$, so that $(t|f) = s_t(\{t, f(0)\}) = 0$.

For (2), the only closed point P of \mathbf{A}_k^1 contributing to the sum is that defined by the polynomial g . Let a be the image of g in $\kappa(P)$, so that $\kappa(P) = k(a)$. Since $\{-a, f(a)\} = s_t(\{t - a, f(a)\})$ (where the specialisation takes place in $\kappa(P)(t)$), applying Corollary 7.4.2 to the unramified extension $\kappa(P)((t))|k((t))$ yields

$$N_{\kappa(P)|k}(\{-a, f(a)\}) = s_t(N_{\kappa(P)(t)|k(t)}(\{t - a, f(a)\})).$$

Therefore the claim is a consequence of the equality

$$N_{\kappa(P)(t)|k(t)}(\{t - a, f(a)\}) = (\psi_P^M \circ \partial_P^M)(\{g, f\}).$$

This equivalently means $N_{\kappa(P)(t)|k(t)}(\{t-a, f(a)\}) = \psi_P^M(f(a))$, which in turn follows from Corollary 7.2.3 applied to $\alpha = N_{\kappa(P)(t)|k(t)}(\{t-a, f(a)\})$, noting that $\partial_P^M(N_{\kappa(P)(t)|k(t)}(\{t-a, f(a)\})) = N_{\kappa(P)|\kappa(P)}(f(a)) = f(a)$ according to Corollary 7.4.3 applied with $K = k(t)$, $K' = \kappa(P)(t)$ and v the valuation defined by P , and moreover $s_{t-1}(N_{\kappa(P)(t)|k(t)}(\{t-a, f(a)\})) = 0$ by Corollary 7.4.2. \square

The second statement of the lemma implies:

Corollary 7.4.7 *The symbol $(f|g)$ depends only on the image of f in the quotient ring $k[t]/(g)$.*

Remark 7.4.8 The properties (1) and (2) of the lemma together with the additivity property characterise the symbol. In fact, Rosset and Tate [1] defined their symbol in such an explicit way, with a slight difference: according to their definition, the right hand side of the formula in property (2) is $N_{k(a)|k}(\{a, f(a)\})$.

To state the main theorem on the Rosset-Tate symbol, introduce the following notation for polynomials $f \in k[t]$: if $f = a_n t^n + a_{n-1} t^{n-1} + \dots + a_m t^m$ with $a_n a_m \neq 0$, put $\ell(P) := a_n$ (the leading coefficient) and $c(P) := a_m$ (the last nonzero coefficient). They depend multiplicatively on f .

Theorem 7.4.9 (Rosset-Tate reciprocity law) *Let $f, g \in k[t]$ be nonzero relatively prime polynomials. Then*

$$(f|g) + \{c(f), c(g)\} = (g|f) + \{\ell(f), \ell(g)\}.$$

Proof: By Corollary 7.2.3 we have

$$\{f, g\} = s_{t-1}(\{f, g\})_{k(t)} + \sum_{\{P: f(P)=0\}} (\psi_P^M \circ \partial_P^M)(\{f, g\}) + \sum_{\{P: g(P)=0\}} (\psi_P^M \circ \partial_P^M)(\{f, g\}),$$

so that

$$\sum_{\{P: g(P)=0\}} (\psi_P^M \circ \partial_P^M)(\{g, f\}) + \{f, g\} = s_{t-1}(\{f, g\})_{k(t)} + \sum_{\{P: f(P)=0\}} (\psi_P^M \circ \partial_P^M)(\{f, g\}).$$

By applying the specialisation map s_t at 0, we obtain

$$(f|g) + s_t(\{f, g\}) = s_{t-1}(\{f, g\}) + (g|f).$$

Finally, writing $f = c(f)t^m \tilde{f}$ and $g = c(g)t^l \tilde{g}$ with $\tilde{f}(0) = \tilde{g}(0) = 1$ we get $s_t(\{f, g\}) = \{c(f), c(g)\}$ by definition of s_t (Proposition 7.1.4). A similar computation shows $s_{t-1}(\{f, g\}) = \{\ell(f), \ell(g)\}$, and the theorem follows. \square

As a corollary, we obtain a bound on the length of the symbol $(f|g)$.

Corollary 7.4.10 *Let f and g be relatively prime polynomials. Then the symbol $(f|g) \in K_2^M(k)$ is of length at most $\deg(g)$, i.e. it is a sum of at most $\deg(g)$ terms of the form $\{a_i, b_i\}$.*

Proof: The proof goes by induction on the degree of g . The degree zero case means $(f|g) = 0$, which holds by Lemma 7.4.6 (1). The same statement and additivity of the symbol allows one to assume in the higher degree case that g is monic. Corollary 7.4.7 allows us to assume $\deg(f) < \deg(g)$, after performing Euclidean division of g by f . Theorem 7.4.9 then shows $(f|g) + \{c(f), c(g)\} = (g|f)$. By the inductive hypothesis the symbol $(g|f)$ has length at most $\deg(f)$, so that $(f|g)$ has length at most $\deg(f) + 1 \leq \deg(g)$. \square

Corollary 7.4.11 *Let $K|k$ be a finite field extension, and let a, b be elements of K^\times . Then the symbol $N_{K|k}(\{a, b\}) \in K_2^M(k)$ has length at most $[k(a) : k]$.*

Proof: By the projection formula, we have

$$N_{K|k}(\{a, b\}) = N_{k(a)|k}(N_{K|k(a)}(\{a, b\})) = N_{k(a)|k}(\{a, N_{K|k(a)}(b)\}).$$

Let g be the minimal polynomial of $-a$ over k . Then $N_{K|k(a)}(b) = f(-a)$ for some polynomial $f \in k[t]$ and $N_{k(a)|k}(\{a, N_{K|k(a)}(b)\}) = (f|g)$ by Lemma 7.4.6 (2), so the previous corollary applies. \square

Remark 7.4.12 The Euclidean division process by which we have proven Corollary 7.4.10 also provides an explicit algorithm for computing the symbol $N_{K|k}(\{a, b\})$.

The main motivation for Rosset and Tate to prove their reciprocity law was the following application to central simple algebras.

Proposition 7.4.13 *Let p be a prime number, and let k be a field of characteristic prime to p containing a primitive p -th root of unity ω . Every central simple k -algebra A of degree p is Brauer equivalent to a tensor product of at most $(p-1)!$ cyclic k -algebras of degree p .*

Note that the proposition proves a special case of the (surjectivity part of the) Merkurjev-Suslin theorem, and moreover it yields a bound on the length of a symbol of order p .

The proof will use the fact that norm maps on K-theory and corestrictions in Galois cohomology are compatible via the Galois symbol. Let's admit this for the moment; a proof will be given in the next section (Proposition 7.5.5).

Proof: If A is split, the statement is trivial. If A is nonsplit, then it is a division algebra split by a degree p extension $K|k$. As k has characteristic prime to p by assumption, the extension $K|k$ is separable. Denote by $\tilde{K}|k$ a Galois closure. Note that $\text{Gal}(\tilde{K}|k)$ is a subgroup of the degree p symmetric group S_p , so it has order dividing $p!$. In particular, each p -Sylow subgroup $P \subset \text{Gal}(\tilde{K}|K)$ has order p , and its fixed field $L := \tilde{K}^P$ has degree at most $(p-1)!$ over k . Choose an integer $m > 1$ with $[L:k]m \equiv 1 \pmod{p}$. Since A has period p , the algebra $B := A^{\otimes m}$ satisfies $[L:k][B] = [A]$ in $\text{Br}(k)$. Moreover, since $A \otimes_k L$ is split by the extension $\tilde{K}|L$, so does $B \otimes_k L$. Hence by Corollary 4.7.7 there exist $a, b \in L^\times$ with $B \otimes_k L \cong (a, b)_\omega$. We have

$$[A] = [L:k][B] = \text{Cor}_k^L([B \otimes_k L]) = \text{Cor}_k^L(h_{L,p}^2(\{a, b\})) = h_{k,p}^2(N_{L|k}(\{a, b\}))$$

using Propositions 4.7.1 and 7.5.5. By the previous corollary, the symbol $N_{L|k}(\{a, b\})$ has length at most $[L:k] \leq (p-1)!$, whence the proposition. \square

Remark 7.4.14 The case $p = 2$ gives back Corollary 1.2.1. In this case, the bound $(p-1)!$ is trivially optimal. However, for $p > 2$ it may be improved to $(p-1)!/2$ in the presence of a p -th root of unity (see Exercise 10). We know little about the optimality of the latter bound. In fact, the following famous question is attributed to Albert: *Is every degree p division algebra isomorphic to a cyclic algebra?* A positive answer for $p = 3$ follows from the above bound (the result is originally due to Wedderburn [3]; see Exercise 9), but the question is open for $p > 3$. Albert proposed conjectural counterexamples for $p = 5$, which were shown to be actually cyclic in the paper Rowen [3], where new putative counterexamples are put forward. A positive answer to the question in characteristic 0 would imply the same in positive characteristic (see Chapter 9, Exercise 4). Positive answers are known in important special cases, such as arithmetic fields (see Corollary 6.3.10 as well as Remarks 6.5.5 and 6.5.6), or function fields of complex surfaces (Ojanguren-Parimala [1]).

7.5 Applications to the Galois Symbol

In this section we collect some useful elementary remarks about the Galois symbol and the Bloch-Kato conjecture. To begin with, we examine compatibility properties for the Galois symbol.

Proposition 7.5.1 *Let K be a field equipped with a discrete valuation v with residue field κ . Assume $\text{char}(k) = \text{char}(\kappa)$, and let m be an integer invertible*

in K . Then for all $n > 0$ the diagram

$$\begin{array}{ccc} K_n^M(K) & \xrightarrow{\partial^M} & K_{n-1}^M(\kappa) \\ h_{K,m}^n \downarrow & & h_{\kappa,m}^{n-1} \downarrow \\ H^n(K, \mu_m^{\otimes n}) & \xrightarrow{\partial_v^n} & H^{n-1}(\kappa, \mu_m^{\otimes(n-1)}) \end{array}$$

commutes, where ∂_v^n is the residue map introduced in Chapter 6, Section 6.8.

Proof: Without loss of generality we may assume K is complete with respect to v . The case $n = 1$ follows immediately from the construction of the maps concerned. In the general case it suffices, as usual, to consider symbols of the shape $\{a, u_2, \dots, u_n\} \in K_n^M(K)$, where the u_i are units for v . Corollary 7.1.10 yields a well-defined section $\lambda_m : K_{n-1}^M(\kappa)/m \rightarrow K_{n-1}^M(K)/m$ to any specialisation map modulo m , sending $\{\bar{u}_2, \dots, \bar{u}_n\} \in K_{n-1}^M(\kappa)$ to $\{u_2, \dots, u_n\} \in K_{n-1}^M(K)$, where the u_i are arbitrary liftings u_i of the \bar{u}_i to units in K . Moreover, the diagram

$$\begin{array}{ccc} K_{n-1}^M(\kappa)/m & \xrightarrow{\lambda_m} & K_{n-1}^M(K)/m \\ h_{\kappa,m}^{n-1} \downarrow & & h_{K,m}^{n-1} \downarrow \\ H^{n-1}(\kappa, \mu_m^{\otimes(n-1)}) & \xrightarrow{\text{Inf}} & H^{n-1}(K, \mu_m^{\otimes(n-1)}) \end{array}$$

commutes, as one verifies using the explicit description of the Kummer maps $h_{K,m}^1$ and $h_{\kappa,m}^1$ in terms of cocycles (see e.g. Remark 3.2.4). The proposition now follows by induction from the case $n = 1$ via Lemma 6.8.4 (applied with $p = 1$, $q = n - 1$, G the absolute Galois group of K , H the inertia group of v , $A = \mu_m$ and $B = \mu_m^{\otimes(n-1)}$). \square

Remark 7.5.2 The restriction $\text{char}(k) = \text{char}(\kappa)$ has been imposed here for the sole reason that in Chapter 6 we have only defined the maps ∂_v^n in this case. But it is possible to define them for an arbitrary discrete valuation and the proposition holds in general.

As a corollary, we get the compatibility between specialisation maps.

Corollary 7.5.3 *Assume moreover that t is a local parameter for v . Then the diagram of specialisation maps*

$$\begin{array}{ccc} K_n^M(K) & \xrightarrow{s_t^M} & K_n^M(\kappa) \\ h_{K,m}^n \downarrow & & h_{\kappa,m}^n \downarrow \\ H^n(K, \mu_m^{\otimes n}) & \xrightarrow{s_t^n} & H^n(\kappa, \mu_m^{\otimes(n-1)}) \end{array}$$

commutes, where s_t^n is the specialisation map introduced in Chapter 6, Section 6.8.

Proof: This follows from the proposition in view of Remark 7.1.6 (1) and the construction of s_t^n in Construction 6.8.6. \square

Another immediate corollary is the compatibility between Milnor’s and Faddeev’s exact sequences.

Corollary 7.5.4 *The diagram with exact rows*

$$\begin{array}{ccccccc}
 0 \rightarrow & K_n^M(k) & \rightarrow & K_n^M(k(t)) & \xrightarrow{\oplus \partial_P^M} & \bigoplus_{P \in \mathbf{P}_0^1 \setminus \{\infty\}} K_{n-1}^M(\kappa(P)) & \rightarrow 0 \\
 & \downarrow h_{k,m}^n & & \downarrow h_{k(t),m}^n & & \downarrow \oplus h_{\kappa(P),m}^{n-1} & \\
 0 \rightarrow & H^n(k, \mu_m^{\otimes n}) & \rightarrow & H^n(k(t), \mu_m^{\otimes n}) & \xrightarrow{\oplus \partial_P^n} & \bigoplus_{P \in \mathbf{P}_0^1 \setminus \{\infty\}} H^{n-1}(\kappa(P), \mu_m^{\otimes(n-1)}) & \rightarrow 0
 \end{array}$$

commutes, where the upper row is the sequence of Theorem 7.2.1, and the lower row that of Corollary 6.9.3.

Finally, we give the already announced compatibility between norm maps in K-theory and corestrictions in cohomology.

Proposition 7.5.5 *Let $K|k$ be a finite separable extension and m an integer invertible in k . Then for all $n \geq 0$ the diagram*

$$\begin{array}{ccc}
 K_n^M(K) & \xrightarrow{N_{K|k}} & K_n^M(k) \\
 h_{K,m}^n \downarrow & & \downarrow h_{k,m}^n \\
 H^n(K, \mu_m^{\otimes n}) & \xrightarrow{\text{Cor}} & H^n(k, \mu_m^{\otimes n})
 \end{array}$$

commutes.

Proof: By property (4) of the norm map and the similar property of corestrictions (which follows easily from their construction), we reduce to the case when $K = k(a)$ is a simple field extension. In this case $N_{K|k} = -\partial_\infty^M \circ \psi_P$, where P is the closed point \mathbf{P}_k^1 defined by the minimal polynomial of a . By Corollary 6.9.4, a similar formula holds for the corestriction map. The two are compatible via the Galois symbol by virtue of Corollary 7.5.4. \square

We now turn to applications to the Bloch-Kato conjecture. The first one is an immediate consequence of Corollary 7.5.4.

Proposition 7.5.6 (Bloch) *Let $m, n > 0$ be integers, with m invertible in k .*

1. *The Galois symbol*

$$h_{k(t),m}^n : K_n^M(k(t))/m \rightarrow H^n(k(t), \mu_m^{\otimes n})$$

is injective (resp. surjective or bijective) if and only if the Galois symbols

$$h_{k,m}^n : K_n^M(k)/m \rightarrow H^n(k, \mu_m^{\otimes n}) \text{ and } h_{L,m}^{n-1} : K_{n-1}^M(L)/m \rightarrow H^{n-1}(L, \mu_m^{\otimes(n-1)})$$

have the same property for all finite simple extensions $L|k$.

2. *Assume that $h_{L,m}^{n-1} : K_{n-1}^M(L)/mK_{n-1}^M(L) \rightarrow H^{n-1}(L, \mu_m^{\otimes(n-1)})$ is bijective for all finite simple extensions $L|k$. Then*

$$\ker(h_{k,m}^n) \cong \ker(h_{k(t),m}^n) \quad \text{and} \quad \text{coker}(h_{k,m}^n) \cong \text{coker}(h_{k(t),m}^n).$$

This gives a means for proving bijectivity of the Galois symbol for $k(t)$ if the bijectivity is already known for fields of smaller transcendence degree.

Here is another (unpublished) criterion of Bloch for the surjectivity of the Galois symbol.

Proposition 7.5.7 (Bloch) *Let $m, n > 0$ be integers, with m invertible in k . Assume that*

- *the Galois symbol $h_{L,m}^{n-1} : K_{n-1}^M(L)/mK_{n-1}^M(L) \rightarrow H^{n-1}(L, \mu_m^{\otimes(n-1)})$ is an isomorphism for all finitely generated extensions $L|k$;*
- *the Galois symbol $h_{k,m}^n : K_n^M(k)/mK_n^M(k) \rightarrow H^n(k, \mu_m^{\otimes n})$ is surjective.*

Then the following statements are equivalent :

1. *The Galois symbol $h_{K,m}^n$ is surjective for all fields K containing k .*
2. *For all field extensions $K|k$ equipped with a discrete valuation v the restriction map $H^n(K, \mu_m^{\otimes n}) \rightarrow H^n(\widehat{K}_v, \mu_m^{\otimes n})$ is surjective, where \widehat{K}_v stands for the completion of K with respect to v .*

In particular, the two statements are equivalent in the case when $n = 2$ and $\text{cd}(k) \leq 1$.

Proof: For (1) \Rightarrow (2) it is enough to establish the surjectivity of the map $K_n^M(K)/mK_n^M(K) \rightarrow K_n^M(\widehat{K}_v)/mK_n^M(\widehat{K}_v)$ induced by $i_{K_v|K}$, which readily follows by combining the second sequence in Proposition 7.1.7 for K with Corollary 7.1.10 for K_v .

For (2) \Rightarrow (1), note first that the first assumption and part (2) of the previous corollary yield an isomorphism $\text{coker}(h_{k,m}^n) \cong \text{coker}(h_{k(t),m}^n)$. Applying statement (2) to the completion \widehat{K}_P of $k(t)$ with respect to the discrete valuation defined by a closed point P gives the surjectivity of the map $H^n(k(t), \mu_m^{\otimes n}) \rightarrow H^n(\widehat{K}_P, \mu_m^{\otimes n})$. By Proposition 6.8.7, the latter group surjects onto $H^n(\kappa(P), \mu_m^{\otimes n})$ via every specialisation map. Taking Corollary 7.5.3 into account, we thus get a surjection $\text{coker}(h_{k,m}^n) \rightarrow \text{coker}(h_{\kappa(P),m}^n)$. Proceeding by induction using this statement and part (2) of the previous corollary, we get surjective maps $\text{coker}(h_{k,m}^n) \rightarrow \text{coker}(h_{K,m}^n)$ for all finitely generated extensions $K|k$. Finally, one may write an arbitrary extension $K|k$ as a direct limit of finitely generated fields $K_i|k$, and obtain $\text{coker}(h_{K,m}^n) \cong \varinjlim \text{coker}(h_{K_i,m}^n)$. Thus the surjectivity of $h_{k,m}^n$ implies that of $h_{K,m}^n$ for all extensions $K|k$.

The last statement of the proposition is obvious, since $h_{K,m}^1$ is an isomorphism for all fields K by Kummer theory, and $H^2(k, \mu_m^{\otimes 2})$ vanishes for fields of cohomological dimension ≤ 1 . \square

Remark 7.5.8 For fields containing a field of cohomological dimension 1 (in particular, for fields of positive characteristic) we thus get a purely cohomological reformulation of the surjectivity part of the Merkurjev-Suslin theorem, which in the case of fields containing a primitive m -th root of unity reduces to an even more suggestive surjectivity statement about the map ${}_m\text{Br}(K) \rightarrow {}_m\text{Br}(K_v)$. Bloch found this argument in the 1970's well before the Merkurjev-Suslin theorem was proven. By a result of Tate, however, the theorem was already known for number fields (see the next section), so in fact Bloch's result rephrased the surjectivity of $h_{K,m}^2$ for all fields K . For higher n it gives an inductive strategy for proving the Bloch-Kato conjecture.

We close this section by an important reduction statement due to Tate, which reduces the proof of the Bloch-Kato conjecture to the case of p -torsion coefficients. It will be used in the proof of the Merkurjev-Suslin theorem.

Proposition 7.5.9 (Tate) *Let $m, n > 0$ be integers, with m invertible in k . Assume that the Galois symbol $h_{k,m}^{n-1}$ is surjective, and that $h_{k,p}^n$ is bijective for all prime divisors p of m . Then the Galois symbol $h_{k,m}^n$ is bijective.*

For the proof we need the following lemma.

Lemma 7.5.10 *Assume k contains a primitive p -th root of unity ω , where p is a prime invertible in k . Then for all $r > 0$ we have a commutative diagram*

$$\begin{array}{ccc} \mu_p \otimes K_{n-1}^M(k) & \xrightarrow{\{\cdot, \cdot\}} & K_n^M(k)/p^r K_n^M(k) \\ \downarrow [\omega] \cup h_{k,p}^{n-1} & & \downarrow h_{k,p^r}^n \\ H^{n-1}(k, \mu_p^{\otimes n}) & \xrightarrow{\delta^n} & H^n(k, \mu_{p^r}^{\otimes n}), \end{array}$$

where $[\omega]$ denotes the class of ω in $H^0(k, \mu_p)$, the upper horizontal map associates with a pair (ω, a) the symbol $\{\omega, a\}$ modulo p^r , and δ^n is a so-called Bockstein homomorphism, i.e. a boundary map coming from the long exact sequence associated with the sequence

$$1 \rightarrow \mu_{p^r}^{\otimes n} \rightarrow \mu_{p^{r+1}}^{\otimes n} \xrightarrow{p^r} \mu_p^{\otimes n} \rightarrow 1 \quad (11)$$

of Galois modules.

Proof: First a word about exact sequence (11). For $n = 0$ it is none but the natural exact sequence

$$0 \rightarrow \mathbf{Z}/p^r \mathbf{Z} \rightarrow \mathbf{Z}/p^{r+1} \mathbf{Z} \xrightarrow{p^r} \mathbf{Z}/p \mathbf{Z} \rightarrow 0,$$

which can be regarded as an exact sequence of $\mathbf{Z}/p^{r+1} \mathbf{Z}$ -modules via the natural maps $\mathbf{Z}/p^{r+1} \mathbf{Z} \rightarrow \mathbf{Z}/p^r \mathbf{Z}$ and $\mathbf{Z}/p^{r+1} \mathbf{Z} \rightarrow \mathbf{Z}/p \mathbf{Z}$ given by multiplication by p and p^r , respectively. The general sequence is obtained by tensoring this sequence by $\mu_{p^{r+1}}^{\otimes n}$ over $\mathbf{Z}/p^{r+1} \mathbf{Z}$. Given a symbol $\alpha \in K_{n-1}^M(k)$, the element $y := h_{k,p}^{n-1}(\alpha)$ comes from the element $y_{r+1} := h_{k,p^{r+1}}^{n-1}(\alpha)$ via the map $H^{n-1}(k, \mu_{p^{r+1}}^{\otimes(n-1)}) \rightarrow H^{n-1}(k, \mu_p^{\otimes(n-1)})$ induced by raising the coefficients to the p^r -th power. Similarly, the element $y_r := h_{k,p^r}^{n-1}(\alpha)$ is the image of y_{r+1} via the map that raises coefficients to the p -th power. Now using Proposition 3.4.8 and the preceding discussion, we have

$$\delta_n([\omega] \cup h_{k,p}^{n-1}(\alpha)) = \delta^n([\omega] \cup y) = \delta^n([\omega] \cup y_{r+1}) = \delta^1([\omega]) \cup y_{r+1} = \delta^1([\omega]) \cup y_r.$$

It is immediately seen by examining the Kummer sequence that $\delta^1([\omega])$ is none but $h_{k,p^r}^1([\omega])$. Hence the right hand side is $h_{k,p^r}^n(\{\omega, \alpha\})$ by definition of the Galois symbol, and the proof is complete. \square

Proof of Proposition 7.5.9: By decomposing m into a product of prime powers we see that it is enough to consider the case $m = p^r$. Moreover, we

may and do assume that k contains a primitive p -th root of unity ω . Indeed, if not, consider the commutative diagrams

$$\begin{array}{ccc}
 K_n^M(k)/p^r & \xrightarrow{h_{k,p^r}^n} & H^n(k, \mu_{p^r}^{\otimes n}) & & K_n^M(k)/p^r & \xrightarrow{h_{k,p^r}^n} & H^n(k, \mu_{p^r}^{\otimes n}) \\
 i_{k(\omega)|k} \downarrow & & \downarrow \text{Res} & \text{and} & \uparrow N_{k(\omega)|k} & & \uparrow \text{Cor} \\
 K_n^M(k(\omega))/p^r & \xrightarrow{h_{k(\omega),p^r}^n} & H^n(k(\omega), \mu_{p^r}^{\otimes n}) & & K_n^M(k(\omega))/p^r & \xrightarrow{h_{k(\omega),p^r}^n} & H^n(k(\omega), \mu_{p^r}^{\otimes n}),
 \end{array}$$

where the second diagram commutes by Proposition 7.5.5. The composite maps $\text{Cor} \circ \text{Res}$ and $N_{k(\omega)|k} \circ \iota$ are both multiplication by the degree $[k(\omega) : k]$ which is prime to p . As the groups involved are p -primary torsion groups, these composite maps are isomorphisms, which implies that the vertical maps are injective in the first diagram and surjective in the second. It follows that the bijectivity of $h_{k(\omega),p^r}^n$ implies that of h_{k,p^r}^n .

For $m = p^r$ the proof goes by induction on r using the exact sequence (11). It induces the bottom row in the exact commutative diagram

$$\begin{array}{ccccccc}
 K_n^M(k)/p^r K_n^M(k) & \xrightarrow{p} & K_n^M(k)/p^{r+1} K_n^M(k) & \longrightarrow & K_n^M(k)/p K_n^M(k) & \longrightarrow & 0 \\
 h_{k,p^r}^n \downarrow \wr & & h_{k,p^{r+1}}^n \downarrow & & h_{k,p}^n \downarrow \wr & & \\
 H^n(k, \mu_{p^r}^{\otimes n}) & \longrightarrow & H^n(k, \mu_{p^{r+1}}^{\otimes n}) & \longrightarrow & H^n(k, \mu_p^{\otimes n}). & &
 \end{array}$$

By the inductive hypothesis the left and the right vertical maps are isomorphisms. A diagram chase then shows that $h_{k,p^{r+1}}^n$ is surjective. For injectivity, we complete the left hand side of the diagram as

$$\begin{array}{ccccc}
 \mu_p \otimes K_{n-1}^M(k) & \xrightarrow{\{\cdot, \cdot\}} & K_n^M(k)/p^r K_n^M(k) & \xrightarrow{p} & K_n^M(k)/p^{r+1} K_n^M(k) \\
 \omega \cup h_{k,p}^{n-1} \downarrow & & h_{k,p^r}^n \downarrow \wr & & h_{k,p^{r+1}} \downarrow \\
 H^{n-1}(k, \mu_p^{\otimes n}) & \xrightarrow{\delta} & H^n(k, \mu_{p^r}^{\otimes n}) & \longrightarrow & H^n(k, \mu_{p^{r+1}}^{\otimes n})
 \end{array}$$

using the lemma above, where the upper row is not necessarily exact but is a complex since $p\{\omega, a\} = 0$ for all $a \in k^\times$. If $\alpha \in K_n^M(k)$ is such that $h_{k,p^{r+1}}^n(p\alpha) = 0$ in $H^2(k, \mu_{p^{r+1}}^{\otimes n})$, the diagram shows that $h_{k,p^r}^n(\alpha)$ is in the image of δ . Now the left vertical map is surjective, as so is $h_{k,p}^{n-1}$ by assumption, and tensor product by μ_p is the identity map by our assumption that $\omega \in k$. Thus we may modify α by a symbol of the form $\{\omega, a\}$ to get $h_{k,p^r}^n(\alpha) = 0$ without changing $p\alpha$. Hence $\alpha \in p^r K_n^M(k)$ by injectivity of h_{k,p^r}^n , so $p\alpha \in p^{r+1} K_n^M(k)$, i.e. $\ker(h_{k,p^{r+1}}^n) = 0$. \square

7.6 The Galois Symbol Over Number Fields

In this section we establish the following basic theorem which was the first substantial result in the direction of the Merkurjev-Suslin theorem.

Theorem 7.6.1 (Tate) *If k is a number field, then the Galois symbol $h_{k,m}^2$ is bijective for all positive integers m .*

Remarks 7.6.2

1. It is known that a number field k has p -cohomological dimension 2 if $p > 2$ or if $p = 2$ and k is totally imaginary (see Serre [4], II.4.4), so the theorem answers (but historically predates) the full Bloch-Kato conjecture for odd m or totally imaginary k .
2. Surjectivity of the Galois symbol is a consequence of the fact that all central simple algebras are cyclic over k (Remark 6.5.6). Recall that this difficult result uses the main theorems of class field theory.

In view of the last remark, we only prove injectivity of the Galois symbol here. This will also use facts from class field theory, but there are purely algebraic ideas involved as well, which are interesting in their own right. We begin by explaining these.

The starting point is the following easy observation.

Lemma 7.6.3 *Let k be a field containing the m -th roots of unity for some m invertible in k , and let a, b be elements in k^\times . If $h_{k,m}^2(\{a, b\}) = 0$, then $\{a, b\} \in mK_2^M(k)$.*

Proof: By Proposition 4.7.1 and Corollary 4.7.5 we find $c \in k(\sqrt[m]{a})$ with $b = N_{k(\sqrt[m]{a})|k}(c)$. Using the projection formula we compute

$$\{a, b\} = \{a, N_{k(\sqrt[m]{a})|k}(c)\} = N_{k(\sqrt[m]{a})|k}(\{a, c\}) = mN_{k(\sqrt[m]{a})|k}(\{\sqrt[m]{a}, c\}),$$

whence the lemma. □

Now given $a, b, x \in k^\times$ with $h_{k,m}^2(\{a, b\}) = h_{k,m}^2(\{b, x\})$, an application of the lemma to $\{a, b\} - \{b, x\} = \{a, b\} + \{x, b\} = \{ax, b\}$ shows that $\{a, b\} = \{b, x\}$ modulo $mK_2^M(k)$. We can then continue this procedure with some $y \in k^\times$ satisfying $h_{k,m}^2(\{b, x\}) = h_{k,m}^2(\{x, y\})$, and so on. If every other pair $(c, d) \in k^\times$ can be reached by a chain of this type, then injectivity of $h_{k,m}^2$ follows, at least for symbols of length 1. The following definition formalises this idea. From now on, we only consider the case when $m = p$ is a prime (which is allowed by Proposition 7.5.9).

Definition 7.6.4 Let k be a field and p a prime number invertible in k . We say that the *chain lemma holds for k and p* if for any two pairs (a, b) and $(c, d) \in k^{\times 2}$ satisfying $h_{k,p}^2(\{a, b\}) = h_{k,p}^2(\{c, d\})$ there exist an integer $n \geq 0$ and elements $x_{-1} = a, x_0 = b, x_1, \dots, x_{n-1} = c, x_n = d$ in k^\times such that

$$h_{k,p}^2(\{x_i, x_{i+1}\}) = h_{k,p}^2(\{x_{i+1}, x_{i+2}\})$$

holds for all $i = -1, 0, \dots, n-2$. We say that the *chain lemma holds with length N* if for all pairs (a, b) and $(c, d) \in k^{\times 2}$ we may choose a chain as above with $n \leq N$.

Remarks 7.6.5

1. It is conjectured that the chain lemma holds for all fields k and all primes p . For $p = 2$ we shall prove this in a moment; for $p = 3$ see Rost [2]. Rost (unpublished) has also proven that the chain lemma always holds for a prime p and a field k having no nontrivial finite extensions of degree prime to p .
2. Variants of the chain lemma occur in quadratic form theory (see Elman and Lam [1]), and in a more general context in Rost [4].

Note that the argument after Lemma 7.6.3 yields:

Corollary 7.6.6 *Assume that the chain lemma holds for k and p . Then the identity $h_{k,p}^2(\{a, b\}) = h_{k,p}^2(\{c, d\})$ implies $\{a, b\} = \{c, d\} \pmod{pK_2^M(k)}$ for all $a, b, c, d \in k^\times$.*

We can now formalise the strategy for proving Theorem 7.6.1.

Proposition 7.6.7 *Let k be a field containing the p -th roots of unity and satisfying the following two conditions:*

- *the chain lemma holds for k ;*
- *for each finite set of elements $a_1, b_1, a_2, b_2, \dots, a_r, b_r$ in k^\times we may find a degree p cyclic extension $K|k$ so that $\text{Res}_k^K(h_{k,p}^2(\{a_i, b_i\})) = 0$ for $1 \leq i \leq r$.*

Then the Galois symbol $h_{k,p}^2$ is injective.

Proof: Let $\alpha = \sum_{i=1}^r \{a_i, b_i\}$ be a symbol in the kernel of $h_{k,p}^2$. Take an extension $K|k$ as in the second condition above and write it as $K = k(\sqrt[p]{c})$ for some $c \in k^\times$ using Kummer theory. By Proposition 4.7.1 and Corollary 4.7.6 we find elements $d_i \in k^\times$ with $h_{k,p}^2(\{a_i, b_i\}) = h_{k,p}^2(\{c, d_i\})$ for $1 \leq i \leq r$. Corollary 7.6.6 shows that under the first assumption $\{a_i, b_i\} = \{c, d_i\} \bmod pK_2^M(k)$ for all i , so setting $d = d_1 d_2 \cdots d_r$ yields $\alpha = \{c, d\} \bmod pK_2^M(k)$. The proposition then follows from Lemma 7.6.3. \square

We next verify that the chain lemma holds for all primes and all number fields. The first step in this direction is:

Lemma 7.6.8 *If $p = 2$, the chain lemma holds with length 3 for all fields k .*

In Chapter 1 we gave a sketch of a proof by Tate in an exercise. We now give another proof due to Rost.

Proof: The condition $h_{k,2}^2(\{a, b\}) = h_{k,2}^2(\{c, d\})$ means that the quaternion algebras (a, b) and (c, d) are isomorphic over k . We may assume they are nonsplit (otherwise use the isomorphisms $(a, b) \cong (1, b)$ and $(c, d) \cong (c, 1)$). Choose $X, Y \in (a, b) \setminus k$ such that $X^2 = b$ and $Y^2 = c$, and define $Z = XY - YX$. Consider the reduced characteristic polynomial $N(t - Z)$ of Z , where N is the quaternion norm. It has degree 2, and the coefficient of t is the quaternion trace $T(Z) = Z + \overline{Z}$ which is 0. Therefore $N(t - Z) = t^2 - z$ with $z := Z^2 \in k$. If $Z \neq 0$, notice that $XZ + ZX = X(XY - YX) + (XY - YX)X = 0$ and similarly $YZ + ZY = 0$. So (X, Z) and (Y, Z) are both quaternion bases of (a, b) , and hence $(a, b) \cong (b, z) \cong (z, c) \cong (c, d)$ is a suitable chain. If $Z = 0$, then Y lies in the 2-dimensional commutative subalgebra $k[X]$. Since moreover its minimal polynomial over k is $t^2 - c$, we must have $Y = \lambda X$ for suitable $\lambda \in k$ and hence $c = \lambda^2 b$. Thus we have a length 3 chain $(a, b) \cong (b, a) \cong (a, c) \cong (c, d)$ in this case as well. \square

Next we have the following lemma of Tate.

Lemma 7.6.9 *If k contains the p -th roots of unity and the p -torsion subgroup ${}_p\text{Br}(k)$ is cyclic, the chain lemma holds for k and p with length 4.*

Proof: Lemma 7.6.8 allows us to assume that p is odd. Assume given a, b, c, d such that $h_{k,p}^2(\{a, b\}) = h_{k,p}^2(\{c, d\})$. As in the above proof, we may assume that both sides are nonzero, and therefore yield a generator α of ${}_p\text{Br}(k) \cong \mathbf{F}_p$. Via this last isomorphism $h_{k,p}^2$ may be identified with a bilinear map $\phi : k^\times/k^{\times p} \times k^\times/k^{\times p} \rightarrow \mathbf{F}_p$ of \mathbf{F}_p -vector spaces, which is moreover anticommutative by Proposition 7.1.1. Our task is to find $x, y \in k^\times$ satisfying

$\phi(b, x) = \phi(x, y) = \phi(y, c) = \alpha$. The linear forms $t \mapsto \phi(b, t)$ and $t \mapsto \phi(t, c)$ are non-zero and hence surjective. If these forms are either linearly independent or equal, then we can take $y = c$ and find an x such that $\phi(b, x) = \alpha$ and $\phi(x, y) = \phi(x, c) = \alpha$. Suppose now that these two linear forms are dependent but not equal. The forms $t \mapsto \phi(t, c)$ and $t \mapsto \phi(d, t) = \phi(t, d^{-1})$ are independent of each other because $\phi(d, c) = -\phi(c, d) \neq 0$. Thus by assumption for $y = cd^{-1}$ the linear forms $t \mapsto \phi(b, t)$ and $t \mapsto \phi(t, y)$ must be linearly independent. As above, we find x satisfying $\phi(b, x) = \phi(x, y) = \alpha$. Finally, note that since p is odd, the anticommutative form ϕ is actually alternating, so that $\phi(d, d) = 0$ and therefore $\phi(y, c) = \phi(cd^{-1}, c) = \phi(d^{-1}, c) = \phi(c, d) = \alpha$, which yields the end of the chain. \square

These were the purely algebraic statements involved in the proof of Theorem 7.6.1. To proceed further, we need some facts from class field theory.

Facts 7.6.10 Let k be a number field. Denote by Ω the set of all places of k , and for each $v \in \Omega$ denote by k_v the completion of k at v . For v finite k_v is a finite extension of \mathbf{Q}_p for some prime p , and for v infinite k_v is isomorphic to \mathbf{R} or \mathbf{C} .

1. For each finite place v there is an isomorphism $\text{inv}_{k_v} : \text{Br}(k_v) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}$, and for a finite extension $L_w|k_v$ one has $\text{inv}_{L_w} \circ \text{Res}_{k_v}^{L_w} = [L_w : k_v] \text{inv}_{k_v}$. See Serre [2], Chapter XIII, Propositions 6 and 7.
2. The restriction maps $\text{Br}(k) \rightarrow \text{Br}(k_v)$ are trivial for all but finitely many $v \in \Omega$, and the map $\text{Br}(k) \rightarrow \bigoplus_{v \in \Omega} \text{Br}(k_v)$ is injective. These statements are contained in the Albert-Brauer-Hasse-Noether theorem already recalled in Remark 6.5.6.
3. If p is an odd prime, then given a finite set S of places of k and characters $\chi_v \in H^1(k_v, \mathbf{Z}/p\mathbf{Z})$ for all $v \in S$, there exists a global character $\chi \in H^1(k, \mathbf{Z}/p\mathbf{Z})$ inducing the χ_v by restriction to k_v . This is a particular case of the Grunwald-Wang theorem (Artin-Tate [1], Chapter X).
4. Let $\alpha_1, \dots, \alpha_r$ be a finite set of elements in ${}_p\text{Br}(k)$ and $a_1, \dots, a_r \in k^\times$. Assume given for each place v of k a character $\chi_v \in H^1(k_v, \mathbf{Z}/p\mathbf{Z})$ such that $\chi_v \cup h_{k_v, p}^1(a_i) = \text{Res}_k^{k_v}(\alpha_i)$ for $1 \leq i \leq r$. Then there exists a character $\chi \in H^1(k, \mathbf{Z}/p\mathbf{Z})$ such that $\chi \cup h_{k, p}^1(a_i) = \alpha_i$ for $1 \leq i \leq r$. This follows from global class field theory: almost the same statement is proven in Cassels-Fröhlich [1], Ex. 2.16, p. 355 (note that condition (i) there follows from the global reciprocity law and that one may choose

$\chi_v = 0$ for all but finitely many v). One may also consult Lemma 5.2 of Tate [4].

We can now prove the chain lemma for number fields.

Lemma 7.6.11 *If k is a number field containing the p -th roots of unity, then the chain lemma holds with length 4 for k and p .*

Proof: Assume given $a, b, c, d \in k^\times$ with $h_{k,p}^2(\{a, b\}) = h_{k,p}^2(\{c, d\})$. We have to find $x, y \in k^\times$ such that

$$h_{k,p}^2(\{b, x\}) = h_{k,p}^2(\{x, y\}) = h_{k,p}^2(\{y, c\}) = h_{k,p}^2(\{c, d\}). \quad (12)$$

Let S be the set of places such that $\text{Res}_k^{k_v}(h_{k,p}^2(\{c, d\})) \neq 0$. For each $v \in S$ the group ${}_p\text{Br}(k_v)$ is cyclic (by Fact 7.6.10 (1) and by $\text{Br}(\mathbf{R}) \cong \mathbf{Z}/2\mathbf{Z}$), so we may apply Lemma 7.6.9 to find elements $x_v, y_v \in k_v^\times$ for each $v \in S$ such that

$$h_{k_v,p}^2(\{b, x_v\}) = h_{k_v,p}^2(\{x_v, y_v\}) = h_{k_v,p}^2(\{y_v, c\}) = h_{k_v,p}^2(\{c, d\}). \quad (13)$$

The last of these equalities implies that $h_{k_v,p}^2(\{dy_v, c\}) = 0$, and therefore $dy_v = N_{k_v(\sqrt[p]{c})|k_v}(t_v)$ for some $t_v \in k_v(\sqrt[p]{c})$ according to Proposition 4.7.1 and Corollary 4.7.5. Fact 7.6.10 (3) together with the Kummer isomorphism $k(\sqrt[p]{c})^\times/k(\sqrt[p]{c})^{\times p} \cong H^1(k(\sqrt[p]{c}), \mathbf{Z}/p\mathbf{Z})$ enable us to find $t \in k(\sqrt[p]{c})$ such that $t_v^{-1}t \in k_v(\sqrt[p]{c})^{\times p}$ for all $v \in S$. Put $y = d^{-1}N_{k(\sqrt[p]{c})|k}(t)$. Then for all $v \in S$ we have $h_{k,p}^2(\{y, c\}) = h_{k,p}^2(\{d^{-1}, c\}) = h_{k,p}^2(\{c, d\})$ by Proposition 4.7.1, and moreover

$$h_{k_v,p}^2(\{y, c\}) = h_{k_v,p}^2(\{y_v, c\}), \quad (14)$$

since $N_{k_v(\sqrt[p]{c})|k_v}(t_v^{-1}t) \in k_v^{\times p}$ by our choice of t . Fixing this y , it remains to find $x \in k^\times$ satisfying the first two equalities in (12). According to (13) and (14), the equations $h_{k,p}^2(\{b, x\}) = h_{k,p}^2(\{y, c\})$ and $h_{k,p}^2(\{x, y\}) = h_{k,p}^2(\{y, c\})$ have simultaneous solutions x_v over k_v for each $v \in S$, and for $v \notin S$ they have the trivial solution by the choice of S . We conclude by Fact 7.6.10 (4), applied with $r = 2$, $a_1 = b^{-1}$, $a_2 = y$, $\alpha_1 = \alpha_2 = h_{k,p}^2(\{y, c\})$ and $\chi_v = h_{k_v,p}^1(x_v)$. \square

We finally come to:

Proof of Theorem 7.6.1: By Proposition 7.5.9 it is enough to treat the case $m = p$. As in the proof of that proposition, we may also assume that k contains the p -th roots of unity. It then suffices to check the conditions of

Proposition 7.6.7. The first one is the previous lemma. To check the second, it is enough to find for a given finite set $\alpha_1, \dots, \alpha_r$ of classes in ${}_p\text{Br}(k)$ a cyclic extension $L|k$ of degree p so that $\text{Res}_k^L(\alpha_i) = 0$ for all i . By Fact 7.6.10 (2) we find a finite set S of places so that $\text{Res}_k^{k_v}(\alpha_i) = 0$ for all i and all $v \notin S$. Choose an element $b \in k^\times$ which does not lie in $k_v^{\times p}$ for any $v \in S$. For instance, one may take $b = u\pi_1 \dots \pi_s$, where u is a unit and the π_i are prime elements for the finite places in S . For p odd this is already sufficient; for $p = 2$ one uses Dirichlet's Unit Theorem (Neukirch [1], Chapter I, Theorem 7.4) to choose u so that b becomes negative in the completions for the real places in S . The extension $L = k(\sqrt[p]{b})|k$ is then cyclic of degree p , and so are the extensions $Lk_v|k_v$ for $v \in S$. Using Fact 7.6.10 (1) and the vanishing of $\text{Br}(\mathbf{C})$ we therefore see that $\text{Res}_k^{Lk_v}(\alpha_i) = 0$ for all i and all v in S . For the other places we already have $\text{Res}_k^{k_v}(\alpha_i) = 0$ by assumption, so that Fact 7.6.10 (2) implies $\text{Res}_k^L(\alpha_i) = 0$ for all i , as required. \square

EXERCISES

1. (Bass, Tate) This exercise studies the K-groups of an algebraically closed field k .
 - (a) Let A, B be two divisible abelian groups. Show that $A \otimes_{\mathbf{Z}} B$ is uniquely divisible, i.e. a \mathbf{Q} -vector space.
 - (b) Show that $K_2^M(k)$ is uniquely divisible. [*Hint*: Use the presentation $0 \rightarrow R \rightarrow k^\times \otimes k^\times \rightarrow K_2^M(k) \rightarrow 0$].
 - (c) Let $K|k$ be a field extension. Show that the map $K_2^M(k) \rightarrow K_2^M(K)$ is injective.
2.
 - (a) Given a field extension $K|k$, show that the natural maps $K_n^M(k) \otimes_{\mathbf{Z}} \mathbf{Q} \rightarrow K_n^M(K) \otimes_{\mathbf{Z}} \mathbf{Q}$ are injective for all $n \geq 1$. [*Hint*: First consider the cases $K|k$ finite and $K = k(t)$.]
 - (b) If k is an uncountable field, show that $K_n^M(k) \otimes_{\mathbf{Z}} \mathbf{Q}$ is uncountable for all $n \geq 1$.
3. Establish isomorphisms $K_n^M(\mathbf{R})/2K_n^M(\mathbf{R}) \cong \mathbf{Z}/2\mathbf{Z}$ for all $n \leq 0$.
4. This exercise gives a simpler proof of Theorem 7.3.2 for $n = 2$ and fields of characteristic 0. Let k be such a field, and let $K|k$ be a finite field extension. Let $N_1 = N_{a_1, \dots, a_r|k}$ and $N_2 = N_{b_1, \dots, b_s|k}$ be two candidates for the norm map $K_2^M(K) \rightarrow K_2^M(k)$. Denote by δ_k the difference $N_1 - N_2$.
 - (a) Observe that $\text{Im}(\delta_k)$ is a torsion group.

- (b) Show that $\delta_{k(t)} : K_2^M(K(t)) \rightarrow K_2^M(k(t))$ takes values in $K_2^M(k)$, where $k(t)|k$ is a rational function field.
- (c) Given $a, b \in k^\times$, show that $\delta_{k(t)}(\{a, (1-t) + tb\}) = 0$. [*Hint*: Use the fact that the evaluation map $k[[t]]^\times \rightarrow k^\times$ has divisible kernel.]
- (d) Conclude by specialisation that $\delta_k(\{a, b\}) = 0$.
5. (Tate) Let m be an integer invertible in k , and assume that k contains a primitive m -th root of unity ω . Denote by A the subgroup of ${}_mK_2^M(k)$ consisting of elements of the form $\{\omega, a\}$ with $a \in k^\times$.
- (a) Show that the equality $A = {}_mK_2^M(k)$ is equivalent to the existence of a homomorphism $f : {}_mK_2^M(k) \rightarrow K_2^M(k)/A$ such that $f(m\alpha) = \alpha \bmod A$ for all $\alpha \in K_2^M(k)$.
- (b) If such an f exists, show that it is unique.
- (c) Given $a, b \in k^\times$, show that $\{a, b\} \in {}_mK_2^M(k)$ if and only if there exists a finite extension $K|k$ and elements $\alpha, \beta \in K$ such that $\alpha^m = a$ and $N_{K|k}(\beta) = b$.
- (d) Verify that for $\{a, b\} \in {}_mK_2^M(k)$ the image of $N_{K|k}(\{\alpha, \beta\})$ in the quotient $K_2^M(K)/A$ depends only on the pair a, b .
- (e) Assume that $\text{cd}(k) \leq 1$. Conclude from (c) that $K_2^M(k)$ is m -divisible, and use (a) and (d) to show that $A = {}_mK_2^M(k)$. [*Hint*: Use that $\text{Br}(L|k)$ is trivial for all finite cyclic extensions $L|k$ of degree m .]
6. Let k be a field, $n > 0$ an integer and α an element of $K_n^M(k(t))$. For each closed point P of the affine line \mathbf{A}_k^1 , write $\kappa(P) = k(a_P)$ with suitable a_P .
- (a) Check that the norm $N_{\kappa(P)(t)|k(t)}(\{t - a_P, \partial_P(\alpha)\})$ is independent of the choice of a_P .
- (b) Establish the following more explicit variant of Corollary 7.2.3:

$$\alpha = s_{t-1}(\alpha)_{k(t)} + \sum_{P \in \mathbf{A}_0^1} N_{k(P)(t)|k(t)}(\{t - a_P, \partial_P(\alpha)\}).$$

[*Remark*: The analogous formula for Galois cohomology may be found in Garibaldi-Merkurjev-Serre [1], Exercise 9.23.]

7. (Optimality of the Rosset-Tate bound) Let p be a prime number and k a field containing a primitive p -th root of unity ω . Consider the purely transcendental extension $E = k(x_1, y_1, x_2, y_2, \dots, x_p, y_p)$ in $2p$ indeterminates. Make the cyclic group $\mathbf{Z}/p\mathbf{Z} = \langle \sigma \rangle$ act on E by $\sigma(x_i) = x_{i+p}$ and $\sigma(y_i) = y_{i+p}$ (where $i+p$ is taken mod p). Let $F \subset E$ be the fixed field under this action. Prove that $N_{E|F}(\{x_1, y_1\})$ cannot be represented in $K_2^M(F)$ by a symbol of length $p-1$. [*Hint*: use the Galois symbol and Exercise 6 of Chapter 6].

8. Let $n > 1$ be an odd integer and k a field containing a primitive n -th root of unity ω . Let $K|k$ be a finite Galois extension whose Galois group is the dihedral group D_n , i.e. it has a presentation of the form

$$\langle \sigma, \tau \mid \sigma^n = 1, \tau^2 = 1, \sigma\tau\sigma = \tau \rangle.$$

Let L be the fixed field of σ in K . This exercise shows that a central simple k -algebra A of degree n split by K is isomorphic to a cyclic algebra.

- (a) Show that there is an element $a \in L^\times$ such that $K = L(\sqrt[n]{a})$ and $N_{L|K}(a) \in (k^\times)^n$. [*Hint*: if $K = L(\sqrt[n]{c})$, take $a = c^n$.]
 (b) Show that $A \otimes_k L \cong (a, b)_\omega$ for some $b \in L^\times$.
 (c) Conclude that $[A] = \text{Cor}_k^L([(a, b)_\omega])$ in $\text{Br}(k)$. If $b \in k^\times$, conclude moreover that A is isomorphic to a cyclic algebra.
 (d) Assume that $b \in L^\times \setminus k^\times$. Show that there exist $a', b' \in k^\times$ such that $aa' + bb' = 0$ or 1 , and prove that the relation

$$[(a, b)_\omega] + [(a, b')_\omega] + [(a', bb')_\omega] = 0$$

holds in $\text{Br}(L)$. Conclude that A is isomorphic to a cyclic algebra in this case as well.

- (e) Adapt the preceding arguments to show that the conclusion also holds in the case when k is of characteristic $p \geq 3$ and $n = p$. [*Hint*: Show that $K = L(c)$ for some c such that $a := c^p - c$ lies in L and $\text{Tr}_{L|k}(a) = u^n - u$ for some $u \in k$.]

[*Remark*: The theorem of this exercise is due to Rowen-Saltman [1]. The above proof is that of Mammone-Tignol [1].]

9. (Wedderburn) Show that every central simple algebra of degree 3 over a field k is isomorphic to a cyclic algebra. [*Hint*: Use the previous exercise.]
 10. Let $p > 2$ be a prime number, and k a field containing a primitive p -th root of unity. Improve the bound of Proposition 7.4.13 by showing that every central simple k -algebra of degree p is Brauer equivalent to the tensor product of at most $(p-1)!/2$ cyclic k -algebras of degree p . [*Hint*: Use Exercise 8 and the fact that the symmetric group S_p contains D_p as a subgroup.]
 11. Let k be a field, and $m > 0$ an integer invertible in k .

- (a) Show that injectivity (resp. surjectivity) of the Galois symbols

$$h_{k,m}^{n-1} : K_{n-1}^M(k)/m \rightarrow H^{n-1}(k, \mu_m^{\otimes(n-1)}) \text{ and } h_{k,m}^n : K_n^M(k)/m \rightarrow H^n(k, \mu_m^{\otimes n})$$

imply the corresponding property for the Galois symbol

$$h_{k((t)),m}^n : K_n^M(k((t)))/m \rightarrow H^n(k((t)), \mu_m^{\otimes n}).$$

- (b) Verify the Bloch-Kato conjecture for the Laurent series field $\mathbf{F}_q((t))$ and m prime to q .

Chapter 8

The Merkurjev-Suslin Theorem

This chapter is devoted to the central result of this book, the celebrated theorem of Merkurjev and Suslin on the bijectivity of the Galois symbol $h_{k,m}^2 : K_2^M(k)/mK_2^M(k) \rightarrow H^2(k, \mu_m^{\otimes 2})$ for all fields k and all integers m invertible in k . Following a method of Merkurjev, we shall deduce the theorem by a specialisation argument from the partial results obtained at the end of the last chapter, using a powerful tool which is interesting in its own right, the K_2 -analogue of Hilbert's Theorem 90. Apart from the case when m is a power of 2, no elementary proof of this theorem is known. To establish it, we first develop the foundations of the theory of Gersten complexes in Milnor K-theory. This material requires some familiarity with the language of schemes. Next comes an even deeper input, a technical statement about the K-cohomology of Severi-Brauer varieties. Its proof involves techniques outside the scope of the present book, so at this point our discussion will not be self-contained. The rest of the argument is then much more elementary and requires only the tools developed earlier in this book, so some readers might wish to take the results of the first three sections on faith and begin with Section 8.4.

The theorem was first proven in Merkurjev [1] in the case when m is a power of 2, relying on a computation by Suslin of the Quillen K-theory of a conic. Later several elementary proofs of this case were found which use no algebraic K-theory at all, at the price of rather involved calculations. Merkurjev himself gave two such proofs (see Wadsworth [1] and Merkurjev [6]); another one by Rost is contained in the book of Kersten [1]. For a proof in the language of quadratic forms, see Arason [2]. The general theorem first appeared in the seminal paper of Merkurjev and Suslin [1]. Its proof was later improved and simplified in Suslin [1], [2] and Merkurjev [2]. Several ideas involved in these proofs, most notably generalisations of Hilbert's Theorem 90 to higher K-groups, play a prominent role in the recent proof of the Milnor conjecture by Voevodsky [1], and in the work currently in progress on the

general Bloch-Kato conjecture.

8.1 Gersten Complexes in Milnor K-theory

Let X be a variety of dimension d over a field k . We regard X as a k -scheme and denote by X_i the set of its points of dimension i (i.e. those scheme-theoretic points whose Zariski closure in X has dimension i). Following Kato, we construct in this section for each integer n complexes of abelian groups

$$S_n(X) : \bigoplus_{P \in X_d} K_{n+d}^M(\kappa(P)) \xrightarrow{\partial} \bigoplus_{P \in X_{d-1}} K_{n+d-1}^M(\kappa(P)) \xrightarrow{\partial} \cdots \xrightarrow{\partial} \bigoplus_{P \in X_0} K_n^M(\kappa(P))$$

called *Gersten complexes in Milnor K-theory*. The degree i term in such a complex will be the one indexed by the points in X_i . By convention, we put $K_n^M(\kappa(P)) := 0$ for $n < 0$. Therefore the complex $S_n(X)$ will be trivial for $n < -d$, and concentrated between the terms of degree d and $-n$ for $-d \leq n < 0$.

When investigating properties of these complexes, we shall be sometimes forced to work at the level of local rings. These are not finitely generated k -algebras any more, so it will be convenient to work at a more general level, that of noetherian *excellent* schemes. For readers less at ease with this concept we note that varieties over fields, their local rings, and completions of these all give rise to excellent schemes according to Grothendieck [4], (7.8.3), and these will be the only cases we need. So *henceforth in this section* X is a noetherian excellent scheme of finite dimension d , and we construct the complexes $S_n(X)$ in this generality.

Construction 8.1.1 We construct the maps ∂ in the sequence $S_n(X)$ as follows. Take a point $P \in X_{i+1}$, and let Z_P be its Zariski closure in X . Each point Q of codimension 1 on Z_P corresponds to a point in X_i . On the normalisation \tilde{Z}_P of Z_P there are finitely many points Q_1, \dots, Q_r lying above Q . The local ring of each Q_j on \tilde{Z}_P is a discrete valuation ring, hence it defines a discrete valuation on the function field $\kappa(P)$ of \tilde{Z}_P . Denoting by $\partial_{Q_j}^M$ the associated tame symbol, we may define maps $\partial_Q^P : K_{n+i+1}^M(\kappa(P)) \rightarrow K_{n+i}^M(\kappa(Q))$ by setting

$$\partial_Q^P := \sum_{j=1}^r N_{\kappa(Q_j)|\kappa(Q)} \circ \partial_{Q_j}^M.$$

Since each function $f \in \kappa(P)$ has only finitely many zeros and poles on \tilde{Z}_P , the valuations $v_{Q_j}(f)$ associated with the codimension 1 points on X

are trivial for all but finitely many Q_j (here Q_j runs over the set of *all* codimension 1 points). *A fortiori*, for fixed $\alpha \in K_{n+i+1}^M(\kappa(P))$ the tame symbols $\partial_{Q_j}^M$ are trivial for all but finitely many Q_j . It therefore makes sense to consider the sum

$$\partial_P := \sum_{Q \in Z_P} \partial_Q^P,$$

and finally, we may define the map ∂ as the direct sum of the maps ∂_P for all $P \in X_{i+1}$.

Theorem 8.1.2 (Kato) *The sequence $S_n(X)$ is a complex for all $n \geq -d$.*

Proof: The proof is in several steps.

Step 1: Reduction to the local case. Let P_0 be a point of dimension i and α an element of $K_{n+i}(\kappa(P_0))$. We have to prove that $(\partial \circ \partial)(\alpha)$ is the zero element in $\bigoplus K_{n+i-2}(\kappa(P))$. This sum is indexed by points of dimension $i - 2$. We may assume $i \geq 2$ (otherwise there is nothing to prove) and reason for each direct summand separately. The construction of ∂ shows that in doing so we may replace X by the normalisation of the closure of P_0 in X ; in particular, we may assume that X is normal. Let P_2 be a point of codimension 2 in X , and denote by A its local ring. The points of codimension 1 involved in the construction of the component of $\partial(\alpha)$ indexed by P_2 all correspond to prime ideals of height 1 in A . This shows that for the proof of $(\partial \circ \partial)(\alpha) = 0$ we may replace $S_n(X)$ by $S_n(\text{Spec}(A))$, and assume that X is the spectrum of an integrally closed local ring of dimension 2.

Step 2: Reduction to the complete case. Next we show that we may replace A by its completion \widehat{A} . To see this, write \widehat{X} for the spectrum of \widehat{A} , K for the fraction field of A and \widehat{K} for that of \widehat{A} . Since A is excellent, here \widehat{A} is integrally closed as well according to Theorem A.5.2 of the Appendix. Furthermore, the first statement of the same theorem applied to A/P shows that $\widehat{A}/P\widehat{A}$ has no nilpotents. Thus each prime ideal P of height 1 in X decomposes as a finite product $P = P_1 \dots P_r$ of distinct of height 1 prime ideals in \widehat{A} (note that since A and \widehat{A} are integrally closed, these are actually principal ideals). In terms of discrete valuations, the valuation defined by each P_i continues that of P with ramification index 1, which shows the commutativity of the first square in the diagram

$$\begin{array}{ccccc} S_n(X) : & K_{n+2}^M(K) & \xrightarrow{\partial} & \bigoplus_{P \in X_1} K_{n+1}^M(\kappa(P)) & \xrightarrow{\partial} & K_n^M(\kappa) \\ & \downarrow i_{\widehat{K}|K} & & \downarrow \bigoplus_{Q \rightarrow P} i_{\kappa(Q)|\kappa(P)} & & \downarrow \text{id} \\ S_n(\widehat{X}) : & K_{n+2}^M(\widehat{K}) & \xrightarrow{\partial} & \bigoplus_{Q \in \widehat{X}_1} K_{n+1}^M(\kappa(Q)) & \xrightarrow{\partial} & K_n^M(\kappa). \end{array}$$

in view of Remark 7.1.6 (2). To check the commutativity of the second square, we consider the quotient ring A/P . Its completion with respect to the maximal ideal M of A is none but the direct sum $\bigoplus \widehat{A}/P_i$, as seen using Proposition A.5.1 of the Appendix and the Chinese Remainder Theorem. But the integral closure of $\bigoplus \widehat{A}/P_i$ in the direct sum of the fraction fields of the A/P_i is none but the completion of the integral closure of A/P , again by Theorem A.5.2 of the Appendix. The maximal ideals in these rings are all induced by M , so there is no ramification and the required commutativity again follows from Remark 7.1.6 (2).

Step 3: Reduction to the case of a power series ring. We have arrived at the case when X is the spectrum of a complete local ring A of dimension 2; denote by κ its residue field. According to a version of the Cohen structure theorem (see Appendix, Theorem A.5.4 (1)), such an A can be written as a finitely generated module over a subring of the form $B[[t]]$, where B is a complete discrete valuation ring with the same residue field κ . Denote by Y the spectrum of $B[[t]]$, by K the fraction field of A and by K_0 that of B . The left square of the diagram

$$\begin{array}{ccccc}
 S_n(X) : & K_{n+2}^M(K) & \xrightarrow{\partial} & \bigoplus_{Q \in X_1} K_{n+1}^M(\kappa(Q)) & \xrightarrow{\partial} & K_n^M(\kappa) \\
 & \downarrow N_{K|K_0} & & \downarrow \bigoplus_P \sum_{Q \rightarrow P} N_{\kappa(Q)|\kappa(P)} & \text{id} \downarrow & \\
 S_n(Y) : & K_{n+2}^M(K_0) & \xrightarrow{\partial} & \bigoplus_{P \in Y_1} K_{n+1}^M(\kappa(P)) & \xrightarrow{\partial} & K_n^M(\kappa)
 \end{array}$$

commutes because of Corollary 7.4.3, and the right square because of Proposition 7.4.1. An inspection of the diagram reveals that if $S_n(Y)$ is a complex, then so is $S_n(X)$, so we may assume $A = B[[t]]$.

Step 4: Conclusion. The ring $B[[t]]$ is a regular local ring, hence a unique factorisation domain. Its prime ideals of height 1 are all principal, generated by either a local parameter π of B or a so-called Weierstrass polynomial, i.e. a monic irreducible polynomial in $B[t]$ whose coefficients, except for the leading one, are divisible by π (see e.g. Lang [3], Chapter IV, theorem 9.3). Thus the multiplicative group of the fraction field K of $B[[t]]$ is generated by the units of B , by π and by Weierstrass polynomials. In order to verify $(\partial \circ \partial)(\alpha) = 0$ for $\alpha \in K_{n+2}^M(K)$, we may reduce, by construction of the tame symbol, to the case $n = 0$ and moreover using bilinearity of symbols we may assume α is a symbol of the form $\{a, b\}$ with a and b chosen among the generators of K^\times described above.

The cases when a or b are units of B are straightforward. Next consider the case when $a = \pi$ and b is a Weierstrass polynomial of degree N . Note

that the residue field $\kappa(P)$ of the prime ideal $P = (b)$ is a degree N finite extension of the fraction field F of B , and hence the discrete valuation v of B extends uniquely to a valuation v_P of $\kappa(P)$, with some ramification index e_P . Its residue field is a finite extension of κ ; write f_P for the degree of this extension. Our assumption that we are dealing with excellent rings implies that $e_P f_P = N$. On the other hand, the image of b in the residue field $\kappa((t))$ of (π) is t^N , whose t -adic valuation is N . Therefore, by definition of the tame symbol we get $(\partial \circ \partial)(\{\pi, P\}) = N - e_P f_P = 0$.

We still have to deal with the cases where a and b are Weierstrass polynomials. These are units for the valuation associated with π , and hence the corresponding tame symbol is trivial. The other discrete valuations to be considered are those coming from Weierstrass polynomials, and these in turn define closed points of the projective line \mathbf{P}_F^1 . The associated tame symbols on K and $F(t)$ are given by the same formula. Viewing $\alpha = \{a, b\}$ as an element of $K_2(F(t))$, we now show that

$$(\partial \circ \partial)(\{a, b\}) = \sum_{P \in \mathbf{P}_{F,0}^1} f_P v_P(\partial_P^M(\{a, b\})), \tag{1}$$

i.e. that the terms coming from points on \mathbf{P}_F^1 other than those defined by Weierstrass polynomials do not contribute to the sum. For the points coming from irreducible polynomials in $F[t]$ which are not Weierstrass polynomials this is straightforward, because the associated tame symbols are trivial on α . There is still one point of \mathbf{P}_F^1 to consider, namely the one at infinity, where t^{-1} is a local parameter. To handle it, write $a = t^N a_1$, $b = t^M b_1$, with $a_1, b_1 \in B[t^{-1}]$ satisfying $a_1(0) = b_1(0) = 1$. Using Lemma 7.1.2 and bilinearity of symbols we get

$$\{a, b\} = \{a_1, b_1\} - N\{t^{-1}, b_1\} - M\{a_1, t^{-1}\} + MN\{t^{-1}, -1\}.$$

We see using the condition $a_1(0) = b_1(0) = 1$ that the tame symbol associated with t^{-1} annihilates the first three terms, and the fourth gets mapped to $(-1)^{MN}$ in F . But $(-1)^{MN}$ is a unit for the valuation of F , and we are done.

Now we may rewrite the right hand side of (1) as

$$\sum_{P \in \mathbf{P}_{F,0}^1} f_P v_P(\partial_P^M(\{a, b\})) = v \left(\sum_{P \in \mathbf{P}_{F,0}^1} N_{\kappa(P)|F}(\partial_P^M(\{a, b\})) \right).$$

Indeed, this follows from the equality $f_P v_P = v \circ N_{\kappa(P)|F}$, which is a very special case of Proposition 7.4.1, because here v_P is none but the tame symbol on $\kappa(P)^\times$ equipped with its canonical valuation, and multiplication by f_P is the norm map on K_0 of the residue field of $\kappa(P)$. To conclude the proof it remains to observe that the sum in parentheses is trivial, by Weil's reciprocity law (Corollary 7.2.4). □

8.2 Properties of Gersten Complexes

In this section X is still an excellent scheme of finite dimension d , but the reader may safely assume it is a variety over a field. However, some arguments will be scheme-theoretic.

Notice that given an open subscheme $U \subset X$, there are natural restriction maps

$$\bigoplus_{P \in X_i} K_{n+i}^M(\kappa(P)) \rightarrow \bigoplus_{P \in U_i} K_{n+i}^M(\kappa(P))$$

for all $n \in \mathbf{Z}$ and $0 \leq i \leq d$, induced by the inclusion map $U \subset X$. These manifestly commute with the boundary maps ∂ in the complex $S_n(X)$, whence a map of complexes $j^* : S_n(X) \rightarrow S_n(U)$. One defines similarly a pushforward map $i_* : S_n(Z) \rightarrow S_n(X)$ induced by the inclusion $i : Z \rightarrow X$ of a closed subscheme.

Proposition 8.2.1 *Let $U \subset X$ be an open subscheme with complement Z .*

1. (Localisation) *For all $n \in \mathbf{Z}$ the natural sequence of complexes*

$$0 \rightarrow S_n(Z) \xrightarrow{i_*} S_n(X) \xrightarrow{j^*} S_n(U) \rightarrow 0$$

is exact.

2. (Mayer-Vietoris) *Let $V \subset X$ be a second open subscheme satisfying $U \cup V = X$. Then the sequence of complexes*

$$0 \rightarrow S_n(X) \xrightarrow{j_U^* \oplus j_V^*} S_n(U) \oplus S_n(V) \xrightarrow{j_{U \cap V}^* - j_{U \cap V}^*} S_n(U \cap V) \rightarrow 0$$

is exact.

3. (Mayer-Vietoris for closed subsets) *Assume there exists a closed subscheme $T \subset X$ such that $Z \cup T = X$. Then the sequence of complexes*

$$0 \rightarrow S_n(Z \cap T) \xrightarrow{i_{(Z \cap T)^*} \oplus i_{(Z \cap T)^*}} S_n(Z) \oplus S_n(T) \xrightarrow{i_{Z^*} - i_{T^*}} S_n(X) \rightarrow 0$$

is exact.

Proof: In all three cases the required exactness is readily checked at the level of each term $\bigoplus_{P \in X_i} K_{n+i}^M(\kappa(P))$ of the complex $S_n(X)$. \square

Definition 8.2.2 For $0 \leq i \leq d$ denote the i -th homology group of the complex $S_n(X)$ (i.e. the homology at the term indexed by the points in X_i) by $A_i(X, K_n^M)$. It is the i -th homology group of X with values in K_n^M .

Example 8.2.3 The case $n = -i$ is especially important for $0 \leq i \leq d$. Here we obtain the group

$$A_i(X, K_{-i}^M) = \text{coker} \left(\bigoplus_{P \in X_{i+1}} (\kappa(P))^\times \rightarrow \bigoplus_{P \in X_i} \mathbf{Z} \right),$$

the *Chow group of dimension i cycles on X* . This observation is the starting point for the application of K-theoretic methods to the study of algebraic cycles. See Colliot-Thélène [3] and Murre [1] for informative surveys on this research area.

With the above notations, Proposition 8.2.1 together with Proposition 3.1.1 yields:

Corollary 8.2.4 *Under the assumptions of Proposition 8.2.1 one has natural long exact sequences*

$$\begin{aligned} \cdots \rightarrow A_i(Z, K_n^M) \xrightarrow{i^*} A_i(X, K_n^M) \xrightarrow{j^*} A_i(U, K_n^M) \rightarrow A_{i-1}(Z, K_n^M) \rightarrow \cdots, \\ \cdots \rightarrow A_i(X, K_n^M) \xrightarrow{j_U^* \oplus j_V^*} A_i(U, K_n^M) \oplus A_i(V, K_n^M) \rightarrow \\ \xrightarrow{j_{U \cap V}^* - j_U^* j_V^*} A_i(U \cap V, K_n^M) \rightarrow A_{i-1}(X, K_n^M) \rightarrow \cdots \end{aligned}$$

and

$$\begin{aligned} \cdots \rightarrow A_i(Z \cap T, K_n^M) \xrightarrow{i_{(Z \cap T)^*} \oplus i_{(Z \cap T)^*}} A_i(Z, K_n^M) \oplus A_i(T, K_n^M) \rightarrow \\ \xrightarrow{i_{Z^*} - i_{T^*}} A_i(X, K_n^M) \rightarrow A_{i-1}(Z \cap T, K_n^M) \rightarrow \cdots \end{aligned}$$

Next we turn to the homotopy invariance property of K_n^M -homology groups. First some notation: for an integer $j \in \mathbf{Z}$, we define the *shifted complex* $S_n(X)[j]$ as the one whose degree i term is the degree $i - j$ term in $S_n(X)$.

Assume given a product $X \times_k Y$ of finite dimensional excellent schemes over a field k , and let j be the dimension of Y . Given a point in X_i , its closure in X is an integral closed subscheme Z . Then $Z \times_k Y$ is an integral closed subscheme in $X \times Y$ of dimension $i + j$, and thus corresponds to a point in $(X \times_k Y)_{i+j}$. This construction defines for all $n \in \mathbf{Z}$ natural maps

$$\bigoplus_{P \in X_i} K_{n+i+j}^M(\kappa(P)) \rightarrow \bigoplus_{P \in (X \times Y)_{i+j}} K_{n+i+j}^M(\kappa(P)),$$

commuting with the differentials in the complexes $S_{n+j}(X)[j]$ and $S_n(X \times_k Y)$. Therefore we obtain maps

$$S_{n+j}(X)[j] \rightarrow S_n(X \times_k Y) \tag{2}$$

for all $n \in \mathbf{Z}$.

Proposition 8.2.5 *Let X be a noetherian excellent scheme of finite dimension over a field k . For all $n \geq 0$ the natural map*

$$S_{n+1}(X)[1] \rightarrow S_n(X \times_k \mathbf{A}_k^1)$$

defined above induces isomorphisms on homology, i.e. the induced maps

$$A_{i-1}(X, K_{n+1}^M) \rightarrow A_i(X \times_k \mathbf{A}_k^1, K_n^M)$$

are isomorphisms for all i .

The proof is an adaptation of an argument by Quillen proving the homotopy invariance of Quillen K-theory. It is based on a suggestion of Joël Riou.

Proof: Without loss of generality we may assume X is reduced. By the noetherian assumption, we may decompose it into a finite union of irreducible closed subschemes, and then a finite number of applications of the Mayer-Vietoris sequence for closed subsets (and induction on dimension) shows that the irreducible case implies the reducible case.

We can therefore assume X is reduced and irreducible, and use induction on dimension. If $\dim(X) = 0$, then $X = \text{Spec}(F)$ for some field extension $F \supset k$, i.e. a point defined over F . The Gersten complex $S_n(\mathbf{A}_F^1)$ takes the shape

$$K_{n+1}^M(F(t)) \rightarrow \bigoplus_{P \in \mathbf{A}_0^1} K_n^M(\kappa(P)).$$

By virtue of Milnor's exact sequence (Theorem 7.2.1) we have $A_0(\mathbf{A}_F^1, K_n^M) = 0$ and $A_1(\mathbf{A}_F^1, K_n^M) = K_n^M(F)$ for all $n \geq 0$, which proves the statement for $\text{Spec}(F)$. Now take a general X and assume that the statement holds for all reduced closed subschemes $Z \subset X$ properly contained in X . Consider the commutative diagram

$$\begin{array}{ccccccc} \cdots & \rightarrow & A_{i-1}(Z, K_{n+1}^M) & \rightarrow & A_{i-1}(X, K_{n+1}^M) & \rightarrow & A_{i-1}(X \setminus Z, K_{n+1}^M) & \rightarrow & \cdots \\ & & \downarrow \alpha_Z^i & & \downarrow \alpha_X^i & & \downarrow \alpha_{X \setminus Z}^i & & \\ \cdots & \rightarrow & A_i(Z \times_k \mathbf{A}_k^1, K_n^M) & \rightarrow & A_i(X \times_k \mathbf{A}_k^1, K_n^M) & \rightarrow & A_i((X \setminus Z) \times_k \mathbf{A}_k^1, K_n^M) & \rightarrow & \cdots \end{array}$$

whose exact rows come from the first sequence in Corollary 8.2.4. The map α_Z^i is an isomorphism by the inductive assumption.

Now consider the system of (possibly reducible) reduced closed subschemes Z properly contained in X . The natural inclusion maps make it into a directed partially ordered set. With respect to this directed index set the

complexes $S_n(Z)$ together with the pushforward maps i_{Z*} form a direct system, hence so do their homology groups. Similarly, the complexes $S_n(X \setminus Z)$ together with the pullback maps $j_{X \setminus Z}^*$ also form a direct system. The direct limit of this system is $S_{n+d}(\text{Spec}(k(X))[d])$, because the only point of X contained in all of the $X \setminus Z$ is the generic point (the shift in degree comes from the fact that the closure of the generic point in X has dimension d , whereas $\text{Spec}(k(X))$ has dimension 0). We get a similar statement for the homology groups, so by the exactness property of the direct limit (Lemma 4.3.2) we obtain a commutative diagram

$$\begin{array}{ccccc} \cdots \rightarrow \varinjlim A_{i-1}(Z, K_{n+1}^M) & \rightarrow & A_{i-1}(X, K_{n+1}^M) & \rightarrow & A_{i-d-1}(\text{Spec}(k(X)), K_{n+d+1}^M) \rightarrow \cdots \\ & & \downarrow \varinjlim \alpha_Z^i & & \downarrow \alpha_X^i & & \downarrow \alpha_{k(X)}^{i-d}[d] \\ \cdots \rightarrow \varinjlim A_i(Z \times_k \mathbf{A}_k^1, K_n^M) & \rightarrow & A_i(X \times_k \mathbf{A}_k^1, K_n^M) & \rightarrow & A_{i-d}(\text{Spec}(k(X)) \times_k \mathbf{A}_k^1, K_{n+d}^M) \rightarrow \cdots \end{array}$$

Here the first vertical map is an isomorphism as a direct limit of the isomorphisms α_Z^i , and the third one is an isomorphism by the zero-dimensional case. The diagram then implies that the map α_X^i in the middle is an isomorphism as well. \square

As an application of the homotopy invariance property, we now compute the K_n^M -homology groups of projective spaces.

Proposition 8.2.6 *For all integers $n, d \geq 0$ we have*

$$A_i(\mathbf{P}^d, K_n^M) \cong \begin{cases} K_{n+i}^M(k) & \text{if } 0 \leq i \leq d; \\ 0 & \text{otherwise.} \end{cases}$$

Proof: The proof goes by induction on d , the case $d = 0$ being obvious. Consider \mathbf{P}^{d-1} embedded in \mathbf{P}^d as a hyperplane; the complement is naturally isomorphic to affine d -space \mathbf{A}^d . In this situation we may combine the localisation sequence of Corollary 8.2.4 with an iterated application of the isomorphism of Proposition 8.2.5 in the commutative diagram

$$\begin{array}{ccccccc} \cdots \rightarrow A_i(\mathbf{P}^{d-1}, K_n^M) & \xrightarrow{i^*} & A_i(\mathbf{P}^d, K_n^M) & \xrightarrow{j^*} & A_i(\mathbf{A}_k^d, K_n^M) & \xrightarrow{\partial} & A_{i-1}(\mathbf{P}^{d-1}, K_n^M) \rightarrow \cdots \\ & & \uparrow & & \cong \uparrow & & \\ & & A_{i-d}(k, K_{n+d}^M) & = & A_{i-d}(k, K_{n+d}^M) & & \end{array}$$

where the vertical maps are morphisms of the type (2). The diagram provides a splitting of the maps j^* , so we get decompositions

$$A_i(\mathbf{P}^d, K_n^M) \cong A_{i-d}(k, K_{n+d}^M) \oplus A_i(\mathbf{P}^{d-1}, K_n^M)$$

for all i and n . Here we have

$$A_{i-d}(k, K_{n+d}^M) \cong \begin{cases} K_{n+d}^M(k) & \text{if } i = d; \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, for $i > d$ the groups $A_i(\mathbf{P}^d, K_n^M)$ obviously vanish. We therefore obtain the result by induction on d . \square

Example 8.2.7 For us the most important case will be that of $n = 2 - d$. In this case we get:

$$A_d(\mathbf{P}^d, K_{2-d}^M) \cong K_2^M(k), \quad A_{d-1}(\mathbf{P}^d, K_{2-d}^M) \cong k^\times, \quad A_{d-2}(\mathbf{P}^d, K_{2-d}^M) \cong \mathbf{Z},$$

and the other groups are 0.

Remark 8.2.8 The *Gersten conjecture* for Milnor K-theory states that if X is the spectrum of an excellent regular local ring of finite dimension d , the complexes $S_n(X)$ are acyclic for all q in all degrees smaller than d . In the case of local rings of a smooth variety over a perfect field, this has been proven by Gabber; see Colliot-Thélène/Hoobler/Kahn [1] or Rost [1] for the proof (both papers work in a more general axiomatic setup).

This theorem has the following remarkable consequence. Given a smooth variety X over a perfect field, the rule $U \mapsto S_n(U)$ for all open subsets of X together with the restriction maps j^* introduced at the beginning of this section define a complex $\mathcal{S}_{n,X}$ of presheaves for the Zariski topology on X . Moreover, one checks easily that that this is actually a complex of *flabby* sheaves (i.e. the restriction maps $S_n(U) \rightarrow S_n(V)$ are surjective for $V \subset U$). Hence if we denote by \mathcal{K}_{n+d}^M the sheaf associated with the presheaf $U \mapsto A_d(U, K_{n+d}^M)$, Gabber's acyclicity theorem implies that $\mathcal{S}_{n,X}$ furnishes a *flabby resolution* of the sheaf \mathcal{K}_{n+d}^M . Thus it can be used to calculate the cohomology groups of the Zariski sheaf \mathcal{K}_n^M , and we get isomorphisms

$$H_{\text{Zar}}^i(X, \mathcal{K}_{n+d}^M) \cong A_{d-i}(X, K_n^M).$$

8.3 A Property of Severi-Brauer Varieties

We now begin the proof of the Merkurjev-Suslin theorem by establishing a crucial technical ingredient needed for the proof of Hilbert's Theorem 90 for K_2 , to be discussed in the next section.

Theorem 8.3.1 *Let k be a field, p a prime invertible in k , and X a Severi-Brauer variety of dimension $d = p - 1$ over k . If $K|k$ is a finite extension of degree p which splits X , the natural maps*

$$A_{d-i}(X, K_{i+1-d}^M) \rightarrow A_{d-i}(X_K, K_{i+1-d}^M)$$

are injective for all $0 \leq i \leq p - 1$.

Remarks 8.3.2

1. Via the isomorphism of Remark 8.2.8, the statement of the theorem becomes equivalent to the injectivity of the maps $H_{\text{Zar}}^i(X, \mathcal{K}_{i+1}^M) \rightarrow H_{\text{Zar}}^i(X_K, \mathcal{K}_{i+1}^M)$, but we shall not need this interpretation. In fact, this injectivity holds for X of any dimension (see Kahn [2]).
2. The theorem also serves in the proof of the general Bloch-Kato conjecture, during the verification of the ‘multiplication principle’ for splitting varieties (see Suslin-Joukhovitski [1]).

Oddly enough, the only currently known proof of the theorem is a somewhat mysterious argument relying on Quillen’s calculation of the algebraic K-theory of X . As a result we cannot give a self-contained exposition of the argument here. Still, we shall explain the method, referring to facts from algebraic K-theory to the literature. The best short introduction to Quillen K-theory is Swan [3]; the original paper Quillen [1] still makes valuable reading, and the book of Srinivas [1] is a useful account. We also have to assume familiarity with spectral sequences, for which we refer to Weibel [1].

We begin by a very succinct review of the construction of Quillen’s K-groups. Given a scheme X , denote by $\mathcal{M}(X)$ the category of coherent sheaves on X , and by $\mathcal{P}(X) \subset \mathcal{M}(X)$ the full subcategory of vector bundles (by which we mean locally free sheaves of finite rank). In the fundamental paper of Quillen [1] a purely categorical construction is introduced, producing new categories $Q\mathcal{M}(X)$ and $Q\mathcal{P}(X)$ out of $\mathcal{M}(X)$ and $\mathcal{P}(X)$. Taking the geometric realisations of the nerves of these categories yields topological spaces $|BQ\mathcal{M}(X)|$ and $|BQ\mathcal{P}(X)|$. One then defines for all $n \geq 0$ the groups $G_n(X)$ and $K_n(X)$ as the homotopy groups $\pi_{n+1}(|BQ\mathcal{M}(X)|)$ and $\pi_{n+1}(|BQ\mathcal{P}(X)|)$, respectively. When X is regular (e.g. a smooth variety over a field), each object in $\mathcal{M}(X)$ has a finite resolution by objects of $\mathcal{P}(X)$. From this one infers via the so-called resolution theorem of Quillen that in this case $G_n(X) = K_n(X)$ for all n .

For a commutative ring A we define the groups $G_n(A)$ and $K_n(A)$ to be $G_n(\text{Spec}(A))$ and $K_n(\text{Spec}(A))$, respectively. As $\mathcal{M}(\text{Spec } A)$ is equivalent

to the category $\mathcal{M}(A)$ of finitely generated A -modules and $\mathcal{P}(\text{Spec } A)$ to the category $\mathcal{P}(A)$ of finitely generated projective A -modules, one may also define $G_n(A)$ and $K_n(A)$ as homotopy groups of the spaces $|BQM(A)|$ and $|BQP(A)|$, respectively. This latter construction immediately generalises to not necessarily commutative A .

Facts 8.3.3 For a field F there exists a natural map from the n -th Milnor K -group $K_n^M(F)$ to the n -th Quillen K -group $K_n(F)$ which is an isomorphism for $n \leq 2$, but the two groups differ in general for $n > 2$. The comparison result for $n \leq 2$ is rather difficult, especially in the case $n = 2$, where it is a famous theorem of Matsumoto (see Milnor [2]).

Moreover, for $n = 1$ and A a not necessarily commutative ring the construction gives back the group $K_1(A)$ defined in Chapter 2.

Let \mathcal{M}^i be the full subcategory of $\mathcal{M}(X)$ consisting of coherent sheaves whose support is of codimension $\geq i$ in X . They define a decreasing filtration of the category $\mathcal{M}(X)$, whence decreasing filtrations

$$G_n(X) = G_n(\mathcal{M}^0) \supset G_n(\mathcal{M}^1) \supset G_n(\mathcal{M}^2) \supset \dots \quad (3)$$

of the groups $G_n(X)$. Quillen has shown that there are long exact sequences

$$\dots \rightarrow G_n(\mathcal{M}^{i+1}) \rightarrow G_n(\mathcal{M}^i) \rightarrow G_n(\mathcal{M}^i/\mathcal{M}^{i+1}) \rightarrow G_{n-1}(\mathcal{M}^{i+1}) \rightarrow \dots \quad (4)$$

and isomorphisms

$$G_n(\mathcal{M}^i/\mathcal{M}^{i+1}) \cong \bigoplus_{P \in X^i} K_n(\kappa(P)), \quad (5)$$

for all $i \geq 0$, where X^i stands for the set of scheme-theoretic points whose closure in X has codimension i .

By the general theory of spectral sequences, the filtration (3) gives rise to an exact couple via the exact sequence (4), and hence to a spectral sequence which converges to $G_n(X)$ if the filtration is finite, i.e. if X has finite dimension. The isomorphism (5) allows one to identify its E_1 -term, thus one obtains a spectral sequence of the shape

$$E_1^{r,s}(X) = \bigoplus_{P \in X^r} K_{-r-s}(\kappa(P)) \Rightarrow G_{-n}(X)$$

called the *spectral sequence of Brown-Gersten-Quillen*. It is a fourth quadrant spectral sequence (i.e. $r \geq 0$ and $s \leq 0$), so the E_1 -terms are zero for $|s| < |r|$. The filtration induced on $G_n(X)$ is precisely (3); the fact that it

is a descending filtration accounts for the negative indices. We denote its i -th term $G_n(\mathcal{M}^i)$ by $F^i(G_n(X))$ and its i -th graded piece $G_n(\mathcal{M}^i/\mathcal{M}^{i+1})$ by $\text{gr}^i(G_n(X))$.

By definition, the E_2 -terms of the spectral sequence are obtained as the homology groups of a complex

$$\bigoplus_{P \in X^0} K_n(\kappa(P)) \rightarrow \bigoplus_{P \in X^1} K_{n-1}(\kappa(P)) \rightarrow \cdots \rightarrow \bigoplus_{P \in X^n} K_0(\kappa(P)), \quad (6)$$

the *Gersten complex in Quillen K -theory*. Up to reindexing, this complex is of a similar shape as the Gersten-Milnor complex constructed in Section 8.1. Moreover, the last three terms of the two complexes are isomorphic by Fact 8.3.3. Quillen has checked that the last coboundary map $\bigoplus K_1(\kappa(P)) \rightarrow \bigoplus K_0(\kappa(P))$ in (6) is induced by the valuation map, and Suslin has checked (Suslin [1], Proposition 6.8) that the penultimate coboundary $\bigoplus K_2(\kappa(P)) \rightarrow \bigoplus K_1(\kappa(P))$ is induced by a map which equals the tame symbol up to a character with values in $\{-1, 1\}$. These facts imply:

Lemma 8.3.4 *Let X be a smooth variety of dimension d over a field. Then there are natural isomorphisms*

$$E_2^{i,-i} \cong CH^i(X) := CH_{d-i}(X) \quad \text{and} \quad E_2^{i,-i-1} \cong A_{d-i}(X, K_{i+1-d}^M)$$

for all $0 \leq i \leq d$.

From now on we assume that X is a smooth variety over a field, so that $K_n(X) = G_n(X)$ for all n . By the lemma and the Brown-Gersten-Quillen spectral sequence we obtain maps $\rho_i : CH^i(X) \rightarrow \text{gr}^i(K_0(X))$. In fact, they are induced by sending a closed subvariety Z of codimension i to the class of \mathcal{O}_Z in $G_0(X) \cong K_0(X)$; in particular they are surjective. The general theory of Chern classes introduced by Grothendieck provides a rational splitting of these maps.

Fact 8.3.5 For each $i \geq 0$ there exists a canonical group homomorphism $c_i : K_0(X) \rightarrow CH^i(X)$ called the *i -th Chern class map* which is trivial on $K_0(\mathcal{M}^{i+1})$, and moreover the composite map $c_i \circ \rho_i : CH^i(X) \rightarrow \text{gr}^i(K_0(X)) \rightarrow CH^i(X)$ equals multiplication by $(-1)^{i-1}(i-1)!$. Consequently, the collection of the Chern class maps induces a direct sum decomposition

$$K_0(X) \otimes \mathbf{Q} \cong \bigoplus_{i=0}^d CH^i(X) \otimes \mathbf{Q}.$$

The claim about the map $c_i \circ \rho_i$ boils down to the formula $[c_i(\mathcal{O}_Z)] = (-1)^{i-1}(i-1)![Z]$ in $CH^i(X)$ for a closed subvariety $Z \subset X$ of codimension i . When Z is smooth, this follows from the Riemann-Roch formula without denominators (Fulton [1], Example 15.3.1). The general case reduces easily to the smooth case (Suslin [1], Proposition 9.3).

We can now easily prove:

Lemma 8.3.6 *Let p be a prime number. For a Severi-Brauer variety X of dimension $d = p - 1$ over a field k , the natural maps $CH^i(X) \rightarrow \text{gr}^i(K_0(X))$ are isomorphisms for all $0 \leq i \leq p - 1$.*

Proof: We have already remarked that the maps in question are surjective. For injectivity it will be enough to show in view of Fact 8.3.5 that the groups $CH^i(X)$ have no torsion elements of order dividing $(i-1)!$ for $0 \leq i \leq p-1$. In fact, they have no torsion prime to p . Indeed, by Proposition 7.4.1 we have a commutative diagram

$$\begin{array}{ccc} \bigoplus_{Q \in X_K^{i-1}} K_1(\kappa(Q)) & \longrightarrow & \bigoplus_{Q \in X_K^i} K_0(\kappa(Q)) \\ \bigoplus_{\kappa(Q)|\kappa(P)} N_{\kappa(Q)|\kappa(P)} \downarrow & & \downarrow \bigoplus_{\kappa(Q)|\kappa(P)} N_{\kappa(Q)|\kappa(P)} \\ \bigoplus_{P \in X^{i-1}} K_1(\kappa(P)) & \longrightarrow & \bigoplus_{P \in X^i} K_0(\kappa(P)) \end{array}$$

where the horizontal maps are induced by valuation maps. According to Example 8.2.3 the cokernels of these maps are respectively $CH^i(X_K)$ and $CH^i(X)$, so the diagram defines a norm map $CH^i(X_K) \rightarrow CH^i(X)$. By a basic property of norm maps, the composite of this norm with the natural flat pullback map $CH^i(X) \rightarrow CH^i(X_K)$ induced by the maps $\iota_{\kappa(Q)|\kappa(P)}$ is multiplication by p . On the other hand, applying Proposition 8.2.6 with $n = -i$ shows that $CH^i(X_K) \cong \mathbf{Z}$ for all i . In particular, these groups are torsion free, so the groups $CH^i(X)$ can only have torsion elements of order dividing p . \square

Corollary 8.3.7 *With notations as in the above lemma, the natural maps $E_2^{i,-i-1} \rightarrow \text{gr}^i(K_1(X))$ coming from the Brown-Gersten-Quillen spectral sequence are isomorphisms for all $0 \leq i \leq p - 1$.*

Proof: All differentials whose target or source is a term $E_m^{i,-i-1}$ come from or land in terms of the shape $E_m^{j,-j}$. According to the first isomorphism in Lemma 8.3.4 and the statement of the lemma above these terms map

isomorphically onto $\text{gr}^i(K_0(X))$ for $m = 2$, and hence for all $m \geq 2$. But then all differentials in question must be zero, whence the corollary. \square

Combining the corollary with the second isomorphism of Lemma 8.3.4 we see that the statement of Theorem 8.3.1 is equivalent to the injectivity of the maps $\text{gr}^i(K(X)) \rightarrow \text{gr}^i(K(X_K))$. Or in other words:

Proposition 8.3.8 *Let X be a Severi-Brauer variety of dimension $d = p - 1$ over a field k split by an extension $K|k$ of degree p , and let $\pi : X_K \rightarrow X$ be the natural projection. The filtration by codimension of support on $K_1(X_K)$ induces that on $K_1(X)$, i.e. $F^i K_1(X_K) \cap \pi^* K_1(X) = F^i K_1(X)$ for all i .*

Here $\pi^* : K_1(X) \rightarrow K_1(X_K)$ is the natural pullback map on K-theory, induced by pulling back vector bundles. The proof relies on Quillen’s calculation on the K -theory of Severi-Brauer varieties.

Fact 8.3.9 Let X be a Severi-Brauer variety of dimension $d - 1$ split by $K|k$, and let A be a corresponding central simple algebra. Then for all $n \geq 0$ there is a decomposition

$$K_n(X) \cong \bigoplus_{j=0}^d K_n(A^{\otimes j}). \tag{7}$$

To construct the decomposition, Quillen shows that there is a rank d vector bundle \mathcal{J} on X equipped with a left action by A which becomes isomorphic to $\mathcal{O}(-1)^{\oplus d}$ after pullback to X_K . The decomposition is then induced (from right to left) by the map (u_0, \dots, u_d) , where $u_j : \mathcal{P}(A^{\otimes j}) \rightarrow \mathcal{P}(X)$ maps a projective $A^{\otimes j}$ -module M to $\mathcal{J}^{\otimes j} \otimes_{A^{\otimes j}} M$. This decomposition is best explained in §12 of Swan [3]; see also the other references cited above.

In the split case $X \cong \mathbf{P}_k^{d-1}$ the decomposition reduces to

$$K_n(X) \cong \bigoplus_{j=0}^d K_n(k), \tag{8}$$

the isomorphism being induced (from right to left) by the map (v_0, \dots, v_d) , where $v_j : \mathcal{P}(k) \rightarrow \mathcal{P}(X)$ maps a k -vector space V to $\mathcal{O}(-j) \otimes V$. To see that this is a special case of the previous construction one uses an easy case of *Morita equivalence* (Rowen [2]) which shows that the module categories of k and $M_d(k)$ are equivalent.

Corollary 8.3.10 *Assume A is a division algebra of prime degree p , and let $N \subset k^\times$ be the image of the reduced norm map $\text{Nrd} : A^\times \rightarrow k^\times$. Then for $n = 1$ the isomorphism (7) becomes $K_1(X) \cong N^{\oplus d}$.*

Proof: By the last fact in 8.3.3, on the right hand side of (7) we are dealing with the groups of Chapter 2 in the case $n = 1$. For each j we may find i with $ij \equiv 1 \pmod{p}$, so that $A^{\otimes ij}$ is Brauer equivalent to A , and hence $K_1(A) \cong K_1(A^{\otimes ij})$ by Lemma 2.8.6. There are injective base change maps $A \rightarrow A^{\otimes j} \rightarrow A^{\otimes ij}$ whose composite induces the isomorphism, so $K_1(A) \cong K_1(A^{\otimes j})$. Finally, the reduced norm map gives rise to an isomorphism $K_1(A) \xrightarrow{\sim} N$ by Wang's theorem (Theorem 2.8.12). \square

To attack the proof of Proposition 8.3.8, we first rewrite the isomorphism (8) for X_K in another way. Consider first the case $n = 0$, and denote by γ the class of $\mathcal{O}(-1)$ in $K_0(X_K)$. The decomposition for $K_0(X_K)$ is then just the direct sum $\bigoplus \mathbf{Z}\gamma^j$. But according to the description of (8), the case of general n reduces to $n = 0$, for it is induced by a product $K_0(X_K) \otimes_{\mathbf{Z}} K_n(K) \rightarrow K_n(X_K)$. Thus we may write

$$K_n(X_K) \cong \bigoplus_{j=0}^d K_n(K)\gamma^j.$$

Lemma 8.3.11 *The filtration by codimension of support on $K_n(X)$ is described by*

$$F^i K_n(X_K) \cong \bigoplus_{j=i}^d K_n(K)(\gamma - 1)^j.$$

Proof: Let H be a hyperplane in $X_K \cong \mathbf{P}_K^{d-1}$. The exact sequence

$$0 \rightarrow \mathcal{O}(-1) \rightarrow \mathcal{O} \rightarrow \mathcal{O}_H \rightarrow 0$$

shows that the class of \mathcal{O}_H in $K_0(X_K)$ is precisely $\gamma - 1$. It generates $\text{gr}^1 K_0(X_K) \cong \mathbf{Z}$, and its powers $[\mathcal{O}_H]^j$ generate $\text{gr}^j K_0(X) \cong \mathbf{Z}$ (see the proof of Lemma 8.3.6), whence the case $n = 0$. To treat the general case, we exploit the isomorphism $K_0(X_K) \otimes_{\mathbf{Z}} K_n(K) \xrightarrow{\sim} K_n(X_K)$. In fact, it is induced by a product map on K-groups coming from tensoring vector bundles on X with trivial bundles coming from $\text{Spec}(K)$ (Swan [3], §8 or Suslin [1], §6). As such, it preserves filtration by codimension of support, and the result follows from the case $n = 0$. \square

For the proof of Proposition 8.3.8 we need one last fact from Quillen K-theory: any proper morphism of finite-dimensional noetherian schemes $\phi: S \rightarrow T$ gives rise to pushforward maps $\phi_*: G_n(S) \rightarrow G_n(T)$ for all n , induced by taking higher direct images of coherent sheaves (Suslin [1], §6). It yields the norm map when $n = 1$ and $S = \text{Spec}(E)$, $T = \text{Spec}(F)$ for a finite

extension $E|F$ of fields, and satisfies the projection formula $\phi_*(x \cdot \phi^*(y)) = \phi_*(x)y$ with respect to the product encountered in the last proof.

Proof of Proposition 8.3.8: We may assume A is a division algebra, for otherwise it is split and the claim is obvious. The pullback map $\pi^* : K_1(X) \rightarrow K_1(X_K)$ respects the decompositions (8) and (7), and moreover using Morita equivalence and Wang's theorem may be identified on the components with the inclusion $N \hookrightarrow K^\times$. Hence it is injective, and its image may be described as the subgroup

$$\bigoplus_{j=0}^d N\gamma^j \subset \bigoplus_{j=0}^d K^\times \gamma^j.$$

The intersection of this subgroup with $F^i K_1(X_K)$ is given by

$$\left(\bigoplus_{j=0}^d N\gamma^j \right) \cap \left(\bigoplus_{j=i}^d K^\times (\gamma - 1)^j \right) = \bigoplus_{j=i}^d N(\gamma - 1)^j$$

by virtue of the previous lemma, so to conclude the proof it remains to show that $N(\gamma - 1)^j \subset \pi^*(F^i K_1(X))$ for $i \leq j$. Pick $\alpha \in N$ and $x \in A$ satisfying $\text{Nrd}(x) = \alpha$. As A is a division algebra of degree p , Proposition 2.6.4 shows that $\alpha = N_{L|k}(x)$ for a degree p subfield $L \subset A$ which is moreover a splitting field for A . Apply the pushforward map $\phi_* : K_1(X_L) \rightarrow K_1(X)$ coming from $\phi : X_L \rightarrow X$ to $x(\gamma - 1)^j$, and consider the decomposition (8) for X_L . Since the class γ is the pullback of the class of the vector bundle \mathcal{J} on X by the construction of Fact 8.3.9, the projection formula for the pushforward map implies $\alpha(\gamma - 1)^j = \phi_*(x(\gamma - 1)^j)$. But by its construction ϕ_* preserves filtration by codimension of support, which proves the proposition, and thereby Theorem 8.3.1. \square

8.4 Hilbert's Theorem 90 for K_2

Recall from Example 2.3.4 that the classical form of Hilbert's Theorem 90 is the following statement: *In a cyclic Galois extension $K|k$ of fields each element of norm 1 can be written in the form $\sigma(a)a^{-1}$, where $a \in K^\times$ and σ is a fixed generator of $\text{Gal}(K|k)$.* In other words, the complex

$$K^\times \xrightarrow{\sigma-1} K^\times \xrightarrow{N_{K|k}} k^\times$$

is exact. In this section we prove an analogue of this statement for the group K_2^M , which is the crucial ingredient in the proof of the Merkurjev-Suslin

theorem. Let $K|k$ be a cyclic extension as above, and consider the sequence of maps

$$K_2^M(K) \xrightarrow{\sigma^{-1}} K_2^M(K) \xrightarrow{N_{K|k}} K_2^M(k).$$

Here σ acts on $K^\times \otimes_{\mathbf{Z}} K^\times$ by $\sigma(a \otimes b) = \sigma(a) \otimes \sigma(b)$, and $K_2^M(K)$ carries the induced action. The sequence is a complex, because the norm map satisfies $N_{K|k}(\sigma(\alpha)) = N_{K|k}(\alpha)$ for all $\alpha \in K_2^M(K)$ (Corollary 7.3.3).

Now the promised result is:

Theorem 8.4.1 (Hilbert's Theorem 90 for K_2) *Let $K|k$ be a cyclic Galois extension of prime degree p , and let σ be a generator of $\text{Gal}(K|k)$. Then the complex*

$$K_2^M(K) \xrightarrow{\sigma^{-1}} K_2^M(K) \xrightarrow{N_{K|k}} K_2^M(k) \tag{9}$$

is exact.

Remark 8.4.2 The theorem in fact holds for arbitrary cyclic extensions (see Exercise 5), but the prime degree case is the crucial one.

First we establish the theorem in an important special case.

Proposition 8.4.3 *Let $K|k$ be a cyclic Galois extension of degree p as above. Assume that*

- *k has no nontrivial finite extensions of degree prime to p ;*
- *the norm map $N_{K|k} : K^\times \rightarrow k^\times$ is surjective.*

Then Theorem 8.4.1 holds for the extension $K|k$.

Before starting the proof, we introduce some notation. Let $K|k$ be a cyclic extension of degree p as above, and let $F \supset k$ be a field. If $K \otimes_k F$ is not a field, then it splits into a direct sum $K \otimes_k F \cong F^{\oplus p}$ of copies of F . In this last case we shall use the notation $K_2^M(K \otimes_k F)$ for $K_2^M(F)^{\oplus p}$ and denote by $N_{K \otimes_k F|F} : K_2^M(K \otimes_k F) \rightarrow K_2^M(F)$ the map $K_2^M(F)^{\oplus p} \rightarrow K_2^M(F)$ given by the sum of the identity maps.

Proof: Consider the map

$$\overline{N}_{K|k} : K_2^M(K)/(\sigma - 1)K_2^M(K) \rightarrow K_2^M(k)$$

induced by the norm $N_{K|k}$. The idea of the proof is to construct an inverse

$$\psi : K_2^M(k) \rightarrow K_2^M(K)/(\sigma - 1)K_2^M(K)$$

for the map $\overline{N}_{K|k}$. To do so, we first define a map

$$\tilde{\psi} : k^\times \times k^\times \rightarrow K_2^M(K)/(\sigma - 1)K_2^M(K)$$

as follows. Let $a, b \in k^\times$. By assumption $a = N_{K|k}(c)$ for some $c \in K^\times$, and we set

$$\tilde{\psi}(a, b) := \{c, b_K\} \in K_2^M(K)/(\sigma - 1)K_2^M(K),$$

where b_K means b viewed as an element of K . To see that $\tilde{\psi}$ is well-defined, take another element $c' \in K^\times$ with $N_{K|k}(c') = a$. Then $c'c^{-1}$ has norm 1, so it is of the form $\sigma(e)e^{-1}$ by the original Theorem 90 of Hilbert recalled above. As $\sigma(b_K) = b_K$, we have

$$\{c', b_K\} - \{c, b_K\} = \{\sigma(e)e^{-1}, b_K\} = (\sigma - 1)\{e, b_K\} \in (\sigma - 1)K_2^M(K).$$

The map $\tilde{\psi}$ is manifestly bilinear, so it extends to a map

$$\tilde{\psi} : k^\times \otimes_{\mathbf{Z}} k^\times \rightarrow K_2^M(K)/(\sigma - 1)K_2^M(K).$$

We next check that $\tilde{\psi}$ respects the Steinberg relation, i.e. $\tilde{\psi}(a \otimes 1 - a) = 0$ for $a \neq 0, 1$. Set $L = k(\alpha)$ for some $\alpha \in \bar{k}$ satisfying $\alpha^p = a$ if $a \notin k^{\times p}$, and set $L = K$ otherwise. The tensor product $M = K \otimes_k L$ is a field for $L \neq K$, and a direct sum of p copies of K for $L = K$. We have $H^1(G, M^\times) = 0$ for $G = \text{Gal}(K|k)$, in the first case by Hilbert's Theorem 90, and in the second one because the group of invertible elements M^\times is a co-induced G -module. Observe that

$$1 - a_K = N_{M|K}(1 - \alpha_M). \quad (10)$$

Indeed, if the extension $L|k$ is purely inseparable, so is $M|K$, and we have $N_{M|K}(1 - \alpha_M) = (1 - \alpha_M)^p = 1 - a_K$. Otherwise, $L|k$ is a cyclic Galois extension generated by some automorphism τ (as by our first assumption k contains the p -th roots of unity), so in L we have a product decomposition

$$x^p - a = \prod_{i=0}^{p-1} (x - \tau^i(\alpha)).$$

Setting $x = 1$ we get $1 - a = \prod(1 - \tau^i(\alpha)) = N_{L|k}(1 - \alpha)$. Since $M|K$ is either a degree p cyclic Galois extension, or a direct sum of p copies of K , this implies (10). We now compute using the projection formula

$$\{c, 1 - a\} = N_{M|K}(\{c_M, 1 - \alpha_M\}) = N_{M|K}(\{c_M \alpha_M^{-1}, 1 - \alpha_M\} + \{\alpha_M, 1 - \alpha_M\}).$$

Here $N_{M|L}(c_M \alpha_M^{-1}) = a(\alpha^p)^{-1} = 1$, because $\sigma(\alpha_M) = \alpha_M$. By the vanishing of $H^1(G, M^\times)$ we may thus write $c_M \alpha_M^{-1} = \sigma(d)d^{-1}$ for some $d \in M$ using Example 3.2.9 (this is just the classical Hilbert 90 if $L \neq K$), and conclude that

$$\{c, 1 - a\} = N_{M|K}(\{\sigma(d)d^{-1}, 1 - \alpha_M\}) = (\sigma - 1)N_{M|K}(\{d, 1 - \alpha_M\}),$$

noting that $N_{M|K}$ commutes with the action of σ and $\sigma(\alpha_M) = \alpha_M$. This is an element lying in $(\sigma - 1)K_2^M(K)$, which finishes the verification.

We have now shown that the map $\tilde{\psi}$ induces a map

$$\psi : K_2^M(k) \rightarrow K_2^M(K)/(\sigma - 1)K_2^M(K).$$

Moreover, for all $a, b \in k^\times$ one has

$$N_{K|k}(\psi(\{a, b\})) = N_{K|k}(\{c, b\}) = \{N_{K|k}(c), b\} = \{a, b\}$$

by the projection formula, which implies in particular that ψ is injective. For surjectivity, note that thanks to the first assumption of the proposition we may apply the corollary to the Bass-Tate lemma (Corollary 7.2.10) according to which the symbol map $K^\times \otimes_{\mathbf{Z}} k^\times \rightarrow K_2^M(K)$ is surjective. Hence so is ψ , and the proof is finally finished. \square

The idea of the proof of Theorem 8.4.1 is then to embed k into some (very large) field extension $F_\infty \supset k$ satisfying the conditions of the proposition above, so that moreover the induced map between the homologies of the complex (9) and the similar one associated with the extension $F_\infty K|F_\infty$ is injective. The proposition will then enable us to conclude. The required injectivity property will be assured by the two propositions below.

Denote by $V(F)$ the homology of the complex

$$K_2^M(K \otimes_k F) \xrightarrow{\sigma-1} K_2^M(K \otimes_k F) \xrightarrow{N_{K \otimes_k F|F}} K_2^M(F),$$

where we keep the notation introduced before the previous proof, the automorphism σ acts on $K \otimes_k F$ via the first factor, and $K_2^M(K \otimes_k F)$ is equipped with the induced action. For a tower of field extensions $E|F|k$, we have natural morphisms $V(k) \rightarrow V(F) \rightarrow V(E)$. We can now state:

Proposition 8.4.4 *Let $k'|k$ be an algebraic extension of degree prime to p . Then the map $V(k) \rightarrow V(k')$ is injective.*

Here in the case of an infinite algebraic extension we mean an extension whose finite subextensions all have degree prime to p .

Proof: Let $L|k$ be a finite extension. The diagram

$$\begin{array}{ccccc}
 K_2^M(K \otimes_k L) & \xrightarrow{\sigma-1} & K_2^M(K \otimes_k L) & \xrightarrow{N_{K \otimes_k L|L}} & K_2^M(L) \\
 N_{K \otimes_k L|K} \downarrow & & N_{K \otimes_k L|K} \downarrow & & N_{L|k} \downarrow \\
 K_2^M(K) & \xrightarrow{\sigma-1} & K_2^M(K) & \xrightarrow{N_{K|k}} & K_2^M(k)
 \end{array}$$

gives rise to a norm map $N_{L|k} : V(L) \rightarrow V(k)$. It follows from the results of Chapter 7, Section 7.3 that the composite $V(k) \rightarrow V(L) \xrightarrow{N_{L|k}} V(k)$ is multiplication by the degree $[L : k]$. In particular, for $L = K$ we get that the composite $V(k) \rightarrow V(K) \xrightarrow{N_{K|k}} V(k)$ is multiplication by p . On the other hand, notice that $V(K)=0$. Indeed, by Galois theory $K \otimes_k K$ splits as a direct product of p copies of K , and σ acts *trivially* on each component, because we defined its action on $K \otimes_k K$ via the first factor. From this the vanishing of $V(K)$ is immediate.

Putting the above together we get that $pV(k) = 0$. On the other hand, if $L = k'$ for a finite extension $k'|k$ of degree prime to p , the composite $V(k) \rightarrow V(k') \rightarrow V(k)$ is multiplication by $[k' : k]$, and therefore the map $V(k) \rightarrow V(k')$ must be injective. To pass from here to the general case of an algebraic extension $k'|k$ of degree prime to p , we write k' as a direct limit of its finite subextensions. The claim then follows from the fact that the functor $L \rightarrow V(L)$ commutes with direct limits (because so do tensor products and exact sequences). □

The second injectivity property, which is the main step in the proof of Theorem 8.4.1, is given by the following proposition.

Proposition 8.4.5 *Let X be a Severi-Brauer variety split by the degree p cyclic extension $K|k$. Then the map $V(k) \rightarrow V(k(X))$ is injective.*

Proof: An element of $\ker(V(k) \rightarrow V(k(X)))$ is given by some $\alpha \in K_2^M(K)$ of trivial norm such that there exists $\beta \in K_2^M(K(X))$ satisfying $\alpha_{K(X)} = (\sigma - 1)\beta$. We would like to prove that β may be chosen in $K_2^M(K)$. Consider

the commutative diagram

$$\begin{array}{ccccc}
 K_2^M(K) & \xrightarrow{\sigma-1} & K_2^M(K) & \xrightarrow{N_{K|k}} & K_2^M(k) \\
 \downarrow & & \downarrow & & \downarrow \\
 \beta \in K_2^M(K(X)) & \xrightarrow{\sigma-1} & K_2^M(K(X)) & \xrightarrow{N_{K|k}} & K_2^M(k(X)), \\
 \partial^M \downarrow & & \partial^M \downarrow & & \partial^M \downarrow \\
 \bigoplus_{P \in X_K^1} \kappa(P)^\times & \xrightarrow{\sigma-1} & \bigoplus_{P \in X_K^1} \kappa(P)^\times & \xrightarrow{N_{K|k}} & \bigoplus_{P \in X^1} \kappa(P)^\times
 \end{array}$$

whose rows and columns are complexes. The lower right square commutes by Proposition 7.4.1; commutativity of the other squares is straightforward. The lower left square shows that $(\sigma - 1)\partial^M(\beta) = 0$, so $\partial^M(\beta)$ is fixed by the action of $\text{Gal}(K|k)$, i.e. it comes from an element of $\bigoplus_{P \in X^1} \kappa(P)^\times$. Moreover, the valuations of this element coming from points of X^2 must be trivial, as so are those of $\partial^M(\beta)$. This means that there is an element γ_0 in

$$Z(X) := \ker \left(\bigoplus_{P \in X^1} \kappa(P)^\times \longrightarrow \bigoplus_{P \in X^2} \mathbf{Z} \right)$$

such that $\partial^M(\beta) = \gamma_{0,K}$. Now look at the commutative diagram

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 K_2^M(k(X))/K_2^M(k) & \xrightarrow{\partial^M} & Z(X) & \longrightarrow & A_{d-1}(X, K_{2-d}^M) & \longrightarrow & 0 \\
 \downarrow & & \downarrow & & \downarrow & & \\
 K_2^M(K(X))/K_2^M(K) & \xrightarrow{\partial^M} & Z(X_K) & \longrightarrow & A_{d-1}(X_K, K_{2-d}^M) & \longrightarrow & 0.
 \end{array}$$

The exact rows of this diagram are given by the definition of the group $A_{d-1}(X, K_{2-d}^M)$. Injectivity of the second vertical map is obvious, and that of the third comes from the case $i = 1$ of Theorem 8.3.1. It follows from the diagram that there exists $\beta_0 \in K_2^M(k(X))$ such that $\partial^M(\beta_0) = \gamma_0$. We may therefore replace β by $\beta - \beta_{0,K}$ without affecting the relation $\alpha = (\sigma - 1)\beta$, so that $\partial^M(\beta) = 0$. This means that β lies in $A_d(X_K, K_{2-d}^M) \subset K_2^M(K(X))$. As X_K is a projective space over K , we get from Example 8.2.7 that β lies in $K_2^M(K)$, which is what we wanted to show. \square

We finally come to the

Proof of Theorem 8.4.1: Define a tower of fields

$$k = F_0 \subset F_1 \subset F_2 \subset F_3 \subset \cdots \subset F_\infty = \bigcup_n F_n$$

inductively as follows:

1. The field F_{2n+1} is a maximal prime to p extension of F_{2n} ;
2. the field F_{2n+2} is the compositum of all function fields of Severi-Brauer varieties associated with cyclic algebras of the form (χ, b) , where χ is a fixed character of $\text{Gal}(F_{2n+1}K|F_{2n+1}) \cong \text{Gal}(K|k)$ and $b \in F_{2n+1}^\times$.

Here some explanations are in order. Concerning the maximal prime to p extension, see Remark 7.2.11. By the compositum of all function fields of a family $\{X_i : i \in I\}$ of varieties we mean the direct limit of the direct system of the function fields of all varieties $X_{i_1} \times \cdots \times X_{i_r}$ for finite subsets $\{i_1, \dots, i_r\} \subset I$, partially ordered by the natural inclusions. Finally, the extensions $KF_j|F_j$ are all cyclic of degree p . Indeed, this property is preserved when passing to an extension of degree prime to p , and also when taking the function field of a product of Severi-Brauer varieties, as these varieties are geometrically integral, and hence the base field is algebraically closed in their function field.

Now Proposition 8.4.4 shows that $V(F_{2n})$ injects into $V(F_{2n+1})$ for $n \geq 0$, and an iterated application of Proposition 8.4.5 implies that $V(F_{2n+1})$ injects into $V(F_{2n+2})$. Therefore $V(k) = V(F_0)$ injects into $V(F_\infty)$. We now show that the field F_∞ satisfies the conditions in Proposition 8.4.3, which will conclude the proof. Indeed, it has no algebraic extension of degree prime to p by construction. To verify the surjectivity of the norm map $N_{KF_\infty|F_\infty}$, use Corollary 4.7.3 which states that under the isomorphism $F_\infty^\times/N_{KF_\infty|F_\infty}((KF_\infty)^\times) \cong \text{Br}(KF_\infty|F_\infty)$ the classes of all elements $b \in F_\infty^\times$ are mapped to the classes of the algebras (χ, b) . But each b comes from some F_{2m+1} , and hence the class of the algebra (χ, b) in $\text{Br}(KF_{2m+2}|F_{2m+2})$ is trivial by Châtelet's theorem. As $\text{Br}(KF_\infty|F_\infty)$ is the direct limit of the $\text{Br}(KF_j|F_j)$ by Lemma 4.3.3, this concludes the verification of the assumptions of Proposition 8.4.3, and therefore the proof of the theorem. \square

Remark 8.4.6 The technique of building towers of fields like the one in the proof above has turned out to be useful in other situations as well. Merkurjev [3] used such a technique for constructing fields of cohomological dimension 2 over which there exist division algebras of period 2 and index 2^d for d arbitrary large (this is to be compared with the discussion of

Remark 4.5.15). In the same paper, Merkurjev gave a counterexample to a conjecture of Kaplansky's in the theory of quadratic forms. Colliot-Thélène and Madore [1] (see also Colliot-Thélène [5]) constructed by means of the above technique a field k of cohomological dimension 1 and characteristic 0 over which there exist smooth projective varieties that are birational to projective space over \bar{k} but have no rational point (note that Severi-Brauer varieties always do, by Theorem 6.1.8).

The theorem has the following important application.

Theorem 8.4.7 *Let $m > 1$ be an integer invertible in k , and assume that k contains a primitive m -th root of unity ω . Then the m -torsion subgroup ${}_m K_2^M(k)$ consists of elements of the form $\{\omega, b\}$, with $b \in k^\times$.*

Proof: We begin with the crucial case when $m = p$ is a prime number. Let K be the Laurent series field $k((t))$, and consider the cyclic Galois extension $K'|K$ given by $K' = k((t'))$, where $t = t'^p$. Let σ be the generator of $\text{Gal}(K'|K)$ satisfying $\sigma(t') = \omega t'$, and let $\alpha = \Sigma\{a_i, b_i\}$ be an element of ${}_p K_2^M(k)$. We compute

$$N_{K'|K}(\alpha_{K'}) = N_{K'|K}\left(\sum\{a_i, b_i\}\right) = \sum\{N_{K'|K}(a_i), b_i\} = \sum\{a_i^p, b_i\} = p\alpha = 0$$

using the projection formula. Hilbert's Theorem 90 for K_2^M then implies that there exists $\beta \in K_2^M(K')$ such that $\alpha_{K'} = (\sigma - 1)\beta$. We denote by $\partial' : K_2^M(K') \rightarrow k^\times$ the tame symbol associated with the canonical valuation of K' and set $\gamma := \partial'(\beta)$. The element $\tilde{\beta} := \beta - \{t', \gamma\}$ then satisfies $\partial'(\tilde{\beta}) = 0$. Since $(\sigma - 1)\{t', \gamma\} = \{\sigma(t')t'^{-1}, \gamma\} = \{\omega, \gamma\}$, replacing β by $\tilde{\beta}$ and α by $\alpha - \{\omega, \gamma\}$ we may assume $\partial'(\beta) = 0$. By definition we have $\alpha = s_{t'}(\alpha_{K'}) = s_{t'}((\sigma - 1)\beta)$, where $s_{t'}$ is the specialisation map associated with t' . But $\partial'(\beta) = 0$ implies, by the first part of Proposition 7.1.7, that β is a sum of symbols of the form $\{u_i, v_i\}$ with some units u_i, v_i in $k[[t']]^\times$. As the extension $K'|K$ is totally ramified, u_i and $\sigma(u_i)$ have the same image modulo (t') , and similarly for the v_i . Thus $s_{t'}((\sigma - 1)\{u_i, v_i\}) = 0$, so that $\alpha = s_{t'}(\beta) = 0$, which concludes the proof in the case $m = p$.

Next assume that $m = p^r$ is a prime power with $r > 1$, and that the statement is already known for all $m = p^j$ with $0 < j < r$. Given $\alpha \in {}_{p^r} K_2^M(k)$, we have $p\alpha = \{\omega^p, b\} = p\{\omega, b\}$ for some $b \in k^\times$ by induction, as ω^p is a primitive p^{r-1} -st root of unity. Therefore $\alpha - \{\omega, b\} = \{\omega^{p^{r-1}}, c\}$ for some $c \in k^\times$ by the case $m = p$, which proves the theorem in this case. Finally, the general case follows by decomposing each m -torsion element in $K_2^M(k)$ into a sum of p_i -primary torsion elements for the prime divisors p_i of m . \square

Theorem 8.4.8 *Assume that $\text{char}(k) = p > 0$. Then ${}_p K_2^M(k) = 0$.*

Proof: We now exploit the Artin-Schreier extension K' of $K = k((t))$ given by $t'^p - t' = t^{-1}$, and denote by σ the generator of $\text{Gal}(K'|K)$ mapping t' to $t' + 1$. Let $\alpha \in {}_p K_2^M(k)$. By the same argument as in the previous proof, we find $\beta \in K_2^M(K')$ satisfying $\partial'(\beta) = 0$ and $\gamma \in k^\times$ such that

$$\alpha_{K'} = (\sigma - 1)(\beta + \{t', \gamma\}) = (\sigma - 1)\beta + \{t' + 1, \gamma\} - \{t', \gamma\}.$$

As above, we use the specialisation map $s_{t'}$ and note that $\partial'(\beta) = 0$ implies $s_{t'}((\sigma - 1)\beta) = 0$. Hence $\alpha = s_{t'}(\alpha_{K'}) = s_{t'}((\sigma - 1)\beta) + \{1, r\} - \{1, r\} = 0$, as was to be shown. \square

8.5 The Merkurjev-Suslin Theorem: A Special Case

In this section we prove the injectivity part of the Merkurjev-Suslin theorem for some special fields. Namely, fix a prime number p , and let k_0 be a finite extension of \mathbf{Q} , or else an algebraically closed field or a finite field of characteristic prime to p . The fields k we shall consider in this section will be extensions of k_0 of the following type: there exists a subfield $k_0 \subset k_p \subset k$ which is a finitely generated purely transcendental extension of k_0 , and moreover $k|k_p$ is a finite Galois extension whose degree is a power of p .

Theorem 8.5.1 *Let k be a field of the above type. Then the Galois symbol*

$$h_{k,p}^2 : K_2^M(k)/pK_2^M(k) \rightarrow H^2(k, \mu_p^{\otimes 2})$$

is injective.

The proof will be by induction on the transcendence degree, so the case of a base field has to be considered first. The case of a finite extension of \mathbf{Q} results from Theorem 7.6.1. For k algebraically closed, the statement is obvious, as $H^2(k, \mu_p^{\otimes 2})$ is then trivial and $K_2^M(k)$ divisible by p (since $k^{\times p} = k^\times$). For k finite, both $K_2^M(k)$ and $H^2(k, \mu_p^{\otimes 2})$ are trivial, the first one by Example 7.1.3, and the second because $\text{cd}(k) \leq 1$ in this case.

Thus we can turn to extensions of the base field. The core of the argument is the following proposition due to Merkurjev.

Proposition 8.5.2 *Let k be an arbitrary field containing a primitive p -th root of unity ω , and let $K = k(\sqrt[p]{a})$ be a cyclic extension of degree p . Assume that the Galois symbol $h_{k,p}^2 : K_2^M(k)/pK_2^M(k) \rightarrow H^2(k, \mu_p^{\otimes 2})$ is injective. Then the sequence*

$$K_2^M(k)/pK_2^M(k) \xrightarrow{i_{K|k} \oplus h_{k,p}^2} K_2^M(K)/pK_2^M(K) \oplus H^2(k, \mu_p^{\otimes 2}) \xrightarrow{h_{K,p}^2 - \text{Res}_k^K} H^2(K, \mu_p^{\otimes 2})$$

is exact.

For the proof we need some preliminary lemmas. The first is a well-known one from group theory.

Lemma 8.5.3 *Let G be a group and p a prime number. In the group algebra $\mathbf{F}_p[G]$ we have an equality*

$$(\sigma - 1)^{p-1} = \sigma^{p-1} + \cdots + \sigma + 1$$

for all $\sigma \in G$, where 1 is the unit element of G .

Proof: By Newton's binomial formula

$$(\sigma - 1)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} \sigma^i (-1)^{p-1-i},$$

where

$$\binom{p-1}{i} = \frac{(p-1) \cdots (p-i)}{1 \cdots i} \equiv (-1)^i \pmod{p},$$

and it remains to use the congruence $(-1)^{p-1} \equiv 1 \pmod{p}$. \square

Lemma 8.5.4 *For k and K as in the proposition, the natural map*

$$\ker(\iota_{K|k}) \rightarrow \ker(\text{Res}_k^K)$$

induced by the commutative diagram

$$\begin{array}{ccc} K_2^M(k)/pK_2^M(k) & \xrightarrow{h_{k,p}^2} & H^2(k, \mu_p^{\otimes 2}) \\ \downarrow \iota_{K|k} & & \downarrow \text{Res}_k^K \\ K_2^M(K)/pK_2^M(K) & \xrightarrow{h_{K,p}^2} & H^2(K, \mu_p^{\otimes 2}) \end{array}$$

is surjective.

Proof: Let c be a class in the kernel of Res_k^K . Since $\mu_p \subset k$, we may identify c with an element in the kernel $\text{Br}(K|k)$ of the map $\text{Br}(k) \rightarrow \text{Br}(K)$, and hence with the class of a cyclic algebra $(a, b)_\omega$ for appropriate $b \in k^\times$, by Corollaries 4.4.10 and 4.7.4. By Proposition 4.7.1 we therefore obtain $c = h_{k,p}^2(\{a, b\})$. But $\{a, b\}$ goes to 0 in $K_2^M(K)/pK_2^M(K)$ as a is a p -th power in K . The lemma follows. \square

Note that in the above proof we did not use the assumed injectivity of $h_{k,p}^2$. Under this hypothesis, the lemma (and its proof) yields:

Corollary 8.5.5 *Assume moreover that $h_{k,p}^2$ is injective. Then the natural map*

$$\ker(\iota_{K|k}) \rightarrow \ker(\text{Res}_k^K)$$

is an isomorphism, and each element of $\ker(\iota_{K|k})$ can be represented by a symbol of the form $\{a, b\}$ with some $b \in k^\times$.

Proof of Proposition 8.5.2: Take $\beta \in K_2^M(K)/pK_2^M(K)$ and $c \in H^2(k, \mu_p^{\otimes 2})$ such that the pair (β, c) lies in the kernel of $h_{K,p}^2 - \text{Res}_k^K$. It will be enough to find $\alpha \in K_2^M(k)/pK_2^M(k)$ for which $\iota_{K|k}(\alpha) = \beta$. Indeed, for such an α the commutative diagram of the previous lemma shows that $h_{k,p}^2(\alpha)$ differs from c by an element of $\ker(\text{Res}_k^K)$. But by the lemma we may modify α by an element of $\ker(\iota_{K|k})$ so that $h_{k,p}^2(\alpha) = c$ holds.

Next, denote by σ the generator of $G = \text{Gal}(K|k)$ mapping $\sqrt[p]{a}$ to $\omega \sqrt[p]{a}$. The idea of the proof is to construct inductively for each $i = 1, \dots, p-1$ elements $\alpha_i \in K_2^M(k)/pK_2^M(k)$ and $\beta_i \in K_2^M(K)/pK_2^M(K)$ satisfying

$$\beta = \iota_{K|k}(\alpha_i) + (\sigma - 1)^i(\beta_i). \quad (11)$$

This will prove the proposition, because for $i = p-1$ we may write using Lemma 8.5.3

$$(\sigma - 1)^{p-1}(\beta_{p-1}) = \sum_{j=0}^{p-1} \sigma^j(\beta_{p-1}) = i_{K|k}(N_{K|k}(\beta_{p-1}))$$

in $K_2^M(K)/pK_2^M(K)$, and hence $\alpha = \alpha_{p-1} + N_{K|k}(\beta_{p-1})$ will do the job.

We begin the construction of the elements α_i and β_i by the case $i = 1$. Using the compatibility of the Galois symbol with norm maps (Proposition 7.5.5), we may write

$$0 = pc = \text{Cor}_k^K(\text{Res}_k^K(c)) = \text{Cor}_k^K(h_{K,p}^2(\beta)) = h_{k,p}^2(N_{K|k}(\beta)).$$

By the assumed injectivity of $h_{k,p}^2$, we find $\alpha_1 \in K_2^M(k)$ with $N_{K|k}(\beta) = p\alpha_1$. Since $N_{K|k}(\alpha_{1,K}) = p\alpha_1$ by Remark 7.3.1 (here as always the subscript $_K$ means image by $i_{K|k}$), an application of Hilbert's Theorem 90 for K_2 shows that

$$\beta - \alpha_{1,K} = (\sigma - 1)\beta_1$$

for some $\beta_1 \in K_2^M(K)$, whence the case $i = 1$ of the required identity. In particular, in the case $p = 2$ this concludes the proof, so we assume $p > 2$ in the sequel.

Now assume that the elements α_j and β_j have been constructed for all $j \leq i$. Making the element $(\sigma - 1)^{p-1-i} \in \mathbf{Z}[G]$ act on both sides of the identity (11) we obtain

$$(\sigma - 1)^{p-1-i}(\beta) = (\sigma - 1)^{p-1-i}(\iota_{K|k}(\alpha_i)) + (\sigma - 1)^{p-1}(\beta_i) = (\sigma - 1)^{p-1}(\beta_i),$$

because σ acts trivially on $\alpha_{i,K}$.

Consider now the group $H^2(K, \mu_p^{\otimes 2})$ equipped with its natural G -action and apply $h_{K,p}^2$ to both sides. Using the compatibility of the Galois symbol with the action of G (an immediate consequence of Lemma 3.3.13 and Proposition 3.4.10 (4)), we get

$$(\sigma - 1)^{p-1-i} \text{Res}_k^K(c) = (\sigma - 1)^{p-1-i} h_{K,p}^2(\beta) = h_{K,p}^2((\sigma - 1)^{p-1}(\beta_i)).$$

Here the left hand side is 0, because the image of the map Res_k^K is fixed by G (this follows from the constructions of the conjugation action and the restriction map in Chapter 3), and $p - 1 - i \geq 1$. Using Lemma 8.5.3 we get from the above

$$0 = h_{K,p}^2(N_{K|k}(\beta_i)_K) = \text{Res}_k^K(h_{k,p}^2(N_{K|k}(\beta_i))).$$

Applying Corollary 8.5.5 we infer

$$h_{k,p}^2(N_{K|k}(\beta_i)) = h_{k,p}^2(\{a, b_i\})$$

for some $b_i \in k^\times$, and from the injectivity of $h_{k,p}^2$ we conclude that

$$N_{K|k}(\beta_i) - \{a, b_i\} = p\delta_i$$

for some $\delta_i \in K_2^M(k)$. Using the equality $N_{K|k}(\sqrt[p]{a}) = a$, we may rewrite this as

$$N_{K|k}(\beta_i - \{\sqrt[p]{a}, b_i\}) = p\delta_i$$

using the projection formula. Therefore, taking the identity $N_{K|k}(\delta_{i,K}) = p\delta_i$ into account, we get that $\beta_i - \{\sqrt[p]{a}, b_i\} - \delta_{i,K}$ is an element of trivial norm. Hence Hilbert's Theorem 90 for K_2^M implies

$$\beta_i - \{\sqrt[p]{a}, b_i\} - \delta_{i,K} = (\sigma - 1)\beta_{i+1}$$

for some $\beta_{i+1} \in K_2^M(K)$. Applying $(\sigma - 1)^i$ yields

$$(\sigma - 1)^i(\beta_i) = (\sigma - 1)^i(\{\sqrt[p]{a}, b_i\}) + (\sigma - 1)^{i+1}\beta_{i+1}.$$

Since $b_i \in k$, here for $i = 1$ we have $(\sigma - 1)(\{\sqrt[p]{a}, b_1\}) = \{\omega, b_1\}_K$ by definition of σ , and therefore $(\sigma - 1)^i(\{\sqrt[p]{a}, b_i\}) = 0$ for $i > 1$. All in all, putting $\alpha_2 := \alpha_1 + \{\omega, b_1\}$ and $\alpha_{i+1} := \alpha_i$ for $i > 1$ completes the inductive step. \square

Notice that the commutative diagram of Lemma 8.5.4 induces a natural map $\text{coker}(h_{k,p}^2) \rightarrow \text{coker}(h_{K,p}^2)$.

Corollary 8.5.6 *Under the assumptions of the previous proposition, the Galois symbol $h_{K,p}^2$ is injective, and so is the map $\text{coker}(h_{k,p}^2) \rightarrow \text{coker}(h_{K,p}^2)$ just defined.*

Proof: For the first statement, take a class $\beta \in \ker(h_{K,p}^2)$ and a class c in the kernel of the restriction map $H^2(k, \mu_p^{\otimes 2}) \rightarrow H^2(K, \mu_p^{\otimes 2})$. By the proposition above, there is a class $\alpha \in K_2^M(k)/pK_2^M(k)$ with $\iota_{K|k}(\alpha) = \beta$ and $h_{k,p}^2(\alpha) = c$. Moreover, such an α is unique by injectivity of $h_{k,p}^2$. On the other hand, by Lemma 8.5.4 our c comes from an element in the kernel of $\iota_{K|k}$, so the above unicity yields $\alpha \in \ker(\iota_{K|k})$ and $\beta = 0$, as desired. The second statement is an immediate consequence of the proposition. \square

We can now proceed to:

Proof of Theorem 8.5.1: To begin with, a restriction-corestriction argument as in the proof of Proposition 7.5.9 shows that for a finite extension $L|K$ of fields which has degree prime to p the natural maps $\ker(h_{K,p}^2) \rightarrow \ker(h_{L,p}^2)$ and $\text{coker}(h_{K,p}^2) \rightarrow \text{coker}(h_{L,p}^2)$ are injective. By virtue of this fact we may enlarge k_0 so that it contains a primitive p -th root of unity.

We then proceed by induction on the transcendence degree. As noted after the statement of the theorem, the statement holds for k_0 . Next choose a tower of field extensions $k_0 \subset k_p \subset k$ as at the beginning of this section. As the Galois symbol $h_{F,p}^1$ is bijective for all fields by virtue of Kummer theory (Theorem 4.3.6), an iterated application of Proposition 7.5.6 (1) shows that the injectivity of $h_{k_0,p}^2$ implies that of $h_{k_p,p}^2$. Finally, we write the Galois extension $k|k_p$ as a tower of Galois extensions of degree p , and obtain injectivity of $h_{k,p}^2$ by an iterated application of the first statement in Corollary 8.5.6. \square

To conclude this section, we note that the above arguments also yield the following interesting consequence.

Proposition 8.5.7 *Assume that k is a field having the property that the Galois symbol $h_{L,p}^2$ is injective for all finite extensions $L|k$. Then $h_{k,p}^2$ is surjective.*

Proof: As in the previous proof, we may assume that k contains a primitive p -th root of unity. Take an element $c \in H^2(k, \mu_p^{\otimes 2})$. There exists a finite Galois extension $L|k$ such that c restricts to 0 in $H^2(L, \mu_p^{\otimes 2})$. Let P be a p -Sylow subgroup of $\text{Gal}(L|k)$ and L^P its fixed field. The extension $L^P|k$ has prime to p degree, so the remark at the beginning of the previous proof shows that the natural map $\text{coker}(h_{k,p}^2) \rightarrow \text{coker}(h_{L^P,p}^2)$ is injective. We may then replace k by L^P , and assume that the degree $[L : k]$ is a power of p . Thus, just

like in the previous proof, an iterated application of the second statement of Corollary 8.5.6 shows that the restriction map $\text{coker}(h_{k,p}^2) \rightarrow \text{coker}(h_{L,p}^2)$ is injective, which implies that $c \in \text{Im}(h_{k,p}^2)$. \square

Thus in order to complete the proof of the Merkurjev-Suslin theorem, it remains to establish the injectivity of the Galois symbol for arbitrary fields. This is the content of the next section.

8.6 The Merkurjev-Suslin Theorem: The General Case

Following Merkurjev, we shall now use the results of the previous section to prove the following crucial fact. The general case of the Merkurjev-Suslin theorem will then be an easy consequence.

Theorem 8.6.1 *Let k be a field containing a primitive p -th root of unity ω , and let $K = k(\sqrt[p]{a})$ be a Galois extension of degree p . The kernel of the natural map*

$$K_2^M(k)/pK_2^M(k) \rightarrow K_2^M(K)/pK_2^M(K)$$

consists of images of symbols of the form $\{a, b\}$ with some $b \in k^\times$.

Note that this result was established in Corollary 8.5.5 under the assumption that $h_{k,p}^2$ is injective. Thus it can be also viewed as a consequence of the injectivity part of the Merkurjev-Suslin theorem. In particular, it holds for fields of the type considered in Theorem 8.5.1.

The idea of the proof is to reduce the statement to the case of the particular fields considered in Theorem 8.5.1 via a specialisation argument. Recall that in Chapter 7 we constructed for a field K equipped with a discrete valuation v with residue field κ specialisation maps $s_t^M : K_n^M(K) \rightarrow K_n^M(\kappa)$ for all $n \geq 0$, depending on the choice of a local parameter t for v . We shall use these maps here for $n = 1$ or 2 , employing the more precise notations s_t^1 and s_t^2 , respectively. Note that they satisfy the formula $s_t^2\{x, y\} = \{s_t^1(x), s_t^1(y)\}$ for all $x, y \in k$. The strategy of the proof is then summarized by the following proposition, which immediately implies Theorem 8.6.1.

Proposition 8.6.2 *Under the assumptions of the theorem, let*

$$\alpha = \{a_1, b_1\} + \cdots + \{a_n, b_n\} \in K_2^M(k)$$

be a symbol satisfying $\iota_{K|k}(\alpha) \in pK_2^M(K)$. Then there exist a subfield $k_0 \subset k$ containing the elements $\omega, a, a_1, \dots, a_n, b_2, \dots, b_n$, an integer $d > 0$ and an iterated Laurent series field $k_d := k_0((t_1)) \cdots ((t_d))$, so that for suitable $B \in k_d^\times$ the element

$$b := (s_{t_1}^1 \circ s_{t_2}^1 \circ \cdots \circ s_{t_d}^1)(B) \in k_0 \subset k$$

satisfies $\{a, b\} = \alpha$ modulo $pK_2^M(k)$, where

$$s_{t_i} : k_0((t_1)) \dots ((t_i)) \rightarrow k_0((t_1)) \dots ((t_{i-1}))$$

is the specialisation map associated with t_i .

To ensure the existence of a suitable $B \in k_d$, the idea is to find elements $A_i, B_i \in k_d$ specialising to a_i and b_i , respectively, so that moreover the elements $A_1, \dots, A_n, B_1, \dots, B_n, a$ and ω all lie in a subfield of k_d which is of the type considered in Theorem 8.5.1, and the symbol $\sum\{A_i, B_i\}$ becomes divisible by p after we adjoin the p -th root $\sqrt[p]{a}$. Once this is done, Theorem 8.5.1 and Corollary 8.5.5 will guarantee the existence of the required B .

This argument prompts the necessity of finding a general criterion for elements $a_1, \dots, a_n, b_1, \dots, b_n$ in a field F which forces the p -divisibility of the symbol $\sum\{a_i, b_i\}$ in $K_2^M(F)$. The next proposition, due to Merkurjev, gives such a criterion.

First some notation: given an integer $N > 0$, denote by \mathcal{A}_N the set of nonzero functions $\alpha : \{1, 2, \dots, N\} \rightarrow \{0, 1, \dots, p-1\}$. For a field F containing a primitive p -th root of unity and elements $a_1, \dots, a_N \in F^\times$ set

$$a_\alpha := \prod_{i=1}^N a_i^{\alpha(i)} \quad \text{and} \quad F_\alpha := F(\sqrt[p]{a_\alpha}),$$

and denote by N_α the norm map $N_{F_\alpha|F} : F_\alpha^\times \rightarrow F^\times$.

Proposition 8.6.3 *Let F be a field containing a primitive p -th root of unity, and let a_1, \dots, a_n be elements in F^\times whose images are linearly independent in the \mathbf{F}_p -vector space $F^\times/F^{\times p}$. Then for all $b_1, \dots, b_n \in F^\times$ the symbol*

$$\sum_{i=1}^n \{a_i, b_i\} \in K_2^M(F)$$

lies in $pK_2^M(F)$ if and only if there exist an integer $N \geq n$ and elements $a_{n+1}, \dots, a_N, c_1, \dots, c_N \in F^\times$ and $w_\alpha \in F_\alpha^\times$ for each $\alpha \in \mathcal{A}_N$ satisfying

$$c_i^p b_i = \prod_{\alpha \in \mathcal{A}_N} N_\alpha(w_\alpha)^{\alpha(i)} \quad (12)$$

for all $1 \leq i \leq N$, where we set $b_i = 1$ for $n < i \leq N$.

Note that although formula (12) does not involve the a_i , the w_α depend on them. For the proof we need:

Lemma 8.6.4 *Let \mathcal{N} be the subgroup of $F^\times \otimes_{\mathbf{Z}} F^\times$ generated by those elements $a \otimes b$ for which b is a norm from the extension $F(\sqrt[p]{a})|F$. The natural map $F^\times \otimes_{\mathbf{Z}} F^\times \rightarrow K_2^M(F)$ induces an isomorphism*

$$(F^\times \otimes_{\mathbf{Z}} F^\times / \mathcal{N}) \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} K_2^M(F)/pK_2^M(F).$$

Proof: Denote by F_a the extension $F(\sqrt[p]{a})$. If $a \otimes b \in \mathcal{N}$, then by definition $b = N_{F_a|F}(b')$ for some $b' \in F_a$, so that in $K_2^M(F)$ we may write using the projection formula

$$\{a, b\} = \{a, N_{F_a|F}(b')\} = N_{F_a|F}(\{a, b'\}) = N_{F_a|F}(\{\sqrt[p]{a}^p, b'\}) = pN_{F_a|F}(\{\sqrt[p]{a}, b'\}).$$

This shows that the natural surjection $F^\times \otimes_{\mathbf{Z}} F^\times \rightarrow K_2^M(F)/pK_2^M(F)$ factors through $(F^\times \otimes_{\mathbf{Z}} F^\times / \mathcal{N}) \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}$. Finally, if some $a \otimes b$ maps to 0 in $K_2^M(k)/pK_2^M(k)$, then it is congruent modulo p to a sum of elements of the form $c \otimes (1 - c)$. But the equality $N_{F_c|F}(1 - \sqrt[p]{c}) = 1 - c$ (obtained as in the proof of Proposition 8.4.3) shows that these elements lie in \mathcal{N} , and the proof is complete. \square

Proof of Proposition 8.6.3: We first prove sufficiency, which does not require the independence assumption on the a_i . Equation (12) yields an equality $b_i = \prod_{\alpha \in \mathcal{A}_N} N_\alpha(w_\alpha)^{\alpha(i)}$ in $F^\times/F^{\times p}$, so that using $b_i = 1$ for $i > n$ we get

$$\sum_{i=1}^n \{a_i, b_i\} = \sum_{i=1}^n \{a_i, b_i\} = \sum_{i=1}^n \sum_{\alpha \in \mathcal{A}_N} \{a_i, N_\alpha(w_\alpha)^{\alpha(i)}\} \quad \text{in } K_2^M(F)/pK_2^M(F).$$

But here

$$\sum_{i=1}^n \{a_i, N_\alpha(w_\alpha)^{\alpha(i)}\} = \{a_\alpha, N_\alpha(w_\alpha)\}$$

by bilinearity of symbols, and $\{a_\alpha, N_\alpha(w_\alpha)\} \in pK_2^M(F)$ by Lemma 8.6.4.

For the converse, assume that $\sum \{a_i, b_i\}$ lies in $pK_2^M(F)$. By Lemma 8.6.4, we may then find elements $e_1, \dots, e_r \in F^\times$ and $w_j \in F(\sqrt[p]{e_j})$ for $i \leq j \leq r$ so that we have an equality

$$\sum_{i=1}^n a_i \otimes b_i = \sum_{j=1}^r e_j \otimes N_{F(\sqrt[p]{e_j})|F}(w_j) \quad \text{in } F^\times \otimes_{\mathbf{Z}} F^\times \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}.$$

We may assume the e_i map to distinct elements in $F^\times/F^{\times p}$. Let V be the \mathbf{F}_p -subspace of $F^\times/F^{\times p}$ generated by the images of $a_1, \dots, a_n, e_1, \dots, e_r$, and choose elements $a_{n+1}, \dots, a_N \in F^\times$ so that a_1, \dots, a_N modulo $F^{\times p}$ yield a basis of V . For each j we may then find $\alpha_j \in \mathcal{A}_N$ so that the images of a_{α_j} and e_j in V are the same. For each $\alpha \in \mathcal{A}_N$ write $w_\alpha := w_j$ if $\alpha = \alpha_j$ for one of the α_j 's just defined, and $w_\alpha := 1$ otherwise. In $F^\times \otimes_{\mathbf{Z}} F^\times \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}$ we may then write

$$\sum_{i=1}^n a_i \otimes b_i = \sum_{i=1}^r e_j \otimes N_{F(\sqrt[p]{e_j})|F}(w_j) = \sum_{\alpha \in \mathcal{A}_N} a_\alpha \otimes N_\alpha(w_\alpha) = \sum_{\alpha \in \mathcal{A}_N} \left(\prod_{i=1}^n a_i^{\alpha(i)} \right) \otimes N_\alpha(w_\alpha).$$

Introducing $b_i = 1$ for $i > n$ and using bilinearity, we rewrite the above as

$$\sum_{i=1}^N a_i \otimes b_i = \sum_{i=1}^N a_i \otimes \left(\prod_{\alpha \in \mathcal{A}_N} N_\alpha(w_\alpha)^{\alpha(i)} \right) \quad \text{in } F^\times \otimes_{\mathbf{Z}} F^\times \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}.$$

As the images of the $a_i \bmod F^{\times p}$ are linearly independent, this is only possible if $b_i = \prod_{\alpha \in \mathcal{A}_N} N_\alpha(w_\alpha)^{\alpha(i)} \bmod F^{\times p}$, whence the existence of the required c_i . \square

We now turn to the proof of Proposition 8.6.2. Our proof is a variant of that of Klingen [1], itself a simplification of Merkurjev’s original argument.

Proof of Proposition 8.6.2: Consider the element $\alpha = \sum \{a_i, b_i\}$ of the proposition. Without loss of generality we may assume that the images of a, a_1, \dots, a_n are linearly independent in $k^\times/k^{\times p}$, and therefore the images of a_1, \dots, a_n are linearly independent in $K^\times/K^{\times p}$. We may then apply Proposition 8.6.3, of which we keep the notations. We find elements $a_{n+1}, \dots, a_N, c_1, \dots, c_N \in K^\times$ as well as $w_\alpha \in K_\alpha^\times$ satisfying (12). Introduce the notations $u := \sqrt[p]{a}$ and $u_\alpha := \sqrt[p]{a_\alpha}$ for all $\alpha \in \mathcal{A}_N$. The w^j for $0 \leq j \leq p-1$ form a k -basis of K , and the $u^i u_\alpha^j$ for $0 \leq i, j \leq p-1$ form a k -basis of K_α for each α . Thus we find elements $a_{ij} \in k$ for $0 \leq j \leq p-1$ and $n+1 \leq i \leq N$, as well as $w_{ij\alpha} \in k$ with $0 \leq i, j \leq p-1$ and $\alpha \in \mathcal{A}_N$ satisfying

$$a_i = \sum_{j=0}^{p-1} a_{ij} u^j \quad \left(\text{resp. } w_\alpha = \sum_{i,j=0}^{p-1} w_{ij\alpha} u^i u_\alpha^j \right)$$

for all $n+1 \leq i \leq N$ (resp. $\alpha \in \mathcal{A}_N$).

Now let f_0 be the subfield of k generated over the prime field by a and the p -th root of unity ω . Introduce independent variables

$$A_i, B_i \quad (1 \leq i \leq n), \quad A_{ij} \quad (n+1 \leq i \leq N, 0 \leq j \leq p-1)$$

and

$$W_{ij\alpha} \quad (0 \leq i, j \leq p-1, \alpha \in \mathcal{A}_N),$$

and take the purely transcendental extension

$$F_0 := f_0(A_i, B_i, A_{ij}, W_{ij\alpha}).$$

We first construct a field extension $L_0|F_0$ containing an element B for which $\sum \{A_i, B_i\} = \{a, B\}$ holds modulo an element in $pK_2^M(L_0)$. To do so, for each $1 \leq i \leq n$ introduce elements $D_i \in F_0(u)$ via the formula

$$D_i := B_i^{-1} \prod_{\alpha \in \mathcal{A}_N} N_\alpha(W_\alpha),$$

where the W_α and the norm maps N_α are defined by setting

$$A_\alpha := \prod_{i=1}^n A_i^{\alpha(i)}, \quad U_\alpha := \sqrt[p]{A_\alpha}, \quad W_\alpha := \sum_{i,j=0}^{p-1} W_{ij\alpha} u^i U_\alpha^j \quad \text{and} \quad N_\alpha := N_{F_0(u, U_\alpha)|F_0(u)},$$

with the conventions $A_i := \sum A_{ij} u^j$ and $B_i := 1$ for $i > n$. Denoting by σ the generator of the Galois group $\text{Gal}(F_0(u)|F_0) \cong \mathbf{Z}/p\mathbf{Z}$ sending u to ωu , pick elements $C_{i,l}$ in some fixed algebraic closure of $F_0(u)$ satisfying $C_{i,l}^p = \sigma^l(D_i)$ for $1 \leq i \leq n$ and $0 \leq l \leq p-1$.

Let L be the finite extension of $F_0(u)$ obtained by adjunction of all the $C_{i,l}$. Observe that the choice of the $C_{i,l}$ among the roots of the polynomials $x^p - \sigma^l(C_i)$ defines an extension of σ to an automorphism in $\text{Gal}(L|F_0)$; we call it again σ , and denote by $L_0 := L^\sigma \subset L$ its fixed field. Note that $L = L_0(u)$. The construction together with Proposition 8.6.3 show that the symbol $\sum\{A_i, B_i\}$ lies in $K_2^M(L_0) \cap pK_2^M(L)$. On the other hand, the field L_0 is a p -power degree Galois extension of the purely transcendental field F_0 , hence by Theorem 8.5.1 the Galois symbol $h_{L_0, p}^2$ is injective. An application of Corollary 8.5.5 then allows one to find $B \in L_0$ with $\sum\{A_i, B_i\} = \{a, B\}$ modulo $pK_2^M(L_0)$.

To complete the proof, we embed L_0 into a field $k_d = k_0((t_1)) \dots ((t_d))$ so that k_0 is a subfield of k containing the elements a_i, b_i , which are moreover exactly the images of the A_i and B_i in k_0 . Define an f_0 -algebra homomorphism $f_0[A_i, B_i, A_{ij}, W_{ij\alpha}] \rightarrow k$ by sending $A_i \mapsto a_i, B_i \mapsto b_i, A_{ij} \mapsto a_{ij}, W_{ij\alpha} \mapsto w_{ij\alpha}$. Its kernel is a prime ideal P in the polynomial ring $f_0[A_i, B_i, A_{ij}, W_{ij\alpha}]$; denote by \mathcal{O}_P the associated localisation. The local ring \mathcal{O}_P is regular (being the local ring of a scheme-theoretic point on affine space), hence by the Cohen structure theorem (see Appendix, Theorem A.5.4 (2)) its completion $\widehat{\mathcal{O}}_P$ is isomorphic to a formal power series ring of the form $\kappa_0[[v_1, \dots, v_d]]$, where $\kappa_0 \subset k$ is the residue field of \mathcal{O}_P . Its fraction field naturally embeds into the iterated Laurent series field $\kappa_d := \kappa_0((v_1)) \dots ((v_d))$. In particular, we have a natural embedding $F_0 \hookrightarrow \kappa_d$, since F_0 is the fraction field of \mathcal{O}_P .

Write K_d for the composite $L\kappa_d$, where $L|F_0$ is the extension constructed above. The automorphism $\sigma \in \text{Gal}(L|F_0)$ induces an element in $\text{Gal}(K_d|\kappa_d)$ which we again denote by σ . Let $k_d := K_d^\sigma$ be its fixed field; note that $L_0 \subset k_d$ and $K_d = k_d(u)$. Extending the discrete valuation defined by v_d to the finite extension $k_d|\kappa_d$ we again get a Laurent series field of the form $k_{d-1}((t_d))$, where k_{d-1} is a finite extension of $\kappa_0((v_1)) \dots ((v_{d-1}))$. This in turn becomes equipped with the unique extension of the valuation defined by v_{d-1} , and so is a Laurent series field $k_{d-2}((t_{d-1}))$ for suitable t_{d-1} . Continuing this process, we may finally write $k_d = k_0((t_1)) \dots ((t_d))$ with some finite extension $k_0|\kappa_0$.

It remains to show that the field k_0 may be embedded into k . For this observe first that the elements $d_i := b_i^{-1} \prod_{\alpha \in \mathcal{A}_N} N_\alpha(w_\alpha)$ of K considered at the beginning of the proof all lie in $\kappa_0(u)$ by construction, and they are precisely the images of the elements D_i in $\kappa_0(u)$ (which are units for all valuations concerned). The elements $\sigma^l(D_i)$ map to $\bar{\sigma}^l(d_i)$ in $\kappa_0(u)$, where $\bar{\sigma}$ is the generator of $\text{Gal}(\kappa_0(u)|\kappa_0)$ sending u to ωu . Extending $\bar{\sigma}$ to the automorphism in $\text{Gal}(K|k)$ with the same property, we see that denoting by $\bar{C}_{i,l}$ the image of $C_{i,l}$ in the residue field $k_0(u)$ of K_d the map $\bar{C}_{i,l} \mapsto \bar{\sigma}^l(c_i)$ induces an embedding $k_0(u) \hookrightarrow K$ compatible with the action of $\bar{\sigma}$. We conclude by taking invariants under $\bar{\sigma}$. \square

We finally arrived at the great moment when we can prove in full generality:

Theorem 8.6.5 (Merkurjev-Suslin) *Let k be a field, and $m > 0$ an integer invertible in k . Then the Galois symbol*

$$h_{k,m}^2 : K_2^M(k)/mK_2^M(k) \rightarrow H^2(k, \mu_m^{\otimes 2})$$

is an isomorphism.

Proof: By virtue of Proposition 7.5.9 it is enough to treat the case when $m = p$ is a prime number, and in view of Proposition 8.5.7 it suffices to prove injectivity. As in the proof of that proposition, we may assume that k contains a primitive p -th root of unity. Take a symbol $\alpha = \{a_1, b_1\} + \cdots + \{a_n, b_n\}$ in $K_2^M(k)$ whose mod p image lies in the kernel of $h_{k,p}^2$. We have to prove $\alpha \in pK_2^M(k)$. We proceed by induction on n , the case $n = 1$ being Lemma 7.6.3. If $a_n \in k^{\times p}$, we are done by the case of symbols of length $n - 1$. Otherwise, set $K = k(\sqrt[p]{a_n})$. Then $i_{K|k}(\alpha) = i_{K|k}(\{a_1, b_1\} + \cdots + \{a_{n-1}, b_{n-1}\})$ in $K_2^M(K)/pK_2^M(K)$, and it lies in the kernel of $h_{K,p}^2$ by compatibility of the Galois symbol with restriction maps. Hence by induction we may assume $i_{K|k}(\alpha) \in pK_2^M(K)$. But then by Theorem 8.6.1 the image of α in $K_2^M(k)/pK_2^M(k)$ equals that of a symbol of the form $\{a_n, b\}$ for some $b \in k^\times$. We conclude by the case $n = 1$. \square

Remark 8.6.6 The above proof of the theorem relies on Theorem 8.5.1, and hence in characteristic 0 on Tate's result for number fields, which has a nontrivial input from class field theory. Note however that this arithmetic input is not necessary in positive characteristic, or for fields containing an algebraically closed subfield. The original proof of injectivity in Merkurjev-Suslin [1] did not use a specialisation argument, but a deep fact from the K -theory of central simple algebras which amounts to generalising the isomorphism $A_d(\mathbf{P}^d, K_{2-d}^M) \cong K_2^M(k)$ of Example 8.2.7 to arbitrary Severi-Brauer

varieties of squarefree degree. They however used a specialisation technique for proving surjectivity of the Galois symbol, which could later be eliminated by the method of Proposition 8.5.2. All in all, there exists a proof of the theorem which uses no arithmetic at all, at the price of hard inputs from K-theory.

EXERCISES

1. (Colliot-Thélène, Raskind) Let X be a smooth variety of dimension d over a field k , and let $K|k$ be a finite Galois extension with group G . Denote by X_K the base change of X to K , and by $Z(X)$ the kernel of the map

$$\bigoplus_{P \in X^1} \kappa(P)^\times \rightarrow \bigoplus_{P \in X^2} \mathbf{Z}$$

- (a) Show that the natural map $Z(X) \rightarrow Z(X_K)^G$ is an isomorphism.
 (b) Establish an exact sequence

$$\begin{aligned} A_{d-1}(X, K_2^M) &\rightarrow A_{d-1}(X_K, K_2^M)^G \xrightarrow{\delta} H^1(G, K_2^M(K(X))/A_d(X_K, K_2^M)) \\ &\rightarrow \ker(CH^2(X) \rightarrow CH^2(X_K)) \rightarrow H^1(G, A_{d-1}(X_K, K_2^M)). \end{aligned}$$

2. Let Γ be the Galois group $\text{Gal}(\mathbf{C}|\mathbf{R})$.
- (a) Show that ${}_2K_2^M(\mathbf{R})$ is a cyclic group of order 2 generated by $\{-1, -1\}$.
 (b) Show that $K_2^M(\mathbf{R})/N_{\mathbf{C}|\mathbf{R}}(K_2^M(\mathbf{C}))$ is also the cyclic group of order 2 generated by $\{-1, -1\}$.
 (c) Let X be the projective conic of equation $x_0^2 + x_1^2 + x_2^2 = 0$ in $\mathbf{P}_{\mathbf{R}}^2$. Show that $H^1(\Gamma, K_2^M(\mathbf{C}(X))/K_2^M(\mathbf{C})) \cong \mathbf{Z}/2\mathbf{Z}$. [*Hint*: Use the previous exercise.]
 (d) Conclude that $H^1(\Gamma, K_2^M(\mathbf{C}(X))) \cong \mathbf{Z}/2\mathbf{Z}$, and try to find an explicit generator.
3. Assume that k is a field having no nontrivial finite extension of degree prime to p , and that $K_2^M(k)/pK_2^M(k) = 0$. Let $K|k$ be a cyclic extension of degree p .
- (a) Show that the norm map $N_{K|k} : K^\times \rightarrow k^\times$ is surjective.
 (b) Conclude that $K_2^M(K)/pK_2^M(K) = 0$. [*Hint*: Use Proposition 8.4.3 and Lemma 8.5.3.]

- (c) Show that $\text{cd}(k) \leq 1$.
4. Let p be a prime number invertible in k , and let $K|k$ be a cyclic Galois extension of degree p^r for some $r \geq 1$. Denote by σ a generator of $\text{Gal}(K|k)$. Define a tower of fields

$$k = F_0 \subset F_1 \subset F_2 \subset F_3 \subset \cdots \subset F_\infty = \bigcup_n F_n$$

inductively as follows:

- the field F_{2n+1} is a maximal prime to p extension of F_{2n} ;
- the field F_{2n+2} is the compositum of all function fields of Severi-Brauer varieties associated with cyclic algebras of the form (a, b) , where $a, b \in F_{2n+1}^\times$.

- (a) Show that F_∞ has no nontrivial prime to p extension and that

$$K_2^M(F_\infty)/pK_2^M(F_\infty) = 0.$$

- (b) Show that the sequence

$$K_2^M(KF_\infty) \xrightarrow{\sigma-1} K_2^M(KF_\infty) \xrightarrow{N_{KF_\infty|F_\infty}} K_2^M(F_\infty)$$

is exact.

[*Hint:* Argue as in the proof of Proposition 8.4.3 using step (b) of the previous exercise.]

5. (Hilbert's Theorem 90 for K_2 in the general case) Let m be an integer invertible in k , and let $K|k$ be a cyclic Galois extension of degree m . Denote by σ a generator of $\text{Gal}(K|k)$. Show that the sequence

$$K_2^M(K) \xrightarrow{\sigma-1} K_2^M(K) \xrightarrow{N_{K|k}} K_2^M(k)$$

is exact. [*Hint:* First use a restriction-corestriction argument as in the proof of Proposition 8.4.4 to reduce to the case when $m = p^r$ is a prime power. Then mimic the proof of Theorem 8.4.1 using the previous exercise.]

6. Let k be a field of characteristic $\neq 2$, $K = k(\sqrt{a})$ a quadratic extension, and $G = \text{Gal}(K|k)$ its Galois group.

- (a) Construct an exact sequence of $\text{Gal}(k)$ -modules

$$0 \rightarrow \mathbf{Z}/2\mathbf{Z} \rightarrow M^G(\mathbf{Z}/2\mathbf{Z}) \xrightarrow{\Sigma} \mathbf{Z}/2\mathbf{Z} \rightarrow 0.$$

(b) Show that the associated long exact sequence takes the form

$$\cdots \rightarrow H^i(k, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{\text{Res}} H^i(K, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{\text{Cor}} H^i(k, \mathbf{Z}/2\mathbf{Z}) \rightarrow \cdots$$

(c) Show that the boundary maps $H^i(k, \mathbf{Z}/2\mathbf{Z}) \rightarrow H^{i+1}(k, \mathbf{Z}/2\mathbf{Z})$ in the above sequence are given by cup-product with the class of a in the group $H^1(k, \mathbf{Z}/2\mathbf{Z})$.

(d) Establish an exact sequence

$$K_2^M(K) \xrightarrow{N_{K|k}} K_2^M(k) \xrightarrow{\phi} H^3(k, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{\text{Res}} H^3(K, \mathbf{Z}/2\mathbf{Z}),$$

where $\phi(\beta) = h_{2,k}^3(\{a, \beta\})$.

[*Remark:* The exercise gives a presentation of the kernel of the restriction map $H^3(k, \mathbf{Z}/2\mathbf{Z}) \rightarrow H^3(K, \mathbf{Z}/2\mathbf{Z})$. For a more general statement involving $\mu_m^{\otimes 2}$ -coefficients, see Merkurjev-Suslin [1], Corollary 15.3.]

Chapter 9

Symbols in Positive Characteristic

In the preceding chapters, when working with Galois cohomology groups or K -groups modulo some prime, a standing assumption was that the groups under study were torsion groups prime to the characteristic of the base field. We now remove this restriction. In the first part of the chapter the central result is Teichmüller's theorem, according to which the p -primary torsion subgroup in the Brauer group of a field of characteristic $p > 0$ is generated by classes of cyclic algebras – a characteristic p ancestor of the Merkurjev-Suslin theorem. We shall give two proofs of this statement: a more classical one due to Hochschild which uses central simple algebras, and a totally different one based on a presentation of the p -torsion in $\text{Br}(k)$ via logarithmic differential forms. The key tool here is a famous theorem of Jacobson-Cartier characterising logarithmic forms. The latter approach leads us to the second main topic of the chapter, namely the study of the differential symbol. This is a p -analogue of the Galois symbol which relates the Milnor K -groups modulo p to a certain group defined using differential forms. As a conclusion to the book, we shall prove the Bloch-Gabber-Kato theorem establishing its bijectivity.

Teichmüller's result first appeared in the ill-famed journal *Deutsche Mathematik* (Teichmüller [1]); see also Jacobson [3] for an account of the original proof. The role of derivations and differentials in the theory of central simple algebras was noticed well before the Second World War; today the most important work seems to be that of Jacobson [1]. This line of thought was further pursued in papers by Hochschild [1], [2], and, above all, in the thesis of Cartier [1], which opened the way to a wide range of geometric developments. The original references for the differential symbol are the papers of Kato [2] and Bloch-Kato [1]; they have applied the theory to questions concerning higher-dimensional local fields and p -adic Hodge theory.

9.1 The Theorems of Teichmüller and Albert

In the sequel k will denote a field of characteristic $p > 0$, and k_s will be a fixed separable closure of k . According to the Merkurjev-Suslin theorem, the m -torsion subgroup of $\text{Br}(k)$ is generated by classes of cyclic algebras for all m prime to p , provided that k contains the m -th roots of unity. For m a power of p , the statement is still valid (without, of course, the assumption on roots of unity); it was proven by Teichmüller as early as 1936. But around the same time Albert obtained an even stronger result: each class of p -power order in the Brauer group can actually be represented by a cyclic algebra. In this section we prove these classical theorems.

First recall some facts that will be used several times in the sequel. For all integers $r > 0$, classes in $H^1(k, \mathbf{Z}/p^r\mathbf{Z})$ correspond to characters $\tilde{\chi}$ of the absolute Galois group $\text{Gal}(k_s|k)$ of order dividing p^r . We shall always denote by χ the character induced by $\tilde{\chi}$ on the finite quotient of $\text{Gal}(k_s|k)$ defined by the kernel of $\tilde{\chi}$. We have a natural pairing

$$j_r : H^1(k, \mathbf{Z}/p^r\mathbf{Z}) \times H^0(k, k_s^\times) \rightarrow {}_{p^r}\text{Br}(k)$$

sending a pair $(\tilde{\chi}, b)$ to $\delta(\tilde{\chi}) \cup b$, where $\delta : H^1(k, \mathbf{Z}/p^r\mathbf{Z}) \rightarrow H^2(k, \mathbf{Z})$ is the coboundary map coming from the exact sequence $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Z} \rightarrow \mathbf{Z}/p^r\mathbf{Z} \rightarrow 0$. According to Proposition 4.7.3, the element $j_r(\tilde{\chi}, b)$ equals the class of the cyclic algebra (χ, b) in $\text{Br}(k)$. As a consequence, bilinearity of the cup-product implies that

$$[(\chi, pb)] = [(p\chi, b)] \quad \text{in } \text{Br}(k). \quad (1)$$

Also, recall from Chapter 2 that in the important case when χ defines a degree p Galois extension of k , the algebra (χ, b) has a presentation of the form

$$(\chi, b) = [a, b] = \langle x, y | x^p - x = a, y^p = b, y^{-1}xy = x + 1 \rangle, \quad (2)$$

for some $a \in k$, and conversely a k -algebra with such a presentation is cyclic.

Another frequently used fact will be the following. Given positive integers $r, s > 0$, consider the short exact sequence

$$0 \rightarrow \mathbf{Z}/p^r\mathbf{Z} \rightarrow \mathbf{Z}/p^{r+s}\mathbf{Z} \xrightarrow{p^r} \mathbf{Z}/p^s\mathbf{Z} \rightarrow 0.$$

Since $\text{cd}_p(k) \leq 1$ (Proposition 6.1.9), the associated long exact sequence ends like this:

$$H^1(k, \mathbf{Z}/p^r\mathbf{Z}) \rightarrow H^1(k, \mathbf{Z}/p^{r+s}\mathbf{Z}) \xrightarrow{p^r} H^1(k, \mathbf{Z}/p^s\mathbf{Z}) \rightarrow 0. \quad (3)$$

Armed with these facts, we now begin the proof of Teichmüller's theorem using a method of Hochschild. The key statement is the following.

Theorem 9.1.1 (Hochschild) *Let $K = k(\sqrt[p^{r_1}]{b_1}, \dots, \sqrt[p^{r_n}]{b_n})$ be a purely inseparable extension. For each class $\alpha \in \text{Br}(K|k)$ we may find characters $\tilde{\chi}_i \in H^1(k, \mathbf{Z}/p^{r_i}\mathbf{Z})$ so that*

$$\alpha = \sum_{i=1}^n [(\chi_i, b_i)] \quad \text{in } \text{Br}(k),$$

where χ_i is the injective character induced by $\tilde{\chi}_i$ on a finite quotient of $\text{Gal}(k_s|k)$.

We start the proof by extending Proposition 4.5.6 to the case of purely inseparable extensions.

Lemma 9.1.2 *Let $K|k$ be a purely inseparable field extension of degree $n = p^r$. Then the boundary map $\delta_n : H^1(k, \text{PGL}_n(k_s)) \rightarrow \text{Br}(k)$ induces a bijection*

$$\ker(H^1(k, \text{PGL}_n(k_s)) \rightarrow H^1(K, \text{PGL}_n(Kk_s))) \cong \text{Br}(K|k).$$

Moreover, if $A|k$ is a central simple algebra of degree n split by K , then K embeds as a commutative k -subalgebra into A .

Proof: We have already shown in the proof of Theorem 4.4.5 the injectivity of δ_n (even of δ_∞), so it suffices to see surjectivity. Denoting by G the Galois group $\text{Gal}(k_s|k)$, consider the short exact sequence of G -modules

$$1 \rightarrow k_s^\times \rightarrow (Kk_s)^\times \rightarrow (Kk_s)^\times/k_s^\times \rightarrow 1,$$

where G naturally identifies to $\text{Gal}(Kk_s|K)$, because the composite Kk_s is a separable closure of K . As $H^1(G, Kk_s^\times) = 0$ by Hilbert's Theorem 90, we get isomorphisms

$$H^1(G, (Kk_s)^\times/k_s^\times) \cong \ker(H^2(G, k_s^\times) \rightarrow H^2(G, (Kk_s)^\times)) \cong \text{Br}(K|k).$$

On the other hand, the choice of a k -basis of K provides an embedding $K \hookrightarrow M_n(k)$, whence a G -equivariant map $\rho : Kk_s \cong K \otimes_k k_s \rightarrow M_n(k_s)$, and finally a map $\bar{\rho} : (Kk_s)^\times/k_s^\times \rightarrow \text{PGL}_n(k_s)$. Arguing as in the proof of Theorem 4.4.5, we obtain a commutative diagram:

$$\begin{array}{ccc} H^1(G, (Kk_s)^\times/k_s^\times) & \xrightarrow{\phi} & H^2(G, k_s^\times) \\ \downarrow & & \downarrow \text{id} \\ H^1(G, \text{PGL}_n(k_s)) & \xrightarrow{\delta_n} & H^2(G, k_s^\times). \end{array}$$

Since $\text{Im}(\phi) = \text{Br}(K|k)$ by the above, the diagram tells us that each element α in $\text{Br}(K|k) \subset H^2(G, k_s^\times)$ comes from some element β in $H^1(G, \text{PGL}_n(k_s))$. But α restricts to 0 in $H^2(G, (Kk_s)^\times)$, so the commutative diagram

$$\begin{array}{ccc} H^1(G, \text{PGL}_n(k_s)) & \xrightarrow{\delta_{n,k}} & H^2(G, k_s^\times) \\ \downarrow & & \downarrow \\ H^1(G, \text{PGL}_n(Kk_s)) & \xrightarrow{\delta_{n,K}} & H^2(G, (Kk_s)^\times). \end{array}$$

and the injectivity of $\delta_{n,K}$ imply that β maps to 1 in $H^1(G, \text{PGL}_n(Kk_s))$, as required.

For the last statement, assume that the class $\alpha \in \text{Br}(K|k)$ considered above is the class of a degree n algebra A . Since β comes from an element of $H^1(G, (Kk_s)^\times/k_s^\times)$, we get that A is isomorphic to the twisted form of M_n by a 1-cocycle z with values in the subgroup $\bar{\rho}((Kk_s)^\times/k_s^\times)$ of $\text{PGL}_n(k_s)$ (see Chapter 2, Section 2.3). Therefore the twisted algebra $A \cong ({}_z M_n)^G$ contains $({}_z \rho(Kk_s))^G$. But $({}_z \rho(Kk_s))^G = (\rho(Kk_s))^G \cong K$, because the conjugation action of $(Kk_s)^\times$ on Kk_s is trivial, and ρ is G -equivariant. \square

We shall also need the following easy lemma.

Lemma 9.1.3 *Let k be a field of characteristic $p > 0$, and let A be a not necessarily commutative k -algebra. For $y \in A$ consider the k -vector space endomorphism $D_y : A \rightarrow A$ defined by $v \mapsto vy - yv$, and let $D_y^{[p]}$ be its p -th iterate. Then $D_y^{[p]} = D_{y^p}$.*

Proof: Consider the maps $L_y : v \mapsto yv$ and $R_y : v \mapsto vy$, and write $D_y = R_y - L_y$. As L_y and R_y commute in the endomorphism ring of the k -vector space A , the binomial formula implies $D_y^{[p]} = (R_y - L_y)^{[p]} = R_y^{[p]} + (-1)^p L_y^{[p]} = D_{y^p}$, as p divides the binomial coefficients $\binom{p}{i}$ for all $0 < i < p$. \square

Proof of Theorem 9.1.1: We start with the case of degree p , i.e. $K = k(\sqrt[p]{b})$. Let α be a nonzero class in $\text{Br}(K|k)$. Lemma 9.1.2 shows that there exists a central simple k -algebra A of degree p containing K with $[A] = \alpha$; it is a division algebra as $\alpha \neq 0$. As $K \subset A$, we find $y \in A$ with $y^p = b$. Consider the k -endomorphism $D_y : A \rightarrow A$ of the lemma above. As b is in the center of A , we get $D_y^{[p]} = D_{y^p} = D_b = 0$ using the lemma. Since A is noncommutative, we find $w \in A$ with $z := D_y(w) \neq 0$ but $D_y(z) = 0$, i.e. $yz = zy$. Setting $x = z^{-1}yw$ we obtain $xy - yx = z^{-1}y(yw - yw) = z^{-1}yz = y$, and hence $y^{-1}xy = x + 1$. As A is a division algebra, the k -subalgebra

$k(x)$ generated by x is a commutative subfield nontrivially containing k , so $[k(x) : k] = p$ by dimension reasons. Moreover, the formula $y^{-1}xy = x + 1$ implies that conjugation by y equips the extension $k(x)|k$ with a nontrivial k -automorphism of order p , so $k(x)|k$ is a cyclic Galois extension of degree p , and $x^p - x = x(x + 1) \dots (x + p - 1)$ lies in k . Setting $a := x^p - x$ we see that A contains a cyclic subalgebra (χ, b) with presentation (2), and this inclusion must be an isomorphism for dimension reasons. This settles the degree p case.

To treat the general case, we use induction on the degree $[K : k]$. Denote by $E \subset K$ the subfield $k(\sqrt[p^{r_1}]{b_1}, \dots, \sqrt[p^{r_{n-1}}]{b_{n-1}})$. Then K is a degree p purely inseparable extension of E generated by $\sqrt[p]{u_n}$, where $u_n := \sqrt[p^{r_n-1}]{b_n}$. Given $\alpha \in \text{Br}(K|k)$, we have $\text{Res}_k^E(\alpha) \in \text{Br}(K|E)$, so by the degree p case we find $\tilde{\chi} \in H^1(k, \mathbf{Z}/p\mathbf{Z}) \cong H^1(E, \mathbf{Z}/p\mathbf{Z})$ with $\text{Res}_k^E(\alpha) = [(\chi, u_n)]$. By exact sequence (3) we find a character $\tilde{\chi}_n \in H^1(k, \mathbf{Z}/p^{r_n}\mathbf{Z})$ with $p^{r_n-1}\tilde{\chi}_n = \tilde{\chi}$. In $\text{Br}(E)$ we have

$$[\chi, u_n] = \text{Res}_k^E(\delta(\tilde{\chi})) \cup u_n = (p^{r_n-1} \text{Res}_k^E(\delta(\tilde{\chi}_n))) \cup u_n = \text{Res}_k^E(\delta(\tilde{\chi}_n)) \cup b_n = [\chi_n, b_n]$$

by bilinearity of the cup-product. Hence $\beta := \alpha - (\delta(\tilde{\chi}_n) \cup b_n) = \alpha - [(\chi_n, b_n)]$ lies in $\text{Br}(E|k)$. By induction we may write β as a sum of classes of the form $[(\chi_i, b_i)]$, and the proof is complete. \square

We now come to

Theorem 9.1.4 (Teichmüller) *The map*

$$j_r : H^1(k, \mathbf{Z}/p^r\mathbf{Z}) \otimes k^\times \longrightarrow {}_{p^r}\text{Br}(k)$$

is surjective for all $r > 0$. In other words, every central simple k -algebra of p -power degree is Brauer equivalent to a tensor product of cyclic algebras.

Remark 9.1.5 Teichmüller’s result holds only up to Brauer equivalence, but not up to isomorphism. Indeed, McKinnie [1] gave examples of central simple k -algebras of period p not isomorphic to a tensor product of cyclic algebras of degree p . This is a characteristic p analogue of the counterexample of Amitsur-Rowen-Tignol cited at the end of Chapter 1. Non-cyclic division algebras of p -power degree were known before (see Amitsur-Saltman [1]).

Before starting the proof of Theorem 9.1.4, recall from field theory that a purely inseparable extension $K|k$ is said to be *of height 1* if $K^p \subset k$, or equivalently if K can be generated by p -th roots of elements of k . We shall need the following easy facts.

Facts 9.1.6 The *maximal* height 1 purely inseparable extension \tilde{k} of k is obtained by adjoining all p -th roots of elements of k . The composite $\tilde{k}k_s$ is none but the separable closure \tilde{k}_s of \tilde{k} . It is also the maximal height 1 purely inseparable extension of k_s : indeed, if $\alpha^p = a$ for some $a \in k_s$, then $f(\alpha^p) = 0$ for a separable polynomial $f \in k[x]$, but then extracting p -th roots from the coefficients of f we get a separable polynomial $g \in \tilde{k}[x]$ with $g(\alpha)^p = g(\alpha) = 0$, so that $\alpha \in \tilde{k}_s$.

Lemma 9.1.7 *Every central simple k -algebra of period p is split by a finite extension $K|k$ of height 1.*

Proof: Consider the maximal height 1 purely inseparable extension \tilde{k} of k described above. It will be enough to show that every central simple k -algebra of period p is split by \tilde{k} , for then it is also split by some finite subextension. As $\tilde{k}_s|k_s$ is the maximal purely inseparable extension of height 1, raising elements to the p -th power induces an isomorphism $\tilde{k}_s^\times \xrightarrow{\sim} k_s^\times$. On the other hand, the composite $k_s^\times \rightarrow \tilde{k}_s^\times \xrightarrow{p} k_s^\times$ is just the multiplication by p map on k_s^\times . Taking Galois cohomology over k (noting that \tilde{k}_s is a $\text{Gal}(k_s|k)$ -module via the isomorphism $\text{Gal}(k_s|k) \cong \text{Gal}(\tilde{k}_s|\tilde{k})$), it follows that the multiplication by p map on $H^2(k, k_s^\times)$ coincides with the composite $H^2(k, k_s^\times) \rightarrow H^2(k, \tilde{k}_s^\times) \xrightarrow{p} H^2(k, k_s^\times)$. As the last map here is an isomorphism by the above, it follows that all p -torsion elements in $\text{Br}(k) \cong H^2(k, k_s^\times)$ must map to 0 in $H^2(k, \tilde{k}_s^\times) \cong H^2(\tilde{k}, \tilde{k}_s^\times) \cong \text{Br}(\tilde{k})$, as was to be shown. \square

Proof of Theorem 9.1.4: We prove surjectivity of j_r by induction on r . The case $r = 1$ follows from Lemma 9.1.7 and Theorem 9.1.1. Now assume that the statement is known for all integers $1 \leq i \leq r$, and consider the commutative diagram

$$\begin{array}{ccccc}
 H^1(k, \mathbf{Z}/p^r\mathbf{Z}) \otimes k^\times & \xrightarrow{\text{id} \otimes \text{id}} & H^1(k, \mathbf{Z}/p^{r+1}\mathbf{Z}) \otimes k^\times & \xrightarrow{p^r \otimes \text{id}} & H^1(k, \mathbf{Z}/p\mathbf{Z}) \otimes k^\times \rightarrow 0 \\
 \downarrow j_r & & \downarrow j_{r+1} & & \downarrow j_1 \\
 {}_p{}^r\text{Br}(k) & \xrightarrow{\text{id}} & {}_p{}^{r+1}\text{Br}(k) & \xrightarrow{p^r} & {}_p\text{Br}(k)
 \end{array}$$

whose exact upper row comes from (3). In view of the diagram, the surjectivity of j_{r+1} follows from that of j_1 and j_r , which we know from the inductive assumption. \square

We now come to the most powerful result of this section.

Theorem 9.1.8 (Albert) *Every central simple k -algebra of p -power degree is Brauer equivalent to a cyclic algebra.*

The proof is based on the following proposition which is interesting in its own right.

Proposition 9.1.9 *Let A_1, A_2 be two cyclic k -algebras of degrees p^{r_1} and p^{r_2} , respectively. Then there exists an integer $r \leq r_1 + r_2$ and an element $b \in k^\times$ so that the extension $k(\sqrt[r]{b})$ splits both A_1 and A_2 .*

Combined with Theorem 9.1.1, the proposition immediately yields:

Corollary 9.1.10 *For A_1 and A_2 as in the proposition, the tensor product $A_1 \otimes_k A_2$ is Brauer equivalent to a cyclic algebra of the form (χ, b) for some character χ of order dividing p^r .*

Once we have Corollary 9.1.10, we can easily *prove Albert's theorem* by exploiting what we already know. Indeed, by induction we get that tensor products of cyclic algebras of p -power degree are Brauer equivalent to a cyclic algebra, and so Albert's theorem follows from that of Teichmüller.

For the proof of Proposition 9.1.9 we need the following lemma from field theory.

Lemma 9.1.11 *Let $K = k(\sqrt[r]{b})|k$ be a purely inseparable extension of degree p^r , and let $L|k$ be a finite separable extension. Then there exists an element $v \in LK$ whose norm $N_{LK|K}(v)$ generates the extension $K|k$.*

Proof: We may assume $[K : k] > 1$. Setting $u = \sqrt[r]{b}$ we have $[K : k(u^p)] = p$, so it will be enough to find $v \in LK$ with $N_{LK|K}(v) \notin k(u^p)$. Using the theorem of the primitive element, we write $L = k(w)$ for appropriate $w \in L$. Let $f = t^m + \alpha_1 t^{m-1} + \cdots + \alpha_m$ be the minimal polynomial of w over k . Grouping exponents into residue classes mod p , we write

$$f = \sum_{i=0}^{p-1} f_i(t^p)t^i.$$

Since f is a separable polynomial, we find $j \neq 0$ such that $f_j \neq 0$. Then $f_j((ut)^p) \in K[t]$ is a nonzero polynomial and since k is an infinite field (otherwise it would have no nontrivial inseparable extension), there exists $\alpha \in k^\times$ such that $f_j((\alpha u)^p) \neq 0$. Now put $v := w - \alpha u$. The minimal

polynomial of v over K is $f(t + \alpha u) = t^m + \cdots + f(\alpha u)$, so $N_{LK|K}(v) = (-1)^m f(\alpha u)$ and

$$f(\alpha u) = \sum_{i=0}^{p-1} f_i((\alpha u)^p) \alpha^i u^i.$$

This is an expression for $f(\alpha u)$ as a linear combination of the basis elements $1, u, \dots, u^{p-1}$ of the $k(u^p)$ -vector space K . Since the coefficient $f_j((\alpha u)^p) \alpha^j$ is nonzero, we have $f(\alpha u) \notin k(u^p)$ and hence $N_{LK|K}(v) \notin k(u^p)$, as desired. \square

Proof of Proposition 9.1.9: For $i = 1, 2$ write $A_i = (\chi_i, b_i)$ with characters χ_i of order p^{r_i} and elements $b_i \in k^\times$. If $b_i = c_i^p$ for some $c_i \in k^\times$, then formula (1) shows that A_i is Brauer equivalent to the cyclic algebra $(p\chi_i, c_i)$. So up to replacing A_i by a Brauer equivalent algebra we may assume that $[k(\sqrt[p^{r_i}]{b_i}) : k] = p^{r_i}$ for $i = 1, 2$. Denote by k_2 the cyclic extension of k defined by the kernel of $\tilde{\chi}_2$. Lemma 9.1.11 provides $v \in k_2(\sqrt[p^{r_1}]{b_1})$ such that $z := N_{k_2(\sqrt[p^{r_1}]{b_1})|k(\sqrt[p^{r_1}]{b_1})}(v)$ generates the extension $k(\sqrt[p^{r_1}]{b_1})|k$. Consider now the purely inseparable extension $E = k(\sqrt[p^{r_1}]{b_1})(\sqrt[p^{r_2}]{zb_2})$ of k . Since z generates $k(\sqrt[p^{r_1}]{b_1})$ over k , the element $y := \sqrt[p^{r_2}]{zb_2}$ generates E over k , and thus we have $[E : k] = p^{r_1+r_2}$. As b_1 is a p^{r_1} -th power in E , the algebra $(\chi_1, b_1) \otimes_k E$ is split. To see that E also splits (χ_2, b_2) , we write

$$(\chi_2, b_2) \otimes_k E \cong (\chi_2, y^{p^{r_2}} z^{-1}) \otimes_k E \cong (\chi_2, y^{p^{r_2}}) \otimes_{k(\sqrt[p^{r_1}]{b_1})} (\chi_2, z^{-1}) \otimes_k E.$$

Since χ_2 has order dividing p^{r_2} , the algebra $(\chi_2, y^{p^{r_2}}) \otimes_k E$ splits. On the other hand, the algebra (χ_2, z^{-1}) splits over $k(\sqrt[p^{r_1}]{b_1})$ according to Corollary 4.7.5, because z is a norm from the extension $k_2(\sqrt[p^{r_1}]{b_1})|k(\sqrt[p^{r_1}]{b_1})$, and therefore it also splits over E . Hence $(\chi_2, b_2) \otimes_k E$ splits, as desired. \square

9.2 Differential Forms and p -torsion in the Brauer Group

We now discuss another method for describing the p -torsion part of the Brauer group of k . The basic idea is the following. For m prime to p , a fundamental tool for studying ${}_m\text{Br}(k)$ was furnished by the exact sequence coming from multiplication by m on k_s^\times , which is surjective with kernel μ_m . In contrast to this, for $m = p$ the multiplication by p map is injective, and it has a nontrivial cokernel which can be described using differential forms, via the dlog map.

To define this map, consider for an arbitrary extension $K|k$ the module $\Omega_K^1 = \Omega_{K/\mathbf{Z}}^1$ of absolute differentials over K . The map $\text{dlog} : K^\times \rightarrow \Omega_K^1$ is then defined by sending $y \in K^\times$ to the logarithmic differential form dy/y .

This is a homomorphism of abelian groups whose kernel is $K^{\times p}$; denote by $\nu(1)_K$ its image. For $K = k_s$ we therefore have an exact sequence

$$0 \rightarrow k_s^\times \xrightarrow{p} k_s^\times \xrightarrow{\text{dlog}} \nu(1)_{k_s} \rightarrow 0. \tag{4}$$

This is in fact an exact sequence of $\text{Gal}(k_s|k)$ -modules, so taking the associated long exact sequence yields an isomorphism

$$H^1(k, \nu(1)) \xrightarrow{\sim} {}_p\text{Br}(k). \tag{5}$$

To proceed further, we would like to have a more explicit presentation of $H^1(k, \nu(1))$. Assume we had a surjective map on $\Omega_{k_s}^1$ whose *kernel* is precisely the image $\nu(1)_{k_s}$ of the dlog map. Then we would have another short exact sequence of the form

$$0 \rightarrow \nu(1)_{k_s} \rightarrow \Omega_{k_s}^1 \rightarrow \Omega_{k_s}^1 \rightarrow 0,$$

and by the associated long exact sequence $H^1(k, \nu(1))$ would arise as a quotient of $(\Omega_{k_s}^1)^G$ which in fact equals Ω_k^1 , as one sees from Proposition A.8.7 of the Appendix. Thus all in all we would get a presentation of ${}_p\text{Br}(k)$ by differential forms.

The required map comes from the theory of the (inverse) Cartier operator. To define it, recall first a construction from linear algebra in characteristic $p > 0$. Given a K -vector space V , we may equip the underlying abelian group of V with another K -vector space structure pV in which $a \in K$ acts via $a \cdot w := a^p w$. A K -linear map $V \rightarrow {}^pW$ is sometimes called a *p-linear* map from V to W . Recall also (from the Appendix) that the subgroup $B_K^1 \subset \Omega_K^1$ is defined as the image of the universal derivation $d : K \rightarrow \Omega_K^1$. Though d is only a k -linear map, the induced map $d : {}^pK \rightarrow {}^p\Omega_K^1$ is already K -linear, in view of the formula $a^p db = d(a^p b)$, where the right hand side is d applied to the product of $b \in {}^pK$ with a . Thus ${}^pZ_K^1$ and ${}^pB_K^1$ are K -subspaces of ${}^p\Omega_K^1$.

Lemma 9.2.1 *There exists a unique morphism of K -vector spaces*

$$\gamma : \Omega_K^1 \rightarrow {}^p\Omega_K^1 / {}^pB_K^1$$

satisfying $\gamma(da) = a^{p-1} da \text{ mod } B_K^1$ for all $a \in K$. Moreover, we have $d \circ \gamma = 0$, where $d : \Omega_K^1 \rightarrow \Omega_K^2$ is the differential of the de Rham complex.

Proof: Recall from the Appendix that the K -vector space Ω_K^1 has a presentation by symbols of the form da for $a \in K$ subject to the relations $d(a + b) = da + db$ and $d(ab) = adb + bda$. Define γ on the elements da by

the formula above and extend by linearity. To see that γ is well-defined, we have to show that it annihilates all elements of the form $d(a+b) - da - db$ or $d(ab) - adb - dba$. For elements of the second type, we compute

$$\gamma(adb + bda) = a^p b^{p-1} db + b^p a^{p-1} da = (ab)^{p-1} (adb + bda) = \gamma(d(ab)).$$

For elements of the first type, we have to see that $(a+b)^{p-1}(da+db) - a^{p-1}da - b^{p-1}db$ belongs to B_K^1 . Notice first that the relation

$$d((x+y)^p) = p(x+y)^{p-1}d(x+y) = p(x^{p-1}dx + y^{p-1}dy) + \sum_{i=1}^{p-1} \binom{p}{i} d(x^i y^{p-i})$$

holds in the space of absolute differentials of the polynomial ring $\mathbf{Z}[x, y]$, which is the free $\mathbf{Z}[x, y]$ -module generated by dx and dy according to Appendix, Example A.8.2. Since all binomial coefficients in the sum are divisible by p , after dividing by p it follows that

$$(x+y)^{p-1}(dx+dy) - x^{p-1}dx - y^{p-1}dy \in B_{\mathbf{Z}[x,y]}^1.$$

We obtain the required identity in Ω_K^1 by specialisation via the homomorphism $\mathbf{Z}[x, y] \rightarrow K$ defined by $x \mapsto a, y \mapsto b$. The last statement follows from the equality $da \wedge da = 0$. \square

For historical reasons, the resulting map is called the *inverse Cartier operator*. We now have the following theorem due to Jacobson and Cartier.

Theorem 9.2.2 *For every field K of characteristic $p > 0$ the sequence of maps*

$$1 \rightarrow K^\times \xrightarrow{p} K^\times \xrightarrow{\text{dlog}} \Omega_K^1 \xrightarrow{\gamma^{-1}} {}^p\Omega_K^1 / {}^pB_K^1$$

is exact.

We postpone the proof of the theorem to the next section, and now consider its application to our problem of presenting elements in $H^1(k, \nu(1))$ by differential forms. The solution is based on the following corollary.

Lemma 9.2.3 *Let k be a field of characteristic $p > 0$ with separable closure k_s . The sequence*

$$1 \rightarrow \nu(1)_{k_s} \longrightarrow \Omega_{k_s}^1 \xrightarrow{\gamma^{-1}} \Omega_{k_s}^1 / B_{k_s}^1 \rightarrow 0$$

is an exact sequence of $\text{Gal}(k_s|k)$ -modules.

The superscripts p disappeared from the last term because we are not interested here in its k_s -vector space structure.

Proof: That the maps $d\log$ and $\gamma - 1$ are Galois equivariant follows from their construction. So in view of Theorem 9.2.2, it remains to prove surjectivity of $\gamma - 1$. Recall first that the Artin-Schreier map $\wp : k_s \rightarrow k_s$ defined by $x \mapsto x^p - x$ is surjective. Hence given a 1-form $adb \in \Omega_{k_s}^1$, we may find $x \in k_s$ with $x^p - x = ab$. Then

$$(\gamma - 1)(xb^{-1}db) = x^p b^{-p} b^{p-1} db - xb^{-1}db = (x^p - x)b^{-1}db = adb$$

according to the defining properties of the operator γ , whence the required surjectivity. \square

We can now prove the following theorem which seems to have been first noticed by Kato.

Theorem 9.2.4 *There exists a canonical isomorphism*

$$\Omega_k^1 / (B_k^1 + (\gamma - 1)\Omega_k^1) \xrightarrow{\sim} {}_p\text{Br}(k).$$

Proof: Denote by G the Galois group $\text{Gal}(k_s|k)$. The exact sequence of Lemma 9.2.3 gives rise to the long exact sequence

$$(\Omega_{k_s}^1)^G \xrightarrow{\gamma-1} (\Omega_{k_s}^1 / B_{k_s}^1)^G \rightarrow H^1(k, \nu(1)) \rightarrow H^1(k, \Omega_{k_s}^1).$$

The G -module $\Omega_{k_s}^1$ is a k_s -vector space, so $H^1(k, \Omega_{k_s}^1) = 0$ by the additive form of Hilbert's Theorem 90 (Lemma 4.3.11). On the other hand, Proposition A.8.7 of the Appendix implies $(\Omega_{k_s}^1)^G = \Omega_k^1$, and hence also $(B_{k_s}^1)^G = B_k^1$, since the differential of the de Rham complex is G -equivariant by construction. It follows that we get an isomorphism

$$\Omega_k^1 / (B_k^1 + (\gamma - 1)\Omega_k^1) \xrightarrow{\sim} H^1(k, \nu(1)),$$

whose composition with the isomorphism (5) yields the isomorphism of the theorem. \square

One can make the isomorphism of the above theorem quite explicit.

Proposition 9.2.5 *The isomorphism of Theorem 9.2.4 sends the class of a 1-form $adb \in \Omega_k^1$ to the class of the cyclic algebra $[ab, b]$ in ${}_p\text{Br}(k)$.*

Proof: As in the proof of Lemma 9.2.3 we find $x \in k_s$ with $x^p - x = ab$ and a 1-form $xb^{-1}db$ satisfying $(\gamma - 1)(xb^{-1}db) = adb$. The image of adb by the coboundary map $(\Omega_{k_s}^1 / B_{k_s}^1)^G \rightarrow H^1(k, \nu(1))$ is represented by the 1-cocycle $c_\sigma : \sigma \mapsto \sigma(xb^{-1}db) - xb^{-1}db = (\sigma(x) - x)d\log(b)$. The character

$\tilde{\chi} : \sigma \mapsto \sigma(x) - x \in \mathbf{Z}/p\mathbf{Z}$ is precisely the one defining the extension of k given by the Artin-Schreier polynomial $x^p - x - ab$, and the cocycle c_σ represents the image of the pair $(\tilde{\chi}, b)$ by the cup-product

$$H^1(k, \mathbf{Z}/p\mathbf{Z}) \times H^0(k, k_s^\times) \rightarrow H^1(k, k_s^\times \otimes \mathbf{Z}/p\mathbf{Z})$$

followed by the isomorphism

$$H^1(k, k_s^\times \otimes \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\sim} H^1(k, \nu(1)) \quad (6)$$

coming from exact sequence (4). Writing δ for the coboundary $H^1(k, \mathbf{Z}/p\mathbf{Z}) \rightarrow H^2(k, \mathbf{Z})$ and δ' for the coboundary $H^1(k, k_s^\times \otimes \mathbf{Z}/p\mathbf{Z}) \rightarrow H^2(k, k_s^\times)$ (which identifies to a coboundary coming from (4) via the isomorphism (6)), we have $\delta'(\tilde{\chi} \cup b) = \delta(\tilde{\chi}) \cup b$ by Proposition 3.4.8. But the latter class in $\text{Br}(k)$ is represented by the cyclic algebra $[ab, b]$, as recalled at the beginning of the previous chapter. \square

Remarks 9.2.6

1. The 1-forms adb generate Ω_k^1 as an abelian group, so one may try to define a map $\Omega_k^1 \rightarrow {}_p\text{Br}(k)$ by sending a finite sum $\sum a_i db_i$ to $\sum [a_i b_i, b_i]$. An easy computation shows that this map annihilates all elements of the form $d(a+b) - da - db$ and $d(ab) - adb - bda$, so it indeed induces a well-defined map $\Omega_k^1 \rightarrow {}_p\text{Br}(k)$. This gives an elementary construction of the map inducing the isomorphism of Theorem 9.2.4.
2. Theorem 9.2.4 and Proposition 9.2.5 together give another proof of Teichmüller's theorem in the case $r = 1$. But we have seen in the previous section that the general case follows from this by an easy induction argument. So we obtain a proof of Teichmüller's theorem which does not use the theory of central simple algebras – but relies, of course, on the nontrivial theorem of Jacobson and Cartier.

9.3 Logarithmic Differentials and Flat p -Connections

In this section we prove Theorem 9.2.2. Following Katz, our main tool in the argument will be the study, for a differential form $\omega \in \Omega_K^1$, of the map $\nabla_\omega : K \rightarrow \Omega_K^1$ defined by

$$\nabla_\omega(a) = da + a\omega. \quad (7)$$

It follows from this definition that the 1-form ω is logarithmic if and only if $\nabla_\omega(a) = 0$ for some $a \in K^\times$; indeed, the latter condition is equivalent to $\omega = -a^{-1}da = d\log(a^{-1})$.

The map ∇_ω is a basic example for a connection on K . For later purposes, we introduce this notion in a more general context. We shall work in the following setup: K will be a field of characteristic $p > 0$, and k a subfield of K containing K^p . The extension $K|k$ is then a purely inseparable extension of height 1. The most important case will be when $k = K^p$, for then we have $\Omega_{K|k}^1 = \Omega_K^1$.

Now define a *connection* on a finite dimensional K -vector space V to be a homomorphism $\nabla : V \rightarrow \Omega_{K|k}^1 \otimes_K V$ of abelian groups satisfying

$$\nabla(av) = a\nabla(v) + da \otimes v$$

for all $a \in K$ and $v \in V$.

A connection ∇ gives rise to a K -linear map $\nabla_* : \text{Der}_k(K) \rightarrow \text{End}_k(V)$ sending a derivation D to the map $\nabla_*(D)$ obtained as the composite

$$\nabla_*(D) : V \xrightarrow{\nabla} \Omega_{K|k}^1 \otimes_K V \xrightarrow{D \otimes id} K \otimes_K V \cong V,$$

where D is regarded as a K -linear map $\Omega_{K|k}^1 \rightarrow K$ via the isomorphism $\text{Der}_k(K) \cong \text{Hom}_k(\Omega_{K|k}^1, K)$. Note that though ∇_* is K -linear, the element $\nabla_*(D)$ is only a k -endomorphism in general (by the defining property of connections), but not a K -endomorphism. A straightforward computation yields the formula

$$\nabla_*(D)(av) = D(a)v + a\nabla_*(D)(v) \tag{8}$$

for all $v \in V$ and $a \in K$.

Example 9.3.1 Given $\omega \in \Omega_{K|k}^1$, the map $\nabla_\omega : K \rightarrow \Omega_{K|k}^1$ defined by (7) is a connection on the 1-dimensional K -vector space K . To see this, we compute

$$\nabla_\omega(ab) = adb + bda + ab\omega = a(db + b\omega) + bda = a\nabla_\omega(b) + da \otimes b,$$

as required. The map $\nabla_{\omega*} : \text{Der}_k(K) \rightarrow \text{End}_k(K)$ sends D to the map $a \mapsto D(a) + aD(\omega)$.

Now recall the following facts from the Appendix. The K -vector space $\text{End}_k(V)$ carries a Lie algebra structure over k , with Lie bracket defined by $[\phi, \psi] = \phi \circ \psi - \psi \circ \phi$. This Lie bracket and the p -operation sending an

endomorphism ϕ to its p -th iterate $\phi^{[p]}$ equip $\text{End}_k(V)$ with the structure of a p -Lie algebra over k (see the Appendix for the precise definition). The K -vector space $\text{Der}_k(K)$ is a k -subspace of $\text{End}_k(K)$ preserved by the Lie bracket and the p -operation of $\text{End}_k(K)$, therefore it is a p -Lie subalgebra. It is then a natural condition for a connection to require that the map ∇_* respects the p -Lie algebra structures on $\text{Der}_k(K)$ and $\text{End}_k(V)$. Accordingly, we say that the connection ∇ is *flat* or *integrable* if ∇_* is a homomorphism of Lie algebras over k , i.e. if $\nabla_*([D_1, D_2]) = [\nabla_*(D_1), \nabla_*(D_2)]$ for all $D_1, D_2 \in \text{Der}_k(K)$, and that ∇ is a p -connection if $\nabla_*(D^{[p]}) = (\nabla_*(D))^{[p]}$ for all $D \in \text{Der}_k(K)$.

Remark 9.3.2 One may introduce important invariants which measure the defect for a connection ∇ from being flat or a p -connection. The first of these is its *curvature* $K_*(\nabla)$, defined as the map $\text{Der}_k(K) \times \text{Der}_k(K) \rightarrow \text{End}_k(V)$ sending the pair (D_1, D_2) to $[\nabla_*(D_1), \nabla_*(D_2)] - \nabla_*([D_1, D_2])$. One may check that $K_*(\nabla)(D_1, D_2)$ equals the composite

$$V \xrightarrow{\nabla} \Omega_{K|k}^1 \otimes_K V \xrightarrow{\nabla_1} \Omega_{K|k}^2 \otimes_K V \xrightarrow{(D_1 \wedge D_2) \otimes id} K \otimes_K V \cong V,$$

where $\nabla_1(\omega \otimes v) := d\omega \otimes v - \omega \wedge \nabla(v)$. Therefore $K_*(\nabla)$ is the map induced on derivations by $\nabla_1 \circ \nabla : V \rightarrow \Omega_{K|k}^2 \otimes_K V$; one often defines the curvature as being the latter map. The second invariant is the p -curvature $\psi_*(\nabla)$, defined as the map $\text{Der}_k(K) \rightarrow \text{End}_k(V)$ sending D to $\nabla_*(D^{[p]}) - (\nabla_*(D))^{[p]}$. We shall not investigate any case where one of these invariants is nonzero.

It turns out that when the differential form ω is logarithmic, the connection ∇_ω on K is a flat p -connection. We shall prove this as part of the following theorem, which is the main result of this section.

Theorem 9.3.3 *Given an extension $K|k$ of fields of characteristic $p > 0$ with $K^p \subset k$, the following are equivalent for a differential form $\omega \in \Omega_{K|k}^1$:*

1. *The 1-form ω is logarithmic, i.e. $\omega = d\log(a)$ for some $a \in K^\times$.*
2. *We have $\gamma(\omega) = \omega \bmod B_{K|k}^1$.*
3. *The connection ∇_ω is a flat p -connection.*

In order to give a sense to statement (2), we have to extend the definition of the inverse Cartier operator to relative differentials for the extension $K|k$. To do so, apply Corollary A.8.10 of the Appendix with $k_0 = K^p$ to obtain a split exact sequence of K -vector spaces

$$0 \rightarrow K \otimes_k \Omega_k^1 \rightarrow \Omega_K^1 \rightarrow \Omega_{K|k}^1 \rightarrow 0. \quad (9)$$

The composite map $\Omega_K^1 \xrightarrow{\gamma} \Omega_K^1/B_K^1 \rightarrow \Omega_{K|k}^1/B_{K|k}^1$ vanishes on $K \otimes_k \Omega_k^1$, and hence the operator γ induces a relative operator $\Omega_{K|k}^1 \rightarrow \Omega_{K|k}^1/B_{K|k}^1$ which we again denote by γ .

Of course, for $k = K^p$ we get back the γ of the previous section. In this case the equivalence (1) \Leftrightarrow (2) is a restatement of Theorem 9.2.2. Indeed, the implication (1) \Rightarrow (2) yields that the sequence of Theorem 9.2.2 is a complex, and it is obviously exact at the first term. Exactness at the second term follows from implication (2) \Rightarrow (1).

For the proof we first investigate the implication (2) \Rightarrow (3). It will result from the following slightly more general proposition:

Proposition 9.3.4 *Let $\omega \in \Omega_{K|k}^1$ be a differential form.*

1. *If $d\omega = 0$, then the connection ∇_ω is flat.*
2. *If $\gamma(\omega) = \omega \bmod B_{K|k}^1$, then ∇_ω is a p -connection.*

Note that the condition in part (2) implies $d\omega = 0$ as well, in view of the last statement of Proposition 9.2.1. For the proof we need the following lemma on derivations.

Lemma 9.3.5 *Let $\omega \in \Omega_{K|k}^1$ be a differential form.*

1. *For all derivations $D_1, D_2 \in \text{Der}_k(K)$ we have*

$$(D_1 \wedge D_2)(d\omega) = D_1(D_2(\omega)) - D_2(D_1(\omega)) - [D_1, D_2](\omega).$$

2. *If $\omega \in B_{K|k}^1$, we have*

$$D^{[p]}(\omega) - D^{[p-1]}(D(\omega)) = 0.$$

3. *For general ω and all derivations $D \in \text{Der}_k(K)$ we have*

$$D(\omega)^p = D^{[p]}(\gamma(\omega)) - D^{[p-1]}(D(\gamma(\omega))).$$

Note that the right hand side of the formula in part (3) is well defined in view of part (2).

Proof: It is enough to check (1) on generators of $\Omega_{K|k}^1$, so we may assume $\omega = adb$, so that $d\omega = da \wedge db$. Therefore on the one hand we have

$$(D_1 \wedge D_2)(d\omega) = D_1(da)D_2(db) - D_2(da)D_1(db) = D_1(a)D_2(b) - D_2(a)D_1(b),$$

where we first regard the D_i as linear maps $\Omega_{K|k}^1 \rightarrow K$, and then as derivations $K \rightarrow K$. On the other hand, we compute

$$D_1(D_2(adb)) - D_2(D_1(adb)) - [D_1, D_2](adb) = D_1(aD_2(b)) - D_2(aD_1(b)) - a[D_1, D_2](b),$$

which may be rewritten as

$$D_1(a)D_2(b) + aD_1(D_2(b)) - D_2(a)D_1(b) - aD_2(D_1(b)) - a(D_1(D_2(b)) - D_2(D_1(b))),$$

so that after cancelling terms we again get $D_1(a)D_2(b) - D_2(b)D_1(a)$, as desired.

To check (2), one simply remarks that for $\omega = da$ one has

$$D^{[p]}(\omega) - D^{[p-1]}(D(\omega)) = D^{[p]}(a) - D^{[p-1]}(D(a)) = 0.$$

For (3), we may assume by p -linearity of γ that $\omega = da$ for some $a \in K$, and so we have to check

$$(D(a))^p = D^{[p]}(a^{p-1}da) - D^{[p-1]}(D(a^{p-1}da)).$$

As already remarked, $D^{[p]}$ is a derivation, so that $D^{[p]}(a^{p-1}da) = a^{p-1}D^{[p]}(a)$. After this substitution, the formula reduces to Hochschild's formula (Proposition A.7.1 of the Appendix). \square

For the proof of the proposition it is convenient to introduce for $a \in K$ the notation L_a for the element in $\text{End}_k(K)$ given by multiplication by a , as in the Appendix. Recall also that for $D \in \text{Der}_k(K)$ we have the equality

$$[D, L_a] = L_{D(a)} \tag{10}$$

in $\text{End}_k(K)$ because of the computation $[D, L_a](x) = D(ax) - aD(x) = D(a)x$.

Proof of Proposition 9.3.4: In the notation above, the formula for ∇_{ω^*} in Example 9.3.1 reads $\nabla_{\omega^*}(D) = D + L_{D(\omega)}$. Hence to prove (1) we may write

$$[\nabla_{\omega^*}(D_1), \nabla_{\omega^*}(D_2)] = [D_1, D_2] + [D_1, L_{D_2(\omega)}] - [D_2, L_{D_1(\omega)}] - [L_{D_1(\omega)}, L_{D_2(\omega)}].$$

Here the last term vanishes as the elements $D_1(\omega), D_2(\omega) \in K$ commute, so using equality (10) we may write

$$[\nabla_{\omega^*}(D_1), \nabla_{\omega^*}(D_2)] = [D_1, D_2] + L_{D_1(D_2(\omega))} - L_{D_2(D_1(\omega))},$$

or else

$$[\nabla_{\omega^*}(D_1), \nabla_{\omega^*}(D_2)] = \nabla_{\omega^*}([D_1, D_2]) - L_{[D_1, D_2](\omega)} + L_{D_1(D_2(\omega))} - L_{D_2(D_1(\omega))}.$$

But according to Lemma 9.3.5 (1) we have

$$L_{D_1(D_2(\omega))} - L_{D_2(D_1(\omega))} - L_{[D_1, D_2](\omega)} = L_{(D_1 \wedge D_2)(d\omega)},$$

which is zero by our assumption $d\omega = 0$.

To handle part (2), we compute $(\nabla_{\omega^*}(D))^{[p]} - \nabla_{\omega^*}(D^{[p]})$ as

$$(D + L_{D(\omega)})^{[p]} - (D^{[p]} + L_{D^{[p]}(\omega)}) = D^{[p]} + L_{D(\omega)^p} + L_{D^{[p-1]}(D(\omega))} - (D^{[p]} + L_{D^{[p]}(\omega)})$$

using Proposition A.7.2 from the Appendix. But by Lemma 9.3.5 (2) and our assumption we may write

$$L_{D(\omega)^p - D^{[p]}(\omega) + D^{[p-1]}(D(\omega))} = L_{D(\omega)^p - D^{[p]}(\gamma(\omega)) + D^{[p-1]}(D(\gamma(\omega)))},$$

which vanishes by Lemma 9.3.5 (3). □

We now turn to implication (3) \Rightarrow (1) in Theorem 9.3.3. Recall that we are working over a field extension $K|k$ with $K^p \subset k$. Given a K -vector space V equipped with a connection $\nabla : V \rightarrow \Omega_{K|k}^1 \otimes_K V$, set

$$V^\nabla := \{v \in V : \nabla(v) = 0\}.$$

The defining property of connections implies that V^∇ is a k -subspace of V . In geometric language, it is the space of ‘horizontal sections’ of the connection ∇ . In accordance with the remarks at the beginning of this section, our goal is to prove that for a flat p -connection we have $V^\nabla \neq 0$.

In the case when the extension $K|k$ is *finite*, this is assured by the following descent statement which can be regarded as an analogue of Speiser’s lemma (Lemma 2.3.8) for finite purely inseparable extensions of height 1.

Theorem 9.3.6 *Let $K|k$ be a finite extension with $K^p \subset k$, and let V be a K -vector space equipped with a flat p -connection ∇ . Then the natural map*

$$K \otimes_k V^\nabla \rightarrow V$$

is an isomorphism.

The following proof is taken from the book of Springer [1].

Proof: Take a p -basis a_1, \dots, a_m of the extension $K|k$. Then the da_i form a basis of the K -vector space $\Omega_{K|k}^1$ (by Proposition A.8.8 of the Appendix). Let ∂_i be the derivation defined by sending da_i to 1 and da_j to 0 for $i \neq j$, and set $D_i := a_i \partial_i$. By construction, the D_i satisfy

$$[D_i, D_j] = 0 \quad \text{for all } i \neq j, \quad \text{and} \quad D_i^{[p]} = D_i \quad \text{for all } i.$$

Now consider the elements $\nabla_*(D_i) \in \text{End}_K(V)$ for $1 \leq i \leq m$. Since ∇ is a flat connection, we have $[\nabla_*(D_i), \nabla_*(D_j)] = \nabla_*([D_i, D_j]) = 0$ for $i \neq j$, since $[D_i, D_j] = 0$. This means that the endomorphisms $\nabla_*(D_i)$ pairwise commute, and hence they are simultaneously diagonalisable by a well-known theorem of linear algebra. Moreover, since ∇ is a p -connection, we have $\nabla_*(D_i)^{[p]} = \nabla_*(D_i^{[p]}) = \nabla_*(D_i)$, which implies that the eigenvalues of the $\nabla_*(D_i)$ all lie in \mathbf{F}_p . Represent elements of \mathbf{F}_p^m by vectors $(\lambda_1, \dots, \lambda_m)$, and for each $(\lambda_1, \dots, \lambda_m)$ put

$$V_{\lambda_1, \dots, \lambda_m} = \{v \in V : \nabla_*(D_i)v = \lambda_i v \text{ for } 1 \leq i \leq m\}.$$

By our remark on simultaneous diagonalisation, we may write V as the direct sum of the $V_{\lambda_1, \dots, \lambda_m}$, and moreover $V^\nabla = V_{0, \dots, 0}$ by definition. On the other hand, as the a_i form a p -basis of $K|k$, we have a direct sum decomposition $K \otimes_k V^\nabla \cong \bigoplus a_1^{\lambda_1} \cdots a_m^{\lambda_m} V^\nabla$. But $a_1^{\lambda_1} \cdots a_m^{\lambda_m} V^\nabla$ is none but $V_{\lambda_1, \dots, \lambda_m}$, and the theorem follows. \square

Remarks 9.3.7

1. Given a k -vector space W with $V \cong K \otimes_k W$, one may define a connection ∇_W on V by setting $\nabla_W(a \otimes w) := da \otimes w$ and extending K -linearly. Then for all $D \in \text{Der}_k(V)$ the K -endomorphism $\nabla_{W*}(D)$ sends $a \otimes w$ to $D(a) \otimes w$. Using this formula one immediately checks that ∇_W is a flat p -connection. Moreover, in the case $W = V^\nabla$ one checks easily that $\nabla_{V^\nabla} = \nabla$. So we may rephrase the theorem by saying that the functor $W \mapsto (W, \nabla_W)$ induces an equivalence of categories between the category of k -vector spaces and that of K -vector spaces equipped with a flat p -connection, the inverse being given by the functor $V \mapsto V^\nabla$.
2. A direct ancestor of the above descent statement is the following analogue of the Galois correspondence for finite purely inseparable extensions $K|k$ of height 1 due to Jacobson. For a Lie subalgebra $\mathfrak{g} \subset \text{Der}_k(K)$ let $K^\mathfrak{g} \subset K$ be the intersection of the kernels of the derivations in \mathfrak{g} . Then the map $\mathfrak{g} \mapsto K^\mathfrak{g}$ induces a bijection between the

Lie subalgebras of $\text{Der}_k(K)$ stable under $D \mapsto D^{[p]}$ and the subextensions of $K|k$, and moreover $[K : K^{\mathfrak{g}}] = p^{\dim_K \mathfrak{g}}$. The proof is similar to that of Theorem 9.3.6; see Jacobson [2], Theorem 8.43 or Springer [1], Theorem 11.1.15. Gerstenhaber [1] has extended this correspondence to infinite purely inseparable extensions of height one, by defining an analogue of the Krull topology.

We now come to:

Proof of Theorem 9.3.3: The implication (1) \Rightarrow (2) follows from the easy calculation $\gamma(a^{-1}da) = a^{-p}a^{p-1}da = a^{-1}da$ for all $a \in K^\times$. As already remarked, the implication (2) \Rightarrow (3) follows from Proposition 9.3.4, so it remains to see (3) \Rightarrow (1). This we first prove in the case when $K|k$ is a finite extension. Indeed, applying Theorem 9.3.6 we conclude that K^{∇_ω} is a k -vector space of dimension 1; in particular, it is nonzero. Therefore we find a nonzero y in K with $\nabla_\omega(y) = 0$. But as already remarked at the beginning of the section, $\nabla_\omega(y) = 0$ is equivalent to $\omega = \text{dlog}(y^{-1})$. To treat the general case, write K as a direct limit of subfields K_λ finitely generated over \mathbf{F}_p and set $k_\lambda := k \cap K_\lambda$. Given $\omega \in \Omega_{K|k}^1$, we find some K_λ as above so that ω comes from an element $\omega_\lambda \in \Omega_{K_\lambda|k_\lambda}^1$. If ∇_ω is a flat p -connection on K , then so is ∇_{ω_λ} on K_λ . As K_λ is finitely generated and $K_\lambda^p \subset k_\lambda$, the extension $K_\lambda|k_\lambda$ is finite, and therefore the previous case yields $y \in K_\lambda \subset K$ with $\omega_\lambda = \text{dlog}(y)$ in $\Omega_{K_\lambda|k_\lambda}^1$. But then $\omega = \text{dlog}(y)$ in $\Omega_{K|k}^1$. \square

9.4 Decomposition of the de Rham Complex

As a preparation for our study of the higher dimensional differential symbol, we now discuss properties of the de Rham complex over fields of characteristic $p > 0$. Let $K|k$ be again a field extension with $K^p \subset k$. Recall from the Appendix that the de Rham complex is a complex of the shape

$$\Omega_{K|k}^\bullet = (K \xrightarrow{d} \Omega_{K|k}^1 \xrightarrow{d} \Omega_{K|k}^2 \xrightarrow{d} \Omega_{K|k}^3 \xrightarrow{d} \dots).$$

Assume moreover that $K|k$ is finite of degree p^r , and choose a p -basis b_1, \dots, b_r . According to Proposition A.8.8 of the Appendix, the elements db_1, \dots, db_r form a K -basis of the vector space $\Omega_{K|k}^1$, and hence the i -fold exterior products $db_{\lambda_1} \wedge \dots \wedge db_{\lambda_i}$ form a K -basis of $\Omega_{K|k}^i$. In particular, this implies that $\Omega_{K|k}^i = 0$ for $i > r$. According to the Appendix, the differential $d : \Omega_{K|k}^i \rightarrow \Omega_{K|k}^{i+1}$ coincides with the universal derivation d for $i = 0$, and satisfies $d(\omega_1 \wedge \omega_2) = d\omega_1 \wedge \omega_2 + (-1)^i \omega_1 \wedge d\omega_2$ for $\omega_1 \in \Omega_{K|k}^i$ and $\omega_2 \in \Omega_{K|k}^j$.

The products $b_1^{\alpha_1} \dots b_r^{\alpha_r}$ with $0 \leq \alpha_i \leq p-1$ form a basis of the k -vector space K . As the extensions $k(b_i)|k$ are linearly disjoint over K , this implies $K \cong k(b_1) \otimes_k \dots \otimes_k k(b_r)$. On the other hand, the elements $b_1^{\alpha_1} \dots b_r^{\alpha_r} db_{\lambda_1} \wedge \dots \wedge db_{\lambda_i}$ form a k -basis of $\Omega_{K|k}^i$, so the above description of differentials and the definition of tensor products of complexes (Chapter 3, Section 3.4) imply:

Proposition 9.4.1 *For $K|k$ and b_1, \dots, b_r as above, the de Rham complex $\Omega_{K|k}^\bullet$ considered as a complex of k -vector spaces decomposes as a tensor product*

$$\Omega_{K|k}^\bullet \cong \Omega_{k(b_1)|k}^\bullet \otimes_k \dots \otimes_k \Omega_{k(b_r)|k}^\bullet.$$

This decomposition will be one of our main tools in the study of the de Rham complex. The other one is the following general lemma on tensor products of complexes which is a special case of the Künneth formula.

Lemma 9.4.2 *Let A^\bullet and B^\bullet be complexes of vector spaces over the same field k , concentrated in nonnegative degrees. Then for all $i \geq 0$ the natural maps*

$$\bigoplus_{p+q=i} H^p(A^\bullet) \otimes_k H^q(B^\bullet) \rightarrow H^i(A^\bullet \otimes_k B^\bullet)$$

are isomorphisms.

Proof: Denote by $Z^\bullet(A)$ (resp. $B^\bullet(A)$) the subcomplexes of A^\bullet obtained by restricting to the subspaces $Z^i(A)$ (resp. $B^i(A)$) of A^i in degree i ; note that all differentials in these complexes are zero. Denoting by $B^\bullet(A)[1]$ the shifted complex with $B^i(A)[1] = B^{i+1}(A)$, one has an exact sequence of complexes

$$0 \rightarrow Z^\bullet(A) \rightarrow A^\bullet \rightarrow B^\bullet(A)[1] \rightarrow 0.$$

Tensoring with B^\bullet yields

$$0 \rightarrow Z^\bullet(A) \otimes_k B^\bullet \rightarrow A^\bullet \otimes_k B^\bullet \rightarrow B^\bullet(A)[1] \otimes_k B^\bullet \rightarrow 0. \quad (11)$$

This sequence is again exact, by the following argument. For each $n \geq 0$ define the truncated complex $B_{\leq n}^\bullet$ by setting all terms of degree $> n$ in B^\bullet to 0. A straightforward induction on n using the exact sequences $0 \rightarrow B_{\leq n-1}^\bullet \rightarrow B_{\leq n}^\bullet \rightarrow B^n[-n] \rightarrow 0$ (where $B^n[-n]$ has a single nonzero term in degree n) then implies that the sequences

$$0 \rightarrow Z^\bullet(A) \otimes_k B_{\leq n}^\bullet \rightarrow A^\bullet \otimes_k B_{\leq n}^\bullet \rightarrow B^\bullet(A)[1] \otimes_k B_{\leq n}^\bullet \rightarrow 0$$

are exact for all n , whence the exactness of (11). Now part of the long exact sequence associated with (11) reads

$$\begin{aligned} H^i(B^\bullet(A) \otimes_k B^\bullet) &\rightarrow H^i(Z^\bullet(A) \otimes_k B^\bullet) \rightarrow H^i(A^\bullet \otimes_k B^\bullet) \rightarrow \\ \rightarrow H^{i+1}(B^\bullet(A) \otimes_k B^\bullet) &\rightarrow H^{i+1}(Z^\bullet(A) \otimes_k B^\bullet). \end{aligned} \tag{12}$$

As $B^\bullet(A) \rightarrow Z^\bullet(A)$ is an injective map of complexes with trivial differentials, so is the map $B^\bullet(A) \otimes_k B^\bullet \rightarrow Z^\bullet(A) \otimes_k B^\bullet$. Thus the last map in (12) is injective, whence the exactness of the sequence

$$H^i(B^\bullet(A) \otimes_k B^\bullet) \rightarrow H^i(Z^\bullet(A) \otimes_k B^\bullet) \rightarrow H^i(A^\bullet \otimes_k B^\bullet) \rightarrow 0.$$

Again using the triviality of differentials in the complexes $Z^\bullet(A)$ and $B^\bullet(A)$, we may identify the the first map here with the map

$$\bigoplus_{p+q=i} B^p(A^\bullet) \otimes_k H^q(B^\bullet) \rightarrow \bigoplus_{p+q=i} Z^p(A^\bullet) \otimes_k H^q(B^\bullet),$$

whence the lemma. □

We now come to applications of the above observations. The first one is another basic result of Cartier concerning the operator γ , usually called the *Cartier isomorphism* in the literature. To be able to state it, we first extend the definition of γ to higher differential forms by setting

$$\gamma(\omega_1 \wedge \cdots \wedge \omega_i) := \gamma(\omega_1) \wedge \cdots \wedge \gamma(\omega_i),$$

where on the right hand side the maps γ are defined as in Proposition 9.2.1 (and extended to the relative case as in the previous section). For $i = 0$ we put $\gamma(a) := a^p$. In this way we obtain K -linear maps

$$\gamma : \Omega_{K|k}^i \rightarrow {}^p Z_{K|k}^i / {}^p B_{K|k}^i$$

for all $i \geq 0$. Note that the differentials of the complex ${}^p \Omega_K^\bullet$ are K -linear by a similar argument as in degree 0, so ${}^p B_{K|k}^i \subset {}^p Z_{K|k}^i$ is a K -subspace.

Theorem 9.4.3 (Cartier) *For all extensions $K|k$ as above and all $i \geq 0$ the map γ is an isomorphism.*

Proof: Assume first $K|k$ is a finite extension of degree p^r , and fix a p -basis b_1, \dots, b_r of $K|k$ as above. Using the above explicit description of $\Omega_{K|k}^\bullet$ and the construction of γ we see that it is enough to check the following:

- $H^0(\Omega_{K|k}^\bullet)$ is the 1-dimensional k -vector space generated by 1;

- $H^1(\Omega_{K|k}^\bullet)$ is the r -dimensional k -vector space generated by the $b_i^{p-1}db_i$;
- $H^i(\Omega_{K|k}^\bullet) \cong \Lambda^i H^1(\Omega_{K|k}^\bullet)$ for $i > 1$.

Now using Proposition 9.4.1, Lemma 9.4.2 and induction on r we see that it is enough to check these statements for $r = 1$, i.e. $K = k(b)$ with $b^p \in k$. In this case, K and $\Omega_{K|k}^1$ are p -dimensional k -vector spaces with bases $\{b^i : 0 \leq i \leq p-1\}$ and $\{b^i db : 0 \leq i \leq p-1\}$, respectively. Moreover, one has $\Omega_{K|k}^i = 0$ for $i > 1$, and the differential $d : K \rightarrow \Omega_{K|k}^1$ sends b^i to $ib^{i-1}db$. It follows that $H^0(\Omega_{K|k}^\bullet)$ and $H^1(\Omega_{K|k}^\bullet)$ are 1-dimensional over k , generated by 1 and $b^{p-1}db$, respectively, and $\Lambda^i H^1(\Omega_{K|k}^\bullet) = 0$ for $i > 0$, which shows that the three required properties are satisfied.

For the general case, write K as a direct limit of subfields K_λ finitely generated over \mathbf{F}_p . Each K_λ is a finite extension of K_λ^p and therefore also of $k \cap K_\lambda$, so that the case just discussed applies, and the theorem follows by passing to the limit. \square

The theorem enables us to define for all $i \geq 0$ the *Cartier operator* $C : {}^pZ_{K|k}^i / {}^pB_{K|k}^i \rightarrow \Omega_{K|k}^i$ as the inverse of γ . It is also customary to regard it as a linear map $C : {}^pZ_{K|k}^i \rightarrow \Omega_{K|k}^i$ defined on closed differential forms. With these notations, Theorem 9.4.3 and Theorem 9.2.2 respectively yield the following characterisation of exact and logarithmic differential forms, which is the form of Cartier's results often found in the literature.

Corollary 9.4.4

1. An i -form $\omega \in \Omega_{K|k}^i$ is exact, i.e. lies in $B_{K|k}^i$, if and only if $d\omega = C(\omega) = 0$.
2. A 1-form $\omega \in \Omega_{K|k}^1$ is logarithmic, i.e. lies in the image $\nu(1)_{K|k}$ of the $d\log$ map, if and only if $d\omega = 0$ and $C(\omega) = \omega$.

Remark 9.4.5 The definition of the inverse Cartier operator γ works over an arbitrary integral domain A of characteristic $p > 0$ in exactly the same way. One can then prove that if A is a finitely generated *smooth* algebra over a perfect field k of characteristic $p > 0$, i.e. it arises as the coordinate ring of a smooth affine k -variety, then the map γ induces an isomorphism of A -modules $\Omega_A^i \xrightarrow{\sim} {}^pH^i(\Omega_A^\bullet)$ for all $i \geq 0$. The idea (due to Grothendieck) is to treat first the case of the polynomial ring $k[x_1, \dots, x_r]$ which is similar to the case of fields treated above, the module $\Omega_{k[x_1, \dots, x_r]|k}^1$ being a free $k[x_1, \dots, x_r]$ -module over the dx_i and the x_i forming a ' p -basis' of $k[x_1, \dots, x_r]$ over $k[x_1^p, \dots, x_r^p]$. The general case then follows from the well-known fact of algebraic geometry (Mumford [1], III.6, Theorem 1) according to which on a smooth k -variety

each point has an open neighbourhood equipped with an étale morphism to some affine space over k , together with the fact an étale morphism induces an isomorphism on modules of differentials. See Katz [1] or Illusie ([1],[2]) for details and a globalisation for smooth varieties.

Another consequence of the tensor product decomposition of the de Rham complex is a direct sum decomposition we shall use later. We consider again an extension $K|k$ and a p -basis b_1, \dots, b_r as at the beginning of this section, and fix a multiindex $\alpha := (\alpha_1, \dots, \alpha_r)$ with $0 \leq \alpha_i \leq p-1$. For each $i \geq 0$ consider the k -subspace $\Omega_{K|k}^i(\alpha) \subset \Omega_{K|k}^i$ generated by the elements $b_1^{\alpha_1} \dots b_r^{\alpha_r} (db_{\lambda_1}/b_{\lambda_1}) \wedge \dots \wedge (db_{\lambda_i}/b_{\lambda_i})$ for $1 \leq \lambda_1 \leq \dots \leq \lambda_i \leq r$; for $i = 0$ this just means the 1-dimensional subspace generated by $b_1^{\alpha_1} \dots b_r^{\alpha_r}$. Since the $(db_{\lambda_1}/b_{\lambda_1}) \wedge \dots \wedge (db_{\lambda_i}/b_{\lambda_i})$ form a K -basis of $\Omega_{K|k}^i$ just like the $db_{\lambda_1} \wedge \dots \wedge db_{\lambda_i}$, the k -vector space $\Omega_{K|k}^i$ decomposes as a direct sum of the subspaces $\Omega_{K|k}^i(\alpha)$ for all possible α . The case $\alpha = (0, \dots, 0)$ is particularly important; we shall abbreviate it by $\alpha = 0$.

Proposition 9.4.6 *Let $K|k$ and α be as above.*

1. *The differentials $d : \Omega_{K|k}^i \rightarrow \Omega_{K|k}^{i+1}$ map each $\Omega_{K|k}^i(\alpha)$ to $\Omega_{K|k}^{i+1}(\alpha)$, giving rise to subcomplexes $\Omega_{K|k}^\bullet(\alpha)$ of $\Omega_{K|k}^\bullet$.*
2. *One has a direct sum decomposition $\Omega_{K|k}^\bullet \cong \bigoplus_\alpha \Omega_{K|k}^\bullet(\alpha)$.*
3. *The complex $\Omega_{K|k}^\bullet(0)$ has zero differentials, and the complexes $\Omega_{K|k}^\bullet(\alpha)$ are acyclic for $\alpha \neq 0$.*

Proof: Using Proposition 9.4.1 (and Lemma 9.4.2 for the third statement) we reduce all three statements to the case $r = 1$. In this case the first two statements are immediate, and the third one follows by the same calculation as at the end of the proof of Theorem 9.4.3. \square

9.5 The Bloch-Gabber-Kato Theorem: Statement and Reductions

As a field K of characteristic p has p -cohomological dimension ≤ 1 , the Galois symbol $h_{K,p}^n$ is a trivial invariant for $n > 1$. However, the discussion of Section 9.2 suggests the investigation of another invariant, the *differential symbol*. To define it, introduce for all $n \geq 0$ the notation

$$\nu(n)_K := \ker(\gamma - \text{id} : \Omega_K^n \rightarrow \Omega_K^n/B_K^n).$$

We shall omit the subscript K if clear from the context. Note that $\nu(0) \cong \mathbf{F}_p$ as we defined γ to be p -th power map for 0-forms, and for $n = 1$ we get back the $\nu(1)_K$ of Section 9.2. Since γ takes its values in Z_K^n/B_K^n , it follows that $\nu(n)_K \subset Z_K^n$. Moreover, since γ is defined for $n > 1$ as the n -th exterior product map of the operator γ on Ω_k^1 , one has a natural map $\nu(1)^{\otimes n} \rightarrow \nu(n)$. This allows one to define

$$\mathrm{dlog} : (K^\times)^{\otimes n} \rightarrow \nu(n)$$

for $n > 1$ by taking the n -th tensor power of the map $\mathrm{dlog} : K^\times \rightarrow \nu(1)_K$ and then composing with the map above.

Lemma 9.5.1 *The map dlog factors through the quotient $K_n^M(K)/pK_n^M(K)$, and thus defines a map*

$$\psi_K^n : K_n^M(K)/pK_n^M(K) \rightarrow \nu(n)_K$$

sending $\{y_1, y_2, \dots, y_n\}$ to $(dy_1/y_1) \wedge \dots \wedge (dy_n/y_n)$ for all $y_1, \dots, y_n \in K^\times$.

Proof: As $p\nu(n) = 0$, the only point to be checked is the Steinberg relation. It holds because for $y \neq 0, 1$

$$\mathrm{dlog}(y) \wedge \mathrm{dlog}(1-y) = \frac{1}{y(1-y)} dy \wedge d(1-y) = -\frac{1}{y(1-y)} dy \wedge dy = 0.$$

□

The remainder of this chapter will be devoted to the following basic theorem, whose surjectivity statement is due to Kato, and whose injectivity statement was proven independently by Bloch-Kato and Gabber (unpublished).

Theorem 9.5.2 (Bloch-Gabber-Kato) *Let K be a field of characteristic $p > 0$. For all integers $n \geq 0$, the differential symbol*

$$\psi_K^n : K_n^M(K)/pK_n^M(K) \rightarrow \nu(n)_K$$

is an isomorphism.

Remarks 9.5.3

1. The surjectivity statement of the theorem generalises Theorem 9.2.2 to higher differential forms.

2. Using the theorem above, Bloch and Kato proved the bijectivity of the Galois symbol $h_{k,p}^n$ for n arbitrary and k a complete discrete valuation field of characteristic 0 with residue field of characteristic p (Bloch-Kato [1], §5; see also Colliot-Thélène [4] for a detailed survey),
3. Building upon Theorem 9.5.2, Bloch and Kato also proved that for a field K of characteristic p the p -primary torsion subgroup of $K_n^M(K)$ is divisible for all $n > 0$ (Bloch-Kato [1], §2.8). Then Izhboldin [1] proved that $K_n^M(K)$ has actually no p -torsion at all (see also Friedlander-Weibel [1] for an exposition). For $n = 2$ this gives back Suslin's theorem (Theorem 8.4.8), but Izhboldin's proof is different, the main ingredient being the result of Bloch and Kato.

In the remaining of this section we perform some preliminary constructions and reductions to be used in the proof.

First we define trace maps $\text{tr}_{K'|K} : \Omega_{K'}^n \rightarrow \Omega_K^n$ for finite separable extensions $K'|K$ (they also exist for inseparable extensions, but the construction is more complicated and will not be used). The construction is based on the fact that for $K'|K$ separable one has $\Omega_{K'}^n \cong K' \otimes_K \Omega_K^n$ by Proposition A.8.7 of the Appendix. Hence the field trace $\text{tr} : K' \rightarrow K$ induces a trace map $\text{tr} = \text{tr} \otimes \text{id} : K' \otimes_K \Omega_K^n \rightarrow \Omega_K^n$ which is the map we were looking for. The composite $\text{tr} \circ \text{id} : \Omega_{K'}^n \rightarrow \Omega_K^n$ is multiplication by $[K' : K]$, and one has the projection formula $\text{tr}(\omega_1 \wedge (\omega_2)_{K'}) = \text{tr}(\omega_1) \wedge \omega_2$ for $\omega_1 \in \Omega_{K'}^n, \omega_2 \in \Omega_K^n$. Moreover, the trace map commutes with differentials and the Cartier operator by construction, so it restricts to a trace map $\text{tr} : \nu(n)_{K'} \rightarrow \nu(n)_K$.

Lemma 9.5.4 *Given a finite separable extension $K'|K$, the diagram*

$$\begin{array}{ccc} K_n^M(K')/pK_n^M(K') & \xrightarrow{\psi_{K'}^n} & \nu(n)_{K'} \\ N_{K'|K} \downarrow & & \text{tr} \downarrow \\ K_n^M(K)/pK_n^M(K) & \xrightarrow{\psi_K^n} & \nu(n)_K \end{array}$$

commutes.

Proof: Let us consider first the case $n = 1$. Let $y \in K'^\times$, and let K_s be a separable closure of K . As the maps $K^\times \rightarrow K_s^\times$ and $\Omega_K^1 \rightarrow \Omega_{K_s}^1$ are injective, we may reason in K_s . There the element $N_{K'|K}(y)$ decomposes as a product $N_{K'|K}(y) = \prod \sigma(y)$, where the product is taken over the K -embeddings of K' into K_s . As these embeddings commute with the dlog map, it follows

that inside $\Omega_{K_s}^1$ one has $\text{dlog}(N_{K'|K}(y)) = \sum \sigma(\text{dlog}(y))$, which is none but $\text{tr}(\text{dlog}(y))$. In the case $n > 1$ we consider a maximal prime to p extension $K^{(p)}|K$ (which is of course separable). The tensor product $K^{(p)} \otimes_K K'$ is a finite direct product of extensions $K_i|K^{(p)}$ and the induced norm map on K_n^M is the sum of the norm maps for these extensions by Lemma 7.3.6. Similarly the trace map on differentials becomes the sum of the traces for the $K_i|K^{(p)}$. Since moreover the map $\Omega_K^n \rightarrow \Omega_{K^{(p)}}^n$ is injective, we are reduced to the case $K = K^{(p)}$. But then according to the Bass-Tate lemma (Corollary 7.2.10) it is enough to treat symbols of the form $\{a_1, \dots, a_n\}$ with $a_1 \in K'$ and $a_i \in K$ for $i > 1$, and the statement reduces to the case $n = 1$ by the projection formula. \square

The trace construction implies the following reduction statement.

Proposition 9.5.5 *Let $K'|K$ a finite extension of degree prime to p . Then the natural map $\ker(\psi_K^n) \rightarrow \ker(\psi_{K'}^n)$ is injective, and the trace map induces a surjection $\text{coker}(\psi_{K'}^n) \rightarrow \text{coker}(\psi_K^n)$.*

In particular, if $\psi_{K'}^n$ is injective (resp. surjective), then so is ψ_K^n .

Proof: The statement about the kernel follows from the injectivity of the map $K_n^M(K)/pK_n^M(K) \rightarrow K_n^M(K')/pK_n^M(K')$ already noted during the proof of Proposition 7.5.9. That about the cokernel comes from the previous lemma, noting that the trace map is surjective, as so is the composite $[K' : K] = \text{tr} \circ \text{id}$, the degree $[K' : K]$ being prime to p and $\nu(n)_K$ being p -torsion. \square

On the other hand, the following reduction statement is immediate by writing K as a union of its finitely generated subfields.

Lemma 9.5.6 *If the differential symbol ψ_F^n is injective (resp. surjective) for all subfields $F \subset K$ which are finitely generated over \mathbf{F}_p , then so is ψ_K^n .*

9.6 Surjectivity of the Differential Symbol

In this section we prove the surjectivity of the differential symbol. Recall the statement:

Theorem 9.6.1 (Kato) *For all $n > 0$, the map $\text{dlog} : (K^\times)^{\otimes n} \rightarrow \nu(n)$ is surjective, i.e. the group $\nu(n)$ is additively generated by the elements of the shape $dx_1/x_1 \wedge \dots \wedge dx_n/x_n$.*

Remark 9.6.2 In the case when K is separably closed this was proven earlier by Bloch (unpublished). See Illusie [1], Theorem 2.4.2 for an exposition of his proof.

Before embarking on the proof, we establish an innocent looking result of linear algebra that will be needed later.

Proposition 9.6.3 *Let E be a field of characteristic p , and let $F = E(b)$ be a purely inseparable extension of degree p . Consider an E -linear map $g : F \rightarrow E$. Then up to replacing E by a finite extension $E'|E$ of degree prime to p , F by FE' and g by the induced map, there exists $c \in F^\times$ satisfying $g(c^i) = 0$ for $1 \leq i \leq p - 1$.*

We begin the proof of the proposition with:

Lemma 9.6.4 *Let $F|E$ be a field extension as in Lemma 9.6.3. Then up to replacing E by E' and F by FE' as above we may write each element of $\Omega_{F|E}^1 \setminus dF$ in the form udy/y with suitable $u \in E^\times$ and $y \in F^\times$.*

Proof: One may write each element $\omega \in \Omega_{F|E}^1$ as $\omega = a(db/b)$ for suitable $a, b \in E^\times$. As the E -vector space $\Omega_{F|E}^1/dF$ is 1-dimensional (see the proof of Theorem 9.4.3), the condition $\omega \notin dF$ implies that its image spans $\Omega_{F|E}^1/dF$. In particular, there exists $\rho \in E^\times$ with $a^p(db/b) = \rho a(db/b)$ in $\Omega_{F|E}^1/dF$. Up to replacing E by the prime-to- p extension $E(u)$ for some u with $\rho = u^{p-1}$, we may assume that such an u exists in E^\times , so division by u^p yields $(u^{-1}a)^p(db/b) = u^{-1}a(db/b)$ in $\Omega_{F|E}^1/dF$. In other words, $u^{-1}\omega = u^{-1}a(db/b)$ lies in the kernel of $\gamma - 1$, and therefore $u^{-1}\omega = dy/y$ according to Theorem 9.3.3. The lemma follows. \square

Proof of Proposition 9.6.3: Take an isomorphism ϕ between the 1-dimensional F -vector spaces F and $\Omega_{F|E}^1$. The E -subspaces $\ker(g) \subset F$ and $dF \subset \Omega_{F|E}^1$ are both of codimension 1, hence up to modifying ϕ by multiplication with an element in F^\times we may assume that $\phi(\ker(g)) = dF$ (this is immediately seen by looking at the dual spaces). Let a be an element of $F \setminus \ker(g)$. Then $\phi(a)$ generates $\Omega_{F|E}^1$ as an F -vector space, and its mod dF class generates the E -vector space $\Omega_{F|E}^1/dF$. By the lemma above we have $\phi(a) = udy/y$ for suitable $y \in F^\times$ and $u \in E^\times$; up to modifying a we may assume $u = 1$. Now by the above choice of ϕ we have the equivalences $g(x) = 0 \Leftrightarrow xa \in \ker(g) \Leftrightarrow xdy/y \in dF$ for all $x \in F$. On the other hand, we have seen during the proof of Theorem 9.4.3 that the elements $y^i dy$ for $0 \leq i \leq p - 2$ span dF . Thus $c = y$ is a good choice. \square

Now return to the field K of Theorem 9.6.1, and let $k \subset K$ be a subfield containing K^p . Assume moreover that $K|k$ is a finite extension of degree p^r , and take a p -basis $\{b_1, \dots, b_r\}$ of $K|k$. Then for $1 \leq i \leq r$ the db_i/b_i form a K -basis of $\Omega_{K|k}^1$. For $n > 1$ we shall use the explicit basis of $\Omega_{K|k}^n$ given as follows. Denote by S_n the set of strictly increasing functions from $\{1, \dots, n\}$ to $\{1, \dots, r\}$, and for all $s \in S_n$ set

$$\omega_s = db_{s(1)}/b_{s(1)} \wedge \cdots \wedge db_{s(n)}/b_{s(n)}.$$

Then the ω_s for $s \in S_n$ form a K -basis of $\Omega_{K|k}^n$. Equip the set S_n with the lexicographic ordering, i.e. for $s, t \in S_n$ set $t < s$ if there exists m in $\{1, \dots, n\}$ so that $t(i) = s(i)$ for all $i < m$ and $t(m) < s(m)$. Denote by $\Omega_{K|k, < s}^n$ the K -subspace of $\Omega_{K|k}^n$ generated by the ω_t with $t < s$, and put $B_{K|k, < s}^n := d(\Omega_{K|k, < s}^{n-1})$. We shall adopt analogous notations for subfields of K .

We may now state the key proposition which will be also useful for proving the injectivity of the differential symbol.

Proposition 9.6.5 *Let $K|k$ be a finite extension of degree p^r as above. Fix $s \in S_n$ and (with the notations above) assume $a \in K$ satisfies*

$$(a^p - a)\omega_s \in \Omega_{K|k, < s}^n + B_{K|k}^n. \quad (13)$$

Then up to replacing K by a finite extension of degree prime to p we have

$$a\omega_s \in \Omega_{K|k, < s}^n + \text{Im}(\text{dlog}).$$

Before proving the proposition, we derive Theorem 9.6.1.

Proof of Theorem 9.6.1: By Lemma 9.5.6 we may assume K is finitely generated over \mathbf{F}_p , so that setting $k = K^p$ the extension $K|k$ is finite. Assume $\omega \in \nu(n)(K)$ is not in the image of the dlog map. Since Ω_K^n is the direct sum of the $\Omega_{K, s}^n$, we may then find a smallest s (with respect to the lexicographic order) so that $\omega = \omega' + \eta$, with $\omega' \in \Omega_{K, < s+1}^n$ and $\eta \in \text{Im}(\text{dlog})$. Write $\omega' = a\omega_s + \omega''$ with suitable $a \in K$ and $\omega'' \in \Omega_{K, < s}^n$. As by construction γ maps $\Omega_{K, < s}^n$ to its image in Ω_K^n/B_K^n , applying $\gamma - 1$ yields $(a^p - a)\omega_s \in \Omega_{K, < s}^n + B_K^n$, noting that $(\gamma - 1)\eta$ and $(\gamma - 1)\omega$ both lie in B_K^n . According to Proposition 9.6.5, after passing to a finite prime to p extension $K'|K$ we have $a\omega_s \in \Omega_{K', < s}^n + \text{Im}(\text{dlog})$, so that $\omega \in \Omega_{K', < s}^n + \text{Im}(\text{dlog})$ as well. Since a p -basis of $K|k$ provides a p -basis of $K'|K^p$ as well, by taking traces and using the formula $\text{tr} \circ \text{id} = [K' : K]$ in a by now familiar way we see that the minimal s for K' cannot be greater than for K , and the above argument shows that it is actually strictly smaller. Thus after taking finitely many

finite prime to p extensions we arrive at an extension where the dlog map is surjective, and then the theorem follows from Proposition 9.5.5. \square

We now come to the proof of the proposition, which is a fairly long calculation. The exposition is largely based on the notes of Colliot-Thélène [4].

Proof of Proposition 9.6.5: With the notations adopted before the proposition define subfields k_0, k_1 and k_2 of K by

$$k_0 := k(b_1, b_2, \dots, b_{s(1)-1}), \quad k_1 := k_0(b_{s(1)}), \quad \text{and} \quad k_2 := k_0(b_{s(1)}, b_{s(1)+1}, \dots, b_{s(n)}).$$

We have $[k_2 : k_0] = p^N$, where N stands for the number of integers j such that $s(1) \leq j \leq s(n)$.

We first show that under the assumption of the proposition the element a belongs to k_2 . To see this, denote by $m(1) < \dots < m(N-n)$ those integers in the interval $[s(1), s(n)]$ which are *not* of the shape $s(j)$, and introduce the elements

$$\omega_m := db_{m(1)}/b_{m(1)} \wedge \dots \wedge db_{m(N-n)}/b_{m(N-n)} \in \Omega_K^{N-n} \quad \text{and} \quad \omega_{\max} := \omega_m \wedge \omega_s \in \Omega_K^N$$

(for $n = 1$ write simply $\omega_m = 1$ and $\omega_{\max} = \omega_s$). Applying d to the equation (13) yields $da \wedge \omega_s \in B_{K, < s}^{n+1}$. But the set $\omega_m \wedge B_{K, < s}^{n+1} \subset \Omega_K^{N+1}$ maps to 0 in $\Omega_{K|k_0}^N$, because the components of an element in $B_{K, < s}^{n+1}$ are either of the form $db_j/b_j \wedge w'$ with $j < s(1)$ and hence have trivial image in $\Omega_{K|k_0}^{n+1}$, or contain some $db_{m(i)}/b_{m(i)}$. In particular, $da \wedge \omega_{\max} = 0$ in $\Omega_{K|k_0}^{N+1}$. Now if a were not in k_2 , then $b_{s(1)}, \dots, b_{s(n)}$ and a would form part of a p -basis of $K|k_0$, which would contradict $da \wedge \omega_{\max} = 0$.

So we have $a \in k_2$, and hence by the choice of k_2 we may consider $a\omega_s$ as an element of $\Omega_{k_2|k_0}^n$. We may thus rewrite our assumption (13) as

$$(a^p - a)\omega_s = \omega + d\omega_1 \quad \text{with} \quad \omega \in \Omega_{k_2|k_0, < s}^n, \quad \omega_1 \in \Omega_{k_2|k_0}^{n-1}. \quad (14)$$

The next step is to replace $b_{s(1)}$ by another generator c of the extension $k_1|k_0$ which has a useful additional technical property. For this we first take the wedge product of both sides by ω_m , whence using $\omega \wedge \omega_m = 0$ in $\Omega_{k_2|k_0}^N$ (same argument as in the previous paragraph) we obtain

$$(a^p - a)\omega_{\max} = d\omega_1 \wedge \omega_m = d(\omega_1 \wedge \omega_m) \quad (15)$$

(recall that $d\omega_m = 0$ because ω_m is logarithmic), so that $(a^p - a)\omega_{\max} \in B_{k_2|k_0}^N$.

Consider now the k_0 -linear map $k_1 \rightarrow \Omega_{k_2|k_0}^N/B_{k_2|k_0}^N$ sending $x \in k_1$ to the class of $x\omega_{\max}$. As $[k_2 : k_0] = p^N$, the space $\Omega_{k_2|k_0}^N/B_{k_2|k_0}^N$ is 1-dimensional

over k_0 and moreover generated by the class of ω_{\max} (recall again the proof of Theorem 9.4.3). Thus by applying Proposition 9.6.3 to $E = k_0$, $F = k_1$ and the above k_0 -linear map we find $c \in k_1^\times$ with

$$c^i a \omega_{\max} \in B_{k_2|k_0}^N \quad \text{for all } 1 \leq i \leq p-1 \quad (16)$$

up to replacing k_0 (and hence ultimately K) by a finite prime to p extension. Moreover, the c we found does not lie in k_0 . Indeed, if it did, then $c a \omega_{\max} \in B_{k_2|k_0}^N$ would imply $a \omega_{\max} \in B_{k_2|k_0}^N$. Taking (15) into account, we would then get $a^p \omega_{\max} \in B_{k_2|k_0}^N$ and finally $\omega_{\max} \in B_{k_2|k_0}^N$, which is impossible.

Thus the above c generates the extension $k_1|k_0$. Henceforth we use c together with the set $\{b_i : i > s(1)\}$ as a p -basis of $k_2|k_0$. Using this p -basis we may rewrite $a \omega_s$ in the following way. For $n = 1$ we have $a \omega_s = a' dc/c$ for suitable $a' \in k_1$. For $n > 1$ we define $s' \in S_{n-1}$ by setting $s'(i) = s(i+1)$ for $1 \leq i \leq n-1$. Then for suitable $a' \in k_2$ we have

$$a \omega_s = a'(dc/c) \wedge \omega_{s'} \in \Omega_{k_2|k_0}^n. \quad (17)$$

In the case $n = 1$ we shall show that $a' \in \mathbf{F}_p$, which will conclude the proof. For $n > 1$ our goal is to show that $\omega_{s'}$ satisfies

$$(a'^p - a') \omega_{s'} \in \Omega_{K|k, < s'}^{n-1} + B_{K|k}^{n-1}. \quad (18)$$

Once this is established, we can apply induction on n to find

$$a' \omega_{s'} = v' + x' \quad (19)$$

for suitable $v' \in \Omega_{K|k, < s'}^{n-1}$ and $x' \in \text{Im}(\text{dlog})$. Note that $dc/c \wedge v' \in \Omega_{K|k, < s}^n$ because c and $b_{s(1)}$ differ only by a constant in $k_1 \subset K$. On the other hand, the kernel of the projection $\Omega_{K|k}^n \rightarrow \Omega_{K|k_0}^n$ lies in $\Omega_{K|k, < s}^n$ by definition of k_0 , so that (17) may be rewritten as

$$a \omega_s = a'(dc/c) \wedge \omega_{s'} + \omega_1 \in \Omega_{K|k}^n \quad \text{with } \omega_1 \in \Omega_{K|k, < s}^n.$$

In view of this formula the proposition will follow from (19) after wedge product with dc/c .

In the direction of (18) we first investigate what additional property the special choice of c implies for a' . For this, write k_2 as a direct sum $k_2 = k_1 \oplus V$, where $V \subset k_2$ is the natural complement of k_1 generated by nontrivial products of the basis elements in $\{b_i : i > s(1)\}$. Write $a' = \sum_{j=0}^{p-1} \alpha_j c^j + a'_1$ with $a'_1 \in V$, $\alpha_i \in k_0$. We contend that here $\alpha_j = 0$ for $j > 0$. Indeed, if $\alpha_j \neq 0$ for some $j > 0$, consider the element

$$c^{p-j} a'(dc/c) \wedge \omega_{s'} \wedge \omega_m \in \Omega_{k_2|k_0}^N \quad (20)$$

and apply the decomposition of Proposition 9.4.6 (2) to the extension $k_2|k_0$ and the p -basis $\{c, b_i : i > s(1)\}$. By our assumption on α_j the element (20) has a nontrivial component in $\Omega_{k_2|k_0}^N(0)$. On the other hand, (16) with $i = p - j$ together with (17) imply that the element (20) lies in $B_{k_2|k_0}^N$. This however contradicts the first part of Proposition 9.4.6 (3) according to which $\Omega_{k_2|k_0}^N(0)$ has trivial differentials. We have thus proven that

$$a' = \alpha_0 + a'_1 \text{ with } \alpha_0 \in k_0, a'_1 \in V. \quad (21)$$

This being said, we apply $\gamma - 1 : \Omega_{k_2|k_0}^n \rightarrow \Omega_{k_2|k_0}^n / B_{k_2|k_0}^n$ to the equation (17) and obtain

$$(a^p - a)\omega_s = (a'^p - a')(dc/c) \wedge \omega_{s'} \text{ mod } B_{k_2|k_0}^n,$$

whence by comparison with (14)

$$(a'^p - a')(dc/c) \wedge \omega_{s'} \in \Omega_{k_2|k_0, < s}^n \text{ mod } B_{k_2|k_0}^n. \quad (22)$$

Wedge product with ω_m therefore shows that the element

$$(a'^p - a')(dc/c) \wedge \omega_{s'} \wedge \omega_m \quad (23)$$

lies in $B_{k_2|k_0}^n$, since $\omega_m \wedge \Omega_{k_2|k_0, < s}^n = 0$ as already noted. In the decomposition of Proposition 9.4.6, the component of the element (23) lying in $\Omega_{k_2|k_0}^N(0)$ is

$$(a'^p - \alpha_0)(dc/c) \wedge \omega_{s'} \wedge \omega_m,$$

with α_0 as in (21). But by Proposition 9.4.6 (3) we have $\Omega_{k_2|k_0}^N(0) \cap B_{k_2|k_0}^N = 0$. Since $(dc/c) \wedge \omega_{s'} \wedge \omega_m$ generates the 1-dimensional k_2 -vector space $\Omega_{k_2|k_0}^N$, we conclude that $a'^p - \alpha_0$ must be 0. Comparison with (21) yields

$$a'^p - a' = -a'_1. \quad (24)$$

All the above holds in the case $n = 1$ as well, with the modification that one should omit the component $\omega_{s'}$ everywhere. Since for $n = 1$ we have $k_2 = k_1$ and hence $V = 0$, equation (24) then reads $a'^p - a' = 0$, i.e. $a' \in \mathbf{F}_p$, as required.

We return to the case $n > 1$. Applying the differential d to (22) and taking (24) into account we obtain

$$d(a'_1 \omega_{s'}) \wedge (dc/c) \in B_{k_2|k_0, < s}^{n+1}.$$

Since dc/c differs from $db_{s(1)}/b_{s(1)}$ by a constant in $k_1 \subset k_2$, we have

$$\Omega_{k_2|k_0, < s}^n \subset \Omega_{k_2|k_0, < s'}^{n-1} \wedge (dc/c).$$

Thus we find $\omega \in \Omega_{k_2|k_0, < s'}^{n-1}$ such that $d(a'_1\omega_{s'}) \wedge (dc/c) = d\omega \wedge (dc/c)$, or in other words

$$d(a'_1\omega_{s'} - \omega) \wedge (dc/c) = 0.$$

As dc/c is part of a basis of $\Omega_{k_2|k_0}^1$, this is only possible if

$$d(a'_1\omega_{s'} - \omega) = (dc/c) \wedge \omega_1 \in \Omega_{k_2|k_0}^n$$

for a suitable $\omega_1 \in \Omega_{k_2|k_0}^{n-1}$ (see the end of the proof of Proposition 9.7.2 below for details on this type of argument). So since $c \in k_1$, the element $d(a'_1\omega_{s'} - \omega)$ vanishes in $\Omega_{k_2|k_1}^n$.

Consider the decomposition of $\Omega_{k_2|k_1}^{n-1}$ coming from the p -basis $\{b_i : i > s(1)\}$ as in Proposition 9.4.6. Since $a'_1 \notin k_1$, we see that $a'_1\omega_{s'}$ has trivial projection to $\Omega_{k_2|k_1}^{n-1}(0)$. This may not be the case for ω , but since $d(\Omega_{k_2|k_1}^{n-1}(0)) = 0$ by Proposition 9.4.6 (3), we may modify ω by an element of $\Omega_{k_2|k_1}^{n-1}(0)$ without affecting the condition $d(a'_1\omega_{s'} - \omega) = 0$. Thus we may assume that $a'_1\omega_{s'} - \omega$ avoids $\Omega_{k_2|k_1}^{n-1}(0)$, and therefore $a'_1\omega_{s'} - \omega \in B_{k_2|k_1}^{n-1}$ by the statement of Proposition 9.4.6 (3) about the other components. Since $\omega \in \Omega_{k_2|k_0, < s'}^{n-1}$, we obtain

$$a'_1\omega_{s'} \in \Omega_{k_2|k_1, < s'}^{n-1} + B_{k_2|k_1}^{n-1},$$

so by (24)

$$(a'^p - a')\omega_{s'} \in \Omega_{k_2|k_1, < s'}^{n-1} + B_{k_2|k_1}^{n-1}.$$

As the kernel of the projection $\Omega_K^{n-1} \rightarrow \Omega_{K|k_1}^{n-1}$ is contained in $\Omega_{K, < s'}^{n-1}$, this implies (18) and concludes the proof. \square

Remark 9.6.6 We record for later use the following byproduct of the above proof. Under the assumption of Proposition 9.6.5 there exist elements $a' \in K$, $\tau \in \Omega_{K, < s}^n$ and $c \in k_1$ such that up to replacing K by a finite extension K' of degree prime to p we have

$$a\omega_s = a'\omega_{s'} \wedge (dc/c) + \tau \quad \text{and} \quad (a'^p - a')\omega_{s'} \in \Omega_{K, < s'}^{n-1} + B_K^{n-1}$$

for $n > 1$, and for $n = 1$ we have $a\omega_s = a'(dc/c) + \tau$ with $a' \in \mathbf{F}_p$. This comes from (17) and (18), the element τ being an element in the kernel of $\Omega_K^n \rightarrow \Omega_{K|k_0}^n$ which is a subset of $\Omega_{K, < s}^n$ by definition of k_0 .

Note moreover that the finite extension $K'|K$ we allow may be chosen to be a tower of Galois extensions. This is seen as follows: $K'|K$ arises by adjoining the $(p-1)$ -st root u of an element in K in the proof of Proposition 9.6.3. This may not be Galois over K , but embeds in $K(\zeta)(u)|K$, where ζ is a primitive $(p-1)$ -st root of unity. The latter extension still has prime to p degree and is a tower of Galois extensions.

9.7 Injectivity of the Differential Symbol

Now that the surjectivity statement of Theorem 9.5.2 is established, we turn to injectivity. For brevity's sake introduce the notation

$$k_n(K) := K_n^M(K)/pK_n^M(K).$$

We then have to prove:

Theorem 9.7.1 *The differential symbol $\psi_K^n : k_n(K) \rightarrow \nu(n)_K$ is injective.*

The first step in the proof is the following analogue of Proposition 7.5.6 (1).

Proposition 9.7.2 *Assume that the differential symbols $\psi_K^n : k_n(K) \rightarrow \nu(n)_K$ and ψ_L^{n-1} are injective, where $L|K$ is an arbitrary finite extension. Then so is $\psi_{K(t)}^n : k_n(K(t)) \rightarrow \nu(n)_{K(t)}$ for a purely transcendental extension $K(t)$.*

Proof: We first construct a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & k_n(K) & \longrightarrow & k_n(K(t)) & \xrightarrow{\oplus \partial_P} & \bigoplus_{P \in (\mathbf{A}_K^1)_0} k_{n-1}(\kappa(P)) & \longrightarrow & 0 \\ & & \psi_K^n \downarrow & & \psi_{K(t)}^n \downarrow & & \oplus i_P \downarrow & & \\ 0 & \longrightarrow & \Omega_{K[t]}^n & \longrightarrow & \Omega_{K(t)}^n & \longrightarrow & \bigoplus_{P \in (\mathbf{A}_K^1)_0} \Omega_{K(t)}^n / \Omega_{K[t]_P}^n & & \end{array}$$

Here the upper row is the Milnor exact sequence modulo p (Theorem 7.2.1), and the lower row comes from the localisation property of differentials (Appendix, Proposition A.8.3 (2)), noting that $K[t]$ is the intersection of the $K[t]_P$. The maps i_P are defined as the composite of $\psi_{\kappa(P)}^{n-1}$ with the map $j_P : \Omega_{\kappa(P)}^{n-1} \rightarrow \Omega_{K(t)}^n / \Omega_{K[t]_P}^n$ given by

$$j_P(x_0 dx_1 \wedge \cdots \wedge dx_{n-1}) = \tilde{x}_0 d\tilde{x}_1 \wedge \cdots \wedge d\tilde{x}_{n-1} \wedge \pi_P^{-1} d\pi_P,$$

where π_P is a local parameter at P and the \tilde{x}_i are arbitrary liftings of the x_i to $K[t]_P$. The map does not depend on the choice of the liftings \tilde{x}_i , since an easy calculation shows that changing \tilde{x}_i to $\tilde{x}_i + u\pi_P$ with some unit in $K[t]_P$ changes the right hand side by an element in $\Omega_{K[t]_P}^n$ (the factor π_P^{-1} gets cancelled). Another easy calculation shows that the right hand square commutes up to a factor $(-1)^{n-1}$; commutativity of the left square is straightforward.

Now the left vertical map is injective by assumption; if we show injectivity of the maps i_P , that of $\psi_{K(t)}^n$ will follow. As $\psi_{\kappa(P)}^{n-1}$ is injective by assumption,

it remains to establish the injectivity of j_P . By definition, this is equivalent to the injectivity of the map $x_0 dx_1 \wedge \cdots \wedge dx_{n-1} \mapsto \tilde{x}_0 d\tilde{x}_1 \wedge \cdots \wedge d\tilde{x}_{n-1} \wedge d\pi_P$. By Proposition A.8.11 of the Appendix $\Omega_{K[t]_P}^1$ is a free $K[t]_P$ -module on a basis consisting of $d\pi_P$ and some other elements da_i ; a basis of $\Omega_{K[t]_P}^n$ is then given by n -fold exterior products of these forms. Hence for an element $\omega \in \Omega_{K[t]_P}^{n-1}$ the relation $\omega \wedge d\pi_P = 0$ can only hold if when writing ω as a linear combination of basis elements only those involving $d\pi_P$ have nonzero coefficient. But then the image of ω in $\Omega_{\kappa(P)}^{n-1}$ is 0, as required. \square

The idea of the proof of Theorem 9.7.1 in the general case is now the following. By Lemma 9.5.6 it is enough to consider the case of a field F finitely generated over \mathbf{F}_p . We apply induction on n , the case $n = 0$ being obvious. If d denotes the transcendence degree of F , then by Corollary A.3.6 of the Appendix there exists a scheme-theoretic point of codimension 1 on the affine space $\mathbf{A}_{\mathbf{F}_p}^{d+1}$ whose local ring R has residue field isomorphic to F . Note that R is a discrete valuation ring (being integrally closed of Krull dimension 1) whose fraction field is purely transcendental over \mathbf{F}_p . To proceed further, we need:

Construction 9.7.3 Let K be the fraction field of the above R , and M its maximal ideal. Define $k_n(R)$ to be the kernel of the residue map $\partial^M : k_n(K) \rightarrow k_{n-1}(F)$; note that it is generated by symbols whose entries are units in R by Proposition 7.1.7. It follows that the differential symbol ψ_K^n restricts to a map $\psi_R^n : k_n(R) \rightarrow \nu(n)_R$, where $\nu(n)_R$ is the kernel of the operator $\gamma - 1 : \Omega_R^n \rightarrow \Omega_R^n/B_R^n$ (see Remark 9.4.5). Denote by $k_n(R, M)$ the kernel of the specialisation map $s_R : k_n(R) \rightarrow k_n(F)$ (which does not depend on generators of M by Remark 7.1.9), and by $\nu(n)_{R, M}$ that of the reduction map $\rho_R : \nu(n)_R \rightarrow \nu(n)_F$. The easy compatibility $s_R \circ \psi_R^n = \psi_F^n \circ s_R$ implies that ψ_R^n restricts to a map $\psi_{R, M}^n : k_n(R, M) \rightarrow \nu(n)_{R, M}$.

Lemma 9.7.4 *With notations as above, assume that the differential symbol $\psi_{R, M}^n : k_n(R, M) \rightarrow \nu(n)_{R, M}$ is surjective. Then the symbol h_F^n is injective.*

Proof: We have the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & k_n(R, M) & \longrightarrow & k_n(R) & \longrightarrow & k_n(F) \longrightarrow 0 \\ & & \psi_{R, M}^n \downarrow & & \psi_R^n \downarrow & & \psi_F^n \downarrow \\ 0 & \longrightarrow & \nu(n)_{R, M} & \longrightarrow & \nu(n)_R & \longrightarrow & \nu(n)_F. \end{array}$$

By Proposition 9.7.2 and our inductive assumption on n the middle vertical map is injective, so the lemma follows by diagram chase. \square

Thus in order to prove Theorem 9.7.1 it suffices to prove the surjectivity of $k_n(R, M) \rightarrow \nu(n)_{R,M}$. In the course of the proof we shall be forced to make finite extensions of the fraction field of R , and the integral closure of R in these extensions will not be local any more, but in general only a semi-local Dedekind ring, i.e. a Dedekind ring with finitely many maximal ideals. We therefore have to extend the statement to these.

Construction 9.7.5 If R is a semi-local Dedekind ring with maximal ideals M_1, \dots, M_r , denote by $I = \cap M_i$ its Jacobson radical. By the Chinese Remainder Theorem $R/I \cong \bigoplus R/M_i$; in particular, it is a direct sum of fields. Therefore we may define $K_n^M(R/I)$ as the direct sum of the $K_n^M(R/M_i)$ and denote its mod p quotient by $k_n(R/I)$. The group $k_n(R) \subset k_n(K)$ is defined as the intersection of the kernels of the residue maps $k_n(K) \rightarrow k_{n-1}(R/M_i)$ associated with the localisations $R_i := R_{M_i}$ of R ; it is generated by symbols coming from the units of R . The group $k_n(R, I)$ is defined as the kernel of the direct sum of specialisation maps $\bigoplus_{s_{R_i}} : k_n(R) \rightarrow \bigoplus k_n(R/M_i)$. As in the case of discrete valuation rings, the symbol ψ_K^n restricts to a symbol $k_n(R) \rightarrow \nu(n)_R$; it is compatible with the direct sum of the symbols ψ_{R/M_i}^n via the specialisation maps. Hence it restricts to a symbol $\psi_{R,I}^n : k_n(R, I) \rightarrow \nu(n)_{R,I}$, where the latter group is the kernel of the map $\nu(n)_R \rightarrow \bigoplus \nu(n)_{R/M_i}$.

Therefore the statement to be proven is:

Proposition 9.7.6 *Let k be a perfect field of characteristic $p > 0$, and R a semi-local Dedekind domain which is obtained as a localisation of a finitely generated k -algebra. Then the differential symbol*

$$\psi_{R,I}^n : k_n(R, I) \rightarrow \nu(n)_{R,I}$$

is surjective.

We first prove some preliminary lemmas.

Lemma 9.7.7 *For R as in the proposition the R -module $\Omega_R^1 = \Omega_{R|k}^1$ is free of finite rank.*

Proof: For each maximal ideal M of R the localisation R_M is a discrete valuation ring, hence $\Omega_{R_M|k}^1$ is free of finite rank by Proposition A.8.5 of the Appendix. It follows that $\Omega_{R|k}^1$ is a finitely generated projective R -module, by Matsumura [1], 7.12 together with Proposition A.8.3 (2) of the Appendix. But then it must be free, since R is semi-local (see Matsumura [1], Theorem 2.5 for the local case; the same proof works in general). \square

Lemma 9.7.8 *Let K be the fraction field of R , and let $K'|K$ be a finite extension of degree prime to p which is a tower of Galois extensions. Let R' be the normalisation of R in K , and denote by I' the Jacobson radical of R' . If the differential symbol $\psi_{R',I'}^n$ is surjective, then so is $\psi_{R,I}^n$.*

Proof: This will follow by the same norm argument as in Proposition 9.5.5, once we show that the norm and trace maps of Lemma 9.5.4 restrict to $k_n(R', I')$ and $\nu(n)_{R',I'}$, giving rise to a commutative diagram

$$\begin{array}{ccc} k_n(R', I') & \xrightarrow{\psi_{R',I'}^n} & \nu(n)_{R',I'} \\ N_{R'|R} \downarrow & & \text{tr} \downarrow \\ k_n(R, I) & \xrightarrow{\psi_{R,I}^n} & \nu(n)_{R,I}. \end{array} \quad (25)$$

To check this, note first that the norm map $N_{K'|K} : k_n(K') \rightarrow k_n(K)$ restricts to a norm map $k_n(R') \rightarrow k_n(R)$ by Proposition 7.4.1 applied to the finitely many residue maps coming from the maximal ideals of R' . It further restricts to a map $k_n(R', I') \rightarrow k_n(R, I)$ using Corollary 7.4.2 (note that it applies since the ramification is tame at each maximal ideal of R by our assumption on $K'|K$ and Corollary A.6.6 of the Appendix). On the other hand, consider the diagram

$$\begin{array}{ccccc} k_n(R') & \xrightarrow{\psi_{R'}^n} & \Omega_{R'}^n & \longrightarrow & \Omega_{K'}^n \\ N_{R'|R} \downarrow & & & & \text{tr} \downarrow \\ k_n(R) & \xrightarrow{\psi_R^n} & \Omega_R^n & \longrightarrow & \Omega_K^n \end{array}$$

where the outer rectangle commutes by virtue of Lemma 9.5.4. It follows from Lemma 9.7.7 that $\Omega_{R'}^n$ and Ω_R^n are free of finite rank, and therefore the horizontal arrows in the right half of the diagram are injective. From this we obtain that the trace map on $\Omega_{K'}^n$ restricts to a map $\text{Im}(\psi_{R'}^n) \rightarrow \text{Im}(\psi_R^n)$. Using compatibilities with specialisation maps one checks that this map sends $\text{Im}(\psi_{R',I'}^n)$ into $\text{Im}(\psi_{R,I}^n)$. By our assumption we have $\text{Im}(\psi_{R',I'}^n) = \nu_{R',I'}^n$, whence the existence of the commutative diagram (25). \square

Another important ingredient in the proof will be the following integral version of Theorem 9.2.2.

Lemma 9.7.9 *Let $R \supset T$ be an extension of semi-local Dedekind rings which arise as localisations of finitely generated algebras over a perfect field k of characteristic $p > 0$. Assume that the arising extension $K|K_0$ of fraction*

fields is finite, and moreover $R^p \subset T$. Then the sequence

$$0 \rightarrow R^\times/T^\times \xrightarrow{\text{dlog}} \Omega_{R|T}^1 \xrightarrow{\gamma_R-1} \Omega_{R|T}^1/B_{R|T}^1$$

is exact, where R^\times (resp. T^\times) denotes the units in R (resp. T).

Proof: Given $\omega \in \ker(\gamma_R - 1)$, we have $\omega = \text{dlog}(f)$ in $\Omega_{K|K_0}^1$ for some f in K^\times by Theorem 9.3.3. Note that R is a principal ideal domain, with prime elements the generators t_i of the finitely many maximal ideals M_1, \dots, M_r (see Matsumura [1], Ex. 11.7). Up to multiplying f with a sufficiently high power of $(t_1 \dots t_r)^p$ we may assume $f \in R$. We now show that $f \in R^\times$, which is equivalent to showing that $f \notin M_i$ for all i . Assume $f \in M_i$ for some i . Then $f = ut_i^m$ for some $m > 0$ with some $u \in R \setminus M_i$; up to dividing f by a power of t_i^p we may assume $(m, p) = 1$. But then $\text{dlog}(f) = (du/u) + m(dt_i/t_i)$ in $\Omega_{K|K_0}^1$. Now notice that dt_i/t_i does not lie in $\Omega_{R_{M_i}|(R_{M_i} \cap K_0)}^1$. Indeed, applying Proposition A.8.3 (4) of the Appendix with $A = k$, $B = R_{M_i}$ and $I = M_i R_{M_i}$ yields that $\Omega_{R_{M_i}|k}^1 \otimes_{R_{M_i}} R/M_i$ has a basis consisting of dt_i and a basis of $\Omega_{(R/M_i)|k}^1$. Hence by Nakayama's lemma (Lang [3], Chapter X, Lemma 4.3) these elements generate $\Omega_{R_{M_i}|k}^1$ and a fortiori $\Omega_{R_{M_i}|(R_{M_i} \cap K_0)}^1$. If dt_i/t_i were an element of this module, then writing it in terms of the above basis we would get $dt_i \in M_i \Omega_{R_{M_i}|(R_{M_i} \cap K_0)}^1$, a contradiction. All in all, we obtain that ω and du/u lie in $\Omega_{R_{M_i}|(R_{M_i} \cap K_0)}^1$ but $m(dt_i/t_i)$ doesn't, which contradicts $\omega = \text{dlog}(f)$ and thus proves the lemma. \square

Finally an easy lemma from Milnor K-theory:

Lemma 9.7.10 *Let M be a maximal ideal of R and R_M the associated localisation. Then for all integers $m, m' > 0$ the product operation*

$$k_m(K) \otimes k_{m'}(K) \rightarrow k_{m+m'}(K)$$

sends $k_m(R_M, MR_M) \otimes k_{m'}(K)$ into $k_{m+m'}(R_M, MR_M)$.

Proof: Note that R_M is a discrete valuation ring. By induction we may assume that $m' = 1$. The group $k_1(K)$ is generated by $k_1(R_M)$ and a local parameter π for M . Since $k_m(R_M, MR_M) \otimes k_1(R_M) \subset k_{m+1}(R_M, MR_M)$, it remains to show that $k_m(R_M, MR_M) \otimes \{\pi\} \subset k_{m+1}(R_M, MR_M)$. Take α in $k_n(R_M, MR_M)$. Then $\partial_M(\{\pi, \alpha\}) = s_{-\pi}(\alpha) = 0$ in $k_n(R/M)$, and therefore $\{\pi, \alpha\} \in k_n(R_M)$. But $s_\pi(\{\pi, \alpha\}) = 0$ as well, so $\{\alpha, \pi\} = (-1)^{m-1} \{\pi, \alpha\}$ lies in $k_{n+1}(R_M, MR_M)$. \square

We now begin the proof of Proposition 9.7.6. The first step is again to choose a suitable p -basis of K .

Lemma 9.7.11 *There exist units b_1, \dots, b_{r-1} in R and a generator b_r of I so that db_1, \dots, db_r form a basis of the free R -module Ω_R^1 , and the mod I images of db_1, \dots, db_{r-1} form a basis of $\Omega_{R/I}^1$.*

Here recall that R/I is a direct sum of fields.

Proof: Take a p -basis $\bar{b}_1, \dots, \bar{b}_{r-1}$ of R/I . By multiplying with a suitable nonsingular matrix with entries in \mathbf{F}_p^\times we may ensure that each \bar{b}_i has nonzero components in the direct sum decomposition $R/I \cong \bigoplus R/M_i$. This implies that if we take arbitrary liftings b_1, \dots, b_{r-1} of the \bar{b}_i , then the b_i are units in R . Moreover, an argument using the exact sequence

$$I/I^2 \xrightarrow{\delta} \Omega_{R|k}^1 \otimes_R R/I \rightarrow \Omega_{(R/I)|k}^1 \rightarrow 0$$

as in the second half of the proof of Lemma 9.7.9 shows that for any generator b_r of I the elements db_1, \dots, db_r generate Ω_R^1 . Note that the map δ in the above sequence must be injective, for if it were 0, then so would be the map $M_i/M_i^2 \rightarrow \Omega_{R M_i|k}^1 \otimes_{R M_i} R/M_i$ for any maximal ideal M_i of R , which would contradict Corollary A.8.6 of the Appendix. Thus db_1, \dots, db_r is a minimal generating system, and hence a basis of the free R -module Ω_R^1 . \square

Fix b_1, \dots, b_r as in the lemma above. By Propositions A.8.3 (2) and A.8.8 of the Appendix they form a p -basis of the extension $K|k$. From now on we take up the notations of the previous section. In particular, we put $\omega_s = (db_{s(1)}/b_{s(1)}) \wedge \cdots \wedge (db_{s(q)}/b_{s(q)})$ for a strictly increasing function $s : \{1, \dots, n\} \rightarrow \{1, \dots, r\}$. Recall that the w_s form a k -basis of Ω_K^n . An element $\sum a_s \omega_s \in \Omega_K$ lies in $\nu(n)(K)$ if and only if $\sum (a_s^p - a_s) \omega_s \in B_K^n$. Moreover, by our choice of the p -basis b_1, \dots, b_r the element $\sum a_s \omega_s$ lies in $\nu(n)(R, I)$ if and only if $a_s \in I$ for all s .

Our goal is then to prove:

Proposition 9.7.12 *Fix $a \in I$ and $s \in S_n$, and assume that*

$$(a^p - a) \omega_s \in \Omega_{K|k, < s}^n + B_{K|k}^n.$$

Then up to replacing K by some finite prime to p extension $K'|K$ which is a tower of Galois extensions, and R by its normalisation in K' , we have

$$a \omega_s \in \Omega_{K|k, < s}^n + \text{Im}(\psi_{R, I}^n).$$

This proposition implies Proposition 9.7.6 by exactly the same argument as Proposition 9.6.5 implies Theorem 9.6.1. So all that remains is to give its proof.

Proof: As in the proof of Proposition 9.6.5, write $k_0 := k(b_1, \dots, b_{s(1)-1})$ and $k_1 := k_0(b_{s(1)})$. According to Remark 9.6.6, there exist elements $a' \in K$, $\tau \in \Omega_{K, < s}^n$ and $c \in k_1$ such that up to replacing K by a finite extension of degree prime to p we have

$$a\omega_s = a'\omega_{s'} \wedge (dc/c) + \tau \tag{26}$$

and

$$(a'^p - a')\omega_{s'} \in \Omega_{K, < s'}^{n-1} + B_K^{n-1} \tag{27}$$

for $n > 1$, and for $n = 1$ we have $a\omega_s = a'(dc/c) + \tau$ with $a' \in \mathbf{F}_p$. We have seen during the proof of Proposition 9.6.5 that this statement implies $a\omega_s \in \text{Im}(\psi_K^n) \bmod \Omega_{K|k, < s}^n$ by induction, but in the present case we have to ensure that $a\omega_s \in \text{Im}(\psi_{R,I}^n) \bmod \Omega_{K|k, < s}^n$. This will be done by suitably modifying the element c .

Write

$$dc/c = \sum_{i=1}^{s(1)} \gamma_i(db_i/b_i)$$

in $\Omega_{k_1}^1$. It follows from (26) that $a = (-1)^{n-1}a'\gamma_{s(1)}$. In particular, since $a \in I$ and $a' \in \mathbf{F}_p$ for $n = 1$, we have $\gamma_{s(1)} \in I$ for $n = 1$. In the general case define ideals

$$J = \bigcap_{\gamma_{s(1)} \in M} M, \quad L = \bigcap_{J \not\subset M} M$$

in R , where M runs over the maximal ideals of R . Let R_J, R_L be the respective localizations, so that JR_J and LR_L are the Jacobson radicals. For $n = 1$ we have $I = J$ and $L = R$. In the general case we have $a' \in LR_L$ by construction.

Write $T := R_J \cap k_0$, and consider the commutative diagram

$$\begin{array}{ccc} \Omega_{R_J}^1 & \longrightarrow & \Omega_K^1 \\ \downarrow & & \downarrow \\ \Omega_{R_J|T}^1 & \longrightarrow & \Omega_{K|k_0}^1 \end{array}$$

where the vertical maps are the natural projections and the horizontal maps are injective by the localisation property of differentials. The forms dc/c and $\gamma_{s(1)}(db_{s(1)}/b_{s(1)})$ have the same image in $\Omega_{K|k_0}^1$; denote it by θ . Since dc/c is in the kernel of $\gamma_K - \text{id}$, this implies that θ lies in the kernel of the operator $\gamma_{R_J|T} - \text{id}$, the restriction of $\gamma_{K|k_0} - \text{id}$ to $\Omega_{R_J|T}^1$. Now put $H = R_J/JR_J$ and

$P = T/J \cap T$. As $\gamma_{s(1)} \in J$ by definition of J , the image of θ in $\Omega_{H|P}^1$ is trivial. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccc}
 & & 0 & & & & \\
 & & \downarrow & & & & \\
 & & (1 + JR_J)/(T^\times \cap (1 + JR_J)^\times) & & & & \\
 & & \downarrow & & & & \\
 0 & \longrightarrow & R_J^\times/T^\times & \xrightarrow{\text{dlog}} & \Omega_{R_J|T}^1 & \xrightarrow{\gamma-\text{id}} & \Omega_{R_J|T}^1/B_{R_J|T}^1 \\
 & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & H^\times/P^\times & \xrightarrow{\text{dlog}} & \Omega_{H|P}^1 & &
 \end{array}$$

where exactness of the middle row follows from Lemma 9.7.9. As θ is annihilated by both maps starting from $\Omega_{R_J|T}^1$, the diagram shows that there exists $\delta \in 1 + JR_J$ such that $\theta = \text{dlog}(\delta)$ in $\Omega_{R_J|T}^1$, whence

$$dc/c = d\delta/\delta + \eta \tag{28}$$

in Ω_K^1 with a suitable $\eta \in R_J \text{Im}(\Omega_T^1 \rightarrow \Omega_{R_J}^1)$. In particular, η is in the K -span of the image of $\Omega_{k_0}^1$ and thus lies in $\Omega_{K, < s(1)}^1$. In the case $n = 1$ the proof ends here, because the equality $J = I$ implies that $\delta \bmod p$ lies in $k_1(R, I)$ and so $d\delta/\delta \in \text{Im}(\psi_{R, I}^1)$. In the case $n > 1$ we only have that $\delta \bmod p$ lies in $k_1(R_J, JR_J)$. On the other hand, since $a' \in LR_L$ as noted before, we may use (27) to apply induction on n to $a'\omega_{s'}$ and obtain

$$a'\omega_{s'} \in \text{Im}(\psi_{R_L, LR_L}^{n-1}) + \Omega_{K, < s'}^{n-1}. \tag{29}$$

Since $\eta \in \Omega_{K, < s(1)}^1$, this implies $a'\omega_{s'} \wedge \eta \in \Omega_{K, < s}^n$, so that from (26), (28) and (29) we obtain

$$a\omega_s = \beta \wedge (d\delta/\delta) \pmod{\Omega_{K, < s}^n}$$

for some $\beta \in \text{Im}(\psi_{R_L, LR_L}^{n-1})$. Since $\delta \bmod p$ lies in $k_1(R_J, J)$, the proposition follows if we check that the natural product map $k_{n-1}(K) \otimes k_1(K) \rightarrow k_n(K)$ sends $k_{n-1}(R_L, LR_L) \otimes k_1(R_J, JR_J)$ to $k_n(R, I)$. Writing $k_n(R, I)$ as the intersection of the groups $k_n(R_M, MR_M)$ where M runs over the maximal ideals of R , it suffices to show that the image is contained in $k_n(R_M, MR_M)$ for each M . But by construction each R_M contains either R_J or R_L , so the claim follows from Lemma 9.7.10. \square

In case the reader felt a bit lost among the numerous reduction steps of the above proof of Theorem 9.7.1, we recapitulate the logical structure of the

argument: Proposition 9.7.12 just proven implies Proposition 9.7.6, which together with Proposition 9.7.2 and induction on n implies Theorem 9.7.1 via Lemma 9.7.4. Thus Theorem 9.7.1 is proven, and with it the theorem of Bloch, Kato and Gabber.

EXERCISES

1. Show that Proposition 9.1.2 is true for an arbitrary finite extension $K|k$, i.e. that the boundary map $\delta_n : H^1(k, \mathrm{PGL}_n) \rightarrow \mathrm{Br}(k)$ always induces a bijection

$$\ker(H^1(k, \mathrm{PGL}_n) \rightarrow H^1(K, \mathrm{PGL}_n)) \cong \mathrm{Br}(K|k),$$

where $n = [K : k]$.

2. Assume that $\mathrm{char}(k) = 2$. Let $A_1 = [a_1, b_1)$ and $A_2 = [a_2, b_2)$ be two central simple algebras of degree 2. Construct an explicit simple purely inseparable field extension $K|k$ which splits both A_1 and A_2 .
3. Let K be a field of characteristic zero complete with respect to a discrete valuation, with residue field κ of characteristic $p > 0$. Denote by A the valuation ring of K , by \tilde{A} the maximal unramified extension of A and by G the absolute Galois group $\mathrm{Gal}(\kappa_s|\kappa)$.
 - (a) Construct a natural isomorphism $H^2(G, \tilde{A}^\times) \xrightarrow{\sim} H^2(G, \kappa_s^\times) \cong \mathrm{Br}(\kappa)$ and a canonical embedding $\rho : \mathrm{Br}(\kappa) \hookrightarrow \mathrm{Br}(K)$. [*Hint*: Argue as in the proof of Proposition 6.3.1.]
 - (b) Show that ρ maps Brauer classes of cyclic κ -algebras to Brauer classes of cyclic K -algebras.
 - (c) Assume moreover that K contains the p -th roots of unity. Show without using the Merkurjev-Suslin theorem that the subgroup $\rho({}_p\mathrm{Br}(\kappa))$ lies in the image of the Galois symbol $h_{K,p}^2 : K_2^M(K)/pK_2^M(K) \rightarrow {}_p\mathrm{Br}(K)$.
4. Keeping the assumptions and the notations of the previous exercise, let A_1 be a central simple k -algebra, and let A_2 be a central simple K -algebra such that $[A_2] = \rho([A_1])$.
 - (a) Show that $\mathrm{ind}_K(A_2)$ divides $\mathrm{ind}_k(A_1)$. [*Hint*: Use Hensel's lemma and Proposition 4.5.8.]
 - (b) Let $K'|K$ be a finite Galois extension which splits A_2 , and let κ' be its residue field. Show that κ' is a splitting field of A_1 .
 - (c) Conclude that if A_2 is isomorphic to a cyclic algebra, then so is A_1 . [In particular, if $p = 2$ or 3 and A_1 has degree p , then A_1 is cyclic by Proposition 1.2.3 and Chapter 7, Exercise 9.]

5. (Katz) Let assumptions and notations be as in Theorem 9.3.6. This exercise gives an explicit formula for the projection $P : V \rightarrow V^\nabla$ whose existence is implied by the direct sum decomposition of V constructed in the proof of that theorem.

Let a_1, \dots, a_m be a p -basis of $K|k$ and ∂_i the derivation sending da_i to 1 and da_j to 0 for $i \neq j$. Define the map $P : V \rightarrow V$ by

$$P = \sum_{\lambda} \prod_{i=1}^m \left(\frac{(-a_i)^{\lambda_i}}{\lambda_i!} \right) \prod_{i=1}^m \nabla_* (\partial_i)^{\lambda_i},$$

where the sum is taken over all m -tuples $\lambda = (\lambda_1, \dots, \lambda_m) \in \mathbf{F}_p^m$. Show that $\text{Im}(P) \subset V^\nabla$ and P induces the identity map on V^∇ .

6. Let K be a field of characteristic $p > 0$ satisfying $[K : K^p] = p$. Let b be a generator of the extension $K|K^p$; then db generates the 1-dimensional K -vector space Ω_K^1 . Define a map $C_b : \Omega_K^1 \rightarrow \Omega_K^1$ as follows. Write $\omega \in \Omega_K^1$ uniquely as $\omega = fdb$ with $f \in K$, and let $c_0, \dots, c_{p-1} \in K$ be the unique elements with $f = \sum_{i=0}^{p-1} c_i^p b^i$. Then put $C_b(\omega) := c_{p-1} db$.

- (a) Show that C_b equals the Cartier operator $C : \Omega_K^1 \rightarrow \Omega_K^1$. [Note that $\Omega_K^1 = Z_K^1$ in this case.]
- (b) (Tate) Verify directly that C_b does not depend on the choice of b .

[*Remark:* The above construction of Tate [1] was the first explicit appearance of the Cartier operator. Serre [1] showed using this description that in the case when K is the function field of a curve X over an algebraically closed field, the restriction of the the map C to global 1-forms identifies to the dual of the Frobenius map on $H^1(X, \mathcal{O}_X)$ via the duality that bears his name.]

7. (suggested by Bouw and Wewers) This exercise gives a simple proof of a special case of Theorem 9.2.2. Let k be an algebraically closed field of characteristic $p > 0$, and consider the rational function field $k(t)$ as a subfield of $k((t))$. Let $f \in k(t)$ be a rational function with Laurent series expansion $f = \sum c_i t^i$, and put $\omega = f dt$.

- (a) Show that the following are equivalent:
- i. $\omega \in \ker(\gamma - \text{id})$;
 - ii. $f^p = -\partial_t^{p-1}(f)$, where ∂_t is derivation with respect to t ;
 - iii. $c_i^p = c_{(i+1)p-1}$ for all $i \in \mathbf{Z}$.
- (b) Deduce that if $\omega \in \ker(\gamma - \text{id})$, then $c_i = 0$ for $i < -1$ and $c_{-1} \in \mathbf{F}_p$.
- (c) Let $a_1, \dots, a_m \in k$ be the finite poles of f and $c_{-1,1}, \dots, c_{-1,m}$ the corresponding residues. Deduce from (b) that if $\omega \in \ker(\gamma - \text{id})$, then

$\omega = \sum c_{-1,j}(t - a_j)^{-1}dt$ and moreover $c_{-1,j} \in \mathbf{F}_p$. [*Hint:* Use the fact from algebraic geometry that there are no differential forms which are everywhere regular on the projective line.]

- (d) Conclude that $\omega \in \ker(\gamma - \text{id})$ if and only if $\omega = \text{dlog}(P)$ for a suitable polynomial $P \in k[t]$.
8. Let k be algebraically closed of characteristic $p > 0$, and let $k(y)|k(x)$ be the extension of rational function fields given by the Artin-Schreier equation $y^p - y = x$. Consider the differential 1-form $\omega = yx^{-1}dx$ in $\Omega_{k(y)}^1$.
- (a) Show that ω is a logarithmic 1-form.
- (b) Find an explicit polynomial $P \in k[y]$ such that $\omega = \text{dlog}(P)$. [*Hint:* Use the previous exercise and partial fraction decomposition.]

Appendix: A Breviary of Algebraic Geometry

This Appendix is strictly utilitarian: we have assembled here some basic notions from algebraic geometry and related algebra needed in the main text (except for the first three sections of Chapter 8, which are more advanced), mostly with references to standard textbooks. Accordingly, the treatment here is far from being the most general or elegant one; its sole purpose is to present the needed facts as quickly as possible. Readers should consult it at their peril.

A.1 Affine and Projective Varieties

In present-day literature by an *algebraic variety* one usually means a separated scheme of finite type over a field, together with a possible integrality condition. In most of this book we only need the notion of affine and projective varieties, which may be defined in a more elementary way. As in the standard texts they are usually discussed only over an algebraically closed base field, we briefly recall the basics.

In the sequel k will be a field, and \bar{k} a fixed algebraic closure of k . Points of *affine n -space* \mathbf{A}_k^n over \bar{k} may be identified with \bar{k}^n . An *affine closed subset* of \mathbf{A}_k^n is defined as the locus of common zeroes of a finite set of polynomials $f_1, \dots, f_m \in \bar{k}[x_1, \dots, x_n]$; we denote it by $X = V(f_1, \dots, f_m)$. The f_i are of course not uniquely determined by X . We say that X is *defined over k* if there is a representation $X = V(f_1, \dots, f_m)$ with $f_i \in k[x_1, \dots, x_n]$ for all i . In this case the quotient ring $\mathcal{O}(X) := k[x_1, \dots, x_n]/(f_1, \dots, f_m)$ is called the *coordinate ring* of X . Moreover, if the ideal $I(X) := (f_1, \dots, f_m)$ is a prime ideal in $k[x_1, \dots, x_n]$ and the ring $\mathcal{O}(X) \otimes_k \bar{k}$ has no nilpotent elements, we say that X is an *affine variety* defined over k . Note that this does not necessarily imply that it is also an affine variety over \bar{k} (think of the ideal $(x^2 + 1)$ in $\mathbf{R}[x]$). Therefore from now on we employ the notation $X_{\bar{k}}$ for X considered as an affine closed set over \bar{k} . More generally, for an algebraic extension $k \subset L \subset \bar{k}$ we define the *base change* X_L of X to L as the closed set defined over L by (f_1, \dots, f_m) , with the f_i regarded as polynomials with coefficients in L . This looks bizarre at first sight, but notice the difference in

the coordinate rings: $\mathcal{O}(X_L) \cong \mathcal{O}(X) \otimes_k L$.

In general the partially ordered set of prime ideals in $k[x_1, \dots, x_n]$ containing $I(X)$ has finitely many minimal elements; the varieties determined by these are called the *irreducible components* of X over k . Over \bar{k} the irreducible components are irreducible closed subsets in $\mathbf{A}_{\bar{k}}^n$, i.e. they cannot be written as a union of two proper closed subsets. The system of affine closed sets defined over k is closed under finite unions and arbitrary intersections, and hence it defines a topology on \mathbf{A}_k^n called the *Zariski topology*. Subsets of \mathbf{A}_k^n are always equipped with the induced topology. If $Y \subset X$ are affine varieties and Y is closed in the Zariski topology of X , we say that Y is a *closed subvariety* of X .

Over \bar{k} , a point $P = (a_1, \dots, a_n)$ of $\mathbf{A}_{\bar{k}}^n$ corresponds to the maximal ideal $(x_1 - a_1, \dots, x_n - a_n)$ in $\bar{k}[x_1, \dots, x_n]$, so it is an affine variety. By Hilbert's Nullstellensatz (Matsumura [1], Theorem 5.3) all maximal ideals in $\bar{k}[x_1, \dots, x_n]$ are of this form. Now let X be an affine closed set over k . In the theory of schemes one considers all prime ideals containing $I(X)$ as points of X ; we refer to these as *scheme-theoretic points*. A scheme-theoretic point P such that $(k[x_1, \dots, x_n]/P) \otimes_k \bar{k}$ has no nilpotents corresponds to a closed subvariety Y of X . In this situation we say that P is the *generic point* of Y . Scheme-theoretic points correspond bijectively to prime ideals of the coordinate ring $\mathcal{O}(X)$ of X . Of particular interest are the scheme-theoretic points associated with maximal ideals; these are called *closed points*. By a more general form of the Nullstellensatz (same reference as above), their residue fields are finite extensions L of k ; in this situation we speak of *points defined over L* . In the case $L = k$ they are called *k -rational points* or *k -points* for short. By the above, over \bar{k} all closed points are \bar{k} -rational.

We now move on to projective varieties. Points of *projective n -space* $\mathbf{P}_{\bar{k}}^n$ over \bar{k} may be identified with the elements in $\bar{k}^{n+1} \setminus \{(0, \dots, 0)\}$ modulo the equivalence relation $(a_1, \dots, a_{n+1}) \sim (\lambda a_1, \dots, \lambda a_{n+1})$ for $\lambda \neq 0$. A *projective closed subset* $X = V(F_1, \dots, F_m)$ in $\mathbf{P}_{\bar{k}}^n$ is defined as the locus of common zeroes of a finite set of *homogeneous* polynomials $F_1, \dots, F_m \in \bar{k}[x_1, \dots, x_{n+1}]$. We say that X is *defined over k* if there is a representation with the F_i lying in $k[x_1, \dots, x_{n+1}]$ for all i ; the quotient $\mathcal{O}(X) := k[x_0, \dots, x_n]/(F_1, \dots, F_m)$ is its *homogeneous coordinate ring*. Projective closed subsets define the Zariski topology of \mathbf{P}^n . If the ideal $I(X) := (F_1, \dots, F_m)$ is a prime ideal in $k[x_1, \dots, x_{n+1}]$ and $\mathcal{O}(X) \otimes_k \bar{k}$ has no nilpotent elements, we say that X is a *projective variety* over k . Henceforth by a 'variety' we shall mean an affine or a projective variety, but in fact all results stated for varieties will hold with the more general definition alluded to at the beginning of this section. Also, notice that the spaces $\mathbf{A}_{\bar{k}}^n$ and $\mathbf{P}_{\bar{k}}^n$ are both k -varieties (they are even defined over the prime field of k), so we drop the subscripts k and \bar{k} in the sequel if

clear from the context.

Projective n -space \mathbf{P}^n has a standard open covering by $n + 1$ copies of \mathbf{A}^n , defined by $D_+(x_i) := \mathbf{P}^n \setminus V(x_i)$. The inclusions $D_+(x_i) \hookrightarrow \mathbf{P}^n$ are homeomorphisms in the Zariski topology. Therefore each projective closed set X has a standard open covering by affine closed sets $X^{(i)} := X \cap D_+(x_i)$. We define its scheme-theoretic points (resp. closed points, k -rational points) as the union of those of the $X^{(i)}$; one checks that this notion does not depend on the choice of i . Scheme-theoretic points correspond to closed subvarieties in the projective case as well (this follows from the easy topological fact that $Y \subset X$ is closed if and only if the $Y \cap D_+(x_i)$ are closed in the $X \cap D_+(x_i)$), so the notion of generic point extends to the projective case.

Proposition A.1.1 *Assume that k is separably closed. Then each variety defined over k has a k -rational point. Moreover, k -rational points are dense in the Zariski topology of X .*

Proof: See Springer [1], Theorem 11.2.7. The learned reader may concoct another proof using the fact (Mumford [1], Section III.6, Theorem 1) that X contains a dense open subvariety equipped with an étale morphism onto an open subset of some affine space (which of course has a dense subset of k -points). \square

The *local ring* $\mathcal{O}_{X,P}$ of a scheme-theoretic point P on an affine variety X is defined as the localisation of $\mathcal{O}(X)$ by the prime ideal P . If $Y \subset X$ is the closed subvariety coming from P , one also speaks of the *local ring of the subvariety* Y and uses the notation $\mathcal{O}_{X,Y}$ for $\mathcal{O}_{X,P}$. The residue field $\kappa(P)$ of this local ring is the *residue field* of the point P ; for closed points it is a finite extension of k . In the case of a closed point P we say that P is a *smooth point* if the Jacobian matrix of a minimal system of generators of P has a maximal subdeterminant whose image in $\kappa(P)$ is nonzero; one checks that this does not depend on the choice of the generators. The non-smooth points are called *singular points*. They form a Zariski closed subset in X (meaning that the singular points of $X_{\bar{k}}$ form a closed subset defined over k) defined by the vanishing of the maximal subdeterminants. This subset is the *singular locus* of X ; if it is empty, we say that X is *smooth over k* .

For a projective variety X one defines the local ring of a scheme-theoretic point P as $\mathcal{O}_{X^{(i)},P}$ for an $X^{(i)}$ containing P ; one checks that it does not depend on i . Likewise, the notion of smooth closed points extends to the projective case. The *function field* $k(X)$ of a variety X defined over k is defined as the common fraction field of its local rings.

A.2 Maps Between Varieties

A *rational function* f on a variety X is an element of its function field $k(X)$. If P is a closed point and $f \in \mathcal{O}_{X,P}$, we may define its *evaluation* $f(P)$ at P as the image of f in the residue field $\kappa(P)$. If P is a k -rational point, then $\kappa(P) = k$ and this is an honest evaluation map. Indeed, the local ring $\mathcal{O}_{X,P}$ being a localisation of $\mathcal{O}(X)$, we may represent f by a quotient of polynomials whose denominator does not vanish at P , and the maximal ideal of $\mathcal{O}_{X,P}$ consists of functions vanishing at P .

Let X be a variety (affine or projective) over k . A *rational map* $X \rightarrow \mathbf{P}^n$ is given by an $(n+1)$ -tuple $\phi = (f_0, \dots, f_n) \in k(X)^{n+1}$ of rational functions, not all identically 0. Two $(n+1)$ -tuples (f_0, \dots, f_n) and (g_0, \dots, g_n) define the same rational map if there exists a rational function $g \in k(X)$ with $f_i = gg_i$ for all i . We say that ϕ is *regular* at a closed point P of X if it may be represented by an $(n+1)$ -tuple (f_0, \dots, f_n) with $f_i \in \mathcal{O}_{X,P}$ for all i and $f_i(P) \neq 0$ for some i . When ϕ is regular at all closed points of X , we say that ϕ is a *morphism*. If $Y \subset \mathbf{P}^n$ is another variety (in the affine case embed it in \mathbf{P}^n by identifying \mathbf{A}^n with $D_+(x_0)$), by a rational map (resp. morphism) $X \rightarrow Y$ we mean a rational map (resp. morphism) $X \rightarrow \mathbf{P}^n$ as above, so that moreover after passing to \bar{k} we have $(f_0(P), \dots, f_n(P)) \in Y_{\bar{k}}$ for all closed points $P \in X_{\bar{k}}$ where ϕ is regular.

In the case when X is projective, we may represent rational functions on X by quotients of homogeneous polynomials of the same degree (see Shafarevich [2], Chapter I, Section 4.3). Hence by multiplying with a common denominator, we may represent rational maps $X \rightarrow \mathbf{P}^n$ by an $(n+1)$ -tuple of homogeneous polynomials of the same degree d .

Example A.2.1 Fix positive integers n and d , and put $N = \binom{n+d}{d} - 1$. We define the *d-uple* (or *Veronese*) embedding $\phi_d : \mathbf{P}^n \rightarrow \mathbf{P}^N$ by setting $\phi_d = (x_0^d, \dots, x_0^{i_0} \cdots x_n^{i_n}, \dots, x_n^d)$, where we have listed in lexicographic order all monomials of degree d in x_0, \dots, x_n . One checks that ϕ_d is a morphism which embeds \mathbf{P}^n as a closed subvariety into \mathbf{P}^N (see Shafarevich [2], Chapter I, Section 4.4). The homogeneous coordinate ring of $\phi_d(X)$ may be identified with the free k -algebra generated by monomials of degree d .

In the case when $\phi : X \rightarrow Y$ is a morphism so that there is a morphism $\psi : Y \rightarrow X$ with $\phi \circ \psi$ and $\psi \circ \phi$ identity maps, we say that ϕ is an *isomorphism* between X and Y . Not surprisingly, isomorphisms $X \rightarrow X$ are called *automorphisms*.

Example A.2.2 All automorphisms of \mathbf{P}^n are linear, i.e. defined by linear polynomials. In other words, we may identify the automorphism group of *the*

projective variety \mathbf{P}^n with the group $\mathrm{PGL}_n(k)$. See Hartshorne [1], Example II.7.1.1 for a proof.

A rational map $\phi : X \rightarrow Y$ is said to be *birational* if its image in Y is dense in the Zariski topology (after passing to \bar{k}) and there is a rational map $\psi : Y \rightarrow X$ with $\phi \circ \psi$ and $\psi \circ \phi$ identity maps at all points where they are regular. Note that these points form open subsets in X , resp. Y : they are the complements of the zero loci of the possible denominators of the rational functions involved. Thus a birational map is actually bijective on points in a Zariski open subset. Another criterion for birationality is that the map $\phi^* : k(Y) \rightarrow k(X)$ induced by composing rational functions with ϕ is an isomorphism (see Shafarevich [2], Chapter II, Section 4.3). We need the simplest nontrivial example of a birational map, that of blowing up a point in projective space.

Example A.2.3 Assume that k is algebraically closed. Given two integers $m, n > 0$, set $N := nm + n + m$. One defines the *product* $\mathbf{P}^n \times \mathbf{P}^m$ of projective spaces as the closed subvariety in \mathbf{P}^N obtained as the image of the *Segre embedding* $S_{n,m} : \mathbf{P}^n \times \mathbf{P}^m \rightarrow \mathbf{P}^N$. By definition, $S_{n,m}$ sends the pair $((x_0, \dots, x_n), (y_0, \dots, y_m))$ of points given in homogeneous coordinates to $(x_0y_0, \dots, x_iy_j, \dots, x_ny_m)$ (with the lexicographic order). For the fact that this is (set-theoretically) an embedding with Zariski closed image we refer to Shafarevich [2], Chapter I, Section 5.1. We keep the coordinates $(x_0, \dots, x_n, y_0, \dots, y_m)$ for points in the product.

Now set $m = n - 1$ and $P_0 = (0, \dots, 0, 1) \in \mathbf{P}^n$. The *blowup* $B_{P_0}(\mathbf{P}^n)$ of \mathbf{P}^n at P_0 is the closed subvariety of $\mathbf{P}^n \times \mathbf{P}^{n-1}$ defined by the polynomials $x_iy_j - x_jy_i$ for all possible $0 \leq i, j \leq n - 1$. The projection $\pi : \mathbf{P}^n \times \mathbf{P}^{n-1} \rightarrow \mathbf{P}^n$ restricted to $B_{P_0}(\mathbf{P}^n)$ is a surjective morphism. It is also birational, for outside P_0 an inverse is given by mapping (x_0, \dots, x_n) to $(x_0, \dots, x_n, x_0, \dots, x_{n-1})$. However, the inverse image $\pi^{-1}(P_0) \subset B_{P_0}(\mathbf{P}^n)$ is the hyperplane $\{P_0\} \times \mathbf{P}^{n-1}$.

Of course, by composition with an automorphism of \mathbf{P}^n one may define the blowup $B_P(\mathbf{P}^n)$ at any point P . Given a subvariety $X \subset \mathbf{P}^n$ of dimension d containing P as a smooth point, one proves (Shafarevich [2], Chapter II, Section 4.3) that the inverse image of X in $B_P(\mathbf{P}^n)$ consists of two components: the hyperplane $\{P\} \times \mathbf{P}^{n-1}$ and a projective variety which one defines to be the blowup $B_P(X)$ of X at P . Moreover, the restriction of π to $B_P(X)$ is a birational morphism onto X which is an isomorphism outside P , and the preimage of P is a subvariety isomorphic to \mathbf{P}^{d-1} . It is called the *exceptional divisor*.

For a discussion of blowups valid over a more general base, see Hartshorne [1], Section II.7.

A.3 Function Fields and Dimension

Let k be a field and $K|k$ a finitely generated extension. Recall that the *transcendence degree* $\text{tr.deg.}(K|k)$ of $K|k$ is defined as the cardinality of a maximal subset of elements of K algebraically independent over k ; such a maximal subset is called a *transcendence basis* of $K|k$. If K is the function field of a variety X over k , we define the *dimension* of X to be $\text{tr.deg.}(K|k)$. Varieties of dimension 0 are points defined over a finite extension of k ; those of dimension 1 are called *curves* and those of dimension 2 *surfaces*. For a closed subvariety $Y \subset X$ we define the *codimension* of Y in X to be $\dim(X) - \dim(Y)$.

On the other hand, for a ring A we have the notion of *Krull dimension* for A : it is the maximum of lengths d of strictly decreasing chains $P_0 \supset P_1 \supset \cdots \supset P_d$ of prime ideals in A . Similarly, one defines the *height* of a prime ideal P in A as the maximum of lengths d of strictly decreasing chains $P \supset P_1 \supset \cdots \supset P_d$ of prime ideals in A . Note that the height of P equals the Krull dimension of the localisation A_P .

Proposition A.3.1 *Let X be an affine variety over a field k , and let $\mathcal{O}(X)$ be its coordinate ring. The dimension of X equals the Krull dimension of $\mathcal{O}(X)$, and the codimension of each closed subvariety $Y \subset X$ equals the height of the corresponding prime ideal in $\mathcal{O}(X)$.*

Proof: See Matsumura [1], Theorem 5.6. □

The notion of Krull dimension extends to a variety X over k : it is defined as the maximum of lengths d of strictly decreasing chains of $Z_1 \supset \cdots \supset Z_d$ of proper nonempty subvarieties of X . For affine varieties we get back the previous notion via the dictionary between subvarieties and prime ideals. One may then derive from the previous proposition:

Corollary A.3.2 *The dimension of a k -variety X equals its Krull dimension.*

Proof: See Mumford [1], I.7, Corollary 2. □

We define the dimension of a closed subset in \mathbf{A}^n or \mathbf{P}^n to be the maximal dimension of its irreducible components.

Corollary A.3.3 *Let f_1, \dots, f_r be homogeneous polynomials in $k[t_0, \dots, t_n]$. If $r \leq n$, the closed subset $V(f_1, \dots, f_r) \subset \mathbf{P}^n$ is nonempty.*

Proof: The previous corollary implies that in the chain

$$V(f_1) \supset V(f_1, f_2) \supset \cdots \supset V(f_1, \dots, f_r)$$

of closed subsets of \mathbf{P}^n the dimension drops by at most 1 in each step. Since \mathbf{P}^n is easily seen to have dimension n , the set $V(f_1, \dots, f_r)$ must be nonempty. \square

Recall that the extension $K|k$ is said to be *separably generated* if there exists a transcendence basis $\{t_1, \dots, t_d\}$ of $K|k$ so that the finite extension $K|k(t_1, \dots, t_d)$ is separable. The significance of this property for algebraic geometry is shown by the following fact.

Proposition A.3.4 *If the function field K of a k -variety X is separably generated over k , then the smooth locus of X is nonempty.*

Proof: Write $K = k(t_1, \dots, t_d, a)$ with a separable over $k(t_1, \dots, t_d)$. Clearing denominators in the minimal polynomial of a we obtain an irreducible polynomial $f \in k[t_1, \dots, t_d, t]$ with $\partial_t f \neq 0$. It follows that the proposition holds for the hypersurface defined by f . As this hypersurface is birational to X by construction and the smooth locus is open and dense in X , the general case follows. \square

The basic theorem on separably generated extensions is the following.

Proposition A.3.5 *If k is perfect, then every finitely generated extension $K|k$ is separably generated.*

Proof: See van der Waerden [1] §155, or modify the proof of Proposition A.3.7 below. \square

We need the following consequence of this in the main text.

Corollary A.3.6 *Let k be perfect, and let $K|k$ be a finitely generated extension of transcendence degree d . Then K arises as the residue field of a scheme-theoretic point of codimension 1 on \mathbf{A}_k^{d+1} .*

Proof: As in the proof of Proposition A.3.4 we may write K as the fraction field of $k[t_1, \dots, t_d, t]/(f)$ for a suitable irreducible polynomial f . The prime ideal $(f) \subset k[t_1, \dots, t_d, t]$ defines the required point. \square

We also need another case of separable generation.

Proposition A.3.7 *Let k be a perfect field, and let K be a finitely generated field extension of $k((t))$ of transcendence degree $d > 0$. Then K is separably generated over $k((t))$.*

Proof: In characteristic 0 there is nothing to prove, so assume k has characteristic $p > 0$. Let n be the minimal number of generators of the extension $K|k((t))$. We prove the lemma by induction on n , the case $n = d$ being obvious. Consider a system u_1, \dots, u_n of generators. We may assume by induction that u_1, \dots, u_d are algebraically independent and that the elements u_{d+2}, \dots, u_n are all separable over $k((t))(u_1, \dots, u_d)$. If u_{d+1} is also separable, we are done. Otherwise take a polynomial $f \in k((t))[x_1, \dots, x_{d+1}]$ with $f(u_1, \dots, u_{d+1}) = 0$; such an f exists as the transcendence degree is d . Assume now that f is not a polynomial in the x_i^p . In this case, we see by regrouping the terms that for some $1 \leq i \leq d$ the element u_i is separable over the field $k((t))(u_1, \dots, u_{i-1}, u_{i+1}, \dots, u_d, u_{d+1})$. This latter field must be purely transcendental over $k((t))$, for its transcendence degree is d . On the other hand, the field K is separable over $k((t))(u_1, \dots, u_{d+1})$ by assumption, so we are done.

It thus remains to see that we may find an f as above which cannot be written as $f(x_1, \dots, x_{d+1}) = F(x_1^p, \dots, x_{d+1}^p)$ for some $F \in k((t))[x_1, \dots, x_{d+1}]$. Suppose this is not the case, and assume that F has minimal degree among all polynomials with $F(u_1^p, \dots, u_{d+1}^p) = 0$. We may assume that the coefficients of F lie in $k[[t]]$, and thus are of the form $a_0 + a_1t + a_2t^2 + \dots$. We may also assume that for some coefficient of F the constant term a_0 is nonzero. Regrouping the relation $F(u_1^p, \dots, u_{d+1}^p) = 0$ according to powers of t , we see that the coefficients of t^j with $p|j$ only involve a_i with $p|i$, and similarly, the coefficients of t^j with $p \nmid j$ only involve a_i with $p \nmid i$. Thus replacing all a_i with $p \nmid i$ by 0 in the coefficients of F we get a polynomial G which satisfies $G(u_1^p, \dots, u_{d+1}^p) = 0$, and moreover only powers of t^p occur in its coefficients. As k is perfect, we have $k^p = k$ and we deduce that the coefficients of G are p -th powers. Hence we may write $G = H^p$ for some H with $H(u_1, \dots, u_{d+1}) = 0$. As G is not identically 0 (recall that some a_0 is nonzero), neither is H , and so by assumption it must be a nontrivial polynomial in the u_i^p . This contradicts the minimality of the degree of F . \square

A.4 Divisors

Throughout the whole section, X will denote a variety over a field k *all of whose local rings are unique factorisation domains*. For example, this is the case when X is smooth over a perfect field, the only one needed in this book.

Denote by $\text{Div}(X)$ the free abelian group with basis the irreducible closed subvarieties in X that are of codimension 1. The elements of $\text{Div}(X)$ are called *(Weil) divisors*, and $\text{Div}(X)$ itself is the *group of divisors* on X . An element $D \in \text{Div}(X)$ is thus of the form $D = \sum m_Y Y$ with some $m_Y \in \mathbf{Z}$ and Y irreducible of codimension 1; the union of the Y appearing with nonzero coefficients is called the *support* of D .

Given a codimension 1 irreducible subvariety $Y \subset X$, the local ring $\mathcal{O}_{X,Y}$ is of dimension 1 and it is a unique factorisation domain by assumption, so it is a discrete valuation ring (Matsumura [1], Theorem 11.2). Denote by $v_Y : k(X) \rightarrow \mathbf{Z} \cup \{\infty\}$ the associated discrete valuation.

Lemma A.4.1 *For a given nonzero rational function $f \in k(X)^\times$ there are only finitely many $Y \subset X$ as above with $v_Y(f) \neq 0$.*

Proof: See Hartshorne [1], Lemma II.6.1. □

In view of the lemma, we may define the *divisor of the rational function* $f \in k(X)^\times$ by

$$\text{div}(f) := \sum v_Y(f) Y \in \text{Div}(X),$$

where the sum is over all codimension 1 irreducible subvarieties in X . The additivity of discrete valuations implies that in this way we get a group homomorphism $\text{div}: k(X)^\times \rightarrow \text{Div}(X)$. We denote the cokernel of this morphism by $\text{Pic}(X)$ and call it the *Picard group* of X . Two divisors D_1 and D_2 are said to be *linearly equivalent* if they have the same class in the Picard group.

Remark A.4.2 The term ‘Picard group’ is nowadays mostly used for the group of isomorphism classes of line bundles on a variety, and the group defined above is sometimes called the *divisor class group* (e.g. in Hartshorne [1]). However, under our assumption on X the two notions coincide (see Hartshorne [1], Prop. 6.11 and 6.13).

Proposition A.4.3 *Assume moreover that X is projective. Then the sequence*

$$1 \rightarrow k^\times \rightarrow k(X)^\times \xrightarrow{\text{div}} \text{Div}(X) \rightarrow \text{Pic}(X) \rightarrow 0$$

is exact.

Proof: Everything results from the definitions, except exactness at $k(X)^\times$, which is a consequence of the fact that on a projective variety all regular functions are constant (see Hartshorne [1], Theorem I.3.4 for a proof over an algebraically closed base field; the general case follows immediately). \square

The next proposition gives the Picard groups of affine and projective space. Note that the Picard group of a point is by definition 0.

Proposition A.4.4

1. For any X as above there is an isomorphism $\text{Pic}(X) \xrightarrow{\sim} \text{Pic}(X \times \mathbf{A}^1)$. Hence $\text{Pic}(\mathbf{A}^d) = 0$ for all $d > 0$.
2. For all $d > 0$ we have $\text{Pic}(\mathbf{P}^d) \cong \mathbf{Z}$, a positive generator being given by the class of a hyperplane.

Proof: See Hartshorne [1], Propositions II.6.6 and II.6.4, or apply Propositions 8.2.5 and 8.2.6 of this book (with $i = d - 1$ and $n = 1 - d$). \square

For a divisor class $[D]$ on \mathbf{P}^d one defines its *degree* as its image in \mathbf{Z} by the isomorphism of statement (2) above.

Remark A.4.5 Assume that k is perfect, \bar{k} is an algebraic closure of k , and $\bar{X} := X \times_k \bar{k}$ is irreducible. The Galois group $G := \text{Gal}(\bar{k}|k)$ permutes the codimension 1 subvarieties of \bar{X} , and thus it acts on the group $\text{Div}(\bar{X})$. Moreover, the map div is compatible with the Galois actions on $\bar{k}(\bar{X})^\times$ and $\text{Div}(\bar{X})$, so there is an induced action on $\text{Pic}(\bar{X})$. Needless to say, all the above holds at the level of finite Galois extensions of the base field as well.

For X projective there is a relation between divisors and rational maps via the notion of a *linear system*. First some terminology: we say that a divisor is *positive* and write $D \geq 0$ if $D = \sum m_Y Y$ with all $m_Y \geq 0$. The *complete linear system* $|D|$ associated with an arbitrary divisor D on X is then defined as the set of positive divisors linearly equivalent to D . This set carries the structure of a projective space over k . Indeed, write $L(D)$ for the k -vector space of functions $f \in k(X)^\times$ satisfying $\text{div}(f) + D \geq 0$; it has finite dimension over k by Shafarevich [2], Chapter VI, Corollary 1 of Section 3.4. For $f \in L(D)$ the element $D_f = \text{div}(f) + D$ lies in $|D|$, and conversely, each element of $|D|$ is of the above form. Since by Proposition A.4.3 the divisor $\text{div}(f)$ determines f up to a constant in k^\times , elements in $|D|$ are in bijection with the projectivisation of the k -vector space $L(D)$.

A *linear system* \mathcal{D} on X is then by definition a projective linear subspace of some $|D|$ as above; it comes from a subspace $M_{\mathcal{D}}$ of $L(D)$. Choosing a k -basis (f_0, \dots, f_m) of $M_{\mathcal{D}}$ defines a rational map $\phi_{\mathcal{D}} : X \rightarrow \mathbf{P}^m$; the choice of a different basis yields a map which differs by an automorphism of \mathbf{P}^m . If the linear system is *base point free*, i.e. if there is no closed point of X contained in the support of all divisors in \mathcal{D} , then the map is actually a morphism. The divisors in \mathcal{D} are then the pullbacks to X of the divisors on $\phi_{\mathcal{D}}(X)$ obtained by intersecting $\phi_{\mathcal{D}}(X)$ with hyperplanes in \mathbf{P}^m (see Shafarevich [2], Chapter III, Section 1.5 or Hartshorne, Remark II.7.8.1 for more details). For instance, given a hyperplane H on \mathbf{P}^n and an integer $d > 0$, the complete linear system $|dH|$ on \mathbf{P}^n yields the d -uple embedding of Example A.2.1. A divisor D is called *ample* if the linear system $|mD|$ induces a closed embedding into some projective space for a suitable $m > 0$.

In the case when X is a *curve*, divisors on X are finite \mathbf{Z} -linear combinations of closed points on X . Thus it makes sense to define the *degree* of a divisor $D = \sum n_P P$ on X as $\deg(D) := \sum n_P [\kappa(P) : k]$. In this way we obtain a homomorphism $\deg : \text{Div}(X) \rightarrow \mathbf{Z}$ of abelian groups called the *degree map*, not to be confused with the one defined above for projective spaces. The fundamental fact about it is:

Proposition A.4.6 *Let X be a smooth projective curve. Then for each $f \in k(X)^{\times}$ one has $\deg(\text{div}(f)) = 0$.*

Proof: See Hartshorne [1], Corollary II.6.10; the proposition is stated there under the extra assumption that k is algebraically closed, but the proof works in general. \square

As a consequence we obtain that the degree map factors through the Picard group and induces a map $\text{Pic}(X) \rightarrow \mathbf{Z}$.

A.5 Complete Local Rings

Let A be a ring and $I \subset A$ an ideal. The *I -adic completion* \widehat{A} of A is defined as the inverse limit of the natural inverse system of quotients A/I^n for all $n \geq 0$ (see Chapter 4 for basics about inverse limits). More generally, the *I -adic completion* of an A -module N is defined as the inverse limit of the A -modules $N/I^n N$. We say that A is *I -adically complete* if the natural map $A \rightarrow \widehat{A}$ is an isomorphism. In the case when A is a local ring with maximal ideal M we simply say completion instead of M -adic completion. Similarly, for semi-local rings (i.e. rings with finitely many maximal ideals) by completion we mean

completion with respect to the intersection of maximal ideals. In fact, if A is a semi-local ring with maximal ideals M_1, \dots, M_r , then the completion of A is isomorphic to the direct product of the completions of the localisations A_{M_i} (Matsumura [1], Theorem 8.15).

For a Noetherian local ring the map $A \rightarrow \widehat{A}$ is always injective by the Krull intersection theorem (Matsumura [1], Theorem 8.10). Another useful fact about Noetherian local rings is:

Lemma A.5.1 *If A is a Noetherian local ring and $J \subset A$ is an ideal, then the completion of the A -module J is isomorphic to $J\widehat{A}$, and moreover $\widehat{A/JA} \cong \widehat{A}/J\widehat{A}$.*

Proof: See Matsumura [1], Theorem 8.11. □

The following is a delicate relation between integral closure and normalisation due to Zariski. Following Grothendieck [4], we formulate it using the general concept of excellent rings defined in §7.8 of *loc. cit.*, but for our applications it suffices to know that local rings of varieties over some field are excellent (Grothendieck [4], (7.8.3) (ii), (iii)).

Theorem A.5.2 *If A is an excellent Noetherian local domain, then the completion \widehat{A} has no nilpotent elements, and the integral closure \bar{A} of A is a finitely generated A -module. Moreover, the completion of the semi-local ring \bar{A} is isomorphic to the integral closure of \widehat{A} in its total ring of fractions.*

Proof: In the case when A is a local ring of a variety over a perfect field, a proof is given in the last section of Zariski-Samuel [1]. The general case follows from Grothendieck [4], (7.6.1) and (7.8.3) (vi). □

There is a beautiful structure theory for complete local rings. We first state the case of equal characteristic discrete valuation rings, which is the one we used most often.

Proposition A.5.3 *Let A be a complete discrete valuation ring with fraction field K and residue field κ . If $\text{char}(K) = \text{char}(\kappa)$, then A is isomorphic to the formal power series ring $\kappa[[t]]$.*

Proof: See Serre [2], Section II.4 for a direct proof, or the references for Theorem A.5.4 below. □

The general structure theorem is the following.

Theorem A.5.4 (Cohen Structure Theorem) *Let A be a complete Noetherian local domain with residue field κ and fraction field K .*

1. *There exists a complete discrete valuation ring B with residue field κ and a power series ring $C = B[[t_1, \dots, t_d]]$ such that $C \subset A$ and A is a finitely generated C -module.*
2. *If A is regular of dimension $d+1$ and $\text{char}(K) = \text{char}(\kappa)$, then we may find C as above with $C \cong A$. In particular, A is a formal power series ring in $d+1$ variables over κ .*

Proof: See Matsumura [1], Theorems 29.4 and 29.7; this reference also contains a complete discussion of the mixed characteristic case. \square

We finally discuss Hensel's lemma. In the literature various related results go under this name, of which the most common one is perhaps the following.

Proposition A.5.5 *Let A be a complete discrete valuation ring with maximal ideal M , and let f be a polynomial with coefficients in A . If $a \in A$ satisfies $f(a) = 0 \pmod{M}$ and $f'(a) \not\equiv 0 \pmod{M}$, then there exists $b \in A$ with $f(b) = 0$ and $a - b \in M$.*

Proof: The proof is by Newton's approximation method; see e.g. Lang [3], Chap. XII, Prop. 7.6, Serre [2], Chap. II, Prop. 7, or the proof of Proposition A.5.6 below. \square

In fact, the proposition holds more generally for an arbitrary complete local ring. However, in the following more refined version for a system of polynomials in several variables we need to restrict to discrete valuation rings.

Proposition A.5.6 *Let A be a complete discrete valuation ring with maximal ideal M , and let $f_1, \dots, f_n \in A[x_1, \dots, x_n]$ be a system of polynomials. Assume that $P = (a_1, \dots, a_n) \in A^n$ satisfies*

$$f_i(a_1, \dots, a_n) \in M^N \quad \text{for } 1 \leq i \leq n$$

with $N > 2\nu$, where $\nu \geq 0$ is the valuation of the Jacobian matrix $J(P)$ of the f_i at P . Then one may find $(b_1, \dots, b_n) \in A^n$ with

$$f_i(b_1, \dots, b_n) = 0 \text{ for all } 1 \leq i \leq n, \text{ and } a_j - b_j \in M^{N-\nu} \text{ for } 1 \leq j \leq n.$$

Proof: It will be enough to construct vectors $P^{(q)} = (b_1^{(q)}, \dots, b_n^{(q)})$ for all $q \geq 0$ such that $b_j^{(0)} = a_j$ for $1 \leq j \leq n$, and moreover

1. $f_i(b_1^{(q)}, \dots, b_n^{(q)}) \in M^{N+q}$ for all $1 \leq i \leq n$,
2. $b_j^{(q)} - b_j^{(q+1)} \in M^{N-\nu+q}$ for all $1 \leq j \leq n$, and
3. $J(P^{(q)})$ has valuation ν .

These then converge in A^n to a vector (b_1, \dots, b_n) with the required properties. Using induction on q and reindexing we reduce to the case $q = 1$. Write F for the column vector formed by the f_i and $F(P)$ for the column vector of their evaluations at $P = (a_1, \dots, a_n)$. Look for $P^{(1)}$ in the form $P^{(1)} = P + t^{N-\nu}Q$, where t is a generator of M and $Q \in A^n$ is a vector to be determined. Taylor's formula in several variables yields an equation

$$F(P^{(1)}) = F(P) + t^{N-\nu}J(P)Q + t^{2N-2\nu}R \quad (30)$$

with a suitable column vector $R \in A^n$. By assumption $F(P) = t^N S$ and $J(P) = t^\nu u$ for some column vector $S \in A^n$ and unit $u \in A \setminus M$. As u is a unit, we may choose Q in such a way that all entries of the vector $S + uQ$ lie in M . With this choice the right hand side of (30) lies in M^{N+1} , so that condition 1 holds for $q = 1$. Condition 2 being automatic, it remains to check condition 3 for $q = 1$. For this we take the Jacobian matrix of both sides in equation (30), and obtain $J(P^{(1)}) = J(P) \bmod M^{N-\nu}$. As $J(P)$ has valuation ν and $\nu < N - \nu$ by assumption, condition 3 follows. \square

A.6 Discrete Valuations

Recall that a *discrete valuation* on a field K is a map $K \rightarrow \mathbf{Z} \cup \{\infty\}$ satisfying the conditions (1) $v(x) = \infty \Leftrightarrow x = 0$, (2) $v(xy) = v(x) + v(y)$, and (3) $v(x + y) \geq \min(v(x), v(y))$. The elements $x \in K$ with $v(x) \geq 0$ form a subring $A_v \subset K$ called the valuation ring of v . This is a local ring whose maximal ideal M_v consists of the elements of positive valuation. The ideal M_v is principal, each element of minimal valuation being a generator. We refer to generators of M_v as *local parameters* for v . A local ring arising as the valuation ring of some discrete valuation of its fraction field is called a *discrete valuation ring*. Other characterisations of discrete valuation rings are:

Lemma A.6.1 *The following are equivalent for an integral domain A .*

1. A is a discrete valuation ring.

2. A is a local principal ideal domain which is not a field.
3. A is an integrally closed local domain of Krull dimension 1.

Proof: See Matsumura [1], Theorem 11.2. □

We collect here some basic results concerning extensions of discrete valuations to finite extensions of the field K . The most important situation where these facts are applied in this book is the following.

Example A.6.2 Let $\phi : X \rightarrow Y$ be a finite morphism of smooth curves over a perfect field k . Recall that this means that each closed point Q of Y has a Zariski open neighbourhood $U \subset Y$ so that both U and $V := \phi^{-1}(U)$ are isomorphic to affine varieties, and the coordinate ring $\mathcal{O}(V)$ becomes a finitely generated $\mathcal{O}(U)$ -module via the map $\mathcal{O}(U) \rightarrow \mathcal{O}(V)$ induced by pulling back functions via ϕ . A nonconstant morphism of smooth projective curves is always finite (see Shafarevich [2], Section II.5, Theorem 8).

By the finiteness condition on ϕ the induced extension $L|K$ is finite, and so is the fibre $\phi^{-1}(Q)$ for the point Q above. The local ring $\mathcal{O}_{Y,Q}$ of Q is a discrete valuation ring, hence it induces a discrete valuation v_Q of the function field K of Y , and similarly the closed points in the fibre $\phi^{-1}(Q)$ induce discrete valuations on the function field L of X . They are exactly the finitely many possible extensions of v_P to L . This holds because X is the *normalisation* of Y in L (see Shafarevich [2], Section II.5, Ex. 1), and on the other hand each discrete valuation ring with fraction field L containing $\mathcal{O}_{Y,Q}$ must contain the integral closure of $\mathcal{O}_{Y,Q}$ in L , being an integrally closed domain.

In general, given a finite extension $L|K$, a discrete valuation v on K may always be extended to a discrete valuation w of L (Matsumura [1], Theorem 9.3 (i)), and there are only finitely many such extensions (*loc. cit.*, Corollary to Theorem 11.7). The maximal ideals of their valuation rings satisfy $M_w \cap K = M_v$, hence there is an induced extension $\kappa(w)|\kappa(v)$ of residue fields. When the extension $L|K$ is Galois, the Galois group acts on the extensions w of v to L via $(\sigma, w) \mapsto w \circ \sigma$.

Proposition A.6.3 *Let $L|K$ be a finite Galois extension with group G , and v a discrete valuation on K .*

1. *The Galois group G acts transitively on the set of discrete valuations w extending v to L .*
2. *For each w the induced extension of residue fields $\kappa(w)|\kappa(v)$ is normal. In particular, if it is separable, then it is a Galois extension.*

Proof: See e.g. Serre [2], Chapter I, Propositions 19 and 20. \square

Given a discrete valuation v on K , the completion \widehat{A}_v of its valuation ring A_v is again a discrete valuation ring by Lemma A.5.1; denote its fraction field by \widehat{K}_v and keep the notation v for the canonical extension of v to \widehat{K}_v . In the case when $\widehat{K}_v = K$ we say that K is *complete with respect to v* .

Proposition A.6.4 *In the above situation let $L|K$ be a finite extension, and assume that the integral closure of A_v in L is a finitely generated A_v -module.*

1. *There is a decomposition*

$$L \otimes_K \widehat{K}_v \cong \bigoplus_{w|v} \widehat{L}_w,$$

where w runs over the extensions of v to L .

2. *If moreover $L|K$ is Galois with group G , then each $\widehat{L}_w|\widehat{K}_v$ is Galois as well, with Galois group isomorphic to the stabiliser of w under the action of G on the set of discrete valuations extending v .*

Proof: See Serre [2], Chapter II, Theorem 1 and its Corollary 4. \square

Remark A.6.5 The assumption of the proposition is satisfied if $L|K$ is separable or if A_v is a localisation of a finitely generated algebra over a field (Matsumura [1], Lemmas 1 and 2 of §33 together with Shafarevich [2], Appendix, §8).

Part (2) of the proposition implies:

Corollary A.6.6 *If $L|K$ is a finite extension that can be written as a tower of Galois extensions and w is an extension of a discrete valuation v of K to L , then the degree of the field extension $\widehat{L}_w|\widehat{K}_v$ divides $[L : K]$.*

The statement of the corollary is not true for an arbitrary finite extension (the reader may construct a counterexample).

Returning to an arbitrary finite extension $L|K$ and w extending v , the value group $v(K^\times)$ is a subgroup of finite index in $w(L^\times)$. This index is called the *ramification index* $e(w|v)$ of w above v . The extension is *unramified* if $e(w|v) = 1$ and the residue field extension $\kappa(w)|\kappa(v)$ is separable. More generally, the ramification is called *tame* if the extension $\kappa(w)|\kappa(v)$ is separable and the characteristic of $\kappa(v)$ does not divide $e(w|v)$; otherwise it is *wild*.

Proposition A.6.7 *Let K be a field equipped with a discrete valuation v , and let $L|K$ be a finite extension. Assume that the integral closure of the valuation ring A_v of v in L is a finitely generated A_v -module. Then*

$$\sum_{w|v} e(w|v)[\kappa(w) : \kappa(v)] = [L : K],$$

where w runs over the extensions of v to L .

Proof: See Serre [2], Section I.4, Proposition 10. □

Proposition A.6.8 *Let K be complete with respect to a discrete valuation v , and $L|K$ a finite extension.*

1. *There is a unique discrete valuation w of L extending v , L is complete with respect to w , and its valuation ring A_w is the integral closure of A_v in L .*
2. *With the notation $f := [\kappa(w) : \kappa(v)]$ one has $w = (1/f)(v \circ N_{L|K})$.*
3. *If the extension $\kappa(w)|\kappa(v)$ is separable, there is a unique unramified extension $N|K$ contained in L satisfying $[N : K] = f$.*
4. *If moreover the ramification is tame, then L is a radical extension of N (i.e. it may be obtained by adjoining a root of a polynomial of the form $x^m - a$).*

Proof: For (1), see Serre [2], Section II.2, Proposition 3; for (2), Corollary 4 of that proposition; for (3), *loc. cit.*, Section III.5, Corollary 2 to Theorem 2, and for (4), Neukirch [1], Chapter II, Theorem 7.7 (and its proof). □

If in the situation of the proposition we assume moreover that the extensions $L|K$ and $\kappa(w)|\kappa(v)$ are Galois, there is a natural group homomorphism $\text{Gal}(L|K) \rightarrow \text{Gal}(\kappa(w)|\kappa(v))$. This map is surjective (Serre [2], Chapter I, Proposition 20); its kernel I is called the *inertia group* of w .

Proposition A.6.9 *Assume moreover that the extension $L|K$ is a tamely ramified Galois extension. Then I is a cyclic subgroup isomorphic to the group $\mu(\kappa(w))$ of roots of unity contained in $\kappa(w)$. Explicitly, this isomorphism is given by $\sigma \mapsto \sigma(\pi)\pi^{-1}$, where π is an arbitrary local parameter for w .*

Proof: See Serre [2], Chapter 4, Proposition 7 and its corollaries. \square

The proposition implies that for a tamely ramified Galois extension the conjugation action of $\text{Gal}(L|K)$ on I induces an action of $\Gamma := \text{Gal}(\kappa(w)|\kappa(v))$ on I . The explicit description of the isomorphism $I \cong \mu(\kappa(w))$ implies:

Corollary A.6.10 *The action of Γ on I corresponds via the isomorphism $I \cong \mu(\kappa(w))$ to the natural Γ -action on $\mu(\kappa(w))$. In particular, if $\mu(\kappa(w))$ is contained in $\kappa(v)$, then I is central in $\text{Gal}(L|K)$.*

We conclude with an extension statement to transcendental extensions.

Proposition A.6.11 *Let A be a discrete valuation ring with maximal ideal M and fraction field K . There is a discrete valuation ring B whose fraction field is the rational function field $K(t)$, whose maximal ideal is MB , and moreover $B \cap K = A$.*

Proof: Let M be the maximal ideal of A , and take B to be the localisation of $A[t]$ by the prime ideal $M[t]$. It is a discrete valuation ring, as it satisfies the criterion of Lemma A.6.1. The other requirements are immediate. \square

A.7 Derivations

Let $A \subset B$ be an extension of rings, and M a B -module. A *derivation* of B into M is a homomorphism of abelian groups $D : B \rightarrow M$ satisfying the *Leibniz rule*: $D(b_1b_2) = b_1D(b_2) + b_2D(b_1)$ for all $b_1, b_2 \in B$. The derivation D is an *A-derivation* if $D(a) = 0$ for all $a \in A$; note that this implies $D(ab) = aD(b)$ for all $a \in A$ and $b \in B$ by the Leibniz rule. We denote the set of A -derivations $B \rightarrow M$ by $\text{Der}_A(B, M)$; this carries a natural B -module structure given by $(bD)(x) = b \cdot D(x)$ for all $b \in B$. In the case $B = M$ we shall write $\text{Der}_A(B)$ instead of $\text{Der}_A(B, B)$.

Given a derivation $D \in \text{Der}_A(B)$ and an integer $n > 0$, we denote by $D^{[n]}$ the n -th iterate $D \circ \cdots \circ D$. Iterating the Leibniz rule then yields

$$D^{[n]}(ab) = \sum_{i=0}^n \binom{n}{i} D^{[i]}(a)D^{[n-i]}(b).$$

Assuming $pB = 0$ for a prime p , the above formula with $n = p$ implies

$$D^{[p]}(ab) = D^{[p]}(a)b + aD^{[p]}(b), \quad (31)$$

i.e. that $D^{[p]}$ is again a derivation.

We also need two other important formulae in characteristic $p > 0$. The best reference for these are the notes of Seshadri [1]; since they are not easily accessible, we give details for the ease of the reader.

Proposition A.7.1 (Hochschild) *Let A be an integral domain of characteristic $p > 0$. For all derivations $D \in \text{Der}_{\mathbf{F}_p}(A)$ and elements $a \in A$ we have*

$$D(a)^p = a^{p-1}D^{[p]}(a) - D^{p-1}(a^{p-1}D(a)).$$

Proof: The idea is to reduce to the universal case. Let $A' = \mathbf{F}_p[x_0, x_1, x_2, \dots]$ be the ring of polynomials in infinitely many variables x_0, x_1, \dots . Define a derivation D' on A' by $D'(x_n) = x_{n+1}$ for all $n \geq 0$. There exists a unique morphism $\phi : A' \rightarrow A$ such that $\phi(x_0) = a$ and $\phi(x_n) = D^n(a)$ for all $n \geq 1$. We have $D \circ \phi = \phi \circ D'$, so it is enough to prove the formula with $A = A'$, $D = D'$ and $a = x_0$. We shall first prove that the element

$$Q := x_0^{p-1}D^{[p]}(x_0) - D^{[p-1]}(x_0^{p-1}D(x_0))$$

lies in A^p . For this, notice first that $D(Q) = 0$, since

$$D(x_0^{p-1}D^{[p]}(x_0)) = (p-1)x_0^{p-2}D(x_0)D^{[p]}(x_0) + x_0^{p-1}D^{[p+1]}(x_0) = D^{[p]}(x_0^{p-1}D(x_0)),$$

using the fact that $D^{[p]}$ is a derivation. Now assume Q is not in A^p , and denote by i the smallest integer such that $Q \in \mathbf{F}_p[x_0, \dots, x_i, x_{i+1}^p, x_{i+2}^p, \dots]$. Denoting by ∂_j the partial derivation with respect to x_j , we have $0 = D(Q) = \sum_j (\partial_j Q) D(x_j) = \sum_{j=0}^i (\partial_j Q) x_{j+1}$. By minimality of i , we have here $\partial_i Q \neq 0$, whence $x_{i+1} \in \mathbf{F}_p(x_0, x_1, \dots, x_i, x_{i+1}^p, \dots)$, which is impossible, and therefore $Q \in A^p$. Now by definition Q is a homogeneous polynomial of degree p in the x_i . On the other hand, consider the grading on $A = \mathbf{F}_p[x_0, x_1, \dots]$ in which x_i has degree i . Then D transforms elements of degree i in elements of degree $i+1$, from which it follows that Q has degree p in this grading as well. Denoting by \tilde{Q} the unique element of A with $\tilde{Q}^p = Q$, we get that \tilde{Q} has degree 1 for both the traditional and the new grading. This is only possible if $\tilde{Q} = mx_1$ for some $m \in \mathbf{F}_p$. On the other hand, the leading term of Q as a polynomial in $x_1 = D(x_0)$ is $-(p-1)!x_1^p$, which equals x_1^p by Wilson's theorem. So $m = 1$ and $Q = x_1^p = D(x_0)^p$, as desired. \square

For the next formula we consider elements of $\text{Der}_{\mathbf{F}_p}(A)$ as \mathbf{F}_p -linear maps on A , and for $a \in A$ we denote by $L_a : A \rightarrow A$ the \mathbf{F}_p -linear endomorphism $A \rightarrow A$ given by $L_a(x) = ax$.

Proposition A.7.2 *Given an integral domain of characteristic $p > 0$, an element $a \in A$ and a derivation $D \in \text{Der}_{\mathbf{F}_p}(A)$, the identity*

$$(D + L_a)^{[p]} = D^{[p]} + L_a^{[p]} + L_{D^{[p-1]}(a)}$$

holds in $\text{End}_{\mathbf{F}_p}(A)$.

The proof uses the notion of *Jacobson polynomials*, which are defined as follows. Given a not necessarily commutative ring R with unit, for each element $w \in R$ we may define a map $\text{ad}_w : R \rightarrow R$ by $\text{ad}_w(x) = wx - xw$. Applying the above to the polynomial ring $R[t]$ in place of R (where t is to commute with all elements of R) and taking two elements $u, v \in R$, we find non-commutative polynomials in two variables $s_i(U, V)$ with \mathbf{Z} -coefficients satisfying

$$(\text{ad}_{tu+v})^{[p-1]}(u) = \sum_{i=1}^{p-1} i s_i(u, v) t^{i-1}, \quad (32)$$

where $\text{ad}_{tu+v}^{[p-1]}$ stands for the $(p-1)$ -st iterate of ad_{tu+v} . Working in the free non-commutative \mathbf{Z} -algebra generated by two elements U, V , one sees that the polynomials $s_i(U, V)$ do not depend on the choice of u, v .

Lemma A.7.3 (Jacobson) *Assume moreover that $pR = 0$. Then the identity*

$$(u + v)^p = u^p + v^p + \sum_{i=1}^{p-1} s_i(u, v)$$

holds for all $u, v \in R$.

Proof: For all $w \in R[t]$ introduce the endomorphisms $L_w, R_w : R[t] \rightarrow R[t]$ defined by $L_w(x) = wx$ and $R_w(x) = xw$, respectively. We have $R_w \circ L_w = L_w \circ R_w$ and $\text{ad}_w = L_w - R_w$. Raising to the $(p-1)$ -st power, we get from the binomial formula

$$\text{ad}_w^{[p-1]} = \sum_{i=0}^{p-1} (-1)^{p-1-i} \binom{p-1}{i} L_w^{[i]} R_w^{[p-1-i]} = \sum_{i=0}^{p-1} L_w^{[i]} R_w^{[p-1-i]}$$

in End_R , as the binomial coefficient is congruent to $(-1)^i$ in characteristic p . In particular, we have

$$\text{ad}_w^{[p-1]}(u) = \sum_{i=0}^{p-1} w^i u w^{p-1-i}. \quad (33)$$

On the other hand, expanding $(tu + v)^p$ with respect to t we find non-commutative polynomials $s'_i(U, V) \in R[U, V]$ satisfying the identity

$$(tu + v)^p = t^p u^p + v^p + \sum_{i=1}^{p-1} s'_i(u, v)t^i. \tag{34}$$

Differentiating with respect to t yields

$$\sum_{i=0}^{p-1} (tu + v)^i u (tu + v)^{p-1-i} = \sum_{i=1}^{p-1} i s'_i(u, v) t^{i-1}$$

(note that the multiplication in $R[t]$ is non-commutative!) Comparing with formula (33) for $w = tu + v$ and applying the defining identity (32) of Jacobson polynomials we get $s'_i(u, v) = s_i(u, v)$, so the lemma follows from (34) by setting $t = 1$. \square

Proof of Proposition A.7.2: We shall apply the lemma with $R = \text{End}_{\mathbf{F}_p}(A)$, $u = D$ and $v = L_a$. The calculation

$$\text{ad}_D(L_a)(x) = DL_a(x) - L_a D(x) = D(ax) - aD(x) = D(a)x = L_{D(a)}(x)$$

shows that $\text{ad}_D(L_a) = L_{D(a)}$, and therefore

$$\text{ad}_{tD+L_a}(D) = (tD + L_a)D - D(tD + L_a) = -\text{ad}_D(L_a) = -L_{D(a)}.$$

Using the fact that L_a and $L_{D(a)}$ commute, we obtain from the above

$$\text{ad}_{tD+L_a}^{[2]}(D) = -\text{ad}_{tD+L_a}(L_{D(a)}) = -\text{ad}_{tD}(L_{D(a)}) = -tL_{D^{[2]}(a)}.$$

Iterating the argument yields

$$\text{ad}_{tD+L_a}^{[p-1]}(D) = -t^{p-2}L_{D^{[p-1]}(a)} = (p-1)t^{p-2}L_{D^{[p-1]}(a)}.$$

A comparison with formula (32) shows that $s_i(D, L_a) = 0$ for $i < p - 1$ and $s_{p-1}(D, L_a) = L_{D^{[p-1]}(a)}$, so the proposition follows from the lemma. \square

Finally we say a few words about the Lie algebra structure on derivations. Assume k is a field, and V is a k -vector space. Then $\text{End}_k(V)$ carries a *Lie bracket* defined by $[\phi, \psi] = \phi \circ \psi - \psi \circ \phi$. This Lie bracket is k -bilinear and satisfies $[\phi, \phi] = 0$ as well as the Jacobi identity $[[\phi, \psi], \rho] + [[\psi, \rho], \phi] + [[\rho, \phi], \psi] = 0$, so it gives $\text{End}_k(V)$ the structure of a Lie algebra. Given $\phi \in \text{End}_k(V)$, the map $\text{ad}(\phi) : \psi \mapsto [\phi, \psi]$ is a Lie algebra endomorphism. If k has characteristic p , we also have the p -operation $\phi \mapsto \phi^{[p]}$ sending an

endomorphism to its p -th iterate. Obviously $(a\phi)^{[p]} = a^p\phi^{[p]}$ for all $a \in k$, $\text{ad}(\phi^{[p]}) = \text{ad}(\phi)^{[p]}$, and moreover $(\phi + \psi)^{[p]} = \phi^{[p]} + \psi^{[p]} + \sum s_i(\phi, \psi)$ by Lemma A.7.3.

In fact, one may check using the definition of Jacobson polynomials that the $s_i(\phi, \psi)$ lie in the Lie subalgebra of $\text{End}_k(V)$ generated by ϕ and ψ , i.e. may be obtained from ϕ and ψ by means of a formula involving additions and Lie brackets. For a (rather complicated) explicit formula, see Demazure-Gabriel [1], II, §7, No. 3. Via this observation one may extend the definition of Jacobson polynomials to arbitrary Lie algebras of characteristic p . In the literature a Lie algebra over a field of characteristic p equipped with a p -operation satisfying the above three properties is called a *restricted p -Lie algebra* or a *p -Lie algebra* for short.

Now consider the case when $V = K$ is a field extension of k . Then every k -derivation $D : K \rightarrow K$ is also an element of $\text{End}_k(K)$. The Lie bracket on $\text{End}_k(K)$ preserves $\text{Der}_k(K)$, in view of the computation

$$\begin{aligned} [D_1, D_2](ab) &= D_1(D_2(ab)) - D_2(D_1(ab)) \\ &= D_1(D_2(a)b) + D_1(aD_2(b)) - D_2(D_1(a)b) - D_2(aD_1(b)) \\ &= (D_1D_2(a))b + a(D_1D_2(b)) - (D_2D_1(a))b - a(D_2D_1(b)) \\ &= ([D_1, D_2](a))b + a([D_1, D_2](b)). \end{aligned}$$

Moreover, the p -th iterate of a derivation is again a k -derivation according to formula (31), so the p -operation of $\text{End}_k(K)$ also preserves $\text{Der}_k(K)$. All in all, $\text{Der}_k(K)$ is a p -Lie subalgebra of $\text{End}_k(K)$.

A.8 Differential forms

One defines differential forms by the following universal property.

Proposition A.8.1 *Let $A \subset B$ be an extension of commutative rings. There exist a B -module $\Omega_{B|A}^1$ and an A -derivation $d : B \rightarrow \Omega_{B|A}^1$ so that for all B -modules M the map $\phi \rightarrow \phi \circ d$ induces an isomorphism*

$$\text{Hom}_B(\Omega_{B|A}^1, M) \xrightarrow{\sim} \text{Der}_A(B, M),$$

functorial in M .

Proof: Let $F(B)$ be the free B -module generated by symbols db for all $b \in B$. Define $\Omega_{B|A}^1$ as the quotient of $F(B)$ by the submodule generated by elements of the form da , $d(b_1 + b_2) - db_1 - db_2$ or $d(b_1b_2) - b_1db_2 - b_2db_1$ for

some $a \in A$ or $b_1, b_2 \in B$, and define d by sending b to db . Verification of the required properties is straightforward. \square

The B -module $\Omega_{B|A}^1$ is called the module of *differential forms* of B relative to A . In the case $A = \mathbf{Z}$ we set $\Omega_{B|\mathbf{Z}}^1 =: \Omega_B^1$, and call it the module of *absolute differential forms*. As $\Omega_{B|A}^1$ is defined by a universal property, it is unique up to unique isomorphism. In Matsumura [1] another construction for $\Omega_{B|A}^1$ is given, which yields the same module by this remark.

Example A.8.2 Assume that B arises as the quotient of the polynomial ring $A[x_1, \dots, x_n]$ by an ideal (f_1, \dots, f_m) . Then $\Omega_{B|A}^1$ is the quotient of the free B -module generated by the dx_i modulo the submodule generated by the elements $\sum_i \partial_i f_j dx_i$ ($1 \leq j \leq m$), where ∂_i denotes the partial derivative with respect to x_i . This follows immediately from the above construction.

Proposition A.8.3 *The module of differentials $\Omega_{B|A}^1$ enjoys the following basic properties.*

1. (Base change) For an A -algebra A' one has $\Omega_{B \otimes_A A'|A'}^1 \cong \Omega_{B|A}^1 \otimes_A A'$.
2. (Localisation) Given a multiplicative subset S of B , one has

$$\Omega_{B_S|A}^1 \cong \Omega_{B|A}^1 \otimes_B B_S.$$

3. (First exact sequence) A tower of ring extensions $A \subset B \subset C$ gives rise to an exact sequence of C -modules

$$\Omega_{B|A}^1 \otimes_B C \rightarrow \Omega_{C|A}^1 \rightarrow \Omega_{C|B}^1 \rightarrow 0.$$

4. (Second exact sequence) A short exact sequence $0 \rightarrow I \rightarrow B \rightarrow C \rightarrow 0$ of A -algebras gives rise to an exact sequence

$$I/I^2 \xrightarrow{\delta} \Omega_{B|A}^1 \otimes_B C \rightarrow \Omega_{C|A}^1 \rightarrow 0$$

of C -modules, where the map δ sends a class $x \bmod I^2$ to $dx \otimes 1$. (Note that the B -module structure on I/I^2 induces a C -module structure.)

Proof: For (1) and (2), see Matsumura [1], Ex. 25.4; for (3) and (4), see Theorems 25.1 and 25.2 of *loc. cit.* \square

Corollary A.8.4 *If $K|k$ is a finitely and separably generated field extension of transcendence degree r , then $\Omega_{K|k}^1$ has dimension r over K .*

Proof: Write K as the fraction field of a quotient $k[t_1, \dots, t_{d+1}]/(f)$ with f separable as in the proof of Proposition A.3.4, and apply part (2) of the proposition together with Example A.8.2. \square

The following statement gives a relation between smoothness, differentials and regularity.

Proposition A.8.5 *Let k be a perfect field, A an integral domain which is a finitely generated k -algebra, and P a prime ideal of A . Denote by d the Krull dimension of A and by m the height of P . Then the following are equivalent:*

1. *The module of differentials $\Omega_{A_P|k}^1$ is free of rank d over A_P ;*
2. *A_P is a regular local ring (i.e. $\dim_{\kappa(P)} P/P^2 = m$).*

For $d = m$ these are both equivalent to the condition that the closed point P is smooth.

Proof: For the first statement, see Matsumura [1], Lemma 1, p. 216 and Theorem 30.3. The case $d = m$ follows easily from the first part using Nakayama's lemma (see Mumford [1], Section III.4). \square

Corollary A.8.6 *Under the equivalent conditions of the proposition the sequence*

$$0 \rightarrow P/P^2 \rightarrow \Omega_{A_P|k}^1 \otimes_{A_P} \kappa(P) \rightarrow \Omega_{\kappa(P)|k}^1 \rightarrow 0$$

is exact, where $\kappa(P)$ is the residue field of P .

Proof: In view of Proposition A.8.3 (4) only injectivity at the left should be checked, and this follows from Corollary A.8.4 and a dimension count using the proposition above. \square

We now turn to differential forms over fields. The first result is:

Proposition A.8.7 *If $K|k$ is an extension of fields and $L|K$ is a finite separable extension, then $\Omega_{L|k}^1 \cong \Omega_{K|k}^1 \otimes_K L$.*

Proof: See Matsumura [1], Theorem 25.3. \square

Next we consider an extension $K|k$ of fields of characteristic $p > 0$ satisfying $K^p \subset k$. In this case there is an interesting relation between generators of $\Omega_{K|k}^1$ and of the extension $K|k$. Namely, one calls a system of elements $\{b_\lambda : \lambda \in \Lambda\}$ a p -basis for the extension $K|k$ if the products $b_{\lambda_1}^{\alpha_1} \dots b_{\lambda_m}^{\alpha_m}$ for all

finite subsets $\{\lambda_1, \dots, \lambda_m\} \subset \Lambda$ and exponents $0 \leq \alpha_i \leq p - 1$ yield a basis of the k -vector space K , i.e. they form a k -linearly independent generating system.

Proposition A.8.8 *Let $K|k$ be an extension of fields of characteristic $p > 0$ satisfying $K^p \subset k$. A system of elements $\{b_\lambda : \lambda \in \Lambda\}$ is a p -basis of $K|k$ if and only if the system $\{db_\lambda : \lambda \in \Lambda\}$ is a basis of the K -vector space $\Omega_{K|k}^1$.*

Proof: See Matsumura [1], Theorem 26.5. □

Corollary A.8.9 *Every finite extension $K|k$ of fields of characteristic $p > 0$ has a p -basis.*

Proof: Choose a K -basis for $\Omega_{K|k}^1$ (using Zorn's lemma). □

Corollary A.8.10 *Let $k_0 \subset k$ be a subfield with $K^p \subset k_0$. Then the sequence of K -vector spaces*

$$0 \rightarrow \Omega_{k|k_0}^1 \otimes_k K \rightarrow \Omega_{K|k_0}^1 \rightarrow \Omega_{K|k}^1 \rightarrow 0$$

is exact. Moreover, the choice of a p -basis of $K|k$ induces a splitting of the exact sequence.

Proof: The only nonobvious points are exactness at $\Omega_{K|k_0}^1$ and the existence of the splitting. For these choose a p -basis $\{x_\lambda : \lambda \in \Lambda_{k|k_0}\}$ of $k|k_0$ and a p -basis $\{x_\lambda : \lambda \in \Lambda_{K|k}\}$ of $K|k$. Together they form a p -basis of $K|k_0$, and the corollary follows from the proposition. □

As an application of the above, we compute the module of absolute differentials for local rings of the affine line over a field K of characteristic $p > 0$. Note that the case when K is perfect already follows from Example A.8.2 and the localisation property of differentials, so the interesting case is when $K \neq K^p$.

Proposition A.8.11 *For each closed point P of the affine line \mathbf{A}_K^1 the $K[t]_P$ -module $\Omega_{K[t]_P}^1$ is free on a basis containing $d\pi_P$, where π_P is a local parameter at P contained in $K[t]$.*

Proof: We first show the freeness of the $K[t]$ -module $\Omega_{K[t]}^1$, which will imply the corresponding property over the localisation $K[t]_P$ by Proposition A.8.3 (2). Applying Proposition A.8.3 (3) with $A = \mathbf{Z}$, $B = K$ and $C = K[t]$ we get an exact sequence

$$\Omega_K^1 \otimes_K K[t] \rightarrow \Omega_{K[t]}^1 \rightarrow \Omega_{K[t]|K}^1 \rightarrow 0.$$

By Example A.8.2 the $K[t]$ -module $\Omega_{K[t]|K}^1$ is free of rank one generated by dt , and therefore it identifies to a direct summand of $\Omega_{K[t]}^1$. It remains therefore to show the injectivity of the map $\Omega_K^1 \otimes_K K[t] \rightarrow \Omega_{K[t]}^1$. As the kernel of this map is in any case a torsion free module over the principal ideal ring $K[t]$, this is equivalent to showing the injectivity of the map $\Omega_K^1 \otimes_K K(t) \rightarrow \Omega_{K[t]}^1 \otimes_{K[t]} K(t)$, which is the same as the natural map $\Omega_K^1 \otimes_K K(t) \rightarrow \Omega_{K(t)}^1$ by Proposition A.8.3 (2). The claim then follows from Corollary A.8.10.

Concerning the statement about $d\pi_P$ we distinguish two cases. If π_P is a separable polynomial in $K[t]$, then the derivative $\partial_t \pi_P$ is prime to π_P in $K[t]$, and therefore a unit in $K[t]_P$. The formula $d\pi_P = (\partial_t \pi_P) d\pi_P$ then shows that $d\pi_P$ is a generator of $\Omega_{K[t]_P|K}^1$, so by the above argument it yields a basis of $\Omega_{K[t]_P}^1$ together with a basis of Ω_K^1 . In the case when π_P is an inseparable polynomial we may write $\pi_P = f(t^{p^r})$ for a suitable $r > 0$ and separable polynomial f . Applying Proposition A.8.3 (3) with $A = \mathbf{Z}$, $B = K[t^{p^r}]$ and $C = K[t]$ we see as above that $\Omega_{K[t]}^1$ is free on a basis consisting of dt and a basis of $\Omega_{K[t^{p^r}]}^1$. But by the separable case $d\pi_P$ may be taken as a basis element in the latter, and the proof is complete. \square

We finally discuss higher differential forms. For an integer $i > 0$ the module of differential i -forms $\Omega_{B|A}^i$ is defined as the i -th exterior power $\Lambda^i \Omega_{B|A}^1$; for $i = 0$ we put $\Omega_{B|A}^0 := B$ by convention. They form the terms of a complex of A -modules, the *de Rham complex*:

$$\Omega_{B|A}^\bullet = (B \xrightarrow{d} \Omega_{B|A}^1 \xrightarrow{d} \Omega_{B|A}^2 \xrightarrow{d} \Omega_{B|A}^3 \xrightarrow{d} \dots)$$

For simplicity, we define the differentials $d : \Omega_{B|A}^i \rightarrow \Omega_{B|A}^{i+1}$ only in the case when $\Omega_{B|A}^1$ is freely generated as a B -module by elements db_λ , the only one we need. In this case, d sends an i -form $bdb_{\lambda_1} \wedge \dots \wedge db_{\lambda_i}$ to $db \wedge db_{\lambda_1} \wedge \dots \wedge db_{\lambda_i}$. Note that for $i = 0$ this gives back the universal derivation $d : B \rightarrow \Omega_{B|A}^1$; the fact that we have a complex is obvious. An easy calculation shows that the differential d satisfies the identity

$$d(\omega_1 \wedge \omega_2) = d\omega_1 \wedge \omega_2 + (-1)^i \omega_1 \wedge d\omega_2$$

for $\omega_1 \in \Omega_{B|A}^i$ and $\omega_2 \in \Omega_{B|A}^j$; in fact, this identity and the fact that it yields the universal derivation for $i = 0$ characterise d . The submodules $\ker(d)$

(resp. $\text{Im}(d)$) of $\Omega_{B|A}^1$ are denoted by $Z_{B|A}^i$ and $B_{B|A}^i$, respectively, and are classically called the module of *closed* (resp. *exact*) i -forms. The quotient $H^i(\Omega_{B|A}^\bullet) := Z_{B|A}^i/B_{B|A}^i$ is the i -th de Rham cohomology group of B over A .

Bibliography

Albert, Adrian A.

- [1] On the Wedderburn norm condition for cyclic algebras, *Bull. Amer. Math. Soc.* **37** (1931), 301–312.
- [2] Normal division algebras of degree four over an algebraic field, *Trans. Amer. Math. Soc.* **34** (1932), 363–372.
- [3] Simple algebras of degree p^e over a centrum of characteristic p , *Trans. Amer. Math. Soc.* **40** (1936), 112–126.
- [4] *Structure of algebras*, American Mathematical Society Colloquium Publications, vol. XXIV, 1939.
- [5] Tensor products of quaternion algebras, *Proc. Amer. Math. Soc.* **35** (1972), 65–66.

Amitsur, Shimshon A.

- [1] Generic splitting fields of central simple algebras, *Ann. of Math. (2)* **62** (1955), 8–43.
- [2] On central division algebras, *Israel J. Math.* **12** (1972), 408–420.

Amitsur, Shimshon, Rowen, Louis H. and Tignol, Jean-Pierre

- [1] Division algebras of degree 4 and 8 with involution, *Israel J. Math.* **33** (1979), 133–148.

Amitsur, Shimshon, and Saltman, David

- [1] Generic Abelian crossed products and p -algebras, *J. Algebra* **51** (1978), 76–87.

Arason, Jón Kristinn

- [1] Cohomologische Invarianten quadratischer Formen, *J. Algebra* **36** (1975), 448–491.
- [2] A proof of Merkurjev’s theorem, in *Quadratic and Hermitian forms (Hamilton, Ont., 1983)*, CMS Conf. Proc., 4, Amer. Math. Soc., Providence, 1984, 121–130.

Artin, Emil

- [1] Kennzeichnung des Körpers der reellen algebraischen Zahlen, *Abh. Math. Sem. Hamburg* **3** (1924), 319–323.

Artin, Emil and Schreier, Otto

[1] Eine Kennzeichnung der reell abgeschlossenen Körper, *Abh. Math. Sem. Hamburg* **5** (1927), 225–231.

Artin, Emil and Tate, John

[1] *Class field theory*, 2nd edition, Addison-Wesley, Redwood, 1990.

Artin, Michael

[1] Brauer-Severi varieties, in *Brauer groups in ring theory and algebraic geometry (Wilrijk, 1981)*, Lecture Notes in Math. **917**, Springer-Verlag, Berlin-New York, 1982, 194–210.

Artin, Michael and Mumford, David

[1] Some elementary examples of unirational varieties which are not rational, *Proc. London Math. Soc. (3)* **25** (1972), 75–95.

Atiyah, Michael Francis and Macdonald, Ian G.

[1] *Introduction to commutative algebra*, Addison-Wesley, Reading, 1969.

Atiyah, Michael Francis and Wall, Charles Terence Clegg

[1] Cohomology of groups, in *Algebraic Number Theory (J. W. S. Cassels and A. Fröhlich, eds.)*, Academic Press, London, 1967, 94–115.

Auslander, Maurice and Brumer, Armand

[1] Brauer groups of discrete valuation rings, *Indag. Math.* **30** (1968), 286–296.

Ax, James

[1] A field of cohomological dimension 1 which is not C_1 , *Bull. Amer. Math. Soc.* **71** (1965), 717.

[2] Proof of some conjectures on cohomological dimension, *Proc. Amer. Math. Soc.* **16** (1965), 1214–1221.

Bass, Hyman, Milnor, John and Serre, Jean-Pierre

[1] Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), *Inst. Hautes Études Sci. Publ. Math.* **33** (1967), 59–137.

Bass, Hyman and Tate, John

[1] The Milnor ring of a global field, in *Algebraic K-theory II*, Lecture Notes in Math. **342**, Springer-Verlag, Berlin, 1973, 349–446.

Beauville, Arnaud

[1] *Surfaces algébriques complexes*, Astérisque No. 54, Société Mathématique de France, Paris, 1978; English translation: *Complex algebraic surfaces*, London Mathematical Society Lecture Note Series, vol. 68, Cambridge University Press, 1983.

Berhuy, Grégory and Frings, Christoph

- [1] On the second trace form of central simple algebras in characteristic two, *Manuscripta Math.* **106** (2001), 1–12.

Bloch, Spencer

- [1] K_2 and algebraic cycles, *Ann. of Math. (2)* **99** (1974), 349–379.
[2] *Lectures on algebraic cycles*, Duke University Mathematics Series IV, Duke University, Durham, 1980.
[3] Torsion algebraic cycles, K_2 , and Brauer groups of function fields, in *The Brauer group (Les Plans-sur-Bex, 1980)*, Lecture Notes in Math. **844**, Springer-Verlag, Berlin, 1981, 75–102.

Bloch, Spencer and Kato, Kazuya

- [1] p -adic étale cohomology, *Inst. Hautes Études Sci. Publ. Math.* **63** (1986), 107–152.

Bogomolov, Fedor A.

- [1] The Brauer group of quotient spaces of linear representations (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **51** (1987), 485–516, 688; English translation in *Math. USSR-Izv.* **30** (1988), 455–485.
[2] Brauer groups of the fields of invariants of algebraic groups (Russian), *Mat. Sb.* **180** (1989), 279–293; English translation in *Math. USSR-Sb.* **66** (1990), 285–299.

Brauer, Richard

- [1] Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen I, *Math. Zeit.* **28** (1928), 677–696; II, *ibid.* **31** (1930), 733–747.
[2] Über die algebraische Struktur von Schiefkörpern, *J. reine angew. Math.* **166** (1932), 241–252.

Brauer, Richard, Hasse, Helmut and Noether, Emmy,

- [1] Beweis eines Hauptsatzes in der Theorie der Algebren, *J. reine angew. Math.* **167** (1932), 399–404.

Brussel, Eric

- [1] Noncrossed products and nonabelian crossed products over $\mathbf{Q}(t)$ and $\mathbf{Q}((t))$, *Amer. J. Math.* **117** (1995), 377–393.

Cartan, Henri, and Eilenberg, Samuel

- [1] *Homological algebra*, Princeton University Press, Princeton, 1956.

Cartier, Pierre

- [1] Questions de rationalité des diviseurs en géométrie algébrique, *Bull. Soc. Math. France* **86** (1958), 177–251.

Cassels, Ian W. S. and Fröhlich, Albrecht (eds.)

[1] *Algebraic Number Theory*, Academic Press, London, 1967.

Clemens, Herbert and Griffiths, Phillip

[1] The intermediate Jacobian of the cubic threefold, *Ann. of Math. (2)* **95** (1972), 281–356.

Châtelet, François

[1] Variations sur un thème de H. Poincaré, *Ann. Sci. Éc. Norm. Sup. III. Sér.* **61** (1944), 249–300.

Chevalley, Claude

[1] Démonstration d’une hypothèse de M. Artin, *Abh. Math. Semin. Hamb. Univ.* **11**, 73–75.

Colliot-Thélène, Jean-Louis

[1] Hilbert’s Theorem 90 for K_2 , with application to the Chow groups of rational surfaces, *Invent. Math.* **71** (1983), 1–20.

[2] Les grands thèmes de François Châtelet, *Enseign. Math. (2)* **34** (1988), 387–405.

[3] Cycles algébriques de torsion et K -théorie algébrique, in *Arithmetic algebraic geometry (Trento, 1991)*, Lecture Notes in Math. **1553**, Springer-Verlag, Berlin, 1993, 1–49.

[4] Cohomologie galoisienne des corps valués discrets henséliens, d’après K. Kato et S. Bloch, in *Algebraic K-theory and its applications (Trieste, 1997)*, World Scientific, River Edge, 1999, 120–163.

[5] Fields of cohomological dimension one versus C_1 -fields, in *Algebra and Number Theory : Proceedings of the Silver Jubilee Conference, University of Hyderabad* (R. Tandon, ed.), Hindustan Book Agency, New Delhi, 2005.

Colliot-Thélène, Jean-Louis, Hoobler, Raymond and Kahn, Bruno

[1] The Bloch-Ogus–Gabber theorem, in *Algebraic K-theory (Toronto, 1996)*, Fields Inst. Commun., vol. 16, Amer. Math. Soc., Providence, 1997, 31–94.

Colliot-Thélène, Jean-Louis, and Madore, David A.

[1] Surfaces de del Pezzo sans point rationnel sur un corps de dimension cohomologique un, *J. Inst. Math. Jussieu* **3** (2004), 1–16.

Colliot-Thélène, Jean-Louis and Ojanguren, Manuel

[1] Variétés unirationnelles non rationnelles: au-delà de l’exemple d’Artin et Mumford, *Invent. Math.* **97** (1989), 141–158.

Colliot-Thélène, Jean-Louis, Ojanguren, Manuel and Parimala, Raman

[1] Quadratic forms over fraction fields of two-dimensional Henselian rings and Brauer groups of related schemes, in *Algebra, arithmetic and geometry*, Tata Inst. Fund. Res. Stud. Math., vol. 16, Bombay, 2002, 185–217.

Colliot-Thélène, Jean-Louis and Sansuc, Jean-Jacques

[1] The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group), preprint available from the first author's homepage.

Demazure, Michel and Gabriel, Pierre

[1] *Groupes algébriques I*, Masson, Paris and North-Holland, Amsterdam, 1970.

Dennis, R. Keith and Stein, Michael R.

[1] K_2 of discrete valuation rings, *Adv. in Math.* **18** (1975), 182–238.

Dickson, Lawrence J.

[1] Linear algebras, *Trans. Amer. Math. Soc.* **13** (1912), 59–73.

Dieudonné, Jean

[1] Les déterminants sur un corps non commutatif, *Bull. Soc. Math. France* **71** (1943). 27–45.

[2] Sur une généralisation du groupe orthogonal à quatre variables, *Arch. Math.* **1** (1949), 282–287.

Draxl, Peter

[1] *Skew fields*, London Mathematical Society Lecture Note Series, vol. 81, Cambridge University Press, 1983.

Elman, Richard and Lam, Tsit Yuen

[1] Pfister forms and K -theory of fields, *J. Algebra* **23** (1972), 181–213.

Faddeev, Dmitri K.

[1] Simple algebras over a field of algebraic functions of one variable (Russian) *Trudy Mat. Inst. Steklova* **38** (1951), 321–344; English translation in Amer. Math. Soc. Transl. (2) **3** (1956), 15–38.

[2] On the theory of homology in groups (Russian), *Izv. Akad. Nauk SSSR. Ser. Mat.* **16** (1952), 17–22.

[3] On the theory of algebras over the field of algebraic functions of one variable (Russian), *Vestnik Leningrad. Univ. Ser. Mat. Meh. Astr.* **12** (1957), 45–51.

Fesenko, Ivan B. and Vostokov, Sergey V.

[1] *Local fields and their extensions*, 2nd edition, Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, 2002.

Fischer, Ernst

[1] Die Isomorphie der Invariantenkörper der endlicher Abelschen Gruppen linearer Transformationen, *Gött. Nachr.* 1915, 77–80.

[2] Zur Theorie der endlichen Abelschen Gruppen, *Math. Ann.* **77** (1915), 81–88.

Friedlander, Eric M. and Weibel, Charles

- [1] An overview of algebraic K -theory, in H. Bass, A. Kuku, C. Pedrini (eds.) *Algebraic K-theory and its applications*, World Scientific, River Edge, 1999, 1–119.

Fulton, William

- [1] *Intersection Theory*, 2nd edition, Springer-Verlag, Berlin, 1998.

Garibaldi, Skip, Merkurjev, Alexander and Serre, Jean-Pierre

- [1] *Cohomological invariants in Galois cohomology*, University Lecture Series **28**, American Mathematical Society, Providence, RI, 2003.

Gerstenhaber, Murray

- [1] On infinite inseparable extensions of exponent one, *Bull. Amer. Math. Soc.* **71** (1965), 878–881.

Graber, Tom, Harris, Joe and Starr, Jason

- [1] Families of rationally connected varieties, *J. Amer. Math. Soc.* **16** (2003), 57–67.

Greenberg, Marvin J.

- [1] Rational points in Henselian discrete valuation rings, *Inst. Hautes Études Sci. Publ. Math.* **31** (1966), 59–64.
 [2] *Lectures on forms in many variables*, W. A. Benjamin, New York-Amsterdam, 1969.

Grothendieck, Alexander

- [1] Technique de descente et théorèmes d'existence en géométrie algébrique I: Généralités. Descente par morphismes fidèlement plats, *Sém. Bourbaki*, exp.190 (1960); reprinted by Société Mathématique de France, Paris, 1995.
 [2] *Revêtements étales et groupe fondamental (SGA 1)*, Lecture Notes in Mathematics, vol. 224, Springer-Verlag, Berlin, 1971; reprinted as vol. 3 of Documents Mathématiques, Société Mathématique de France, Paris, 2003.
 [3] Le groupe de Brauer I, II, III, in *Dix Exposés sur la Cohomologie des Schémas*, North-Holland, Amsterdam/Masson, Paris, 1968, 46–188.
 [4] *Éléments de géométrie algébrique IV: Étude locale des schémas et des morphismes de schémas*, 2^e partie, *Pub. Math. IHES*, vol. 24, 1965.

Hartshorne, Robin

- [1] *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York-Heidelberg, 1977.

Heuser, Ansgar

- [1] Über den Funktionenkörper der Normfläche einer zentral einfachen Algebra, *J. reine angew. Math.* **301** (1978), 105–113.

Hochschild, Gerhard

- [1] Cohomology of restricted Lie algebras, *Amer. J. Math.* **76** (1954). 555–580.
- [2] Simple algebras with purely inseparable splitting fields of exponent 1, *Trans. Amer. Math. Soc.* **79** (1955). 477–489.

Hochschild, Gerhard and Nakayama, Tadasi

- [1] Cohomology in class field theory, *Ann. of Math.* **55** (1952), 348–366.

Iskovskih, Vasiliy A. and Manin, Yuri I.

- [1] Three-dimensional quartics and counterexamples to the Lüroth problem (Russian), *Mat. Sb.* **86 (128)** (1971), 140–166.

Illusie, Luc

- [1] Complexe de de Rham-Witt et cohomologie cristalline, *Ann. Sci. École Norm. Sup.* (4) **12** (1979), 501–661.
- [2] Frobenius et dégénérescence de Hodge, in J.-P. Demailly et al., *Introduction à la théorie de Hodge*, Soc. Math. France, Paris, 1996, 113–168.

Izhboldin, Oleg T.

- [1] On p -torsion in K_*^M for fields of characteristic p , *Adv. Soviet Math.* **4** (1991), 129–144.

Jacob, Bill

- [1] Indecomposable division algebras of prime exponent, *J. reine angew. Math.* **413** (1991), 181–197.

Jacobson, Nathan

- [1] Abstract derivations and Lie algebras, *Trans. Amer. Math. Soc.* **42** (1937), 206–224.
- [2] *Basic Algebra II*, 2nd edition, W. H. Freeman & Co., New York, 1989.
- [3] *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.

Jahnel, Jörg

- [1] The Brauer-Severi variety associated with a central simple algebra: a survey, preprint available from the author's homepage.

de Jong, Aise Johan

- [1] The period-index problem for the Brauer group of an algebraic surface, *Duke Math. J.* **123** (2004), 71–94.

de Jong, Aise Johan and Starr, Jason

- [1] Every rationally connected variety over the function field of a curve has a rational point, *Amer. J. Math.* **125** (2003), 567–580.

Kahn, Bruno

- [1] La conjecture de Milnor (d'après V. Voevodsky), Séminaire Bourbaki, exp. 834, *Astérisque* **245** (1997), 379–418.
- [2] Motivic cohomology of smooth geometrically cellular varieties, in *Algebraic K-theory* (W. Raskind and C. Weibel, eds.), Proc. Sympos. Pure Math. **67**, Amer. Math. Soc., Providence, 1999, 149–174.

Kang, Ming-Chang

- [1] Constructions of Brauer-Severi varieties and norm hypersurfaces, *Canad. J. Math.* **42** (1990), 230–238.

Kato, Kazuya

- [1] A generalization of local class field theory by using K -groups I, *J. Fac. Sci. Univ. Tokyo* **26** (1979), 303–376; II, *J. Fac. Sci. Univ. Tokyo* **27** (1980), 603–683.
- [2] Galois cohomology of complete discrete valuation fields, in *Algebraic K-theory II (Oberwolfach, 1980)*, Lecture Notes in Math., **967**, Springer-Verlag, Berlin-New York, 1982, 215–238.
- [3] Residue homomorphisms in Milnor K -theory, in *Galois groups and their representations (Nagoya, 1981)*, Adv. Stud. Pure Math., **2**, North-Holland, Amsterdam, 1983, 153–172,
- [4] Milnor K -theory and the Chow group of zero cycles, in *Applications of algebraic K-theory to algebraic geometry and number theory*, Contemp. Math., **55/2**, Amer. Math. Soc., Providence, 1986, 241–253.

Kato, Kazuya and Kuzumaki, Takako

- [1] The dimension of fields and algebraic K -theory, *J. Number Theory* **24** (1986), 229–244.

Katz, Nicholas M.

- [1] Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin, *Inst. Hautes Études Sci. Publ. Math.* **39** (1970), 175–232.
- [2] Algebraic solutions of differential equations (p -curvature and the Hodge filtration), *Invent. Math.* **18** (1972), 1–118.

Kersten, Ina

- [1] *Brauergruppen von Körpern*, Vieweg, Braunschweig, 1990.
- [2] Noether's problem and normalization, *Jahresber. Deutsch. Math.-Verein.* **100** (1998), 3–22.

Klingen, Norbert

- [1] A short remark on the Merkurjev-Suslin theorem, *Arch. Math.* **48** (1987), 126–129.

Kneser, Martin

- [1] Konstruktive Lösung p -adischer Gleichungssysteme, *Nachr. Akad. Wiss. Göttingen Math.-Phys.* (1978), 67–69.

Knus, Max-Albert

- [1] Sur la forme d'Albert et le produit tensoriel de deux algèbres de quaternions, *Bull. Soc. Math. Belg. Sér. B* **45** (1993), 333–337.

Knus, Max-Albert, Merkurjev, Alexander, Rost, Markus and Tignol, Jean-Pierre

- [1] *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, 1998.

Krull, Wolfgang

- [1] Galoissche Theorie der unendlichen algebraischen Erweiterungen, *Math. Ann.* **100** (1928), 687–698.

Lam, Tsit-Yuen

- [1] *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, 2005.

Lang, Serge

- [1] On quasi-algebraic closure, *Ann. of Math. (2)* **55** (1952), 373–390.
[2] Algebraic groups over finite fields, *Amer. J. Math.* **78** (1956), 555–563.
[3] *Algebra*, 3rd edition, Addison-Wesley, 1993.

Lenstra, Hendrik W.

- [1] Rational functions invariant under a finite abelian group, *Invent. Math.* **25** (1974), 299–325.
[2] K_2 of a global field consists of symbols, in *Algebraic K-theory*, Lecture Notes in Math., vol. 551, Springer-Verlag, Berlin, 1976, pp. 69–73.

Lichtenbaum, Stephen

- [1] The period-index problem for elliptic curves, *Amer. J. Math.* **90** (1968), 1209–1223.

Mammone, Pascal and Tignol, Jean-Pierre

- [1] Dihedral algebras are cyclic, *Proc. Amer. Math. Soc.* **101** (1987), 217–218.

Matsumura, Hideyuki

- [1] *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, 1989.

McKinnie, Kelly

- [1] Noncyclic and indecomposable p -algebras, preprint, 2004, available at the author's homepage.

Merkurjev, Alexander S.

- [1] On the norm residue symbol of degree 2 (Russian), *Dokl. Akad. Nauk SSSR* **261** (1981), 542–547.
- [2] K_2 of fields and the Brauer group, in *Applications of algebraic K-theory to algebraic geometry and number theory* (S. Bloch et al., eds.), Contemp. Math., vol. 55/1, Amer. Math. Soc., Providence, 1986, 529–546.
- [3] Kaplansky's conjecture in the theory of quadratic forms (Russian), *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.* **175** (1989), 75–89, 163–164; English translation in *J. Soviet Math.* **57** (1991), 3489–3497.
- [4] K -theory of simple algebras, in *K-theory and algebraic geometry: connections with quadratic forms and division algebras* (B. Jacob and J. Rosenberg, eds.), Proc. Sympos. Pure Math., vol. 58, Part 1, Amer. Math. Soc., Providence, 1995, 65–83.
- [5] On the norm residue homomorphism of degree two, to appear in *St. Petersburg Mathematics Journal*.

Merkurjev, Alexander S. and Suslin, Andrei A.

- [1] K -cohomology of Severi-Brauer varieties and the norm residue homomorphism (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **46** (1982), 1011–1046, 1135–1136.
- [2] Norm residue homomorphism of degree three (Russian) *Izv. Akad. Nauk SSSR Ser. Mat.* **54** (1990), 339–356; English translation in *Math. USSR Izv.* **36** (1991), 349–367.
- [3] The group K_3 for a field (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **54** (1990), 522–545; English translation in *Math. USSR Izv.* **36** (1991), 541–565.

Milne, James S.

- [1] Duality in the flat cohomology of a surface, *Ann. Sci. École Norm. Sup.* **9** (1976), 171–201.
- [2] *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, 1980.
- [3] *Arithmetic duality theorems*, Academic Press, Boston, 1986.
- [4] Jacobian varieties, in *Arithmetic geometry* (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, New York, 1986, 167–212.

Milnor, John W.

- [1] Algebraic K -theory and quadratic forms, *Invent. Math.* **9** (1969/1970), 318–344.
- [2] *Introduction to algebraic K-theory*, Annals of Mathematics Studies No. 72. Princeton University Press, 1971.

Mumford, David

[1] *The Red Book of varieties and schemes*, Lecture Notes in Mathematics **1358**, Springer-Verlag, Berlin, 1988.

Murre, Jacob P.

[1] Applications of algebraic K -theory to the theory of algebraic cycles, in *Algebraic geometry, Sitges (Barcelona), 1983*, Lecture Notes in Math. **1124**, Springer-Verlag, Berlin, 1985, 216–261.

Neukirch, Jürgen

[1] *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.

Neukirch, Jürgen, Schmidt, Alexander and Wingberg, Kay

[1] *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2000.

Ojanguren, Manuel and Parimala, Raman

[1] Algebras of prime degree on function fields of surfaces, preprint, 2005.

Peyre, Emmanuel

[1] Unramified cohomology of degree 3 and Noether's problem, preprint, 2003, available from the author's homepage.

Pfister, Albrecht

[1] *Quadratic forms with applications to algebraic geometry and topology*, London Mathematical Society Lecture Note Series, vol. 217, Cambridge University Press, 1995.

Pierce, Richard

[1] *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer-Verlag, New York-Berlin, 1982.

Platonov, Vladimir P.

[1] On the Tannaka-Artin problem, *Dokl. Akad. Nauk SSSR* **221** (1975), 1038–1041.

Quillen, Daniel

[1] Higher algebraic K -theory I, in *Algebraic K-theory I: Higher K-theories*, Lecture Notes in Math. **341**, Springer-Verlag, Berlin 1973, 85–147.

Rieffel, Marc A.

[1] A general Wedderburn theorem, *Proc. Nat. Acad. Sci. USA* **54** (1965), 1513.

Roquette, Peter

- [1] On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras, *Math. Ann.* **150** (1963), 411–439.
- [2] Splitting of algebras by function fields of one variable, *Nagoya Math. J.* **27** (1966), 625–642.
- [3] Class Field Theory in characteristic p : Its origin and development, in *Class Field Theory - Its Centenary and Prospect* (K. Miyake, ed.), Advanced Studies in Pure Mathematics **30**, Tokyo, 2000, 549–631.
- [4] The Brauer-Hasse-Noether theorem in historical perspective. preprint available from the author's homepage, to appear in *Sitzungsberichte der Heidelberger Akademie der Wissenschaften*.

Rosset, Shmuel and Tate, John

- [1] A reciprocity law for K_2 -traces, *Comment. Math. Helv.* **58** (1983), 38–47.

Rost, Markus

- [1] Chow groups with coefficients, *Doc. Math.* **1** (1996), 319–393.
- [2] The chain lemma for Kummer elements of degree 3, *C. R. Acad. Sci. Paris Sér. I Math.* **328** (1999), 185–190.
- [3] Hilbert's Satz 90 for K_3 for quadratic extensions, preprint, 1988, available from the author's homepage.
- [4] Chain lemma for splitting fields of symbols, preprint, 1998, available from the author's homepage.

Rowen, Louis Halle

- [1] Cyclic division algebras, *Israel J. Math.* **41** (1982), 213–234; Correction, *Israel J. Math.* **43** (1982), 277–280.
- [2] *Ring theory II*, Academic Press, Boston, 1988.
- [3] Are p -algebras having cyclic quadratic extensions necessarily cyclic? *J. Algebra* **215** (1999), 205–228.

Rowen, Louis Halle and Saltman, David J.

- [1] Dihedral algebras are cyclic, *Proc. Amer. Math. Soc.* **84** (1982), 162–164.

Saltman, David J.

- [1] Generic Galois extensions and problems in field theory, *Adv. in Math.* **43** (1982), 250–283.
- [2] Noether's problem over an algebraically closed field, *Invent. Math.* **77** (1984), 71–84.
- [3] *Lectures on division algebras*, American Mathematical Society, Providence, 1999.
- [4] Division algebras over p -adic curves, *J. Ramanujan Math. Soc.* **12** (1997), 25–47; correction, *ibid.* **13** (1998), 125–129.

Scharlau, Winfried

[1] Über die Brauer-Gruppe eines algebraischen Funktionenkörpers in einer Variablen, *J. reine angew. Math.* **239/240** (1969), 1–6.

[2] *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften, vol. 270, Springer-Verlag, Berlin, 1985.

Segre, Beniamino

[1] Questions arithmétiques sur les variétés algébriques, *Colloques Internat. CNRS*, vol. 24 (1950), 83–91.

Serre, Jean-Pierre

[1] Sur la topologie des variétés algébriques en caractéristique p , in *Symposium internacional de topologia algebraica*, Mexico City, 1958, 24–53.

[2] *Corps Locaux*, Hermann, Paris, 1962; English translation: *Local Fields*. Springer-Verlag, 1979.

[3] *Lectures on the Mordell-Weil Theorem*, Vieweg, Braunschweig, 1989.

[4] *Cohomologie Galoisienne*, 5e éd., révisée et complétée. Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin, 1994; English translation: *Galois Cohomology*. Springer-Verlag, Berlin, 2002.

Seshadri, Conjeerveram Srirangachari

[1] L'opérateur de Cartier. Applications. *Séminaire Chevalley*, année 1958/59, exposé 6.

Severi, Francesco

[1] Un nuovo campo di ricerche nella geometria sopra una superficie e sopra una varietà algebrica, *Mem. Accad. Ital., Mat.* **3** (1932), 1–52.

Shafarevich, Igor R.

[1] On the Lüroth problem (Russian), *Trudy Mat. Inst. Steklov* **183** (1990), 199–204; English translation in *Proc. Steklov Inst. Math.* (1991), No. 4., 241–246.

[2] *Basic Algebraic Geometry I-II*, Springer-Verlag, Berlin, 1994.

Shatz, Stephen S.

[1] *Profinite groups, arithmetic, and geometry*, Annals of Mathematics Studies, No. 67, Princeton University Press, 1972.

Soulé, Christophe

[1] K_2 et le groupe de Brauer (d'après A. S. Merkurjev et A. A. Suslin), *Séminaire Bourbaki*, exp. 601, Astérisque **105-106**, Soc. Math. France, Paris, 1983, 79–93.

Speiser, Andreas

[1] Zahlentheoretische Sätze aus der Gruppentheorie, *Math. Zeit.* **5** (1919), 1–6.

Springer, Tonny A.

[1] *Linear algebraic groups*, 2nd edition, Progress in Mathematics, vol. 9, Birkhäuser, Boston, MA 1998.

Sridharan, Ramaiyengar

[1] (in collaboration with Raman Parimala) *2-Torsion in Brauer Groups: A Theorem of Merkurjev*, notes from a course held at ETH Zürich in 1984/85, available from the homepage of M.-A. Knus.

Srinivas, Vasudevan

[1] *Algebraic K-theory*, 2nd edition, Progress in Mathematics, vol. 90, Birkhäuser, Boston, 1996.

Suslin, Andrei A.

[1] Algebraic K -theory and the norm residue homomorphism (Russian), in *Current problems in mathematics* **25** (1984), 115–207.

[2] Torsion in K_2 of fields, *K-Theory* **1** (1987), 5–29.

[3] SK_1 of division algebras and Galois cohomology, *Adv. Soviet Math.* **4**, Amer. Math. Soc., Providence, 1991, 75–99.

Suslin, Andrei A. and Joukhovitski, Seva

[1] Norm varieties, preprint, 2005, available as preprint No. 742 at <http://www.math.uiuc.edu/K-theory/>.

Suslin, Andrei A. and Voevodsky, Vladimir

[1] Bloch-Kato conjecture and motivic cohomology with finite coefficients, in *The arithmetic and geometry of algebraic cycles* (B. Brent Gordon et al., eds.), Kluwer, Dordrecht, 2000, 117–189.

Suzuki, Michio

[1] *Group theory I*, Grundlehren der Mathematischen Wissenschaften, vol. 247, Springer-Verlag, New York, 1982.

Swan, Richard G.

[1] Invariant rational functions and a problem of Steenrod, *Invent. Math.* **7** (1969), 148–158.

[2] Noether's problem in Galois theory, in *Emmy Noether in Bryn Mawr*, Springer-Verlag, New York-Berlin, 1983, 21–40.

[3] Higher algebraic K -theory, in *K-theory and algebraic geometry: connections with quadratic forms and division algebras* (B. Jacob and J. Rosenberg, eds.), Proc. Sympos. Pure Math., **58/1**, Amer. Math. Soc., Providence, 1995, 247–293.

Szabó Endre

[1] *Severi-Brauer varieties*, preprint.

Tate, John

- [1] Genus change in inseparable extensions of function fields, *Proc. Amer. Math. Soc.* **3** (1952), 400–406.
- [2] Global class field theory, in *Algebraic Number Theory* (J. W. S. Cassels and A. Fröhlich, eds.), Academic Press, London, 1967, 162–203.
- [3] Symbols in arithmetic, in *Actes du Congrès International des Mathématiciens (Nice, 1970)*, Tome 1, Gauthier-Villars, Paris, 1971, 201–211.
- [4] Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), 257–274.
- [5] On the torsion in K_2 of fields, in *Algebraic number theory (Kyoto, 1976)*, Japan Soc. Promotion Sci., Tokyo, 1977, 243–261.

Teichmüller, Oswald

- [1] p -Algebren, *Deutsche Math.* **1** (1936), 362–388.

Tignol, Jean-Pierre

- [1] Algèbres indécomposables d'exposant premier, *Adv. in Math.* **65** (1987), 205–228.

Tits, Jacques

- [1] Sur les produits tensoriels de deux algèbres de quaternions, *Bull. Soc. Math. Belg. Sér. B* **45** (1993), 329–331.

Tregub, Semion L.

- [1] Birational equivalence of Brauer-Severi manifolds, *Uspekhi Mat. Nauk* **46** (1991), 217–218; English translation in *Russian Math. Surveys* **46** (1992), 229.

Tsen, Chiung-Tse

- [1] Divisionsalgebren über Funktionenkörpern, *Gött. Nachr.* 1933, 335–339.

Voevodsky, Vladimir

- [1] Motivic cohomology with $\mathbf{Z}/2$ -coefficients, *Publ. Math. Inst. Hautes Études Sci.* **98** (2003), 59–104.
- [2] On motivic cohomology with \mathbf{Z}/l -coefficients, 2003, available as preprint No. 639 at <http://www.math.uiuc.edu/K-theory/>

Voevodsky, Vladimir, Suslin, Andrei A., Friedlander, Eric M.

- [1] *Cycles, transfers, and motivic homology theories*, Ann. of Math. Studies, vol. 143, Princeton Univ. Press, 2000.

Voskresensky, Valentin E.

- [1] On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $\mathbf{Q}(x_1, \dots, x_n)$ (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **34** (1970), 366–375; English translation in *Math. USSR Izv.* **4** (1971), 371–380.

[2] *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs, vol. 179, American Mathematical Society, Providence, 1998.

Wadsworth, Adrian

[1] Merkurjev's elementary proof of Merkurjev's theorem, in *Applications of algebraic K-theory to algebraic geometry and number theory* (S. Bloch et al., eds.), Contemp. Math., vol. 55/2, Amer. Math. Soc., Providence, 1986, 741–776.

van der Waerden, Bartel Leendert

[1] *Algebra I* (7te Auflage) *II* (5te Auflage), Springer-Verlag, Berlin, 1966–67. English translation: Springer-Verlag, New York, 1991.

Wang, Shianghaw

[1] On the commutator group of a simple algebra, *Amer. J. Math.* **72** (1950), 323–334.

Warning, Ewald

[1] Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, *Abh. Math. Semin. Hamb. Univ.* **11** (1935), 76–83.

Wedderburn, Joseph Henry Maclagan

[1] A theorem on finite algebras, *Trans. Amer. Math. Soc.* **6** (1905), 349–352.

[2] On hypercomplex numbers, *Proc. London Math. Soc.* **6** (1908), 77–118.

[3] On division algebras, *Trans. Amer. Math. Soc.* **22** (1921), 129–135.

Weibel, Charles

[1] *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, 1994.

[2] *Introduction to Algebraic K-Theory*, book in preparation, parts available at the author's homepage.

Weil, André

[1] Sur la théorie du corps de classes, *J. Math. Soc. Japan* **3** (1951), 1–35.

[2] The field of definition of a variety, *Amer. J. Math.* **78** (1956), 509–524.

[3] *Basic Number Theory*, Basic number theory, 3rd edition, Grundlehren der Mathematischen Wissenschaften, vol. 144, Springer-Verlag, New York-Berlin, 1974.

Witt, Ernst

[1] Über ein Gegenbeispiel zum Normensatz, *Math. Z.* **39** (1934), 462–467.

[2] Schiefkörper über diskret bewerteten Körpern, *J. reine angew. Math.* **176** (1936), 153–156.

Zariski, Oscar and Samuel, Pierre

[1] *Commutative algebra*, vol. II, Van Nostrand, Princeton, 1960.

Index

- 1-cocycle, 37, 73
- 2-cocycle, 73

- absolute Galois group, 98
 - of finite field, 100
 - of Laurent series field, 100
- acyclic complex, 66
- affine closed set, 333
- affine variety, 333
- Albert form, 24
- Albert's cyclicity problem, 235
- Albert's theorem
 - on algebras in characteristic p , 295
 - on algebras of degree four, 27
 - on biquaternion algebras, 24
- Albert-Brauer-Hasse-Noether theorem, 181
- Amitsur's conjecture, 145
- Amitsur's counterexample, 35
- Amitsur's theorem, 145
- Amitsur-Rowen-Tignol counterexample, 27
- ample divisor, 343
- Artin-Schreier theorem, 131, 203
- Artin-Schreier theory, 112
- Ax's counterexample, 162

- Bass-Tate lemma, 218
- biquaternion algebra, 23
- birational invariant, 182
- Bloch-Gabber-Kato theorem, 312
- Bloch-Kato conjecture, 126, 239
- blowup, 337

- Bockstein homomorphism, 240
- Bogomolov's theorem, 185
- Brauer equivalence, 44
- Brauer group, 45
 - m -torsion part of, 117
 - and differential forms, 299
 - and purely inseparable base extension, 203
 - as first cohomology group, 45
 - as second cohomology group, 117
 - inverse of an element in, 44
 - is a torsion group, 117
 - of \mathbf{R} , 131
 - of $\mathbf{F}((t))$, 171
 - of $\mathbf{F}(C)$, 178, 180
 - of $k_s((t))$, 169
 - of a number field, 181
 - of cyclic extension, 118, 129
 - relative, 45
 - unramified, 183

- C_1 -field, 161
- C_r -field, 161
- C'_r -field, 161
- Cartier isomorphism, 309
- Cartier operator, 310, 330
 - inverse, 297
 - over rings, 310
- Castelnuovo's theorem, 182
- central algebra over a field, 15
- central simple algebra, 29
 - as twisted form of matrix algebra, 32
 - base change of, 33

- dimension of, 34
- of prime degree, 234
- over $\mathbf{F}((t))$, 171
- over $\mathbf{F}(C)$, 164
- over a Laurent series field, 170
- over a number field, 181
- over algebraically closed field, 32
- product of, 43
- Châtelet's theorem, 135, 144
- chain lemma, 243
 - for quaternion algebras, 28, 244
 - over number fields, 246
- Chevalley's theorem, 162
- Chow group, 257
- closed point, 334
- co-induced module, 76, 77
 - for cohomology of profinite groups, 105
- coboundary, 72
- coboundary map, 67
 - in group cohomology, 74
- cochain, 72
 - continuous, 131
 - inhomogeneous, 73
 - normalised, 74
- cocycle, 72
- codimension, 338
- Cohen structure theorem, 344
- cohomological dimension
 - of $\hat{\mathbf{Z}}$, 156
 - of a field, 158
 - of a finite field, 161
- cohomology group, 70
 - of profinite group, 104
- completion of ring, 343
- complex of modules, 66
- conic
 - as Severi-Brauer variety, 139, 149
 - associated with quaternion algebra, 17
- conjugation action on cohomology, 80
- connecting homomorphism, 67
- connection, 301
- coordinate ring, 333
- coresidue map, 202
- corestriction map, 78
 - and coresidue map, 202
 - and Galois symbol, 237
 - for cohomology of profinite groups, 105
 - for purely inseparable extensions, 199
- crossed product, 35
- cup-product, 88
 - and conjugation, 92
 - and inflation maps, 92
 - and long exact sequences, 90, 91
 - and restriction maps, 92
 - associativity of, 89
 - for cohomology of profinite groups, 107
 - functoriality of, 88
 - graded-commutativity of, 89
- cyclic algebra, 46
 - Brauer class of, 127, 128
 - in characteristic p , 49, 290
 - presentation of, 46, 49
 - splitting of, 129, 130
- cyclic group, cohomology of, 75, 76, 93
- d -uple embedding, 137, 336
- de Rham complex, 358
 - decomposition of, 308
- degree
 - of central simple algebra, 34

- of divisor class on Severi-Brauer variety, 146
 - of divisor on curve, 172, 343
 - of divisor on curve over a finite field, 179
- derivation, 350
- descent for inseparable extensions
 - of height one, 305
- differential forms, 355
 - higher, 358
 - logarithmic, 302
- differential symbol, 312
 - and norm map, 313
 - injectivity of, 321
 - surjectivity of, 314
- dimension of variety, 338
- dimension shifting, 84
- direct limit, 103
 - of cohomology groups, 109
 - of exact sequences, 108
- direct system, 103
- discrete valuation, 346
 - ring, 346
- division algebra, 12
- divisor, 341
 - exceptional, 337
 - of rational function, 341
 - positive, 342
 - support of, 341
- dlog map, 296
- double complex, 85
- excellent
 - local ring, 344
 - scheme, 252
- Faddeev's exact sequence, 176
 - for Brauer groups, 177
 - with finite coefficients, 199
- Fischer's theorem, 185
- flat connection, 302
- free module, 68
- Frobenius's theorem, 131
- function field, 335
 - of conic, 20
- G -module, 65
 - continuous, 103
- Galois cohomology, 104
 - is torsion, 104
 - of \mathbf{Q} -vector space is trivial, 105
- Galois descent, 38
 - for central simple algebras, 42
 - for quadratic forms, 39
 - for Severi-Brauer varieties, 137
- Galois symbol, 126
 - and specialisation map, 236
 - and tame symbol, 235
 - and transcendental extensions, 238
 - over number fields, 242
 - surjectivity of, 238
- Galois theory for infinite extensions, 102
- generic point, 334
 - of conic, 20
- Gersten complex in Milnor K-theory, 252
 - localisation property of, 256
 - Mayer-Vietoris property of, 256
- Gersten conjecture, 260
- graded-commutative, 85
- Greenberg's approximation theorem, 165
- group extension, 74
 - and alternating forms, 189
 - cohomology class of, 74
 - pullback of, 80
 - pushforward of, 75
- $H^1(G, A)$ for non-commutative A , 38

- Hasse invariant, 171
- height of prime ideal, 338
- Hensel's lemma, 345
 - refined, 345
- Hilbert's Theorem 90, 38
 - for K_2 , 268, 287
 - for Galois cohomology, 111
 - for the additive group, 112
 - generalisation of, 55
 - original form of, 39, 76
- Hochschild's formula, 351
- Hochschild's theorem, 291
- homogeneous coordinate ring, 334
- index
 - of central simple algebra, 118
 - and base extension, 122
 - and degrees of splitting fields, 121
 - of Brauer class, 118
 - of Severi-Brauer variety, 144
- inertia group, 349
- inflation map, 79
 - for cohomology of profinite groups, 105
- inflation-restriction sequence, 81, 83
 - for cohomology of profinite groups, 110
- inverse Cartier operator, 297
- inverse limit, 98
- inverse system, 98
- irreducible component, 334
- Izhdobdin's theorem, 313
- Jacobson correspondence, 306
- Jacobson polynomial, 352
- Jacobson's formula, 352
- Jacobson-Cartier theorem, 298, 302, 310, 330
- K_1 of a ring, 55
- Künneth formula, 308
- Kang's construction, 137
- K^M -homology, 256
 - and Zariski cohomology, 260
 - homotopy invariance of, 258
 - of projective space, 259
- Krull dimension
 - of ring, 338
 - of variety, 338
- Kummer theory, 111
- Lüroth's theorem, 182
- Lang's theorem
 - on abelian varieties over finite fields, 178
 - on Laurent series fields, 165
- Lichtenbaum's theorem, 149
- Lie algebra of derivations, 353
- linear system, 343
- linearly equivalent divisors, 341
- local parameter, 346
- local ring, 335
 - of subvariety, 335
- long exact sequence, 66
 - for cohomology of profinite groups, 108
 - for noncommutative H^1 , 53, 113
- matrix algebra
 - automorphism group of, 42
 - is simple, 30
 - left ideals in, 30
- maximal prime to p extension, 220
- Merkurjev's theorem, 27
- Merkurjev-Suslin theorem, 50, 127, 285
- Milnor K-theory, 126
 - p -torsion in, 274
 - functoriality of, 207
 - graded-commutativity of, 208
 - of a field of cohomological dimension one, 248

- of a finite field, 209
 - of algebraically closed field, 247
 - products in, 208
 - torsion in, 274
- Milnor's exact sequence, 214
 - and Faddeev's exact sequence, 237
- morphism of varieties, 336
- No-name lemma, 205
- Noether's problem, 193
- norm group, 154
- norm map
 - on K_1 , 217
 - and Galois symbol, 237
 - for Milnor K-theory, 216, 221, 247
 - for Milnor K-theory and base extension, 222
 - on the cohomology of a subgroup, 95
- opposite algebra, 44
- p -basis, 356
- p -cohomological dimension, 156
 - and the Brauer group, 158
 - of a field, 158
 - of a pro- p group, 157
 - of fields of characteristic p , 160
 - strict, 156
- p -Lie algebra, 354
- p -connection, 302
- period
 - of central simple algebra, 122
 - of Severi-Brauer variety, 137
- period-index questions, 123
- Picard group, 341
 - of affine space, 342
 - of projective space, 342
- point
 - rational, on conic, 18
- pointed set, 38
- primary decomposition of central simple algebra, 123
- pro- p -Sylow subgroup, 106
- profinite completion, 99
- profinite group, 99
 - cohomology of, 104
 - has torsion cohomology groups, 104
 - topology of, 101
- projection formula
 - in group cohomology, 92
 - in Milnor K-theory, 218
- projective
 - module, 68
 - resolution, 69
- projective closed set, 334
- projective variety, 334
- pure quaternion, 13
- purely inseparable extension of height one, 293
- quaternion, 11
 - conjugate of, 12
- quaternion algebra, 12
 - has period two, 24
 - over finite field, 19
 - split, 13
- quaternion norm, 12, 13
 - as reduced norm, 17
- ramification
 - tame, 348
 - wild, 348
- ramification index, 348
- rational function, 336
- rational map, 336
- rational point, 334
- rational variety, 181
- reduced norm, 51
 - and norm group of Severi-Brauer variety, 154

- cokernel of, 54
 - for K_1 , 60
 - on division algebra, 51
- reduced trace, 51
- residue field of a point, 335
- residue map
 - and cup-products, 195
 - for Milnor K-theory, 210
 - for the Brauer group, 168
 - for the cohomology of function fields, 174
 - with finite coefficients, 196
- Residue Theorem, 175, 204
- restriction map, 78
 - for cohomology of profinite groups, 105
- Rieffel's lemma, 31
- Rosset-Tate reciprocity law, 233
- Rosset-Tate symbol, 232

- Saltman's example, 192
- Saltman's theorem, 151
- scheme-theoretic point, 334
- Schur's lemma, 31
- separably generated field, 339
- Severi-Brauer variety, 134
 - Brauer class of, 144
 - minimal, 144
- Shafarevich's example, 189
- Shapiro's lemma, 77
 - for cohomology of profinite groups, 105
- simple algebra, 29
- singular
 - locus, 335
 - point, 335
- Skolem-Noether theorem, 54
- smooth
 - point, 335
 - variety, 335
- snake lemma, 67

- specialisation map
 - and Galois symbol, 236
 - and norm map, 230
 - for Galois cohomology, 197
 - for Milnor K-theory, 210
- Speiser's lemma, 40
- splitting field, 34
 - Galois, 35, 136
 - of Severi-Brauer variety, 134
 - separable, 34, 119, 136
 - solvable, 50
- stably birational, 145
- standard resolution, 72
- Steinberg relation
 - for cyclic algebras, 63
 - for Galois symbol, 125
 - for Milnor K-theory, 207
 - for quaternion algebras, 18
 - for the Galois symbol, 205
- symbol
 - in Milnor K-theory, 126
 - of length one, 242
 - splitting of, 130
- tame symbol, 210, 211
 - and base extension, 212
 - and Galois symbol, 235
 - and norm map, 229
 - and specialisation map, 211
 - kernel and cokernel of, 212
- Tate's theorem on the Galois symbol, 242
- Teichmüller's theorem, 293, 300
- tensor product of complexes, 85
- trace map for differential forms, 313
- transcendence basis, 338
- transcendence degree, 338
- transgression map, 83
- Tsen's theorem, 163
- twisted form, 37
- twisted-linear subvariety, 135

- Brauer class of, 140, 141
- twisting by a cocycle, 39

- unirational variety, 181
- unramified Brauer group, 183
- unramified extension, 348

- Voevodsky's theorem, 127

- Wang's theorem, 61
- Wedderburn's theorem
 - on algebras of degree 3, 249
 - on finite fields, 163
 - on simple algebras over a field, 30
- Weil reciprocity law, 216, 231
- Whitehead's Lemma, 56
- Witt's theorem
 - on quaternion algebras, 20, 149
 - on the Brauer group of a Laurent series field, 170

- Zariski topology, 334