Elementary theory of *L*-functions and Eisenstein series

HARUZO HIDA

London Mathematical Society
Student Texts **26**

LONDON MATHEMATICAL SOCIETY STUDENT TEXTS

Managing editor: Dr C.M. Series, Mathematics Institute
University of Warwick, Coventry CV4 7AL, United Kingdom

1 Introduction to combinators and λ-calculus, J.R. HINDLEY & J.P. SELDIN
2 Building models by games, WILFRID HODGES
3 Local fields, J.W.S. CASSELS
4 An introduction to twistor theory, S.A. HUGGETT & K.P. TOD
5 Introduction to general relativity, L.P. HUGHSTON & K.P. TOD
6 Lectures on stochastic analysis: diffusion theory, DANIEL W. STROOCK
7 The theory of evolution and dynamical systems, J. HOFBAUER & K. SIGMUND
8 Summing and nuclear norms in Banach space theory, G.J.O. JAMESON
9 Automorphisms of surfaces after Nielsen and Thurston, A.CASSON & S. BLEILER
10 Nonstandard analysis and its applications, N.CUTLAND (ed)
11 Spacetime and singularities, G. NABER
12 Undergraduate algebraic geometry, MILES REID
13 An introduction to Hankel operators, J.R. PARTINGTON
14 Combinatorial group theory: a topological approach, DANIEL E. COHEN
15 Presentations of groups, D.L. JOHNSON
16 An introduction to noncommutative Noetherian rings, K.R.GOODEARL & R.B. WARFIELD,JR.
17 Aspects of quantum field theory in curved spacetime, S.A. FULLING
18 Braids and coverings: selected topics, VAGN LUNDSGAARD HANSEN
19 Steps in commutative algebra, R.Y. SHARP
21 Representations of finite groups of Lie type, FRANÇOIS DIGNE & JEAN MICHEL
22 Designs, codes and graphs and their linkages, P. CAMERON & J. VAN LINT
23 Complex algebraic curves, F. KIRWAN
24 Lectures on elliptic curves, J.W.S. CASSELS
25 Hyperbolic geometry, B. IVERSEN
26 Elementary theory of L-functions and Eisenstein series. H. HIDA
27 Hilbert space: compact operators and the trace theorem, J.R. RETHERFORD

London Mathematical Society Student Texts 26

Elementary Theory of *L*-functions and Eisenstein Series

Haruzo Hida
Department of Mathematics,
University of California at Los Angeles

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521434119

First published 1993

A catalogue record for this publication is available from the British Library

ISBN-13 978-0-521-43411-9 hardback
ISBN-10 0-521-43411-4 hardback

ISBN-13 978-0-521-43569-7 paperback
ISBN-10 0-521-43569-2 paperback

Transferred to digital printing 2006

Contents

Preface

Number theory is very rich with surprising interactions of fundamentally different objects. A typical example which springs first to mind is the special values of L-functions, in particular, the Riemann zeta function $\zeta(k)$ (which will be explained in detail in Chapter 2). For each integer k, we sum up all positive integers n, raising to a negative power n^{-k}

$$\zeta(k) = \sum_{n=1}^{\infty} n^{-k}.$$

Since $n^{-k} = \frac{1}{n^k}$ gets smaller and smaller as n grows, we really get this number $\zeta(k)$ (if $k > 1$) sitting somewhere on the positive real coordinate line. Number theorists are supposed to study numbers, and in particular, integers. Thus this kind of sum of all integers should be interesting. Of course, one hopes to sum positive integer powers n^k. Obviously, even squares n^2 get larger and larger as n grows, and there seems to be no way of summing up all squares of integers. Nevertheless, in the mid-18th century, Euler computed the sum of positive integer powers. He introduced an auxiliary variable t and looked at

$$\zeta(-k) = t+2^k t^2+3^k t^3+4^k t^4+\cdots \Big|_{t=1}.$$

For example:

$$\zeta(0) = t+t^2+t^3+\cdots = \frac{t}{1-t}\Big|_{t=1} \quad \text{(the geometric series).}$$

Knowing that the derivative (with respect to t) of $t^n = \frac{dt^n}{dt} = nt^{n-1}$, we differentiate the right-hand side of the above formula and get $1+2t+3t^2+4t^3+\cdots$ which is quite near to $t+2t^2+3t^3+4t^4+\cdots$. Thus we get

$$\zeta(-1) = t\frac{d}{dt}(t+t^2+t^3+\cdots)\Big|_{t=1} = t\frac{d}{dt}\left\{\frac{t}{1-t}\right\}\Big|_{t=1}$$

and similarly, taking the derivatives k times, we get

$$\zeta(-k) = \left(t\frac{d}{dt}\right)^k (t+t^2+t^3+\cdots)\Big|_{t=1} = \left(t\frac{d}{dt}\right)^k \left\{\frac{t}{1-t}\right\}\Big|_{t=1}.$$

Still one cannot get the answer, because we cannot replace t by 1 in $\frac{t}{1-t}$. Now, when number theorists get to this point, in a hunt, they start to smell something interesting and will never give up the chance. Let's separate the sum into two parts, that is, the sum over even integers and the sum over odd integers. Then we see that

$$(1-2^{k+1})\zeta(-k) = (t+2^k t^2+3^k t^3+4^k t^4+\cdots\,|_{t=1})-2(2^k t+4^k t^2+6^k t^3+8^k t^4+\cdots\,|_{t=1})$$
$$= t-2^k t^2+3^k t^3-4^k t^k-\cdots = \left(t\frac{d}{dt}\right)^k (t-t^2+t^3-t^4+t^5-\cdots) = \left(t\frac{d}{dt}\right)^k \left\{\frac{t}{1+t}\right\}\Big|_{t=1}.$$

This time we have won, because we can really put 1 in place of t and get a number, which (after dividing by $(1-2^{k+1})$) Euler declared to be the value $\zeta(-k)$. It is then easy to see that $\zeta(-k) = 0$ for even integers $k > 0$; thus we may concentrate on the odd negative ζ-values $\zeta(1-2m)$ for positive integer m. The most remarkable fact Euler discovered in this context is the following relation (whose proof will be given in §2.2 and in Chapter 8):

$$\zeta(2m) = (-1)^m\frac{(2\pi)^{2m}}{2(2m-1)!}\zeta(1-2m) = (1-2^{2m})^{-1}(-1)^m\frac{(2\pi)^{2m}}{2(2m-1)!}\left(t\frac{d}{dt}\right)^k\left\{\frac{t}{1+t}\right\}\Big|_{t=1}.$$

The left-hand side is the actual sum of negative powers n^{-2m} over positive integers and the right-hand side is the value of the ratio of suitable polynomials in t. This is a remarkable interaction of an infinite sum and derivatives of a polynomial created by Euler.

There is another example of this kind. Let us fix one prime, say 5. Suppose you live in a country under a very crazy dictator, who decreed that two points are 'near' if the distance between them measured by meters is divisible by very high power of 5; so if you sit $5^3 = 125$ meters distance from a friend, you are 'near' to him. If you sit $5^5 = 3125$ meters distance away, then you are 'very close' to him, and so on. This type of topology (called the p-adic topology) was created by Kummer and his student Hensel in the 19th century. Naturally, the world with this topology is very different from our own one, but number theorists free from any worldly restrictions can look into such strange places (see §1.3 for details). Looking into Euler's formula of $\zeta(-k)$, Kummer discovered that if k is close to k' in his (5-adic) sense, $\zeta(-k)$ is again close to $\zeta(-k')$. In other words, if $k-k'$ is divisible by $5^n 4$, then $\zeta(-k)-\zeta(-k')$ is divisible by 5^{n+1}. Thus ζ is not only a function of integers but is a function of numbers in this new 5-adic world. The newly obtained function is called the 5-adic ζ-function. Of course, one can work choosing a prime p different from 5 and create the world measured by the power of p: the p-adic topology. Then we again find the p-adic ζ-function (this perspective of viewing results of Kummer as p-adic zeta functions was introduced by Kubota and Leopoldt in the 1960's). This is the world in which I have a great interest. The reader will find many p-adic L-functions in this book along the way of studying the values of L-functions of modular forms on the algebraic groups $GL(1)$ and $GL(2)$. The modular p-adic L-functions for $GL(2)$ have many variables (see Chapter 7 and 10), and the discovery of a new set of natural variables for the modular p-adic L-functions may be the only legitimate "raison d'être" of this book apart from the educational point of view. This means that for

the zeta functions of algebraic groups, the interaction of their values is much more intense than in the classical abelian case of GL(1). Moreover, the p-adic or complex L-functions and Eisenstein series studied in this book are naturally associated to analytic Galois representations into GL_n $(1 \leq n \leq 2)$. We briefly touch this point in Chapter 7.

The principal text is an outgrowth of courses given at UCLA (U.S.A.), Hokkaido University (Japan), Université de Paris-Sud and Université de Grenoble (France). It is my pleasure to acknowledge encouragement from the small audiences I always had in all of these lectures. Many people helped me to write correct Mathematics and correct English. Especially, I am grateful to A. Bluher, K. Chandrashekhar, Y. Maeda, J. Tilouine and B. Wilson for reading some of the chapters and giving me many useful suggestions. I should also acknowledge the help I got, in writing a readable text in a precise format, from D. Tranah who is the publishing director at the Cambridge university press. While I was writing this book, I was partially supported by a grant from the National Science Foundation and by a fellowship from John Simon Guggenheim Memorial Foundation.

September 25, 1992 at Los Angeles

Haruzo Hida

Suggestions to the reader

The principal text of this book consists of 10 Chapters. The first chapter summarizes results from the theory of Linear algebras, algebraic number fields and p-adic numbers, which is used in later chapters. For the first reading, the reader is suggested to start from Chapter 2 skipping Chapter 1 and, from time to time, to consult Chapter 1 when results there are quoted in the principal text. After Chapter 2, all the chapters (and the sections) are ordered from basics to more sophisticated subjects, although logically several chapters are independent. Within the same section, the numbered formula (or statement) is quoted just by its number. If the formula or statement is quoted from another section within the same chapter, the section number precedes the number of the formula or the statement. Namely, the formula (1) in Section 2 is quoted as (2.1), and Theorem 2 in Section 3 is quoted as Theorem 3.2. This principle also applies when a numbered statement or a formula is quoted from different chapters; for example, Proposition 3.2.1 implies Proposition 1 in Section 2 of Chapter 3.

We use the standard symbols in the books. For example, $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ and $\mathbf{C}$ denote the ring of rational integers, the field of rational numbers, the field of real numbers and the field of complex numbers, respectively. The symbol $\mathbf{N}$ is used for the set of non-negative integers including 0. The ring of p-adic integers is denoted by $\mathbf{Z}_p$ for each prime p whose field of fractions is written as $\mathbf{Q}_p$, the field of p-adic numbers. We write $\overline{\mathbf{Q}}$ for the field of all numbers algebraic over $\mathbf{Q}$ in $\mathbf{C}$. Any subfield of $\overline{\mathbf{Q}}$ which is of finite dimension over $\mathbf{Q}$ is called a *number field.* Thus $\overline{\mathbf{Q}}$ is already embedded into $\mathbf{C}$. We sometimes but not so often write this embedding as ι_∞. We fix once and for all an algebraic closure $\overline{\mathbf{Q}}_p$ and an embedding ι_p of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_p$. Thus $\overline{\mathbf{Q}}$ is also a subfield of $\overline{\mathbf{Q}}_p$. We denote by $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ the group of all field automorphisms of $\overline{\mathbf{Q}}$. Each element $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $\overline{\mathbf{Q}}$ from the right, and the composition gives the group structure on $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. We make the group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ into a profinite topological group declaring every subgroup fixing a number field to be an open subgroup (see [N, Chapter 1]).

For each commutative ring A with identity, we denote by $A^\times$ for the group of all invertible elements (i.e. units) in A. We denote by $M_n(A)$ the ring of all $n \times n$ square matrices with entries in A. We then define

$$GL_2(A) = \{X \in M_n(A) \mid \det(A) \in A^\times\} \text{ and } SL_n(A) = \{X \in M_n(A) \mid \det(X) = 1\}.$$

We write $GL(n)$ and $SL(n)$ for the linear algebraic group which assign to each commutative algebra A, the group $GL_n(A)$ and $SL_n(A)$, respectively. For any maps $f : X \to Y$ and $g : Y \to Z$, we write $g \circ f : X \to Z$ for the map given by composition $g \circ f(x) = g(f(x))$.

Chapter 1. Algebraic Number Theory

To make this text as self-contained as possible, we give a brief but basically self-contained sketch of the theory of algebraic number fields in §1.2. We also summarize necessary facts from linear (and homological) algebra in §1.1 and from the theory of p-adic numbers in §1.3. For a first reading, if the reader has basic knowledge of these subjects, he or she may skip this chapter and consult it from time to time as needed in the principal text of the book. We suppose in §1.2 basic knowledge of elementary number theory, concerning rational numbers and algebraic numbers, which is found in any standard undergraduate level text. We shall concentrate on what will be used in the later chapters. Readers who want to know more about algebraic number theory should consult [Bour1,3], [FT], [W1] and [N].

§1.1. Linear algebra over rings

We summarize in this section some facts from linear algebra and some from homological algebra. We will not give detailed proofs.

Let A be a commutative ring with identity. For two A-modules M and N, we write $\mathrm{Hom}_A(M,N)$ for the A-module of all A-linear maps of M into N. In particular, $M^* = \mathrm{Hom}_A(M,A)$ is called the A-dual module of M. A sequence of A-linear maps $M \xrightarrow{\alpha} N \xrightarrow{\beta} L$ is called "exact" (at N) if $\mathrm{Im}(\alpha) = \mathrm{Ker}(\beta)$. A sequence $\cdots \to M_{i-1} \to M_i \to M_{i+1} \to \cdots$ is called exact if it is exact at M_i for every i. It is easy to check that if $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} L \to 0$ is an exact sequence of A-modules, then for any A-module E,

(1a) $\quad 0 \to \mathrm{Hom}_A(L,E) \xrightarrow{\beta^*} \mathrm{Hom}_A(N,E) \xrightarrow{\alpha^*} \mathrm{Hom}_A(M,E)$ is exact,

where "*" indicates the natural pull back, i.e. $\beta^*\phi = \phi\circ\beta$. Similarly, we can show

(1b) $\quad 0 \to \mathrm{Hom}_A(E,M) \xrightarrow{\alpha_*} \mathrm{Hom}_A(E,N) \xrightarrow{\beta_*} \mathrm{Hom}_A(E,L)$ is exact,

where $\alpha_*\phi = \alpha\circ\phi$. The map β_* is known to be surjective if E is a projective A-module [HiSt, I.4.7]. For a given A-module M, we consider the exact sequence $0 \to R \xrightarrow{\alpha} P \to M \to 0$ in which P is a projective A-module. Then the first extension module $\mathrm{Ext}^1_A(M,N)$ for another A-module N is defined to be

$$\mathrm{Ext}^1_A(M,N) = \mathrm{Coker}(\alpha^* : \mathrm{Hom}_A(P,N) \to \mathrm{Hom}_A(R,N)).$$

It is well known that $\mathrm{Ext}^1_A(M,N)$ is well defined (up to isomorphism) independently of the choice of the projective module P [HiSt, III.2]. Now, out of the commutative diagram with exact rows:

$$\begin{array}{ccccccc} & & E & \xrightarrow{\alpha} & F & \xrightarrow{\beta} & G \to 0 \\ & & \downarrow a & & \downarrow b & & \downarrow c \\ 0 \to & M & \xrightarrow{\gamma} & N & \xrightarrow{\delta} & L, & \end{array}$$

we get the following long exact sequence (the snake lemma [HiSt, III, Lemma 5.1], [Bour1, I.1.4]):

$$\mathrm{Ker}(a) \xrightarrow{\alpha} \mathrm{Ker}(b) \xrightarrow{\beta} \mathrm{Ker}(c) \xrightarrow{d} \mathrm{Coker}(a) \xrightarrow{\gamma} \mathrm{Coker}(b) \xrightarrow{\delta} \mathrm{Coker}(c),$$

where the connecting map d is defined as follows. For any $x \in \mathrm{Ker}(c)$, we take $y \in F$ so that $\beta(y) = x$. Then $b(y)$ falls in $\mathrm{Ker}(\delta)$ because of the commutativity of the right square of the diagram. Thus we can find $z \in M$ so that $\gamma(z) = b(y)$ by the exactness at N. Then $d(x)$ is defined to be z modulo $a(E)$. We apply the above lemma in the following situation. Let $0 \to M \to N \to L \to 0$ be an exact sequence of A-modules. For a given A-module E, we take a projective A-module P and an A-module R to get an exact sequence $0 \to R \xrightarrow{a} P \xrightarrow{b} E \to 0$. Then we have the following commutative diagram whose rows are exact:

$$\begin{array}{ccccccc} 0 \to & \mathrm{Hom}_A(E,M) & \to & \mathrm{Hom}_A(E,N) & \to & \mathrm{Hom}_A(E,L) & \\ & \downarrow b_M{}^* & & \downarrow b_N{}^* & & \downarrow b_L{}^* & \\ 0 \to & \mathrm{Hom}_A(P,M) & \to & \mathrm{Hom}_A(P,N) & \to & \mathrm{Hom}_A(P,L) & \to 0 \\ & \downarrow a_M{}^* & & \downarrow a_N{}^* & & \downarrow a_L{}^* & \\ 0 \to & \mathrm{Hom}_A(R,M) & \to & \mathrm{Hom}_A(R,N) & \to & \mathrm{Hom}_A(R,L). & \end{array}$$

Note that $\mathrm{Coker}(a_X{}^*) = \mathrm{Ext}^1_A(E,X)$ for $X = M$, N and L. Then the snake lemma shows

Theorem 1. *For each exact sequence* $0 \to M \to N \to L \to 0$ *of* A*-modules and for each* A*-module* E, *we have the following seven term exact sequence:*

$$0 \to \mathrm{Hom}_A(E,M) \to \mathrm{Hom}_A(E,N) \to \mathrm{Hom}_A(E,L)$$
$$\to \mathrm{Ext}^1_A(E,M) \to \mathrm{Ext}^1_A(E,N) \to \mathrm{Ext}^1_A(E,L).$$

The above sequence is a part of the long exact sequence of extension groups [HiSt, IV.7.5]. By the above sequence, the group $\mathrm{Ext}^1_A(E,M)$ measures the deviation from being surjective of the map β_* in (1b).

When A is a valuation ring with a prime element ϖ, we can easily compute $\mathrm{Ext}^1_A(E,M)$ for some E and M. By definition, if E is projective, $\mathrm{Ext}^1_A(E,M) = 0$. We now compute $\mathrm{Ext}^1_A(E,A)$ when $E = A/\varpi^r A$. We have the exact sequence $0 \to A \xrightarrow{\varpi^r} A \to E \to 0$. Then by Theorem 1 and (1a), we have the following exact sequence:

$$0 \to \mathrm{Hom}_A(A,A) \cong A \xrightarrow{\varpi^r} \mathrm{Hom}_A(A,A) \cong A \to \mathrm{Ext}^1_A(E,A) \to 0,$$

which shows $\mathrm{Ext}^1_A(A/\varpi^r A,A) \cong A/\varpi^r A$. Each torsion A-module E of finite type is a direct sum of finitely many cyclic modules of the form $A/\varpi^r A$. As is easily seen from the definition, the functor Ext^1_A satisfies

(2) $\mathrm{Ext}^1_A(E\oplus E',M) \cong \mathrm{Ext}^1_A(E,M)\oplus \mathrm{Ext}^1_A(E',M)$ (see [HiSt, III.4.1]).

This shows

Corollary 1. *Suppose that* A *is a valuation ring. Let* E *be a torsion* A*-module of finite type. Then* $\mathrm{Ext}^1_A(E,A) \cong E$ *(canonically).*

Let M and N be two A-modules. We define the tensor product $M\otimes_A N$ with a bilinear map $\iota : M\times N \to M\otimes_A N$ as a solution of the following universality problem. For any given A-bilinear map $\phi : M\times N \to E$ for any given third A-module E, there is a unique A-linear map $\phi_* : M\otimes_A N \to E$ such that $\phi = \phi_*\circ\iota$. We write $\iota(a,b) = a\otimes b \in M\otimes_A N$. If $M\otimes_A N$ exists, the uniqueness of $M\otimes_A N$ up to isomorphism is clear. We can construct $M\otimes_A N$ as follows. Let $A[M\times N]$ be the free A-module generated by elements of $M\times N$. We consider the A-submodule X in $A[M\times N]$ generated by elements of the form

$$(x+x',y)-(x,y)-(x',y),\ (x,y+y')-(x,y)-(x,y') \text{ and } (ax,y)-(x,ay)$$

for $x \in M$, $y \in N$ and $a \in A$. Then $A[M\times N]/X$ satisfies the required universal property of $M\otimes_A N$, where $x\otimes y$ is the image of (x,y) in the quotient. We see easily the following properties:

$$\begin{array}{ccc} M\otimes_A N \cong N\otimes_A M & \text{and} & (M\otimes_A N)\otimes_A E \cong M\otimes_A(N\otimes_A E) \\ x\otimes y \leftrightarrow y\otimes x & & (x\otimes y)\otimes z \leftrightarrow x\otimes(y\otimes z), \end{array}$$

and

$$\begin{array}{c} M\otimes_A E \xrightarrow{\alpha\otimes id} N\otimes_A E \xrightarrow{\beta\otimes id} L\otimes_A E \to 0 \text{ is exact} \\ m\otimes e \mapsto \alpha(m)\otimes e;\ n\otimes e \mapsto \beta(n)\otimes e \end{array}$$

for each exact sequence $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} L \to 0$. As a dual version of the extension functor Ext, we can now construct the torsion functor Tor as follows. For each A-module M, we take an exact sequence.

$$0 \to R \xrightarrow{\alpha} P \to M \to 0 \text{ for a projective A-module } P.$$

Then we define for another A-module N

$$\mathrm{Tor}_1^A(M,N) = \mathrm{Ker}(\alpha\otimes id : R\otimes N \to P\otimes N).$$

Similarly to Theorem 1 (see [HiSt, III.8.3]), we get

Theorem 2. *For each exact sequence* $0 \to M \to N \to L \to 0$ *of* A*-modules, and for each A-module* E*, we have the following seven term exact sequence:*

$$\mathrm{Tor}_1^A(M,E) \to \mathrm{Tor}_1^A(N,E) \to \mathrm{Tor}_1^A(L,E) \to M\otimes_A E \to N\otimes_A E \to L\otimes_A E \to 0.$$

When B and C are A-algebras, $B\otimes_A C$ is naturally an A-algebra via the multiplication $(b\otimes c)(b'\otimes c') = bb'\otimes cc'$. We now suppose that A is a field K of characteristic 0. For any K-vector spaces V with basis $\{v_i\}_{i\in I}$ and W with basis $\{w_j\}_{j\in J}$, it is obvious from the definition that $\{v_i\otimes w_j\}_{(i,j)\in I\times J}$ form a basis of $V\otimes_K W$. Thus if V and W are finite dimensional,

$$\dim_K(V\otimes_K W) = (\dim_K V)(\dim_K W). \tag{3}$$

Let M/K and F/K be field extensions in a fixed algebraically closed field Ω containing K. Suppose that M/K is finite and F contains all conjugates of M over K. Then it is well known that the set of all the field embeddings $I = I(M/K)$ into F is linearly independent over K in $\mathrm{Hom}_K(M,F)$ (a theorem of Dedekind [Bour3, V.7.5]). Note that $\sigma \in I$ induces $\sigma\otimes\mathrm{id} : M\otimes_K F \to F$, which is a homomorphism of K-algebras. Thus we have a K-algebra homomorphism:

$$\iota : M\otimes_K F \to F^I \text{ given by } \iota(m\otimes f) = (f\sigma(m))_{\sigma\in I},$$

where F^I is the product of I copies of F. The morphism ι is injective because of the theorem of Dedekind. By comparing the dimensions, we know that

$$M\otimes_K F \cong F^I \text{ as K-algebras.} \tag{4}$$

This applies when $F = \mathbf{C}$ for example and we have $M\otimes_{\mathbf{Q}}\mathbf{C} \cong \mathbf{C}^{[M:\mathbf{Q}]}$. The situation for $F = \mathbf{R}$ is a little bit different. We have from (4)

$$M\otimes_{\mathbf{Q}}\mathbf{R} \cong \mathbf{R}^I \ (I = I(M/\mathbf{Q})) \text{ if M is totally real.} \tag{5a}$$

Here M is called "totally real" if all the field embeddings of M into $\mathbf{C}$ in fact have values in $\mathbf{R}$. If M is not totally real, we split $I(M/\mathbf{Q}) = I(\mathbf{R})\coprod I(\mathbf{C})$ for real embeddings $I(\mathbf{R})$ and non-real embeddings $I(\mathbf{C})$. Then we can further split $I(\mathbf{C}) = \Sigma\coprod\Sigma c$ for complex conjugation c, and we consider the map $\iota : M\otimes_{\mathbf{Q}}\mathbf{R} \to \mathbf{R}^{I(\mathbf{R})}\times\mathbf{C}^{\Sigma}$ given by $\iota(m\otimes r) = (\sigma(m)r)_{\sigma\in I(\mathbf{R})\coprod\Sigma}$. Then the range and the domain of ι have the same dimension over $\mathbf{R}$. The injectivity of ι follows from Dedekind's theorem, and hence we obtain

$$M\otimes_{\mathbf{Q}}\mathbf{R} \cong \mathbf{R}^{I(\mathbf{R})}\times\mathbf{C}^{\Sigma} \text{ for } I(M/\mathbf{Q}) = I(\mathbf{R})\coprod\Sigma\coprod\Sigma c. \tag{5b}$$

We now note a simple fact about the existence of a basis of $\mathbf{Z}$-modules. If M is

a $\mathbf{Z}$-submodule of finite type in $\mathbf{Q}$, then we can find $t \in \mathbf{Q}$ such that $M = t\mathbf{Z} = \{mt \mid m \in \mathbf{Z}\}$. In fact, M can be written as $M = t_1\mathbf{Z}+t_2\mathbf{Z}+\cdots+t_r\mathbf{Z}$. Thus M has a unique minimal positive element t provided $M \neq 0$. For each $0 \neq m \in M$, by the Euclid division algorithm, we can write $m = tq+r$ with the quotient $q \in \mathbf{Z}$ and remainder r with $0 \leq r < t$. The remainder has to be 0 by the minimality of t. Thus $M = t\mathbf{Z}$. If V is a one dimensional $\mathbf{Q}$-vector-space, we can identify V with $\mathbf{Q}$ by taking a basis of V. Thus any $\mathbf{Z}$-submodule of finite type in V is generated over $\mathbf{Z}$ by one element. Now let V be a $\mathbf{Q}$-vector-space of finite dimension n. Let M be a $\mathbf{Z}$-submodule of finite type which contains a basis of V. Then we can find a basis $\{t_1, \ldots, t_n\}$ of V such that $M = \sum_{i=1}^{n} \mathbf{Z}t_i$. This can be shown by induction on n as follows. Taking a subspace W of V of dimension n-1, $M \cap W$ is of finite type over $\mathbf{Z}$ [Bour3, VIII.2]. By induction, $M \cap W$ has a basis $t_1, \ldots, t_{n-1}$, so $M/M \cap W$ is a $\mathbf{Z}$-submodule of finite type in the one dimensional space V/W and hence has a unique generator over $\mathbf{Z}$. Thus taking any $t_n \in M$ whose image in $M/M \cap W$ is a generator, we see that $\{t_1, \ldots, t_n\}$ gives a basis of M.

§1.2. Algebraic number fields

In this section, we denote by F a number field and by $\mathcal{O}$ the integer ring of F. By a number field, we mean a finite dimensional field extension of the rational number field $\mathbf{Q}$. Then $\mathcal{O}$ is the set of all elements in F satisfying a monic integral polynomial equation. Since $\mathbf{Z}$ is a principal ideal domain, $\mathcal{O}$ is of finite type as a $\mathbf{Z}$-module ([Bour1, V.1.6]), and we know that

(1a) $\mathcal{O}$ is a ring and has a basis $\{\omega_1, \ldots, \omega_d\}$ over $\mathbf{Z}$ for $d = \dim_{\mathbf{Q}} F$.

An $\mathcal{O}$-submodule $\mathfrak{a} \neq \{0\}$ of F which is of finite type over $\mathcal{O}$ (i.e. finitely generated over $\mathcal{O}$) is called a fractional ideal of F. A non-zero $\mathcal{O}$-submodule $\mathfrak{a}$ is a fractional ideal if and only if $\mathcal{O} \supset \lambda\mathfrak{a}$ for some $\lambda \in F^{\times}$. By this fact, $\mathfrak{a}$ is of finite type over $\mathbf{Z}$ and $\mathfrak{a} \otimes_{\mathbf{Z}} \mathbf{Q} \cong F$ via $a \otimes b \mapsto ab$. Taking a generator α_1 of $\mathbf{Q}\omega_1 \cap \mathfrak{a}$, whose existence is assured by the above claim, we consider the quotient $\mathfrak{a}/\mathbf{Z}\alpha_1$. We see that $\dim_{\mathbf{Q}}(\mathfrak{a}/\mathbf{Z}\alpha_1) \otimes \mathbf{Q}$ is one less than that of $\mathfrak{a} \otimes \mathbf{Q}$. Thus by induction on the dimension, we have

(1b) Any fractional ideal $\mathfrak{a}$ has a basis $\{\alpha_1, \ldots, \alpha_d\}$ over $\mathbf{Z}$.

Fixing a basis $\{\omega_1, \ldots, \omega_d\}$ of $\mathcal{O}$ over $\mathbf{Z}$, which is also a basis of F over $\mathbf{Q}$, we can express for $a \in F$, $a\omega_i = \sum_{j=1}^{d} a_{ji}\omega_j$ with $a_{ij} \in \mathbf{Q}$. In parcular, $a_{ij} \in \mathbf{Z}$ if $a \in \mathcal{O}$. We now define $\rho(a) \in M_d(\mathbf{Q})$ by

$$(a\omega_1,\ldots,a\omega_d) = (\omega_1,\ldots,\omega_d)\rho(a) \text{ with } \rho(a) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & \cdots & a_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{pmatrix} \in M_d(\mathbf{Q}).$$

Note that $\rho(a) = a1_d$ if $a \in \mathbf{Q}$, where 1_d is the $d\times d$ identity matrix. We see $\rho(ab) = \rho(a)\rho(b)$ and thus $\rho : F \to M_d(\mathbf{Q})$ is a $\mathbf{Q}$-algebra homomorphism, which is called the regular representation of F over $\mathbf{Q}$, and a is a root of the characteristic polynomial $\det(X1_d-\rho(a))$. We define

$$\mathrm{Tr}(a) = \mathrm{Tr}_{F/Q}(a) = \mathrm{Tr}(\rho(a)) \text{ and } N_{F/Q}(a) = N(a) = \det(\rho(a)).$$

We know that the trace Tr is $\mathbf{Q}$-linear and the norm N is a multiplicative map (i.e. $N(ab) = N(a)N(b)$ and $N(1) = 1$). When K/F is a finite extension and $\{w_1, \ldots, w_r\}$ is a basis of K over F, then obviously $\{\omega_i w_j\}_{i=1,\ldots,d,\, j=1,\ldots,r}$ gives a basis of K. The regular representation ρ_K of K with respect to this basis satisfies

$$\rho_K(a) = \rho(a)\otimes 1_r \text{ for the } r\times r \text{ identity matrix } 1_r \text{ for all } a \in F.$$

This shows that $N_{K/Q}(a) = N_{F/Q}(a)^{[K:F]}$.

Let I be the set of all fractional ideals of F. We define the product $\mathfrak{a}\mathfrak{b}$ of $\mathfrak{a}, \mathfrak{b} \in I$ by $\mathfrak{a}\mathfrak{b} = \{\sum_i \lambda_i a_i b_i : \text{finite sum} \mid \lambda_i \in \mathcal{O},\ a_i \in \mathfrak{a} \text{ and } b_i \in \mathfrak{b}\}$. The set $\mathfrak{a}\mathfrak{b}$ is clearly an $\mathcal{O}$-submodule of F. If α_i (resp. β_j) generates $\mathfrak{a}$ (resp. $\mathfrak{b}$), then $\alpha_i\beta_j$ generates $\mathfrak{a}\mathfrak{b}$ and hence $\mathfrak{a}\mathfrak{b}$ is finitely generated; i.e., it is a fractional ideal. We note that

(1c) *I is a group with the identity $\mathcal{O}$ under the above multiplication.*

This follows from the following lemma:

Lemma 1. *For a given fractional ideal $\mathfrak{a}$, there is another fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \alpha\mathcal{O}$ for $\alpha \in F^\times$.*

By the lemma, $\mathfrak{a}^{-1} = \alpha^{-1}\mathfrak{b}$ and I is a group. We first prove

Sublemma. *Let $f(X) = \sum_{i=0}^m a_i X^{m-i}$ and $g(X) = \sum_{j=0}^n b_j X^{n-j}$ be polynomials with coefficients in $\mathcal{O}$ ($a_0b_0 \neq 0$). Let $0 \neq \lambda \in \mathcal{O}$. If all the coefficients of $f(X)g(X)$ are divisible by λ in $\mathcal{O}$, then a_ib_j is divisible by λ for all (i,j).*

Proof. We claim that if all coefficients of a polynomial P(X) are algebraic integers, then for each root ξ of $P(X) = 0$, all the coefficients of the polynomial $\frac{P(X)}{X-\xi}$ are algebraic integers. In fact, if $P(X) = aX+b$, then $\frac{P(X)}{X-\xi} = a$ as a

polynomial and hence the assertion is true in this case. Now we complete the proof by induction on $\deg(P(X))$. Write $\deg(P(X)) = n$ and write a for the coefficient in X^n of $P(X)$. Then $P(X)-a(X-\xi)X^{n-1}$ has degree less than n and hence by the induction hypothesis, $\frac{P(X)}{X-\xi} - aX^{n-1}$ has (algebraic) integer coefficients. Thus $\frac{P(X)}{X-\xi}$ itself has (algebraic) integer coefficients. This proves the claim. Write $\xi_1, \ldots, \xi_n$ for the roots of $P(X)$, i.e. $P(X) = a(X-\xi_1)(X-\xi_2)\cdot\cdots\cdot(X-\xi_n)$; then, by the above claim, $a\prod_{i\in A}(X-\xi_i)$ has integral coefficients for any subset A of $\{1, 2, \ldots, n\}$, that is, $a\prod_{i\in A}(X-\xi_i)\,|_{X=0} = \pm a\prod_{i\in A}\xi_i$ is an algebraic integer. Returning to the lemma, we apply this fact to the roots of $f(X)g(X)/\lambda = 0$. Let $\xi_1,\ldots, \xi_m$ be all the roots of $f(X) = 0$ and $\eta_1, \ldots, \eta_n$ be all the roots of $g(X)$. Then by the above argument, for any subsets A of $\{1, 2, \ldots, m\}$ and B of $\{1, 2, \ldots, n\}$, $\frac{a_0b_0}{\lambda}\prod_{i\in A}\xi_i\prod_{i\in B}\eta_i$ is an algebraic integer. On the other hand, $a_i = \pm\sum_{\#(A)=i}a_0\prod_{\alpha\in A}\xi_\alpha$ and $b_j = \pm\sum_{\#(B)=j}a_0\prod_{\beta\in B}\eta_\beta$. Thus $\frac{a_ib_j}{\lambda}$ is the sum of several algebraic integers of the form $\frac{a_0b_0}{\lambda}\prod_{i\in A}\xi_i\prod_{i\in B}\eta_i$, and hence is an algebraic integer, i.e., a_ib_j is divisible by λ.

Now we prove the lemma. Let $\mathfrak{a} = a_1\mathbf{Z}+\cdots+a_d\mathbf{Z}$. We may assume that $\mathfrak{a}$ is integral. Let $a_i^{(j)}$ $(a_i^{(1)} = a_i)$ be all the conjugates of a_i and put

$$f(X) = a_1X^{d-1}+a_2X^{d-2}+\cdots+a_d \text{ and } g(X) = \prod_{j=2}^{d}(a_1^{(j)}X^{d-1}+a_2^{(j)}X^{d-2}+\cdots+a_d^{(j)}).$$

Since $g(X) = N_{F/Q}(f(X))/f(X) = \sum_{i=0}^{n}b_iX^{n-i} \in \mathcal{O}[X]$ and $f(X)g(X) = \sum_{j=0}^{m}c_jX^{m-j} \in \mathbf{Z}[X]$, we can think of the greatest common divisor d of all the coefficients of $g(X)f(X)$. Let $\mathfrak{b} = b_0\mathcal{O}+b_1\mathcal{O}+\cdots+b_n\mathcal{O}$ which is an ideal of $\mathcal{O}$. Then by the sublemma, a_ib_j is divisible by d (i.e. $a_ib_j \in d\mathcal{O}$) and hence $d\mathcal{O} \supset \mathfrak{ab}$. But by definition, d is the greatest common divisor of $c_1, \ldots, c_m$ and hence $d\mathbf{Z} = c_1\mathbf{Z}+c_2\mathbf{Z}+\cdots+c_m\mathbf{Z}$ which is contained in $\mathfrak{ab}$. This shows $\mathfrak{ab} \supset d\mathcal{O}$ and so $\mathfrak{ab} = d\mathcal{O}$.

Theorem 1. *Let $\mathcal{P}$ be the subgroup of I generated by principal ideals $\alpha\mathcal{O}$ for $\alpha \in F^\times$. Then the index of $\mathcal{P}$ in I is finite.*

The number $h = h(F) = (I:\mathcal{P})$ is called the class number of F. The quotient group $Cl_F = I/\mathcal{P}$ is called the class group of F. Before proving the theorem, we extend the norm map to ideals. Let $\mathfrak{a} \neq 0$ be a fractional ideal. Choosing a basis $\alpha = (\alpha_1,\ldots,\alpha_d)$ of $\mathfrak{a}$, we can identify $\mathfrak{a} \cong \mathbf{Z}^d$. Since α is also a basis of F over $\mathbf{Q}$, we can identify F with $\mathbf{Q}^d$ via α. Then $F_\mathbf{R} = F\otimes_\mathbf{Q}\mathbf{R}$ can be identified with

the formal real span of α and thus $F_{\mathbf{R}} \cong \mathbf{R}^d$ as real vector spaces. That is, $F_{\mathbf{R}}/\mathfrak{a} \cong (\mathbf{R}/\mathbf{Z})^d$, which is compact. For any point $x \in F$, we can find a small neighborhood U in $F_{\mathbf{R}}$ so that U is isomorphically projected into $F_{\mathbf{R}}/\mathfrak{a}$. Thus, for any fractional ideal $\mathfrak{b}$ containing $\mathfrak{a}$, the image of $\mathfrak{b}$ in $F_{\mathbf{R}}/\mathfrak{a}$ is discrete because $\mathfrak{b}$ has only finitely many generators over $\mathbf{Z}$. Since $F_{\mathbf{R}}/\mathfrak{a}$ is compact, $\mathfrak{b}/\mathfrak{a}$ is a finite group. We now define for all fractional ideals $\mathfrak{a}$

$$N(\mathfrak{a}) = \frac{\#(\mathcal{O}/\mathcal{O}\cap\mathfrak{a})}{\#(\mathfrak{a}/\mathfrak{a}\cap\mathcal{O})} \in \mathbf{Q}^\times.$$

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *relatively prime* (or $\mathfrak{a}$ is *prime* to $\mathfrak{b}$), if $\mathfrak{a}+\mathfrak{b} = \mathcal{O}$. We then have an exact sequence

$$0 \to \mathfrak{a}\cap\mathfrak{b} \to \mathcal{O} \to (\mathcal{O}/\mathfrak{a})\oplus(\mathcal{O}/\mathfrak{b}) \to 0$$
$$x \mapsto (x \bmod \mathfrak{a})\oplus(x \bmod \mathfrak{b}).$$

Thus $N(\mathfrak{a}\cap\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ if $\mathfrak{a}+\mathfrak{b} = \mathcal{O}$. Since $\mathcal{O} \supset \mathfrak{a}$, multiplying by $\mathfrak{b}$, we see that $\mathfrak{b} = \mathfrak{b}\mathcal{O} \supset \mathfrak{a}\mathfrak{b}$. Similarly we see that $\mathfrak{a} \supset \mathfrak{a}\mathfrak{b}$ and hence $\mathfrak{a}\cap\mathfrak{b} \supset \mathfrak{a}\mathfrak{b}$. If $\mathfrak{a}+\mathfrak{b} = \mathcal{O}$, we can find $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a+b = 1$. Then we see that $x = xa+xb$ for any $x \in \mathfrak{a}\cap\mathfrak{b}$. Thus $x \in \mathfrak{a}\mathfrak{b}$. This shows that $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b}$ if $\mathfrak{a}+\mathfrak{b} = \mathcal{O}$. That is, we have

(2a) $$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}) \text{ if } \mathfrak{a}+\mathfrak{b} = \mathcal{O}.$$

Let L and L' be free $\mathbf{Z}$-modules of finite rank. Let $(\ ,\ )$ be an inner product on $L\times L'$ which is non-degenerate on both sides. Thus $\mathrm{rank}_{\mathbf{Z}}(L) = \mathrm{rank}_{\mathbf{Z}}(L')$. Let e_1 be the smallest positive integer in $\{(x,y) \mid x \in L \text{ and } y \in L'\}$. We take x_1 and y_1 such that $(x_1,y_1) = e_1$. Let $L_1 = \{w \in L \mid (w,y_1) = 0\}$. Then $L = x_1\mathbf{Z}\oplus L_1$. By definition, $x_1\mathbf{Z}\cap L_1$ is orthogonal to everything and hence is reduced to $\{0\}$. Let $z \in L$ with $(z,y_1) \neq 0$. By the division algorithm, $(z,y_1) = e_1q+r$ with $0 \le r < e_1$. Then $(z-qx_1,y_1) = r$. By the minimality, r has to be 0, that is, $z-qx_1 \in L_1$, or in other words, $x_1\mathbf{Z}+L_1 = L$. We also know that $(L,y_1) \subset e_1\mathbf{Z}$. Similarly $L' = y_1\mathbf{Z}\oplus L_1'$ for $L_1' = \{w \in L' \mid (x_1,w) = 0\}$. Repeating this process, we find two bases $x_1, \ldots, x_d$ of L and $y_1, \ldots, y_d \in L'$ such that $e_i = (x_i,y_j)\delta_{ij}$ for the Kronecker symbol δ_{ij} and $e_i \mid e_{i+1}$. We can apply this argument to the inner product $(x,y) = xA^ty$ for $x,y \in \mathbf{Z}^d$ and a matrix $A \in M_d(\mathbf{Z})$ with $\det(A) \neq 0$. Then we see $|\det(A)| = \det((x_i,y_j)) = \prod_{i=1}^d e_i = \#(\mathbf{Z}^d/\mathbf{Z}^dA)$. Applying this argument to $A = \rho(a)$ for $a \in \mathcal{O}$, we know that

(2b) $$N(a\mathcal{O}) = |N(a)|.$$

Thus $N : I \to \mathbf{Q}^\times$ coincides with the norm map on $\mathcal{P}$ up to absolute value. Thus N is a homomorphism of multiplicative group $\mathcal{P}$. Now take an ideal $\mathfrak{a}$

and its basis $\alpha = (\alpha_1,\ldots,\alpha_d)$. We identify a with $\mathbf{Z}^d$ via this basis. We then define the regular representation $\rho' : F \to M_d(\mathbf{Q})$ by

$$a\alpha = (a\alpha_i)_i = \sum_{j=1}^{d} a_{ji}\alpha_j = \alpha\rho'(a) \text{ with } \rho'(a) = (a_{ij}).$$

If we write $\alpha = \omega A$ for a basis $\omega = (\omega_1,\ldots,\omega_d)$ of O, we see $A\rho'(a)A^{-1} = \rho(a)$. Thus $N(a) = \det(\rho'(a))$. Then applying the above argument replacing O by a, we see that

(2c) $$|N(a)| = \#(a/aa) = N(aO).$$

Finally from the equality $\#(O/aa) = \#(O/a)\#(a/aa)$, we conclude that

(2d) $$N(aa) = N(aO)N(a).$$

Combining (2a-d), we see that

(3a) $N : I \to \mathbf{Q}_+ = \{a \in \mathbf{Q} \mid a > 0\}$ *is a homomorphism of multiplicative groups.*

Indeed, for any integral ideals a and b, we can find $a \in O$ such that $aa+b = O$. Then we see that

$$|N(a)|N(a)N(b) \overset{(2c,d)}{=} N(aa)N(b) \overset{(2a)}{=} N(aab) = |N(a)|N(ab)$$

and hence (3a). Since $N_{K/Q} : I \to \mathbf{Q}_+$ for any finite extension K/F is a multiplicative map satisfying $N_{K/Q}(aO_K) = N_{F/Q}(aO)^{[K:F]}$ for $a \in F^\times$, we see easily that

(3b) *for fractional ideals* a *of* F, $N_{K/Q}(aO_K) = N_{F/Q}(a)^{[K:F]}$.

To prove Theorem 1, we first prove the following lemma:

Lemma 2. *There exists a constant* C *depending only on* F *such that any ideal* a *in* O *contains a non-zero element* $\alpha \in a$ *with* $|N(\alpha)| \le CN(a)$.

Proof. Let $O = \mathbf{Z}\omega_1+\cdots+\mathbf{Z}\omega_d$. Let g be the greatest integer $[\sqrt[d]{N(a)}]$ not exceeding $\sqrt[d]{N(a)}$. Consider the set of numbers

$$S = \{n_1\omega_1+\cdots+n_d\omega_d \in O \mid 0 \le n_i \le \sqrt[d]{N(a)}\}.$$

Then $\#(S) = (g+1)^d > N(a) = \#(O/a)$. Thus there are at least two distinct elements $\beta, \gamma \in S$ such that $\beta \equiv \gamma \bmod a$. That is $0 \ne \alpha = \beta-\gamma = m_1\omega_1+\cdots+m_d\omega_d$ with $|m_i| \le \sqrt[d]{N(a)}$. Let $M = \max_{i,j}(|\omega_i^{(j)}|)$. Then

$$|N(\alpha)| = \prod_{j=1}^{d} |m_1\omega_1^{(j)}+\cdots+m_d\omega_d^{(j)}| \le d^dM^dN(a).$$

We can take d^dM^d as C.

We now give the proof of Theorem 1 (which is due to Hurwitz). Let c be a class in $I/\mathcal{P}$. Take an integral ideal a in c^{-1} and choose α as in the

lemma. Since $a \supset \alpha O$, we can find another integral ideal b such that $ab = \alpha O$. Thus $b \in$ c. On the other hand, $N(a)N(b) = |N(\alpha)| \le CN(a)$. Thus $N(b) \le C$. Thus every class c contains an ideal of norm less than C. The number of integral ideals of norm less than C is finite because the number of submodules of $\mathbf{Z}^d$ with index less than C is finite. Hence h is finite.

By the above proof, the constant C gives a bound of integral ideals with minimum norm in each ideal class and hence is very important. For example, if one can show that all integral ideals with norm less than C are principal, then h = 1. The constant $d^d M^d$ given in the proof of the lemma is not the best possible bound. The following estimates of C are well known:

(4) Minkowski's estimate: $C \le |\sqrt{D_F}| \frac{2^{2t} d!}{\pi^t d^d}$ (see below);

Siegel's estimate: $C \le \left(\frac{r}{d}\right)^d |D_F|$ when F is totally real [Si];

here $D_F = \det(\mathrm{Tr}(\omega_i\omega_j))$ for a basis $\{\omega_1, \ldots, \omega_d\}$ of O is the discriminant of F/**Q**, t is the number of complex places of F and $r = \left[\frac{d}{6}\right]$ or $\left[\frac{d}{6}\right]+1$ according as $d \equiv 1 \bmod 6$ or not. (Here [a] is the greatest integer not exceeding a.)

Exercise 1. Let

$$\mathcal{P}_+ = \{\alpha O \mid \alpha \in F,\ \alpha^\sigma > 0 \text{ for all field embeddings } \sigma \text{ of } F \text{ into } \mathbf{R}\},$$

$$I(m) = \{b = \frac{n}{d} \mid n \text{ and } d \text{ are integral and prime to } m\}$$

for a given ideal m, and $\mathcal{P}_+(m) = \mathcal{P}_+ \cap \{\alpha O \mid \alpha \in F^\times,\ \alpha \equiv 1 \bmod^\times m\}$, where $\alpha \equiv 1 \bmod^\times m$ means that $\alpha O \in I(m)$ and there exists $\beta \in \mathcal{P}_+$ such that $\beta O \in I(m)$, $\beta \in O$, $\alpha\beta \in O$ and $\alpha\beta \equiv \beta \bmod m$. Then show that $\mathcal{P}_+(m)$ is a subgroup of finite index in $I(m)$.

The finite group $CL_F(m) = I(m)/\mathcal{P}_+(m)$ is called the strict ray class group modulo m.

Exercise 2. (a) Using (4), show that the class number h(F) = 1 for the following fields: $\mathbf{Q}(\zeta)$, $\mathbf{Q}(\zeta+\zeta^{-1})$ for $\zeta^7 = 1$ but $\zeta \ne 1$, and $\mathbf{Q}(\sqrt[3]{2})$.
(b) Show that $h(F) \ge 2$ for $F = \mathbf{Q}(\sqrt{-5})$.

Exercise 3 (Minkowski). Using the estimate (4), show that $|D_F| > 1$ for any number field $F \ne \mathbf{Q}$.

An ideal p of O is called a prime ideal, if the residue ring O/p is an integral domain (i.e. having no zero divisor). When a prime ideal p is non-zero, O/p is

a finite integral domain. Thus for every $0 \neq a \in \mathcal{O}/p$, the sequence of elements $a, a^2, a^3, \ldots, a^n, \ldots$ in $\mathcal{O}/p$ has to overlap. Thus for some $i > j$, $a^i = a^j$. So $a^{i-j} = 1$. Thus we can always find a positive integer h such that $a^h = 1$. Therefore $a^{-1} = a^{h-1} \in \mathcal{O}/p$. Thus every non-zero element of $\mathcal{O}/p$ has an inverse and hence $\mathcal{O}/p$ is a finite field. Since ideals of a field are either $\{0\}$ or the total ring, there are no proper ideals in $\mathcal{O}$ containing p. Thus p is maximal. By definition, the ring $\mathcal{O}$ is normal (i.e. any element in F integral over $\mathcal{O}$ belongs to $\mathcal{O}$). A normal integral domain whose non-zero prime ideals are maximal is called a Dedekind domain (for further study of such rings, see [Bour1, VII.2]). For any ideal $\mathfrak{a}$, by Zorn's lemma, there exists a maximal ideal p containing $\mathfrak{a}$. Then $p^{-1}\mathfrak{a}$ is again an ideal of $\mathcal{O}$. In fact, multiplying $p \supset \mathfrak{a}$ by p^{-1}, we get $\mathcal{O} = pp^{-1} \supset \mathfrak{a}p^{-1}$. Thus $\mathfrak{a} = p\mathfrak{b}$ with an ideal $\mathfrak{b}$ of $\mathcal{O}$, and we have $N(\mathfrak{b}) < N(\mathfrak{a})$. Therefore, inductively, we can decompose $\mathfrak{a} = \prod_{p \text{ prime}} p^{e(p)}$ for finitely many maximal ideals p. We now claim as follows:

Theorem 2 (Dedekind). *Each fractional ideal $\mathfrak{a}$ can be decomposed uniquely as a product $\mathfrak{a} = \prod_{p \text{ prime}} p^{e(p)}$ of finitely many prime ideals (allowing negative powers). The ideal $\mathfrak{a}$ is integral (i.e. is contained in $\mathcal{O}$) if and only if $e(p) \geq 0$ for all p.*

Proof. The ring $\mathcal{O}/p$ has no zero-divisors, for if $a, b \in \mathcal{O}$ and $ab \in p$, then either $a \in p$ or $b \in p$. We now show for ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$, if a prime ideal p contains $\mathfrak{a}\mathfrak{b}$, then either $p \supset \mathfrak{a}$ or $p \supset \mathfrak{b}$. We may suppose that $\mathfrak{a}$ is not contained in p. Thus we have $a \in \mathfrak{a}$ with $a \notin p$. Since for each $b \in \mathfrak{b}$, $p \supset \mathfrak{a}\mathfrak{b} \ni ab$, we see $b \in p$ and hence $p \supset \mathfrak{b}$. We now suppose that an ideal $\mathfrak{a}$ in $\mathcal{O}$ has two prime decompositions $\mathfrak{a} = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ allowing repetition of primes. Since either $p \supset \mathfrak{a}$ or $p \supset \mathfrak{b}$ if $p \supset \mathfrak{a}\mathfrak{b}$, by renumbering the prime ideal q_i's, we may assume that $p_1 \supset q_1$. Since q_1 is a prime ideal, it is a maximal ideal, and hence $p_1 = q_1$. Dividing both sides by p_1, we get a new identity $p_2 \cdots p_m = q_2 \cdots q_n$. Repeating the above process, we finally know that $m = n$ and $p_i = q_i$ for $i = 1, \ldots, n$ after renumbering the q_i's. This shows the uniqueness of the prime decomposition. By definition, each fractional ideal $\mathfrak{f}$ can be written as $\mathfrak{f} = \frac{\mathfrak{a}}{\mathfrak{b}}$ for integral ideals $\mathfrak{a}$ and $\mathfrak{b}$. By the uniqueness of prime factorization for $\mathfrak{a}$ and $\mathfrak{f}\mathfrak{b}$ and $\mathfrak{b}$, the ideal $\mathfrak{f}$ has a prime factorization which is unique.

If p and q are distinct maximal ideals of $\mathcal{O}$, then $p+q = \mathcal{O}$. Taking $p \in p$ and $q \in q$ such that $p+q = 1$, for any given positive integer n, we can find a large N such that $1 = (p+q)^N \in p^n + q^n$. Thus $p^n + q^n = \mathcal{O}$. Similar reasoning shows that $\mathfrak{a}+\mathfrak{b} = \mathcal{O}$ if and only if there are no common prime factors in the prime factorizations of two ideals $\mathfrak{a}$ and $\mathfrak{b}$. We say that two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime if in the prime factorizations of $\mathfrak{a}$ and $\mathfrak{b}$ there are no common

prime factors in both the denominator and the numerator. We write $(a,b) = 1$ when a and b have no common prime factors.

Let $\mu(F)$ be the group of all roots of unity in $\mathcal{O}$. Let $\sigma_1, \ldots, \sigma_r : F \to \mathbf{R}$ denote all distinct real embeddings and choose complex embeddings $\sigma_{r+1}, \ldots, \sigma_{r+2t} : F \to \mathbf{C}$ so that $\{\sigma_{r+1}, \ldots, \sigma_{r+t}, \sigma_{r+t+1} = c\sigma_{r+1}, \ldots, \sigma_{r+2t} = c\sigma_{r+t}\}$ makes the set of all complex embeddings of F into $\mathbf{C}$, where c denotes complex conjugation. We simply write $\alpha^{(i)}$ for α^{σ_i} for $\alpha \in F$. For each fractional ideal a of F, taking a basis $\alpha = (\alpha_1, \ldots, \alpha_d)$ of a over $\mathbf{Z}$, we find the following formula:

$$(5) \qquad |\det(\alpha_j^{(i)})| = N(a)\sqrt{|D|} \text{ for } D = D_F.$$

To see this, we embed F into $F_{\mathbf{R}} = \mathbf{R}^r \times \mathbf{C}^t$ by $\iota : a \mapsto (a^{(i)})_{i=1,\ldots,r+t}$. Then we define a measure $d\mu$ on $F_{\mathbf{R}}$ by $\otimes_{i=1}^{r} dx_i \otimes_{j=1}^{t} |dx_j \otimes d\bar{x}_j|$, where for a variable $z = x+iy$ on $\mathbf{C}$ $(x, y \in \mathbf{R})$, $|dz \otimes d\bar{z}| = 2dxdy$. Then for d $(= r+2t)$ linearly independent vectors $v_j = (x_{ij})_{i=1,\ldots,r+t} \in F_{\mathbf{R}}$, it is an easy computation to see that the volume with respect to $d\mu$ of the parallelotope $V = V(v_1, \ldots, v_d)$ spanned by $v_1, \ldots, v_d$ is given by

$$\int_V d\mu = \begin{vmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,d} \\ \vdots & \vdots & \ddots & \vdots \\ x_{r+t,1} & x_{r+t,2} & \cdots & x_{r+t,d} \\ \bar{x}_{r+1,1} & \bar{x}_{r+1,2} & \cdots & \bar{x}_{r+1,d} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{r+t,1} & \bar{x}_{r+t,2} & \cdots & \bar{x}_{r+t,d} \end{vmatrix}.$$

Thus writing

$$A = A(a) = A(\alpha) = \begin{pmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \cdots & \alpha_d^{(1)} \\ \alpha_1^{(2)} & \alpha_2^{(2)} & \cdots & \alpha_d^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{(d)} & \alpha_2^{(d)} & \cdots & \alpha_d^{(d)} \end{pmatrix},$$

we see that $|\det(A)|$ is the volume of $V(\iota(\alpha_1), \ldots, \iota(\alpha_d))$, which is the fundamental domain for $F_{\mathbf{R}}/a$. Thus we see $N(a) = [\mathcal{O}:a] = \dfrac{|\det(A(a))|}{|\det(A(\mathcal{O}))|}$. Since $A^tA = (\mathrm{Tr}(\alpha_i\alpha_j))$, we get (5).

Now we want to determine the structure of the unit group $\mathcal{O}^\times$. Let $\mu(F)$ be the group of all roots of unity in $\mathcal{O}$. We simply write $\alpha^{(i)}$ for α^{σ_i} for $\alpha \in F$. First we prove

Lemma 3 (Kronecker). *For an integer* $\alpha \in \mathcal{O}$, *if* $|\alpha^{(i)}| = 1$ *for all* $i = 1,\ldots, r+t$, *then* α *is a root of unity.*

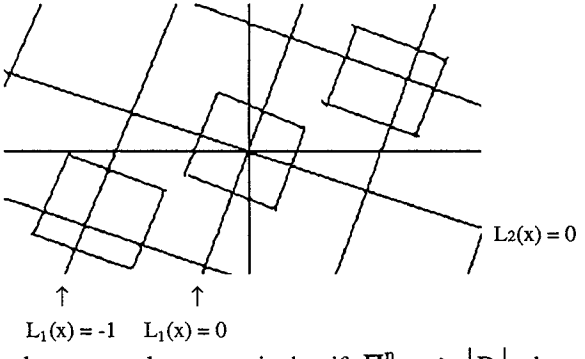
Proof. We can identify $F\otimes_{\mathbf{Q}}\mathbf{R}$ with $\mathbf{R}^r\times\mathbf{C}^t$ so that the projection of F to the i-th factor $\mathbf{R}$ or $\mathbf{C}$ is given by σ_i (see (1.5b)). Since a basis of $\mathcal{O}$ over $\mathbf{Z}$ is a basis of F over $\mathbf{Q}$ and hence is a basis of $F\otimes_{\mathbf{Q}}\mathbf{R}$ over $\mathbf{R}$, $\mathcal{O}$ is a (closed) discrete $\mathbf{Z}$-submodule of $\mathbf{R}^r\times\mathbf{C}^t$ (because identifying $\mathbf{R}^r\times\mathbf{C}^t$ with $\mathbf{R}^d$ via the basis of $\mathcal{O}$ over $\mathbf{Z}$, we know that the image of $\mathcal{O}$ in $\mathbf{R}^d$ is $\mathbf{Z}^d$). On the other hand, $S = \{(x_i) \in \mathbf{R}^r\times\mathbf{C}^t \mid |x_i| = 1\} \cong \{\pm 1\}^r\times S_1{}^t$ (with the circle S_1 of radius 1 in $\mathbf{C}$) is a compact set. Thus $\mathcal{O}\cap S$ is a discrete and compact set and hence is finite. Let $\mu = \{x \in \mathcal{O} \mid |x^{(i)}| = 1\}$. Then μ is a subgroup of $\mathcal{O}^\times$ and is contained in $S\cap\mathcal{O}$ and hence is a finite group. Thus μ is made of roots of unity.

Lemma 4 (Minkowski). *For given n-real linear forms* $L_i(x) = \sum_{q=1}^n a_{iq}x_q$ *on* $\mathbf{R}^n$, *suppose that* $D = \det(a_{pq}) \neq 0$. *Then for any positive numbers* $\kappa_1, \ldots, \kappa_n$ *such that* $\prod_{i=1}^n \kappa_i \geq |D|$, *there exist* $m = (m_1, \ldots, m_n) \in \mathbf{Z}^n$ *with not all* m_i *zero such that* $|L_i(m)| \leq \kappa_i$ *for all* i.

Proof. Consider the parallelotope $P_0 = \{x \in \mathbf{R}^n \mid |L_i(x)| \leq \frac{\kappa_i}{2}$ for all $i\}$. Similarly we consider the translation

$$P_m = \{x \in \mathbf{R}^n \mid |L_i(x-m)| \leq \frac{\kappa_i}{2} \text{ for all } i\}$$

whose center is an integer vector m. We can give the following illustration of the situation when $n = 2$:



If P_m and $P_{m'}$ for $m \neq m'$ have non-trivial intersection, then for $x \in P_m\cap P_{m'}$, we have $|L_i(x-m)| \leq \frac{\kappa_i}{2}$ and $|L_i(x-m')| \leq \frac{\kappa_i}{2}$ for all i. So we see $|L_i(m-m')| \leq \kappa_i$. Thus what we need to prove is that if $\prod_{i=1}^n \kappa_i \geq |D|$, then P_m and $P_{m'}$ intersect for some $m \neq m'$. We shall show that if $P_m\cap P_m' = \varnothing$ for all $m \neq m'$, then $\prod_{i=1}^n \kappa_i < |D|$. In fact then the volume J of the P_m's in a square $S(L) = \{x \in \mathbf{R}^n \mid |x_i| \leq L\}$ for any given L is less than 2^nL^n. Let $c = \mathrm{Max}_{x\in P_0}\{|x_1|,\ldots,|x_n|\}$. Then for $m \in \mathbf{Z}^n$, $|m_i| \leq L$ if and only if

$S(L+c) \supset P_m$. There are $(2L+1)^n$ such m's for each integer L. This shows that $(2L+1)^n \mathrm{vol}(P_0) < 2^n(L+c)^n$. By making L large, we know that $\mathrm{vol}(P_0) \le 1$ since $\lim_{L\to\infty} \frac{2^n(L+c)^n}{(2L+1)^n} = 1$. On the other hand, we see that

$$\mathrm{vol}(P_0) = \int\cdots\int_{P_0} dx_1dx_2\cdots dx_n$$
$$\overset{L_i(x)=y_i}{=} |D|^{-1}\int_0^{\kappa_1}\cdots\int_0^{\kappa_n} dy_1dy_2\cdots dy_n = |D|^{-1}\kappa_1\cdot\cdots\cdot\kappa_n.$$

This shows that $\kappa_1\cdot\cdots\cdot\kappa_n \le |D|$. By our assumption, $P_m \cap P_{m'} = \varnothing$ for all $m \ne m'$, P_0 does not contain any non-zero integer point. Since P_0 is a compact set, and $\mathbf{Z}^n-\{0\}$ is a closed discrete set, $\delta = \min_{x\in P_0,\, y\in \mathbf{Z}^n-\{0\}} (|x_1-y_1|, \ldots, |x_n-y_n|)$ exists and is a positive number. Thus if $0 < \varepsilon < \delta$, the system of inequalities $|L_i(x)| \le \kappa_i+\varepsilon$ has no integer solutions. Thus

$$\kappa_1\cdot\cdots\cdot\kappa_n < (\kappa_1+\varepsilon)\cdot\cdots\cdot(\kappa_n+\varepsilon) \le |D|,$$

which shows the desired assertion.

Corollary 1. *Let a be an ideal of O. There exists a constant C depending only on F such that for any given positive numbers $\kappa_1, \ldots, \kappa_d$ such that $\prod_{i=1}^d \kappa_i \ge CN(a)$ and $\kappa_i = \kappa_{i+t}$ for $r < i \le r+t$, we can find a non-zero element $\alpha \in a$ such that $|\alpha^{(i)}| < \kappa_i$ for all i.*

Proof. When all the field embeddings σ_i $(i=1, \ldots, d)$ of F into $\mathbf{C}$ actually take F into $\mathbf{R}$ (i.e. F is totally real), then we apply the above lemma to linear forms $L_i(x) = \sum_{j=1}^d \alpha_j^{(i)} x_j$ for a basis $\alpha_1, \ldots, \alpha_d$ of a over $\mathbf{Z}$. Then (by (5)), $|\det(\alpha_j^{(i)})| = N(a)\,|\sqrt{D}\,|$ for the discriminant $D = D_F$ of F and hence is non-zero. Let $C = \varepsilon + |\sqrt{D}\,|$ for some $\varepsilon > 0$. Then for any set of positive numbers $\kappa_1, \ldots, \kappa_d$ with $\kappa_1\cdot\cdots\cdot\kappa_d \ge CN(a)$, we can find slightly smaller $\kappa'_i < \kappa_i$ such that $\kappa_1\cdot\cdots\cdot\kappa_d \ge CN(a) > \kappa'_1\cdot\cdots\cdot\kappa'_d \ge N(a)|\sqrt{D}|$. Applying the lemma to κ'_i, we find $0 \ne m \in \mathbf{Z}^d$ such that $|L_i(m)| \le \kappa'_i < \kappa_i$. Then for $0 \ne a = m_1\alpha_1+\cdots+m_d\alpha_d \in a$, $|a^{(i)}| < \kappa_i$. When some embedding of F into $\mathbf{C}$ is not real, we apply the lemma to the constant $\kappa'_i = \kappa_i$ for $1 \le i \le r$ and $\kappa'_i = \kappa'_{i+t} = \kappa_i/\sqrt{2}$ for $r < i \le r+t$ and the linear forms $L_i(x) = \sum_{j=1}^d \alpha_j^{(i)} x_j$ for $1 \le i \le r$ and $L_i(x) = \mathrm{Re}(\sum_{j=1}^d \alpha_j^{(i)} x_j)$, $L_{i+t}(x) = \mathrm{Im}(\sum_{j=1}^d \alpha_j^{(i)} x_j)$ for $i > r$. Then the desired assertion is true again for $C = \varepsilon + |\sqrt{D}|$ for any $\varepsilon > 0$.

Exercise 4. (a) Write down all the steps of the proof of the above corollary when F is not totally real.
(b) By using the argument of the proof of Lemma 4 and Corollary 1, show that we can take $|\sqrt{D}|$ as the constant C in Lemma 2.

Now we prove the Dirichlet unit theorem:

Theorem 3 (Dirichlet). *There exists a free* $\mathbf{Z}$*-submodule* E *of rank* $r+t-1$ *in* $\mathcal{O}^\times$ *such that* $\mathcal{O}^\times = \mu(F)\times E$, *where we consider the multiplicative group* E *as an additive* $\mathbf{Z}$*-module.*

Proof. First we shall show that the multiplicative group $\mathcal{O}^\times$ contains $r+t-1$ multiplicatively independent elements (i.e., if one writes the group $\mathcal{O}^\times$ additively, we shall show that in $\mathcal{O}^\times$, there are $r+t-1$ linearly independent elements). Fix a basis $\omega_1,\dots,\omega_d$ of $\mathcal{O}$ over $\mathbf{Z}$. By Lemma 4, we have a positive constant C so that we can find an integer vector $m \in \mathbf{Z}^d$ such that $|\sum_{i=1}^d m_i\omega_i^{(j)}| < \kappa_i$ for all i if $\kappa_i\cdot\cdots\cdot\kappa_d \geq C$; thus, we can find a non-trivial algebraic integer $0 \neq \alpha \in \mathcal{O}$ such that $|\alpha^{(i)}| < \kappa_i$ for all i. In particular, applying this to $\kappa_i = \sqrt[d]{C}$ for all i, we can find $0 \neq \alpha \in \mathcal{O}$ such that $|N(\alpha)| < C$. Then we redefine $\kappa_i = |\alpha^{(i)}|$ for $i > 1$ and $\kappa_1 = C|\alpha^{(1)}|/|N(\alpha)|$ and applying Lemma 4, we can find $0 \neq \alpha_1 \in \mathcal{O}$ such that $|\alpha_1^{(1)}| < C\dfrac{|\alpha^{(1)}|}{|N(\alpha)|}$ and $|\alpha_1^{(i)}| < |\alpha^{(i)}|$ for all $i > 1$. In the same manner, we can find inductively $0 \neq \alpha_n \in \mathcal{O}$ such that

$$|\alpha_n^{(1)}| < C|\alpha_{n-1}^{(1)}|/|N(\alpha_{n-1})| \quad\text{and}\quad |\alpha_n^{(i)}| < |\alpha_{n-1}^{(i)}| \quad\text{for all } i > 1.$$

Then

$$|N(\alpha_n)| = \prod_{i=1}^d |\alpha_n^{(i)}| < C\frac{|\alpha_{n-1}^{(1)}|}{|N(\alpha_{n-1})|}\prod_{i=2}^d |\alpha_{n-1}^{(i)}| = C.$$

Since the number of ideals in $\mathcal{O}$ of norm less than C is finite, there are integers $0 < p < q$ such that $\alpha_p\mathcal{O} = \alpha_q\mathcal{O}$. Namely $\varepsilon_1 = \alpha_q/\alpha_p$ is a unit and $|\varepsilon_1^{(i)}| = |\alpha_q^{(i)}/\alpha_p^{(i)}| < 1$ for all $1 < i \leq r+t$. Since $|N(\varepsilon)| = 1$, we conclude $|\varepsilon_1^{(1)}| > 1$. Similarly, we can find a unit ε_j $(j = 1, \dots, r+t-1)$ such that $|\varepsilon_j^{(i)}| < 1$ for all $i \neq j$ and $1 \leq i \leq r+t$ and $|\varepsilon_j^{(j)}| > 1$. Now we want to show that $\varepsilon_1,\dots,\varepsilon_{r+t-1}$ are multiplicatively independent. That is, we want to show that the relation

$$\zeta\varepsilon_1^{n_1}\cdot\cdots\cdot\varepsilon_s^{n_s} = 1 \text{ for } \zeta \in \mu(F) \text{ and } s = r+t-1 \tag{6}$$

holds only when $\zeta = 1$ and $n_1 = n_2 = \cdots = n_s = 0$. For $\alpha \in F$, we write $l_i(\alpha) = log(|\alpha^{(i)}|)$ for $1 \leq i \leq r$ and $l_i(\alpha) = 2log(|\alpha^{(i)}|)$ for $r < i \leq r+t$. Then the multiplicative independence of ε_j is equivalent to

$$\det(R) \neq 0 \text{ for } R = \begin{pmatrix} l_1(\varepsilon_1) & l_1(\varepsilon_2) & \cdots & l_1(\varepsilon_s) \\ l_2(\varepsilon_1) & l_2(\varepsilon_2) & \cdots & l_2(\varepsilon_s) \\ \vdots & \vdots & \ddots & \vdots \\ l_s(\varepsilon_1) & l_s(\varepsilon_2) & \cdots & l_s(\varepsilon_s) \end{pmatrix} \tag{7}$$

Since $|\varepsilon_j^{(i)}| < 1$ for all $i \neq j$ and $1 \leq i \leq r+t$ and $|\varepsilon_j^{(j)}| > 1$, we know that $l_i(\varepsilon_j) < 0$ if $i \neq j$ and $l_j(\varepsilon_j) > 0$ and

$$\sum_{j=1}^{s} l_j(\varepsilon_i) = log(|N(\varepsilon_i)/\varepsilon_i^{s+1}|) > 0.$$

Generally $\det(a_{ij}) \neq 0$ under the following three conditions:

(i) $a_{ij} < 0$ for $i \neq j$, (ii) $a_{ii} > 0$ for all i and (iii) $\sum_{j=1}^{s} a_{ji} > 0$ for all i.

In fact, if $xA = 0$ for $A = (a_{ij})$ and a non-trivial $(x_1, \ldots, x_s) \in \mathbf{R}^s$, then we see that $a_{1p}x_1 + \cdots + a_{pp}x_p + \cdots + a_{sp}x_s = 0$. However, from $\sum_{j=1}^{s} a_{jp} > 0$, we know that $a_{pp} > -(a_{1p} + \cdots + a_{p-1p} + a_{p+1p} + \cdots + a_{sp})$ and from $a_{pp} = |a_{pp}|$ and $|a_{ip}| = -a_{ip}$ for $i \neq p$, we know that

$$|a_{pp}x_p| > -(a_{1p} + \cdots + a_{p-1p} + a_{p+1p} + \cdots + a_{sp})|x_p| \text{ if } x_p \neq 0.$$

Then taking the index p so that $|x_p| = \max(|x_i|)$,

$$\begin{aligned} |a_{pp}x_p| &> |a_{1p} + \cdots + a_{p-1p} + a_{p+1p} + \cdots + a_{sp}|\,|x_p| \\ &\geq |a_{1p}x_p| + \cdots + |a_{p-1p}x_p| + |a_{p+1p}x_p| + \cdots + |a_{sp}x_p| \quad (\text{because } a_{ip} = -|a_{ip}|) \\ &\geq |a_{1p}x_1| + \cdots + |a_{p-1p}x_{p-1}| + |a_{p+1p}x_{p+1}| + \cdots + |a_{sp}x_s| \\ &\geq |a_{1p}x_1 + \cdots + a_{p-1p}x_{p-1} + a_{p+1p}x_{p+1} + \cdots + a_{sp}x_s|, \end{aligned}$$

which is a contradiction. Thus A is invertible. We conclude that the only possible solution of (7) is $n_1 = n_2 = \cdots = n_s = 0$ and hence $\zeta = 1$.

Next we shall show that $H = \{\varepsilon_1^{n_1} \cdot \cdots \cdot \varepsilon_s^{n_s} \mid n = (n_1, \ldots, n_s) \in \mathbf{Z}^s\}$ is of finite index in $\mathcal{O}^\times$, which finishes the proof of the theorem. We consider $e = (l_1(\varepsilon), \ldots, l_s(\varepsilon)) \in \mathbf{R}^s$ for $\varepsilon \in \mathcal{O}^\times$. Since R is invertible, we can find a solution $x \in \mathbf{R}^s$ such that $Rx = e$; that is

$$|\varepsilon^{(i)}| = |(\varepsilon_1^{(i)})^{x_1} \cdot \cdots \cdot (\varepsilon_s^{(i)})^{x_s}| \text{ for all } i \leq s-1.$$

However, this is true even for $i = s$ because $|N(\varepsilon)| = |N(\varepsilon_i)| = 1$. Let $n_i = [x_i]$ be the maximal integer not exceeding x_i and define $\eta = \varepsilon_1^{n_1} \cdot \cdots \cdot \varepsilon_s^{n_s}$. Then $|(\varepsilon\eta^{-1})^{(i)}| \leq \operatorname{Sup}_{0 \leq x_i \leq 1} ((\varepsilon_1^{(i)})^{x_1} \cdot \cdots \cdot (\varepsilon_s^{(i)})^{x_s}) = M$, which is independent of the choice of ε. The number of integers with $|\alpha^{(i)}| \leq M$ for all i is finite and hence $(\mathcal{O}^\times : H) < +\infty$.

Exercise 5. Show that for any proper subset $S \neq \emptyset$ of $I = \{1, 2, \ldots, r+t\}$, there exists a unit $\varepsilon \in \mathcal{O}^\times$ such that $|\varepsilon^{(i)}| < 1$ for $i \in S$ and $|\varepsilon^{(i)}| > 1$ for any $i \in I\text{-}S$.

§1.3. p-adic numbers

We briefly recall the construction and properties of p-adic numbers in this section. We refer to [Kb] for more details. Recall the construction of real numbers out of rational numbers using Cauchy sequences. A sequence $\{a_n\}_{n\in\mathbf{N}}$ of rational numbers is called a Cauchy sequence if for any given small positive ε, there exists a large integer M such that if $m,n > M$, then $|a_m-a_n| < \varepsilon$. Then defining an equivalence relation on the totality $\mathcal{C}$ of Cauchy sequences by $\{a_n\} \approx \{b_n\}$ if $|a_n-b_n| \to 0$ as $n \to \infty$, we define the set of real numbers $\mathbf{R}$ to be $\mathcal{C}/\approx$. By assigning the constant sequence $\{a\}$ to each rational number a, the set of rational numbers $\mathbf{Q}$ is embedded into $\mathbf{R}$. The multiplication (resp. addition) of two Cauchy sequences $\{a_n\}$ and $\{b_n\}$ is defined to be the Cauchy sequence $\{a_nb_n\}$ (resp. $\{a_n+b_n\}$). This well defined ring structure induces a field structure on $\mathbf{R}$ which makes $\mathbf{R}$ an extension field of $\mathbf{Q}$. By construction, any Cauchy sequence of $\mathbf{R}$ has its limit inside $\mathbf{R}$.

Obviously we can perform the above process of completing $\mathbf{Q}$ for any absolute value $\| \ \|$ which is a function on $\mathbf{Q}$ having values in the non-negative real line (and may be different from the usual absolute value $| \ |$) satisfying

$$\|ab\| = \|a\|\,\|b\|, \quad \|a\| = 0 \Leftrightarrow a = 0 \text{ and } \|a+b\| \le \|a\|+\|b\|.$$

We can extend the absolute value to the completion by $\|b\| = \lim_{n\to\infty}\|b_n\|$ for the number b represented by the Cauchy sequence $\{b_n\}$. We list some examples of different absolute values in a somewhat more general setting. Let F be a number field and $\mathcal{O}$ be its integer ring. We fix a prime ideal $p \neq (0)$ of $\mathcal{O}$. For any $0 \neq x \in F$, we decompose the ideal $x\mathcal{O}$ into a product of (non-zero) prime ideals in $\mathcal{O}$ as guaranteed in Theorem 1.2.2. Let $v(x) = v_p(x)$ be the exponent of p in $x\mathcal{O}$. When the prime ideal p does not show up in the prime decomposition of $x\mathcal{O}$ (i.e. $x\mathcal{O}$ is prime to p), we simply put $v(x) = 0$. We also put $v(0) = \infty$ (i.e. (0) is divisible by p infinitely many times). Then we put $|x|_p = N(p)^{-v(x)}$. Then $x \mapsto |x|_p$ is a function having values in the non-negative real line, $|x|_p = 0 \Leftrightarrow x = 0$ and $|x|_p = 1 \Leftrightarrow x\mathcal{O}$ is prime to p. It is easy to check the following fact which implies the triangle inequality $\|a+b\| \le \|a\|+\|b\|$:

(1) $|x+y|_p \le \max(|x|_p, |y|_p)$, and the equality holds when $|x|_p \neq |y|_p$.

Let us now compute $|n!|_p$ for a given prime p and $n \in \mathbf{N}$. Let m be a unique integer such that $p^m \le n < p^{m+1}$. We define a sequence of integers $0 \le n_i < p^{m+1-i}$ and $0 \le a_i < p$ for $i = 0, 1, \ldots, m$ inductively as follows. First we put $n_0 = n$. We define $a_0 \in \mathbf{N}$ as the quotient of n_0 divided by p^m and n_1 as the remainder: $n_0 = a_0p^m+n_1$. Then we repeat this process replacing n_0 by n_1

and define a_1 and n_2 by $n_1 = a_1p^{m-1}+n_2$. Thus after having defined a_i and n_{i+1}, we define a_{i+1} and n_{i+2} by $n_{i+1}=a_{i+1}p^{m-i-1}+n_{i+2}$. Then we have

$$n = a_0p^m+a_1p^{m-1}+\cdots+a_m \text{ with } 0 \le a_i < p.$$

Let $s = a_0+a_1+\cdots+a_m$. Then we claim that $v_p(n!) = \frac{n-s}{p-1}$. Writing k_i for the number of multiples of p^i in the integers from 1 to n, we see that k_i is the largest integer not exceeding $\frac{n}{p^i}$, i.e.,

$$k_i = \left[\frac{n}{p^i}\right] = a_0p^{m-i}+a_1p^{m-i-1}+\cdots+a_{m-i},$$

and thus

$$v_p(n!) = \sum_{i=1}^{m} k_i = a_0(1+p+\cdots+p^{m-1})+a_1(1+p+\cdots+p^{m-2})+\cdots+a_{m-1} = \frac{n-s}{p-1}.$$

Thus we have

$$|n!|_p = p^{(s-n)/(p-1)} \text{ for } n \in \mathbf{N}. \tag{2}$$

Here is another example. Let $\sigma : F \to \mathbf{C}$ be a field embedding. Then we define $|x|_\sigma = |x^\sigma|$ using the usual absolute value $|\ |$ on $\mathbf{C}$. Then obviously $|\ |_\sigma$ is an absolute value. We denote by Σ the set of all absolute values on F. Two absolute values are said to be equivalent if they give an equivalent topology on F. Here the topology associated to a norm $|\ |$ is given by the metric $\rho(x,y) = |x-y|$. Each equivalence class of absolute values of F is called a place. Thus we have attached a place both to each maximal ideal p and to each complex embedding σ. It is known that the set of places of F corresponds bijectively to the disjoint union of the set of all (non-zero) prime ideals of $\mathcal{O}$ and the set of all complex embeddings of F modulo right multiplication by complex conjugation (see [Bour1, VI.6.4] or [W1, I]). Anyway, we hereafter identify the set of all places of F with the disjoint union of the set of all (non-zero) prime ideals of $\mathcal{O}$ and the set of all complex embeddings of F modulo right multiplication by complex conjugation c.

Exercise 1. Show that $|\ |_\sigma$ and $|\ |_\tau$ are different as places of F if the two embeddings σ and τ into $\mathbf{R}$ are different.

Let $|\ |_v$ be a place of F. Then v is either a complex embedding or a prime ideal of $\mathcal{O}$. We perform the completion process (sketched for $\mathbf{Q}$ for the usual absolute value) for this absolute value $|\ |_v$. The resulting field will be denoted by F_v. Thus F_v can be identified with the equivalence classes of Cauchy sequences under $|\ |_v$, and there is a natural embedding of F into F_v. When $v = p$, F_p is called the p-adic completion of F. When $F = \mathbf{Q}$, any (non-zero) prime ideal of $\mathbf{Z}$ is spanned by a unique positive prime number p. In this case,

we write $\mathbf{Q}_p$ for $\mathbf{Q}_{(p)}$. The closure of $\mathbf{Z}$ in $\mathbf{Q}_p$ is called the p-adic integer ring, denoted by $\mathbf{Z}_p$.

Let n be an integer. Then we can find a unique integer $[n]_p$ such that $n \equiv [n]_p \bmod p$ and $0 \le [n]_p < p$. Let $a_0 = [n]_p$, and applying this process to $\frac{n-[n]_p}{p}$, we define a_1 as $\left[\frac{n-[n]_p}{p}\right]_p$. We iterate this process and define, after having defined a_m, $a_{m+1} = \left[\frac{n-a_0-a_1p-\cdots-a_mp^m}{p^{m+1}}\right]_p$. Then

$$\{b_m = a_0+a_1p+a_2p^2+\cdots+a_mp^m\}_{m\in\mathbf{Z}}$$

is a Cauchy sequence converging to n under $|\ |_p$, and we can write $n = \sum_{m=0}^{\infty} a_m p^m$. We can inductively solve the formal equation

$$\{\textstyle\sum_{m=0}^{\infty} a_m p^m\}\{\sum_{m=0}^{\infty} x_m p^m\} = 1 \text{ if } a_0 \text{ is prime to } p \text{ (i.e. } n \text{ is prime to } p).$$

By definition, every p-adic integer z in $\mathbf{Z}_p$ actually has such an expansion $z = \sum_{n=0}^{\infty} a_n(z)p^n$ for unique integers $a_n(z)$ with $0 \le a_n(z) < p$. In particular, z is invertible in $\mathbf{Z}_p$ if and only if a_0 is prime to p. Thus all the ideals of $\mathbf{Z}_p$ are exhausted by $p^n\mathbf{Z}_p$ and they are all distinct. We can write $p^n\mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid |x|_p \le p^{-n}\}$. Thus $\mathbf{Z}_p$ is a valuation ring and hence is a principal ideal domain. In particular, all finitely generated torsion-free modules over $\mathbf{Z}_p$ have a basis (i.e. are in fact free).

Let $\mathcal{O}_p$ be the closure of $\mathcal{O}$ in F_p. Taking an element ϖ in $\mathcal{O}$ with $v_p(\varpi) = 1$ and fixing a representative set R in $\mathcal{O}$ for $\mathcal{O}/p$, we can expand in the same manner as in the case of $\mathbf{Z}_p$ any $z \in \mathcal{O}_p$ into a unique expansion

$$z = \textstyle\sum_{n=0}^{\infty} a_n(z)\varpi^n \text{ with } a_n(z) \in R.$$

Thus again all the ideals of $\mathcal{O}_p$ are of the form $\varpi^n\mathcal{O}_p$ for some n (allowing $n = \infty$), and therefore $\mathcal{O}_p$ is a valuation ring. The above process of expanding $z \in \mathcal{O}_p$ into a power series of ϖ can be performed in the finite ring $\mathcal{O}/p^m$ and of course in this case the series is a finite sum: $z_m = \sum_{n=0}^{m-1} a_n(z_m)\varpi^n$ for $z_m = z \bmod p^m$ with $a_n(z_m) = a_n(z) \bmod p^m$. Then the sequence $\{z_m \in \mathcal{O}/p^m\}_m$ satisfies $z_m \equiv z_n \bmod p^n$ whenever $m \ge n$. Thus z naturally determines an element

$$\underline{z} = \varprojlim_m z_m \text{ in } \varprojlim_m (\mathcal{O}/p^m).$$

On the other hand, for any given element $\underline{z} = \varprojlim_m z_m$, we can recover $z = \sum_{n=0}^{\infty} a_n(z)\varpi^n$ in $\mathcal{O}_p$ because $\{a_n(z_m)\}$ uniquely determine $\{a_n(z)\}$. Thus we have an expression

(3a) $$\mathcal{O}_p = \varprojlim_m (\mathcal{O}/p^m) \text{ and } \mathbf{Z}_p = \varprojlim_m (\mathbf{Z}/p^m\mathbf{Z}).$$

It is easy to check that the topologies of both sides coincide (see [Bour2, I.4.4, III.3.3, III.7], [Bour1, III.2.6]). In particular, this shows that

(3b) $$\mathcal{O}_p/p^m\mathcal{O}_p \cong \mathcal{O}/p^m \text{ and } \mathbf{Z}_p/p^m\mathbf{Z}_p \cong \mathbf{Z}/p^m\mathbf{Z}.$$

For any $z \in \mathcal{O}_p$, we simply put $z_m = \sum_{n=0}^{m-1} a_n(z)\varpi^n \in \mathcal{O}$. Thus we can always find an infinite sequence in $\mathcal{O}$ converging to a given z in $\mathcal{O}_p$; i.e. $\mathcal{O}$ is dense in $\mathcal{O}_p$. When $\mathcal{O} = \mathbf{Z}$, $a_n(z)$ is always non-negative by our choice, i.e., $z_m \in \mathbf{N}$ for all m. Thus

(3c) *the set of natural numbers* $\mathbf{N}$ *is dense in* $\mathbf{Z}_p$ *and* $\mathcal{O}$ *is dense in* $\mathcal{O}_p$.

Exercise 2. Let $q = \#(\mathcal{O}/p)$ for a (non-zero) prime p of $\mathcal{O}$. Show that for an integer x in $\mathcal{O}$, (i) $\{x^{q^n}\}_{n\in\mathbf{N}}$ is a Cauchy sequence in $\mathcal{O}_p$, (ii) if x is prime to p, $\zeta = \lim_{n\to\infty} x^{q^n}$ is a (q-1)-th root of unity, (iii) if x is prime to p, $|\zeta - x^{q^{n-1}(q-1)}|_p \le p^{-n}$ and (iv) all the (q-1)-th roots of unity are obtained in this way.

Naturally $\mathcal{O}_p$ contains $\mathbf{Z}_p$ for a unique prime p in $\mathbf{Z}$ such that $p \cap \mathbf{Z} = p\mathbf{Z}$. Thus $\mathcal{O}_p$ is the integral closure of $\mathbf{Z}_p$. The natural homomorphism of $\mathcal{O}\otimes_{\mathbf{Z}}\mathbf{Z}_p$ to $\mathcal{O}_p$ is surjective, because $\mathcal{O}\otimes_{\mathbf{Z}}\mathbf{Z}_p$ is compact and its image contains the dense subring $\mathcal{O}$ of $\mathcal{O}_p$. Thus $\mathcal{O}_p$ is finitely generated over $\mathbf{Z}_p$, and we can find a basis $\{w_1, \ldots, w_f\}$ $(f \le r)$ of $\mathcal{O}_p$ over $\mathbf{Z}_p$. In particular, for any $\alpha \in \mathcal{O}_p$, defining a matrix $\rho(\alpha)$ by $(w_1\alpha,\ldots,w_f\alpha) = (w_1,\ldots,w_f)\rho(\alpha)$, we know that α satisfies the characteristic polynomial of $\rho(\alpha)$, which is a monic polynomial with coefficients in $\mathbf{Z}_p$. Thus $\mathcal{O}_p$ is integral over $\mathbf{Z}_p$. We now show the converse. It is well known that any valuation ring is normal (i.e., if $x \in F_p$ satisfies a monic equation with coefficients in $\mathcal{O}_p$, it belongs to $\mathcal{O}_p$). In fact, writing $x = u\varpi^{-m}$ with $|u|_p = 1$ and $m \ge 0$, if $x^n = \sum_{i=1}^{n} a_i x^{n-i}$ with $a_i \in \mathcal{O}_p$, we have

$$\frac{u^n}{\varpi^m} = a_1u^{n-1} + a_2u^{n-2}\varpi^m + \cdots + a_n\varpi^{m(n-1)}$$

whose right-hand side belongs to $\mathcal{O}_p$. Hence m has to be 0. This shows that $x \in \mathcal{O}_p$ and shows the normality of $\mathcal{O}_p$. In particular, $\mathcal{O}_p$ is the integral closure of $\mathbf{Z}_p$. For this reason, $\mathcal{O}_p$ is called the *p-adic integer ring* of F_p.

Let K/F be a finite extension. Let $\mathcal{O}_K$ be the integer ring of K. For a non-zero prime ideal p of $\mathcal{O}$, we decompose $p\mathcal{O}_K = \prod_{\mathcal{P}} \mathcal{P}^{e(\mathcal{P})}$ for prime ideals $\mathcal{P}$ of $\mathcal{O}_K$. Thus $\mathcal{O}_K/p\mathcal{O}_K \cong \prod_{\mathcal{P}} (\mathcal{O}_K/\mathcal{P}^{e(\mathcal{P})})$. Since as an $\mathcal{O}$-module, $\mathcal{O}_K/\mathcal{P} \cong (\mathcal{O}/p)^{f(\mathcal{P})}$ for a positive integer $f(\mathcal{P})$, by (2.3b),

(4a) $$[K:F] = \sum_{\mathcal{P}} f(\mathcal{P})e(\mathcal{P}).$$

Then the $\mathcal{P}$-adic completion $R = \mathcal{O}_{K,\mathcal{P}}$ is free of rank $e(\mathcal{P})f(\mathcal{P})$ because R/pR is of dimension $e(\mathcal{P})f(\mathcal{P})$ over $\mathcal{O}/p$ by (3b) and (4a). Similarly as in (1.5b), we know that

(4b) $$K \otimes_F F_p \cong \prod_{\mathcal{P}|p} K_{\mathcal{P}} \text{ and } \mathcal{O}_K \otimes_{\mathcal{O}} \mathcal{O}_p \cong \prod_{\mathcal{P}|p} \mathcal{O}_{K_{\mathcal{P}}}$$

Let E be a finite extension of F_p and R be its p-adic integer ring (i.e. the integral closure of $\mathcal{O}_p$). Taking a basis $\{\omega_1,\ldots,\omega_d\}$ of E/F_p, we easily see that $\varpi^{\alpha}\omega_i \in R$ for sufficiently large integer α. Thus $FR = E$. This implies that, if $w_1, \ldots, w_r \in R$ are $\mathcal{O}_p$-linearly independent, then $r \le d$. This shows that R is free of rank $[E:F_p]$ over $\mathcal{O}_p$. Since $R \cong \mathcal{O}_p^d$, R is p-adically complete. If $pR = \mathcal{P}_1^{e_1}\cdot\cdots\cdot\mathcal{P}_s^{e_s}$ for non-zero prime ideals $\mathcal{P}_i$ of R, then

$$R = \varprojlim_{\alpha}(R/p^{\alpha}R) \cong \prod_{j=1}^{s} \varprojlim_{\alpha}(R/\mathcal{P}_j^{\alpha}R),$$

because $R/p^{\alpha}R \cong \prod_{j=1}^{s}(R/\mathcal{P}_j^{\alpha e_j}R)$ by the Chinese remainder theorem. Since R is an integral domain, s has to be equal to 1 and R is a valuation ring. By definition, if we write $pR = \mathcal{P}^e$ and $f = \dim_{\mathcal{O}/p}(R/\mathcal{P})$, then

(5) $$[E:F_p] = ef \text{ and } |a|_{\mathcal{P}} = |a|_p^{[E:F]} \text{ for } a \in F.$$

Thus we can extend $|\ |_p$ to E by putting $|x|_p = |x|_{\mathcal{P}}^{1/[E:F]}$ for $x \in E$. The norm $|\ |_p$ is the unique norm extending $|\ |_p$ on F and defines the same topology as that given by $|\ |_{\mathcal{P}}$.

We now introduce the p-adic exponential function exp and the p-adic logarithm function log for later use. To define these functions, we use the following power series expansions:

(*) $$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \text{ and } \log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}.$$

By the strong triangle inequality, any power series $f(x) = \sum_{n=0}^{\infty} a_n x^n$ is convergent at $x \in \mathcal{O}_p$ if and only if $\lim_{n\to\infty} |a_n x^n|_p = 0$. Here $|\ |_p$ is the normalized p-adic norm: $|x|_p = |x|_p^{1/[E_p:Q_p]}$. Thus the radius of convergence is given by

$$R = (\limsup |a_n|_p^{1/n})^{-1}$$

(i.e. R is the largest real number which is a accumulation point of the sequence $\{|a_n|_p^{-1/n}\}$). We know that $|n!|_p^{1/n} = p^{-(1-(s/n))/(p-1)}$ by (2) for the integer $s = s_n$

$= \sum_{m=0}^{\infty} a_m(n)$ for the finite p-adic expansion $n = \sum_{m=0}^{\infty} a_m(n)p^m$. Note that $|s| \le (p-1)(1+\log_p|n|)$ for the complex logarithm $\log_p$ with base p. Thus $\lim_{n\to\infty} \left|\frac{s_n}{n}\right| = 0$ and we have

(6a) The radius of convergence of exp with respect to $|\ |_p$ is $p^{-1/(p-1)}$.

As for the logarithm function, since $|n|_p \le p^{-[\log_p|n|]}$,

(6b) The radius of convergence of $\log(1+x)$ with respect to $|\ |_p$ is 1.

Writing $D(x,r) = \{y \in F_p \mid |y-x|_p < r\}$, we define

$$\exp : D(0,p^{-1/(p-1)}) \to \mathcal{O}_p^{\times} \text{ and } \log : D(1,1) \to \mathcal{O}_p$$

by the p-adically convergent power series (*). Let $\mathbf{p}$ be 4 if $p = 2$ and $\mathbf{p} = p$ if $p > 2$. Then for $x \in \mathbf{Z}_p$ with $|x-1|_p \le \mathbf{p}^{-1}$, $\log(x) \in D(0,p^{-1/(p-1)})$, and we define $x^s = \exp(s\log(x))$ for $s \in \mathbf{Z}_p$. Using the formal identities in the power series ring, we can verify the following properties:

(7a) $\exp(x+y) = \exp(x)\exp(y)$ and $\log(xy) = \log(x)+\log(y)$,

(7b) $\log(x^s) = s\log(x)$ for $s \in \mathbf{Z}_p$,

(7c) $\exp(\log(x)) = x$ and $\log(\exp(x)) = x$,

Exercise 3. Give a proof of the above identities.

If $f(s) = \sum_{n=0}^{\infty} a_n(s-a)^n$ is a power series converging around $a \in \mathcal{O}_p$, then its formal derivative $\frac{df}{ds}(s) = \sum_{n=1}^{\infty} a_n n(s-a)^{n-1}$ also converges at a. This is clear from the inequality $\limsup |a_n|_p^{1/n} \ge \limsup |(n+1)a_{n+1}|_p^{1/n}$, since $|n+1|_p \le 1$. Writing $f^{(n)}$ for the formal n-th derivative of f, we have

(8a) $$a_n = \frac{f^{(n)}(a)}{n!} \text{ for all } n \in \mathbf{N}.$$

In particular, we see

(8b) $$\frac{dx^s}{ds} = x^s\log(x).$$

Let Ω be the p-adic completion of the algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$ under $|\ |_p$ which is the unique extension of $|\ |_p$ on $\mathbf{Q}_p$. Let $A = \{x \in \Omega \mid |x|_p \le 1\}$. For any $x \in \Omega^{\times}$, we see that $x|x|_p \in A^{\times}$. Since $\overline{\mathbf{Q}}_p$ is dense in Ω, for any positive n and any $x \in A^{\times}$, we can find a finite extension $K_n/\mathbf{Q}_p$ and $x_n \in K_n$ such that $|x-x_n|_p < p^{-n}$. As seen in Exercise 2, $\omega(x_n) = \lim_{m\to\infty} x_n^{p^{m!}}$ is well

defined in K_n. Note that $\omega(x_n)$ is independent of n, for which we write $\omega(x)$. Then we have

$$|\omega(x)-x_n^{q^n(q-1)}|_p < p^{-n}$$

where $q = p^{[K_n:\mathbf{Q}_p]}$. Thus $|\omega(x)-x^{q^n(q-1)}|_p < p^{-n}$. Then for $x \in A^\times$, $\omega(x) = \lim_{n\to\infty} x^{p^{n!}}$ is a unique root of unity with $|x-\omega(x)|_p < 1$. We thus see that

$$\Omega^\times = p^{\mathbf{Q}} \times \mu_\infty \times \Gamma_\infty$$

where $\mu_\infty = \{\zeta \in \Omega^\times \mid \zeta^N = 1$ for some integer N prime to p$\}$,

$p^{\mathbf{Q}} = \{p^r \mid r \in \mathbf{Q}\}$ and $\Gamma_\infty = \{x \in A^\times \mid |x-1|_p < 1\}$.

The projection to Γ_∞ written as $x \mapsto \langle x\rangle$ is given by $\omega(x|x|_p)^{-1}(x|x|_p)$. On Γ_∞, log is well defined. We then extend log to $\Omega^\times$ by

(9a) $\log(x) = \log(\langle x\rangle) \qquad (x \in \Omega^\times)$.

By definition, we still have

(9b) $\log(xy^{-1}) = \log(x)-\log(y)$.

We conclude this section by giving a brief explanation of the Frobenius element. Let F be a p-adic field with p-adic integer ring $\mathcal{O}$. We fix an algebraic closure $\overline{F}$ of F. Let $\overline{\mathcal{O}}$ be the integral closure of $\mathcal{O}$ in $\overline{F}$. We write $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ for the maximal ideals of $\mathcal{O}$ and $\overline{\mathcal{O}}$, respectively. We also write $\mathbf{F} = \mathcal{O}/\mathfrak{p}$ and $\overline{\mathbf{F}} = \overline{\mathcal{O}}/\overline{\mathfrak{p}}$, which is an algebraic closure of $\mathbf{F}$. We note here that $\overline{F}$ is not p-adically complete [BGR, 3.4.3]. By definition, every automorphism of $\overline{F}$ leaves $\overline{\mathcal{O}}$ and $\overline{\mathfrak{p}}$ stable and induces an automorphism of $\overline{\mathbf{F}}$ over $\mathbf{F}$. Thus we have a natural homomorphism of groups:

$$\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F}).$$

The kernel of ρ is called the inertia subgroup, which we write I. Note that all non-zero elements of $\overline{\mathbf{F}}$ are roots of unity. Then, it is easy to check that ρ is surjective by considering the extension $F(\zeta)$ for various roots of unity ζ ([Bour1, VI.8.5]). There is a canonical generator π in $\mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F})$: $\pi(x) = x^q$ for $q = \#(\mathbf{F})$. The element π is called the Frobenius element of $\mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F})$. If K/F is a (finite or infinite) Galois extension of F (see [N, Chapter I] for the Galois theory of infinite extensions) and if K is fixed by I, K is called unramified over F. If this is the case, on the residue field $\mathbf{F}'$ of $\mathcal{O}_K$, ρ induces a canonical isomorphism $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(\mathbf{F}'/\mathbf{F})$. Thus in this case, we have a naturally specified element $\rho^{-1}(\pi) = \mathrm{Frob}$ in Gal(K/F), which we call the Frobenius element of Gal(K/F).

Now we suppose F to be a number field in a fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. We pick a maximal ideal $\mathfrak{p}$ of the integer ring $\mathcal{O}$ of F. Let K/F be a (finite or infinite) Galois extension of F inside $\overline{\mathbf{Q}}$. We pick a maximal ideal $\mathcal{P}$ of $\mathcal{O}_K$ over $\mathfrak{p}$, where $\mathcal{O}_K$ is the integer ring of K. Then $\sigma \in \mathrm{Gal}(K/F)$ naturally acts

on maximal ideals of $\mathcal{O}_K$. We denote by $D = D(\mathcal{P}/p)$ the stabilizer of $\mathcal{P}$ in Gal(K/F). This group $D(\mathcal{P}/p)$ is called the decomposition group for $\mathcal{P}/p$. By definition

(10a) $$D(\mathcal{P}^\sigma/p) = \sigma D(\mathcal{P}/p)\sigma^{-1} \text{ for each } \sigma \in \mathrm{Gal}(K/F).$$

Since $\sigma \in D$ preserves $\mathcal{P}$, σ is continuous with respect to the $\mathcal{P}$-adic topology on K and hence induces an element of $\mathrm{Gal}(K_\mathcal{P}/F_p)$. It is known that

(10b) $$D(\mathcal{P}/p) \cong \mathrm{Gal}(K_\mathcal{P}/F_p) \quad ([N, IV.1]).$$

We write $I(\mathcal{P}/p)$ for the inertia subgroup in $D(\mathcal{P}/p)$. If $I(\mathcal{P}/p) = \{1\}$, we say $\mathcal{P}$ is unramified over p. If all the maximal ideals over p in $\mathcal{O}_K$ are unramified over p, we call p unramified in K/F. If $\mathcal{P}/p$ is unramified, we can consider its Frobenius element $\mathrm{Frob}(\mathcal{P}/p)$ in $D(\mathcal{P}/p)$. By (10a), we know that

(10c) $$\mathrm{Frob}(\mathcal{P}^\sigma/p) = \sigma\mathrm{Frob}(\mathcal{P}/p)\sigma^{-1} \text{ if } \mathcal{P}/p \text{ is unramified.}$$

Thus the conjugacy class of $\mathrm{Frob}(\mathcal{P}/p)$ is well determined by p, which we write Frob_p. Sometimes, we identify Frob_p with $\mathrm{Frob}(\mathcal{P}/p)$, which is actually a representative of the Frobenius conjugacy classes. We quote the following well known density theorem:

Theorem 1 (Chebotarev). *Suppose that only finitely many prime ideals in* F *are ramified in* K/F. *Then under the Krull topology on* Gal(K/F) *(see [N, I.1]), the set of Frobenius elements*

$$\Sigma = \{\mathrm{Frob}(\mathcal{P}/p) \in \mathrm{Gal}(K/F) \mid \mathcal{P}/p \text{ unramified in } K/F\}$$

is dense in Gal(K/F).

We do not prove this theorem here, because we need a large amount of either analytic number theory or class field theory to give a proof. We only refer for this to [N, V.6].

Chapter 2. Classical L-functions and Eisenstein series

In this chapter, we will deal with basic analytic properties and some algebraic properties of abelian L-functions in a classical setting. To give an illustration of what we will do, let us start with a typical example of such results.

§2.1. Euler's method of computing ζ-values

In the following, a continuous $\mathbf{C}$-valued function f defined in an open subset U of $\mathbf{C}$ is called *holomorphic* (or *analytic)* on U if f is differentiable on U and $\frac{\partial f}{\partial z} = 0$ for the variable z on U. By Cauchy's theorem, any holomorphic function on U can be expanded into a power series of $z-u$ convergent absolutely on an open neighborhood of each $u \in U$. A function defined on a dense open subset V of U is called meromorphic if there exist two holomorphic functions g and $h \neq 0$ such that $f = \frac{g}{h}$ on V.

The simplest example of an L-function is the Riemann ζ-function given by the infinite sum

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \quad \text{for complex numbers} \quad s \in \mathbf{C}.$$

This infinite sum converges absolutely if $\mathrm{Re}(s) > 1$ and gives an analytic function in this region. In fact, it is clear that

$$|\zeta(s)| \leq \zeta(\mathrm{Re}(s)) \leq 1 + \int_1^{\infty} x^{-\mathrm{Re}(s)} dx$$

and the integral converges absolutely if $\mathrm{Re}(s) > 1$. Moreover we shall find in §2.2 an analytic function $f(s)$ defined on all $s \in \mathbf{C}$ such that $f(s) = (s-1)\zeta(s)$ if $\mathrm{Re}(s) > 1$. This function $f(s)$ is necessarily unique by the Cauchy integral formula. The uniqueness can be shown as follows. If ϕ is an analytic function on the domain $\Omega_r = \{z \in \mathbf{C} \mid |z| < r\}$, then by Cauchy's integral formula (see [Hör, 1.2]),

$$\phi(s) = (2\pi\sqrt{-1})^{-1} \int_{|z|=t} \frac{\phi(z)}{z-s} dz \quad \text{if} \quad |s| < t < r.$$

Moreover we see that

$$\begin{aligned}
\frac{\partial \phi}{\partial s}(s) &= \lim_{\Delta s \to 0} \frac{\phi(s+\Delta s) - \phi(s)}{\Delta s} \\
&= (2\pi\sqrt{-1})^{-1} \lim_{\Delta s \to 0} \int_{|z|=t} \phi(z) \left\{ \frac{(z-s-\Delta s)^{-1} - (z-s)^{-1}}{\Delta s} \right\} dz \\
&= (2\pi\sqrt{-1})^{-1} \int_{|z|=t} \phi(z) \lim_{\Delta s \to 0} \left\{ \frac{(z-s-\Delta s)^{-1} - (z-s)^{-1}}{\Delta s} \right\} dz \\
&= (2\pi\sqrt{-1})^{-1} \int_{|z|=t} \phi(z) \frac{\partial}{\partial s} (z-s)^{-1} dz = (2\pi\sqrt{-1})^{-1} \int_{|z|=t} \phi(z)(z-s)^{-2} dz.
\end{aligned}$$

Here the interchange of the integral and the limit is possible because

$$\lim_{\Delta s\to 0}\left\{\frac{(z-s-\Delta s)^{-1}-(z-s)^{-1}}{\Delta s}\right\}$$

converges uniformly on the circle $\{z\in \mathbf{C}\mid |z|=t\}$. In particular, we have

$$\frac{\partial\phi}{\partial s}(0) = (2\pi\sqrt{-1})^{-1}\int_{|z|=t}\phi(z)z^{-2}dz.$$

Repeating the above process, we have

$$\phi^{(n)}(0) = n!(2\pi\sqrt{-1})^{-1}\int_{|z|=t}\phi(z)z^{-n-1}dz.$$

Exercise 1. Give a detailed proof of the above formula.

Since $|s|<|z|$, we see that $\frac{1}{z-s} = z^{-1}\frac{1}{1-z^{-1}s}$ and $|z^{-1}s|<1$. Thus

$$\begin{aligned}\frac{1}{z-s} = z^{-1}\frac{1}{1-z^{-1}s} &= z^{-1}(1+z^{-1}s+z^{-2}s^2+\cdots+z^{-n}s^n+\cdots)\\ &= z^{-1}+z^{-2}s+z^{-3}s^2+\cdots+z^{-n-1}s^n+\cdots.\end{aligned}$$

Of course, this series is absolutely and uniformly convergent on any compact subset in Ω_r. Thus we have

$$\begin{aligned}\phi(s) &= (2\pi\sqrt{-1})^{-1}\int_{|z|=t}\frac{\phi(z)}{z-s}dz\\ &= (2\pi\sqrt{-1})^{-1}\int_{|z|=t}\phi(z)(z^{-1}+z^{-2}s+z^{-3}s^2+\cdots+z^{-n-1}s^n+\cdots)dz\\ &= (2\pi\sqrt{-1})^{-1}\sum_{n=0}^{\infty}\left\{\int_{|z|=t}\phi(z)z^{-n-1}dz\right\}s^n = \sum_{n=0}^{\infty}(\phi^{(n)}(0)/n!)s^n.\end{aligned}$$

Here we can again interchange the integral and the summation because the power series expansion of $(z-s)^{-1}$ converges uniformly on the compact subset $\{z\mid |z|=t\}$. If ϕ is analytic on $\mathbf{C}$, changing variables by $z\mapsto z+w$ (thus $s\mapsto s+w$) in the above argument, we see that

$$\phi(s+w) = \sum_{n=0}^{\infty}(\phi^{(n)}(w)/n!)s^n \text{ or } \phi(s) = \sum_{n=0}^{\infty}(\phi^{(n)}(w)/n!)(s-w)^n.$$

This implies that if $\phi=0$ on a neighborhood of w, we see $\phi^{(n)}(w)=0$ and hence $\phi=0$ identically. Thus if $f(s)=(s-1)\zeta(s)=g(s)$ on $\{s\in\mathbf{C}\mid \mathrm{Re}(s)>1\}$ for two analytic functions f and g, we know that $f=g$ on $\mathbf{C}$. Now we write $\zeta(s)$ for the meromorphic function $f(s)/(s-1)$. We will show here and in §2.2 that $\zeta(s)$ has a singularity at $s=1$, $\mathrm{Res}_{s=1}\zeta(s)=1$; and also that $\zeta(s)$ has the following functional equation:

$$\zeta(s) = \frac{(2\pi)^s\zeta(1-s)}{2\Gamma(s)\cos(\pi s/2)}.$$

Here $\Gamma(s)$ is the Gamma function defined by $\int_0^\infty e^{-t}t^{s-1}dt$ if $\mathrm{Re}(s)>0$ and satisfies $\Gamma(n)=(n-1)!$ for positive integers n. Therefore, essentially the value of $\zeta(s)$ can be defined by the infinite series when either $\mathrm{Re}(s)>1$ or

$\mathrm{Re}(s) < 0$. Now there is an interesting way to compute the value of $\zeta(1-n)$ for positive integers n, which was invented by Euler in 1749. We consider instead of $\zeta(s)$ the alternating sum:

$$1-2^{-s}+3^{-s}-4^{-s}+\cdots+(-1)^{n+1}n^{-s}+\cdots = \sum_{n=1}^{\infty} n^{-s} - 2\sum_{n=1}^{\infty}(2n)^{-s} = (1-2^{1-s})\zeta(s).$$

We want to compute $(1-2^{m+1})\zeta(-m)$ for $m \geq 0$. Euler's idea is to introduce an auxiliary variable t and consider

$$g(t) = \sum_{n=1}^{\infty}(-1)^{n-1}n^m t^n = \left(t\frac{d}{dt}\right)^m (t-t^2+t^3-t^4+\cdots+(-1)^{n+1}t^n+\cdots) = \left(t\frac{d}{dt}\right)^m\left(\frac{t}{1+t}\right).$$

Then Euler pretended that the above series were convergent at $s = -m$ and concluded by replacing t by 1:

$$(1) \qquad (1-2^{m+1})\zeta(-m) = \left(t\frac{d}{dt}\right)^m\left(\frac{t}{1+t}\right)\Big|_{t=1} \quad \text{for every integer} \quad m \geq 0.$$

Here the right-hand side is the value of a rational function at $t = 1$ and hence a rational number. Thus if the above argument is correct, we have

$$(2) \qquad \zeta(-n) \in \mathbf{Q} \quad \text{for} \quad n \geq 0.$$

Of course the above argument needs justification, but the result and the formula (1) are actually true.

Exercise 2. (a) Show that the rational function $\left(t\frac{d}{dt}\right)^m\left(\frac{t}{1+t}\right)$ does not have $(t-1)$ as a factor in its denominator.
(b) Explain why the argument of Euler is a little problematic.

Of course, Euler was fully aware of the shakiness of his argument. Here is how he justified it. First he replaced t by e^x. By the chain rule, we see that $t\frac{d}{dt}f(t)\big|_{t=1} = \frac{d}{dx}f(e^x)\big|_{x=0}$. Thus if you believe the formula (1), we have

$$(3) \qquad (1-2^{m+1})\zeta(-m) = \left(\frac{d}{dx}\right)^m\left(\frac{e^x}{1+e^x}\right)\Big|_{x=0} \quad \text{for each integer} \quad m \geq 0.$$

Instead of x, we put $2\pi\sqrt{-1}\,z$ and write $e(z) = e^{2\pi i z}$ $(i = \sqrt{-1})$. We then consider the function $F(z) = \frac{e(z)}{1+e(z)}$. By (believing) (3), the Taylor expansion of F at $z = 0$ is given by

$$(4) \qquad F(z) = \sum_{n=0}^{\infty}(F^{(n)}(0)z^n/n!) = \sum_{n=0}^{\infty}((1-2^{n+1})\zeta(-n)(2\pi\sqrt{-1}\,z)^n/n!).$$

By another formula of Euler, $e^{i\theta} = \cos\theta + \sqrt{-1}\sin\theta$, we know that

$$\cos(z) = \frac{e^{iz}+e^{-iz}}{2}, \quad \sin(z) = \frac{e^{iz}-e^{-iz}}{2\sqrt{-1}}.$$

From this fact,

$$\cot(z) = \sqrt{-1}\frac{e^{iz}+e^{-iz}}{e^{iz}-e^{-iz}} = \sqrt{-1}\frac{e^{2iz}+1}{e^{2iz}-1}.$$

Therefore we have

$$\pi\cot(\pi z) = \pi\sqrt{-1}\frac{e(z)+1}{e(z)-1}.$$

On the other hand, the function cot has the following partial fraction expansion:

$$\pi\cot(\pi z) = \varepsilon_1(z) = \frac{1}{z} + \sum_{n=1}^{\infty}\left\{\frac{1}{z+n} + \frac{1}{z-n}\right\}. \tag{5}$$

For the moment, let us believe this expansion (which is absolutely convergent if $z \notin \mathbf{Z}$). By the expansion of geometric series, we know, if $|z| < 1$ and $z \neq 0$, that

$$\frac{1}{z+n} = n^{-1}\frac{1}{1+z/n} = n^{-1}\sum_{r=0}^{\infty}(-z/n)^r = \sum_{r=0}^{\infty}(-1)^r n^{-r-1}z^r, \quad \frac{1}{z-n} = -\sum_{r=0}^{\infty}n^{-r-1}z^r.$$

Then we see that

$$\begin{aligned}\varepsilon_1(z) &= \frac{1}{z} + \sum_{n=1}^{\infty}\sum_{r=0}^{\infty}\left\{(-1)^r n^{-r-1}z^r - n^{-r-1}z^r\right\} \\ &= \frac{1}{z} - 2\left\{\sum_{n=1,k=1}^{\infty} n^{-2k}z^{2k-1}\right\} \overset{?}{=} \frac{1}{z} - 2\sum_{k=1}^{\infty}\zeta(2k)z^{2k-1}.\end{aligned} \tag{6}$$

Here only the terms for odd r survive and then we have written $r+1 = 2k$.

Exercise 3. (a) Suppose that $z \notin \mathbf{Z}$. Show that absolute convergence of $\sum_{n=1}^{\infty}\{\frac{1}{z+n} + \frac{1}{z-n}\}$ and also show that $\sum_{n=-\infty}^{\infty}\frac{1}{z+n}$ is not absolutely convergent.
(b) In (6), justify the interchange of the summations with respect to k and n (i.e. show rigorously the equality marked by ? in (6)).

From (6), we know that

$$\begin{aligned}-(\sqrt{-1}\pi)^{-1}\sum_{k=1}^{\infty} 2(1-2^{2k})\zeta(2k)z^{2k-1} &\overset{(6)}{=} (\sqrt{-1}\pi)^{-1}(\varepsilon_1(z)-2\varepsilon_1(2z)) \\ &= \frac{e(z)+1}{e(z)-1} - 2\frac{e(2z)+1}{(e(z)-1)(e(z)+1)} = -\frac{e(z)^2-2e(z)+1}{e(2z)-1} = -\frac{(e(z)-1)^2}{(e(z)-1)(e(z)+1)} \\ &= \frac{1}{e(z)+1} - \frac{e(z)}{e(z)+1} = \frac{e(-z)}{e(-z)+1} - \frac{e(z)}{e(z)+1} = F(-z) - F(z) \\ &\overset{(4)}{=} -\sum_{k=1}^{\infty} 2(1-2^{2k})\zeta(1-2k)(2\pi\sqrt{-1}z)^{2k-1}/(2k-1)!.\end{aligned}$$

This shows that $\zeta(2k) = \dfrac{(\sqrt{-1}\,\pi)(2\pi\sqrt{-1})^{2k-1}}{(2k-1)!}\zeta(1-2k) = \dfrac{(2\pi)^{2k}}{2(2k-1)!(-1)^k}\zeta(1-2k).$

By specializing the functional equation $\zeta(s) = \dfrac{(2\pi)^s\zeta(1-s)}{2\Gamma(s)\cos(\pi s/2)}$ at $s = 2k$, this equality is in fact true, because $\cos(k\pi) = (-1)^k$ and $\Gamma(2k) = (2k-1)!$. At the time of Euler, the functional equation was not known and in this way, Euler predicted its form.

To make sure of our logic, we summarize our argument. Introducing an auxiliary variable t, Euler related the value $\left(\dfrac{d}{dx}\right)^m\left(\dfrac{e^x}{1+e^x}\right)\Big|_{x=0}$ with $\zeta(-m)$; so we write $(1-2^{m+1})a_m$ for this value, which is not yet proven to be equal to $(1-2^{m+1})\zeta(-m)$. Then by definition, the formula (4) read

$$F(z) = \frac{e(z)}{1+e(z)} = \sum_{n=0}^{\infty}(1-2^{n+1})a_n(2\pi\sqrt{-1}\,z)^n/n!.$$

On the other hand, by using the partial fraction expansion of the cotangent function, we computed the power series expansion in (6):

$$(\sqrt{-1}\,\pi)\frac{e(z)+1}{e(z)-1} = \frac{1}{z} - 2\sum_{k=1}^{\infty}\zeta(2k)z^{2k-1}.$$

Since $F(-z)-F(z) = \dfrac{e(z)+1}{e(z)-1} - 2\dfrac{e(2z)+1}{e(2z)-1}$, equating the power series coefficients of the two sides using the above two formulas, we obtain

$$\zeta(2k) = \frac{(2\pi)^{2k}a_{2k-1}}{2(2k-1)!(-1)^k}.$$

Thus we know

Proposition 1. $\zeta(2k) \in \pi^{2k}\mathbf{Q}$ *for all* $0 < k \in \mathbf{Z}$.

On the other hand, by specializing the functional equation (which we have not proved yet) at $s = 2k$, we have

$$\zeta(2k) = \frac{(2\pi)^{2k}\zeta(1-2k)}{2(2k-1)!(-1)^k}.$$

Then we conclude, assuming the functional equation, that

$$\zeta(1-2k) = a_{2k-1} = (1-2^{2k})^{-1}\left(\frac{d}{dx}\right)^{2k-1}\left(\frac{e^x}{1+e^x}\right)\Big|_{x=0}.$$

Here are some remarks. (a) By the formula (1), one can compute $\zeta(2k)$ or $\zeta(1-2k)$. Here are some examples:

$$\zeta(2) = 1 + 2^{-2} + 3^{-2} + \cdots = \frac{\pi^2}{6}, \ \ldots,$$

$$\zeta(12) = 1 + 2^{-12} + 3^{-12} + \cdots = \frac{691\pi^{12}}{3^6 5^3 7^2 11\cdot 13}, \text{ etc.}$$

For more examples, see the table given in [Wa, p.352].

(b) The primes appearing in the numerator of $\zeta(2k)$, for example 691, are called irregular primes and have arithmetic significance. In fact, the class number of the cyclotomic extension $\mathbf{Q}(\zeta_p)$ for a root of unity ζ_p with $\zeta_p{}^p = 1$ but $\zeta_p \neq 1$ is divisible by p if and only if the prime p appears in the numerator of $\zeta(1\text{-}2k)$ for some k with $2k < p\text{-}1$. This is the famous theorem of Kummer proved in the mid 19th century and immediately implies the impossibility of a non-zero integer solution to the Fermat equation $x^p + y^p = z^p$ if p is regular (i.e. not irregular). We refer to [Wa] for more details of this direction of research and to [Ri] for the approach using modular forms.

(c) The nature of the value $\zeta(2k+1)$ for a positive odd integer is quite different from the even values $\zeta(2k)$ and they are supposed not to equal a rational number times a power of π.

We insert here a sketch of the proof of (5) due to Eisenstein and Weil [W2, II]. We shall show that the right-hand side of (5) satisfies the differential equation $y' = -y^2\text{-}\pi^2$. The solution of this equation which goes to ∞ at $z = 0$, as is easily shown by a standard argument, is unique and equals $\pi\cot(\pi z)$. We put

$$\varepsilon_r(z) = \begin{cases} \frac{1}{z} + \sum_{n=1}^{\infty} \{\frac{1}{z+n} + \frac{1}{z-n}\} & \text{if } r = 1, \\ \sum_{n=-\infty}^{\infty} (z+n)^{-r} & \text{if } r > 1. \end{cases}$$

These series are absolutely convergent. Here note that $\frac{d\varepsilon_r}{dz} = -r\varepsilon_{r+1}$. Taking two independent variables p and q and putting $r = p+q$, we get $\frac{1}{pq} = \frac{1}{pr} + \frac{1}{qr}$. Differentiating once by $\frac{\partial}{\partial p}$ and $\frac{\partial}{\partial q}$, we get (keeping the fact that $r = p+q$ in mind)

$$\frac{1}{p^2q^2} = \frac{1}{p^2r^2} + \frac{1}{q^2r^2} + \frac{2}{pr^3} + \frac{2}{qr^3} \quad \text{or} \quad \frac{1}{p^2q^2} - \frac{1}{p^2r^2} - \frac{1}{q^2r^2} = \frac{2}{pr^3} + \frac{2}{qr^3}.$$

In this equality, we put $p = z+n$, $q = w+m-n$ with integers m and n. Then $r = z+w+m$ and summing up with respect to n keeping m constant, we have

$$\sum_n \left\{\frac{1}{p^2q^2} - \frac{1}{p^2r^2} - \frac{1}{q^2r^2}\right\} = 2r^{-3}\sum_n \left\{\frac{1}{p} + \frac{1}{q}\right\} = 2(z+w+m)^{-3}\{\varepsilon_1(z)+\varepsilon_1(w)\}.$$

Now we sum with respect to m:

$$(7)\quad \varepsilon_2(z)\varepsilon_2(w) - \varepsilon_2(z)\varepsilon_2(z+w) - \varepsilon_2(w)\varepsilon_2(z+w) = \sum_m\sum_n \left\{\frac{1}{p^2q^2} - \frac{1}{p^2r^2} - \frac{1}{q^2r^2}\right\}$$

$$= 2\{\varepsilon_1(z)+\varepsilon_1(w)\}\sum_m (z+w+m)^{-3} = 2\varepsilon_3(z+w)\{\varepsilon_1(z)+\varepsilon_1(w)\}.$$

Differentiating (6) with respect to z (noting the fact that $\frac{d\varepsilon_1}{dz} = -\varepsilon_2$), we get

$$\varepsilon_2(w) = w^{-2} + \sum_{r=1}^{\infty} (2r\text{-}1)2\zeta(2r)w^{2r-2} = w^{-2} + 2\zeta(2) + 6\zeta(4)w^2 + \cdots.$$

Now expanding $\varepsilon_2(z+w)$ into a power series in w at $w=0$ regarding z as a constant, we have, by the formula $\frac{d\varepsilon_r}{dz} = -r\varepsilon_{r+1}$,

$$\varepsilon_2(z+w) = \sum_{r=0}^{\infty} (\varepsilon_2^{(r)}(z)w^r/r!) = \sum_{r=0}^{\infty} (-1)^r(r+1)\varepsilon_{r+2}(z)w^r,$$

$$\varepsilon_3(z+w) = \sum_{r=0}^{\infty} (-1)^r(r+1)(r+2)\varepsilon_{r+3}(z)w^r/2.$$

Then the constant term of the left-hand side of (7) in the power series expansion with respect to w is given by

$$2\zeta(2)\varepsilon_2(z) - \varepsilon_2(z)^2 - 3\varepsilon_4(z) - 2\zeta(2)\varepsilon_2(z) = -\varepsilon_2(z)^2 - 3\varepsilon_4(z).$$

The constant term of the right-hand side is (by using (6))

$$2\varepsilon_3(z)\varepsilon_1(z)-6\varepsilon_4(z).$$

Thus we have

(8a) $$3\varepsilon_4(z) = \varepsilon_2(z)^2 + 2\varepsilon_3(z)\varepsilon_1(z).$$

Similarly by expanding both sides of (7) into a power series in $x = z+w$ at $x = 0$ regarding z as a constant and equating the constant term, we have

(8b) $$\varepsilon_2(z)^2 = \varepsilon_4(z) + 4\zeta(2)\varepsilon_2(z).$$

Eliminating ε_4 using (8a,b), we know that

(8c) $$\varepsilon_1\varepsilon_3 = \varepsilon_2^2 - 6\zeta(2)\varepsilon_2.$$

Differentiating this formula, we know from $\frac{d\varepsilon_r}{dz} = -r\varepsilon_{r+1}$ that

(8d) $$\varepsilon_2\varepsilon_3 - 4\zeta(2)\varepsilon_3 = \varepsilon_1\varepsilon_4.$$

Multiplying (8b) by ε_1 and eliminating $\varepsilon_1\varepsilon_4$ using (8d), we have

$\varepsilon_1\varepsilon_2^2-4\zeta(2)\varepsilon_1\varepsilon_2 = \varepsilon_2\varepsilon_3-4\zeta(2)\varepsilon_3$ or equivalently $\varepsilon_2(\varepsilon_3-\varepsilon_1\varepsilon_2) = 4\zeta(2)(\varepsilon_3-\varepsilon_1\varepsilon_2)$.

Since ε_2 is not the constant $4\zeta(2)$, we know that $\varepsilon_3 = \varepsilon_1\varepsilon_2$. In (8c), we replace ε_3 by $\varepsilon_1\varepsilon_2$ and then divide by ε_2 to obtain

$$\varepsilon_1^2 = \varepsilon_2 - 6\zeta(2).$$

Then by the facts $\frac{d\varepsilon_1}{dz} = -\varepsilon_2$ and $6\zeta(2) = \pi^2$, we know that ε_1 satisfies the differential equation $y' = -y^2-\pi^2$. The fact $6\zeta(2) = \pi^2$ will be shown independently of this argument.

Now we give a generalization of the formula (1):

$$(1-2^{m+1})\zeta(-m) = \left(t\frac{d}{dt}\right)^m\left(\frac{t}{1+t}\right)\Big|_{t=1} \quad \text{for each integer } m \geq 0,$$

which was found by Katz [K1]. Instead of 2, we fix an integer $a \geq 2$. We define a function $\xi : \mathbf{Z} \to \mathbf{Z}$ by

$$\xi(n) = \begin{cases} 1 & \text{if } n \not\equiv 0 \bmod a, \\ 1-a & \text{if } n \equiv 0 \bmod a. \end{cases}$$

We note that $\sum_{b=0}^{a-1}\xi(b) = \sum_{b=1}^{a}\xi(b) = 0$. We consider, instead of $\frac{t}{1+t}$, the rational function $\Phi(t) = \frac{t+1}{t-1} - a\frac{t^a+1}{t^a-1}$. Then we see that

$\Phi(e(z)) = (\sqrt{-1}\,\pi)^{-1}(\pi\cot(\pi z)-a\pi\cot(a\pi z)) = -(\sqrt{-1}\,\pi)^{-1}\sum_{k=1}^{\infty} 2(1-a^{2k})\zeta(2k)z^{2k-1}$.

In the special case of $a = 2$, we have

$$\Phi(t) = \frac{t+1}{t-1} - 2\frac{t^2+1}{t^2-1} = \frac{(t+1)^2-2(t^2+1)}{t^2-1} = \frac{1-t}{t+1}.$$

By computation, we see that

$$\begin{aligned}\Phi(t) &= \frac{(t+1)(1+t+t^2+\cdots+t^{a-1})-at^a-a}{t^a-1}\\ &= \frac{1-a+2(t+t^2+\cdots+t^{a-1})+t^a(1-a)-2(\xi(0)+\xi(1)+\cdots+\xi(a-1))}{t^a-1}\\ &= \frac{2(t-1)+2(t^2-1)+\cdots+2(t^{a-1}-1)+(1-a)(t^a-1)}{t^a-1}\\ &= \frac{2\sum_{b=1}^{a}\xi(b)(1+t+t^2+\cdots+t^{b-1})}{1+t+t^2+\cdots+t^{a-1}} - (1-a).\end{aligned}$$

Now we put $\Psi(t) = \frac{-\sum_{b=1}^{a}\xi(b)(1+t+t^2+\cdots+t^{b-1})}{1+t+t^2+\cdots+t^{a-1}} = \frac{\sum_{b=1}^{a}\xi(b)t^b}{1-t^a}$. The last equality follows from $\sum_{b=1}^{a}\xi(b) = 0$. When $a = 2$, we have $\Psi(t) = \frac{t}{1+t}$. In general, we have $-2\Psi(t) = \Phi(t)-(a-1)$. Then by the formula which we have already looked at,

$$\Phi(e(z)) = -(i\pi)^{-1}\sum_{k=1}^{\infty}2(1-a^{2k})\zeta(2k)z^{2k-1},$$

we now know that

$$-2\left(\frac{d}{dz}\right)^{2k-1}\Psi(e(z))\Big|_{z=0} = -(i\pi)^{-1}(2k-1)!2(1-a^{2k})\zeta(2k).$$

To relate this formula with the values of ζ at negative integers, we consider

$$(1-a^{s+1})\zeta(-s) = \sum_{n=1}^{\infty} n^s - a\sum_{n=1}^{\infty}(an)^s = \sum_{n=1}^{\infty}\xi(n)n^s.$$

Putting $g(t) = \sum_{n=1}^{\infty}\xi(n)t^n$, we get

$$\left(t\frac{d}{dt}\right)^m g(t) = \sum_{n=1}^{\infty}\xi(n)n^m t^n,$$

and hence formally

$$\left(t\frac{d}{dt}\right)^m g(t)\Big|_{t=1} = (1-a^{m+1})\zeta(-m).$$

On the other hand, we have

$$(1-a^{m+1})\zeta(-m) = \left(t\frac{d}{dt}\right)^m g(t)\Big|_{t=1} = \left(t\frac{d}{dt}\right)^m\left\{\sum_{b=1}^{a}\xi(b)t^b\sum_{n=0}^{\infty}t^{na}\right\}\Big|_{t=1}$$

$$= \left(t\frac{d}{dt}\right)^m\left\{\frac{\sum_{b=1}^{a}\xi(b)t^b}{1-t^a}\right\}\Big|_{t=1} = (2\pi\sqrt{-1})^{-m}\left(\frac{d}{dz}\right)^m\Psi(e(z))\Big|_{z=0}.$$

This formal computation can be justified by applying a functional equation (to be proved in the following section) to the right-hand side of

$$(1-a^{2k})\zeta(1-2k) = (2\pi\sqrt{-1})^{-2k}(2k-1)!2(1-a^{2k})\zeta(2k).$$

Thus we obtain

Theorem 1. *Let* $a > 1$ *be an integer. Then for each positive integer* m, *we have* $(1-a^{m+1})\zeta(-m) = \left(t\frac{d}{dt}\right)^m\Psi(t)\Big|_{t=1}$, *where* $\Psi(t) = \frac{\sum_{b=1}^{a}\xi(b)t^b}{1-t^a}$.

Exercise 4. We have only proved the theorem when m is an odd positive integer. Give a proof of the theorem for even positive integers m. (First show $\left(\frac{d}{dx}\right)^m\left(\frac{e^x}{1+e^x}\right)\Big|_{x=0} = 0$ for $0 < m \in 2\mathbf{Z}$ by making the substitution $x \mapsto -x$ and then show $\zeta(-m) = 0$ by using the functional equation.)

Exercise 5 (the Lipschitz-Sylvester theorem). By using Theorem 1, show that $a^{m+1}(1-a^{m+1})\zeta(-m) \in \mathbf{Z}$ for every integer $a > 1$, where m is a non-negative integer.

Exercise 6. (a) For each prime p, show that $(\mathbf{Z}/p\mathbf{Z})^\times$ is a cyclic group.
(b) For a positive even integer k, show that if the denominator of $\zeta(1-k)$ is divisible by a prime p, then k is divisible by $p-1$.

§2.2. Analytic continuation and the functional equation

As seen through Euler's argument, we now know the importance of the function $F(z) = \frac{e(z)}{1+e(z)}$ in the theory of the Riemann zeta function $\zeta(s)$. Here we modify this function a little to deal with $\zeta(s)$ directly (instead of $(1-2^{-s})\zeta(s)$). Put $G(z) = \frac{e^{-z}}{1-e^{-z}}$ for $z \in \mathbf{C}$. First we give an integral expression for $\zeta(s)$. For that, we need several properties of the Γ-function. Let us recall some of them. We may take the following integral as a definition of the Γ-function:

$$\Gamma(s) = \int_0^\infty e^{-y}y^{s-1}dy \quad \text{if } \operatorname{Re}(s) > 0. \tag{1}$$

This integral is convergent only when $\mathrm{Re}(s) > 0$. To show this, we remark that for a fixed real number $\varepsilon > 0$ and for any real number σ, there exists $M > 0$ such that if $y > \varepsilon$, then $My^{-2} > e^{-y}y^{\sigma-1}$. Thus writing $\sigma = \mathrm{Re}(s)$, we see that

$$|\Gamma(s)| = \left|\int_0^\infty e^{-y}y^{s-1}dy\right| \le \int_0^\infty |e^{-y}y^{s-1}|\,dy = \int_0^\infty e^{-y}y^{\sigma-1}dy.$$

In particular, we know that

$$\left|\int_\varepsilon^\infty e^{-y}y^{s-1}dy\right| \le \int_\varepsilon^\infty e^{-y}y^{\sigma-1}dy \le M\int_\varepsilon^\infty y^{-2}dy = M[-y^{-1}]_\varepsilon^\infty = M\varepsilon^{-1}.$$

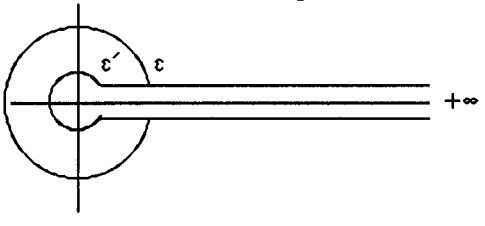
Thus the integral $\int_\varepsilon^\infty e^{-y}y^{s-1}dy$ converges for all s and gives an analytic function of s. The problem of divergence lies in the other integral:

$$\left|\int_0^\varepsilon e^{-y}y^{s-1}dy\right| \le \int_0^\varepsilon e^{-y}y^{\sigma-1}dy \le \int_0^\varepsilon y^{\sigma-1}dy \le [y^\sigma/\sigma]_0^\varepsilon = \varepsilon^\sigma/\sigma \quad \text{if } \sigma > 0.$$

To find the analytic continuation of $\Gamma(s)$, we consider $e^{-y}y^{s-1}$ as a function of the complex variable y. Here note that the function $y \mapsto y^s$ is not well defined because $y^s = e^{s\,log(y)}$ and log is multivalued. To fix a branch, we write $y = |y|e^{i\theta}$ with $0 \le \theta \le 2\pi$ and define $log(y) = log|y| + i\theta$ and $y^s = e^{s\,log(y)}$. When $\theta = 0$ or 2π (i.e. y is on the positive real axis), we write y^s when $\theta = 0$ and y_-^s when $\theta = 2\pi$. Note that $y^n = y_-^n$ for integers n. We fix a positive real number ε and denote by $\partial D(\varepsilon)$ the integral path which is the circle of radius ε with center 0 starting from $\varepsilon = |\varepsilon|e^{i0}$ and with counterclockwise orientation, by $P_+(\varepsilon)$ the path on the real line from $+\infty$ to ε and by $P_-(\varepsilon)$ the path on the real line from ε to $+\infty$. We consider that $\theta = 0$ on $P_+(\varepsilon)$ and $\theta = 2\pi$ on $P_-(\varepsilon)$. We write the total path as $P(\varepsilon) = P_+(\varepsilon)\cup\partial D(\varepsilon)\cup P_-(\varepsilon)$. We similarly write $\partial D(\varepsilon,\varepsilon')$ for the boundary of the annulus cut along the real axis:

$$\{P_+(\varepsilon')-P_+(\varepsilon)\}\cup\partial D(\varepsilon)\cup\partial D_-(\varepsilon')\cup\{P_-(\varepsilon')-P_-(\varepsilon)\} \quad \text{for } \varepsilon > \varepsilon' > 0,$$

where $\partial D_-(\varepsilon') = \partial D(\varepsilon')$ as a path but has the clockwise orientation:



Then $\int_{P_+(\varepsilon)} e^{-y}y^{s-1}dy$ and $\int_{P_-(\varepsilon)} e^{-y}y_-^{s-1}dy$ converge for all s and give analytic functions on $\mathbf{C}$. Note that

$$\int_{P_+(\varepsilon)} e^{-y}y^{s-1}dy = -\int_\varepsilon^\infty e^{-y}y^{s-1}dy \text{ and } \int_{P_-(\varepsilon)} e^{-y}y_-^{s-1}dy = e^{2\pi is}\int_\varepsilon^\infty e^{-y}y^{s-1}dy.$$

Changing variables by $y = \varepsilon e^{i\theta}$ ($dy = i\varepsilon e^{i\theta}d\theta$), we have, for a sufficiently small ε,

$$\left|\int_{\partial D(\varepsilon)} e^{-y}y^{s-1}dy\right| \le M\varepsilon^\sigma \int_0^{2\pi} d\theta = 2\pi M\varepsilon^\sigma \text{ if } \sigma > 0,$$

where M is a constant independent of ε. Thus if $\sigma = \mathrm{Re}(s) > 0$, we know that

$$\lim_{\varepsilon\to 0}\int_{P(\varepsilon)} e^{-y}y^{s-1}dy = (e^{2\pi is}-1)\Gamma(s).$$

The function $e^{-y}y^{s-1}$ has no singularity on $\partial D(\varepsilon,\varepsilon')$ and hence, by Cauchy's integral formula (see [Hör, 1.2]),

$$\int_{\partial D(\varepsilon,\varepsilon')} e^{-y}y^{s-1}dy = (2\pi\sqrt{-1})\sum_{z:\text{poles in } D(\varepsilon,\varepsilon')} \mathrm{Res}_{y=z} e^{-y}y^{s-1} = 0.$$

Then we have

$$\int_{P(\varepsilon)} e^{-y}y^{s-1}dy - \int_{P(\varepsilon')} e^{-y}y^{s-1}dy = \int_{\partial D(\varepsilon,\varepsilon')} e^{-y}y^{s-1}dy = 0.$$

Thus we know that the holomorphic function $\int_{P(\varepsilon)} e^{-y}y^{s-1}dy$ of s is independent of ε and gives $(e^{2\pi is}-1)\Gamma(s)$ if $\sigma > 0$. Thus we have the meromorphic continuation of $\Gamma(s)$ given by

$$\Gamma(s) = (e^{2\pi is}-1)^{-1}\int_{P(\varepsilon)} e^{-y}y^{s-1}dy \text{ for all } s \in \mathbf{C}. \tag{2}$$

Since $(e^{2\pi is}-1)^{-1}$ has singularities only at integers $s \in \mathbf{Z}$, which are simple poles, $\Gamma(s)$ has at most simple poles at non-positive integers. Through integration by parts, we have the well known functional equation

$$\Gamma(s+1) = \int_0^\infty e^{-y}y^s dy = [-e^{-y}y^s]_0^\infty + s\int_0^\infty e^{-y}y^{s-1}dy = s\Gamma(s).$$

The analytic continuation of $\Gamma(s)$ can be also proven by using this functional equation, which shows that $\Gamma(s)$ has in fact simple poles at integers $m \le 0$.

Exercise 1. Show that for each positive integer n

$$\lim_{s\to 1-n}(e^{2\pi is}-1)\Gamma(s) = \frac{(-1)^{n-1}(2\pi\sqrt{-1})}{(n-1)!}.$$

Now we go into the integral expression of $\zeta(s)$ using $G(z)$. Expanding G into a geometric series, we know that

$$G(y) = \frac{e^{-y}}{1-e^{-y}} = \sum_{n=1}^\infty e^{-ny}. \tag{3}$$

This series is convergent when $|e^{-y}| < 1$ ($\Leftrightarrow \mathrm{Re}(y) > 0$). We first formally integrate G on $\mathbf{R}_+$:

$$\int_0^\infty G(y)y^{s-1}dy = \int_0^\infty \sum_{n=1}^\infty e^{-ny}y^{s-1}dy \overset{?}{=} \sum_{n=1}^\infty \int_0^\infty e^{-ny}y^{s-1}dy$$
$$\overset{ny \mapsto y}{=} \sum_{n=1}^\infty n^{-s}\int_0^\infty e^{-y}y^{s-1}dy = \Gamma(s)\zeta(s).$$

We need to justify the interchange of $\sum_{n=1}^\infty$ and $\int_0^\infty$ made at the equality marked by "?". For that, we look at the poles of $G(y) = \frac{e^{-y}}{1-e^{-y}}$. Since $1-e^{-y}$ has zeros only at $2\pi\sqrt{-1}\,\mathbf{Z} = \{2\pi\sqrt{-1}\,n \mid n \in \mathbf{Z}\}$, $G(y)$ can have a pole only at 0 on $\mathbf{R}$.

Exercise 2. Show that $|yG(y)|$ is bounded (independently of y) in the unit disk of radius one with center 0 (hint: show $\lim_{y\to 0} yG(y) = 1$ and deduce the result from this).

On the other hand, since $e^{-y} \to 0$ as $y \to +\infty$, there is a constant $M > 0$ such that $|yG(y)| \le Me^{-y/2}$ by the above exercise. This shows first of all, for $\sigma = \mathrm{Re}(s)$,

$$\left|\int_0^\infty G(y)y^{s-1}dy\right| \le \int_0^\infty |G(y)y|\,y^{\sigma-2}dy \le M\int_0^\infty e^{-y/2}y^{\sigma-2}dy = 2^{\sigma-1}M\Gamma(\sigma-1).$$

Thus $\int_0^\infty G(y)y^{s-1}dy$ is convergent if $\sigma > 1$. Since the domain of integration $\mathbf{R}_+$ is not compact, the uniform convergence of (1) is not sufficient to get the interchange of $\sum_{n=1}^\infty$ and $\int_0^\infty$. In order to assure the interchange, we shall use the following dominated convergence theorem in the integration theory (due to Lebesgue): If a sequence of continuous (actually integrable) functions $f_n(x)$ (on an interval $[a,b]$ in $\mathbf{R}$; a and b can be $\pm\infty$) is dominated by a continuous and integrable function and $f(x) = \lim_{n\to\infty} f_n(x)$ at every point x, then

$$\int_a^b \lim_{n\to\infty} f_n(x)dx = \lim_{n\to\infty}\int_a^b f_n(x)dx.$$

We apply this result to $G_n(y)y^{s-1} = \sum_{m=1}^n e^{-my}y^{s-1}$ which is dominated by the integrable function $|G(y)|\,y^{\sigma-1}$ (if $\sigma > 1$) and converges to $\sum_{n=1}^\infty e^{-ny}y^{s-1}$. In fact, we see that

$$|G_n(y)y^{s-1}| = \left|\sum_{m=1}^n e^{-my}y^{s-1}\right| \le \sum_{m=1}^\infty \left|e^{-my}y^{s-1}\right| = |G(y)|\,y^{\sigma-1} \text{ if } y > 0.$$

Therefore we have

$$\sum_{n=1}^\infty \int_0^\infty e^{-ny}y^{s-1}dy = \lim_{n\to\infty}\int_0^\infty G_n(y)dy = \int_0^\infty \lim_{n\to\infty} G_n(y)dy = \int_0^\infty \sum_{n=1}^\infty e^{-ny}y^{s-1}dy.$$

This justifies the interchange and we have

Proposition 1. $\Gamma(s)\zeta(s) = \int_0^\infty G(y)y^{s-1}dy$ *if* $\mathrm{Re}(s) > 1$.

We cannot extend (naively) this integral expression to the left half plane $\{s \mid \mathrm{Re}(s) \le 1\}$ because $\zeta(s)$ has a simple pole at $s = 1$.

Since $G(y)$ has singularities only at $y = 0$ in a small neighborhood of $\mathbf{R}_+$, we know, in the same manner as in the case of the analytic continuation of $\Gamma(s)$, that if $0 < \varepsilon < 2\pi$ and $\mathrm{Re}(s) > 1$,

$$\Gamma(s)\zeta(s) = \int_0^\infty G(y)y^{s-1}dy = (e^{2\pi is}-1)^{-1}\int_{P(\varepsilon)}G(y)y^{s-1}dy.$$

The integral of the right-hand side converges for all s and gives an analytic function of s. Thus we have as a corollary of the proposition.

Corollary 1. $(e^{2\pi is}-1)\Gamma(s)\zeta(s)$ *can be continued to a holomorphic function on* $\mathbf{C}$ *and has an integral expression:*

$$(e^{2\pi is}-1)\Gamma(s)\zeta(s) = \int_{P(\varepsilon)}G(y)y^{s-1}dy \quad \textit{for} \quad 0 < \varepsilon < 2\pi.$$

Exercise 3. (a) Prove Corollary 1 rigorously along the lines of the proof of the analytic continuation of $\Gamma(s)$. (b) Compute $\mathrm{Res}_{s=1}\zeta(s)$ by using the above integral expression.

We now want to compute the value of $\int_{P(\varepsilon)}G(y)y^{s-1}dy$ at $s = 1\text{-}n$ for positive integers n. As in Exercise 1, we know that

$$\int_{P(\varepsilon)}G(y)y^{-n}dy = \int_{\partial D(\varepsilon)}G(y)y^{-n}dy = (2\pi\sqrt{-1})\mathrm{Res}_{y=0}(G(y)y^{-n}).$$

We define the Bernoulli numbers B_n by

$$zG(z) = \frac{ze^{-z}}{1-e^{-z}} = \frac{z}{e^z-1} = \sum_{n=0}^{\infty} B_n\frac{z^n}{n!}.$$

We see that $B_n = \left(\frac{d}{dx}\right)^n\{xG(x)\}\big|_{x=0}$. Since $\mathrm{Res}_{y=0}G(y)y^{-n} = \frac{B_n}{n!}$, we know that $\int_{P(\varepsilon)}G(y)y^{-n}dy = (2\pi\sqrt{-1})\frac{B_n}{n!}$. Then by Exercises 1 and 4(b) below, we know

Theorem 1. *For each positive integer* n, *we have* $\zeta(1\text{-}n) = -\frac{B_n}{n}$ *if* n *is even,* $\zeta(0) = -\frac{1}{2}$ *and* $\zeta(1\text{-}n) = 0$ *if* $n > 1$ *is odd.*

This agrees with Euler's computation via Exercise 1.4.

Numerical Example. We list here several Bernoulli numbers:

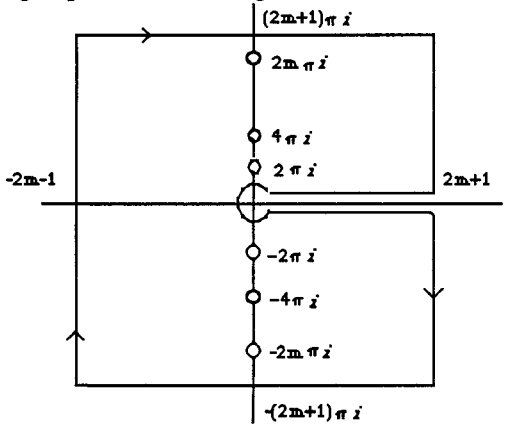
$$B_2 = \frac{1}{6} = \frac{1}{2\cdot 3},\ B_4 = B_8 = -\frac{1}{30} = -\frac{1}{2\cdot 3\cdot 5},\ B_6 = \frac{1}{42} = \frac{1}{2\cdot 3\cdot 7},\ B_{10} = \frac{5}{66} = \frac{5}{2\cdot 3\cdot 11},$$

$$B_{12} = -\frac{691}{2730} = -\frac{691}{2\cdot 3\cdot 5\cdot 7\cdot 13},\ B_{14} = \frac{7}{2\cdot 3}.$$

(See [Wa, p.374] for more Bernoulli numbers).

Exercise 4. (a) Show that B_{2n} is positive if n is odd and B_{2n} is negative if n is even (Use the functional equation of $\zeta(s)$).
(b) Show that $B_n = 0$ if n is odd and $n > 1$.
(c) Show that the denominator of B_n consists of primes p such that n is divisible by $p-1$ (use Exercise 6(b) in the previous section).

Now we prove the functional equation. The idea is to relate the function of s given by $\int_{P(\varepsilon)} G(y)y^{s-1}dy$ with the integration of $G(y)y^{s-1}$ on the following integral path for each integer $m > 0$:



We denote this integral path by $\Delta(m)$, where the orientation is clockwise on the outside rectangle. Since the orientation of $\Delta(m)$ is clockwise if you look from a point inside of $\Delta(m)$, by Cauchy's integral formula, we know that

$$\int_{\Delta(m)} G(y)y^{s-1}dy = -(2\pi\sqrt{-1})\sum_{w \text{ pole inside } \Delta(m)} \mathrm{Res}_{y=w}(G(y)y^{s-1}),$$

where $\mathrm{Res}_{y=w}\phi(y)$ is the coefficient of $(y-w)^{-1}$ in the Laurent expansion $\phi(y) = \sum_{n>-\infty} c(n)(y-w)^n$. Since $1-e^{-y} = 0$ if and only if $y \in 2\pi\sqrt{-1}\mathbf{Z}$, the function $G(y)y^{s-1} = \dfrac{e^{-y}}{1-e^{-y}}y^{s-1}$ has simple poles only at $2\pi\sqrt{-1}n$ for integers n with $0 < |n| \le m$ inside $\Delta(m)$. The residue at $y = 2\pi\sqrt{-1}n$ can be easily computed and is given by

$$\text{(4)} \qquad \mathrm{Res}_{y=2\pi i n}(G(y)y^{s-1}) = \begin{cases} -\sqrt{-1}\,|2n\pi|^{s-1}e^{s\pi i/2} & \text{if } n > 0, \\ \sqrt{-1}\,|2n\pi|^{s-1}e^{3s\pi i/2} & \text{if } n < 0. \end{cases}$$

Exercise 5. Write down every detail of how one obtains the formula (4).

Thus we have

$$\int_{\Delta(m)} G(y)y^{s-1}dy = (2\pi)^s e^{\pi is}(e^{\pi is/2}-e^{-\pi is/2})\sum_{n=1}^{m} n^{s-1}.$$

Therefore, if $\mathrm{Re}(s) < 0$, we already know that $\lim_{m\to\infty}\sum_{n=1}^{m} n^{s-1}$ converges to $\zeta(1-s)$ and hence we obtain

$$(5)\quad \lim_{m\to\infty}\int_{\Delta(m)} G(y)y^{s-1}dy = (2\pi)^s e^{\pi is}(e^{\pi is/2}-e^{-\pi is/2})\zeta(1-s) \text{ if } \mathrm{Re}(s) < 0.$$

On the other hand, if we denote by $Q(m)$ the square of side length $4m+2$ centered at 0 with clockwise orientation and by $P(\varepsilon,m)$ the complement of $Q(m)$ in $\Delta(m)$, then we have

$$\begin{aligned}(6)\quad \lim_{m\to\infty}\int_{\Delta(m)} G(y)y^{s-1}dy &= \lim_{m\to\infty}\int_{P(\varepsilon,m)} G(y)y^{s-1}dy + \lim_{m\to\infty}\int_{Q(m)} G(y)y^{s-1}dy \\ &= \int_{P(\varepsilon)} G(y)y^{s-1}dy + \lim_{m\to\infty}\int_{Q(m)} G(y)y^{s-1}dy \\ &= (e^{2\pi is}-1)\Gamma(s)\zeta(s) + \lim_{m\to\infty}\int_{Q(m)} G(y)y^{s-1}dy.\end{aligned}$$

We now show that $\lim_{m\to\infty}\int_{Q(m)} G(y)y^{s-1}dy = 0$. Then after a minor modification, we will have the functional equation. We write $Q_{\pm}(m)$ for the upper and lower edge of $Q(m)$ and $Q_r(m)$ (resp. $Q_l(m)$) for the right (resp. left) edge of $Q(m)$. Here we only prove that

$$\lim_{m\to\infty}\int_{Q_+(m)} G(y)y^{s-1}dy = 0.$$

The computation for the other edges will be left to the reader as an exercise. First note that, writing $y = x+\pi\sqrt{-1}(2m+1)$ on $Q_+(m)$ for $x = \mathrm{Re}(y)$, we have

$$e^{-y} = e^{-\pi i}e^{-2m\pi i}e^{-x} = -e^{-x}, \quad |1-e^{-y}| = 1+e^{-x} > e^{-x}$$

and

$$|G((2m+1)\pi\sqrt{-1}+x)((2m+1)\pi\sqrt{-1}+x)^{s-1}| \le M|(2m+1)\pi\sqrt{-1}+x|^{\sigma-1}$$

for a constant M depending only on s and for $\sigma = \mathrm{Re}(s) < 0$. Hence, we have $|G(y)| = \dfrac{e^{-x}}{1+e^{-x}} \le 1$ for all $y \in Q_+(m)$. This shows that

$$\begin{aligned}\left|\int_{Q_+(m)} G(y)y^{s-1}dy\right| &= \left|\int_{-2m-1}^{2m+1} G((2m+1)\pi\sqrt{-1}+x)((2m+1)\pi\sqrt{-1}+x)^{s-1}dx\right| \\ &\le \int_{-2m-1}^{2m+1} |G((2m+1)\pi\sqrt{-1}+x)((2m+1)\pi\sqrt{-1}+x)^{s-1}|dx \\ &\le M\int_{-2m-1}^{2m+1} |(2m+1)\pi\sqrt{-1}+x|^{\sigma-1}dx \le M\int_{-2m-1}^{2m+1} ((2m+1)^2\pi^2+x^2)^{(\sigma-1)/2}dx.\end{aligned}$$

If $\sigma < 1$, then $\sigma-1 < 0$ and we see that

$$((2m+1)^2\pi^2+x^2)^{(\sigma-1)/2} \le ((2m+1)\pi)^{\sigma-1}.$$

Then we have

$$\int_{-2m-1}^{2m+1} ((2m+1)^2\pi^2+x^2)^{(\sigma-1)/2}dx \le \int_{-2m-1}^{2m+1} ((2m+1)\pi)^{(\sigma-1)}dx = 2\pi^{\sigma-1}(2m+1)^{\sigma}$$

which goes to 0 as $m \to +\infty$ if $\sigma < 0$. This shows the assertion.

Exercise 6. Show that $\lim_{m\to\infty} \int_{Q_r(m)} G(y)y^{s-1}dy = 0$. (First show that on $Q_r(m)$, $|G(y)| \le 2$ and proceed in the same manner as above.)

By the above estimate and Exercise 6, we obtain

$$(e^{2\pi is}-1)\Gamma(s)\zeta(s) = (2\pi)^s e^{\pi is}(e^{\pi is/2}-e^{-\pi is/2})\zeta(1-s)$$

or multiplying by $e^{-\pi is}$, we have

$$(e^{\pi is}-e^{-\pi is})\Gamma(s)\zeta(s) = (2\pi)^s(e^{\pi is/2}-e^{-\pi is/2})\zeta(1-s).$$

By the fact that $\dfrac{e^{\pi is/2}-e^{-\pi is/2}}{e^{\pi is}-e^{-\pi is}} = \{2\cos(\frac{\pi s}{2})\}^{-1}$, we deduce

Theorem 2 (Riemann). *We have* $\zeta(s) = \dfrac{(2\pi)^s\zeta(1-s)}{2\Gamma(s)\cos(\pi s/2)}$.

§2.3. Hurwitz and Dirichlet L-functions

Now we extend our argument to Dirichlet L-functions. Let χ be a character of the multiplicative group $(\mathbf{Z}/N\mathbf{Z})^\times$. Thus $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ is a homomorphism of the finite multiplicative group $(\mathbf{Z}/N\mathbf{Z})^\times$ into $\mathbf{C}^\times$. We extend χ to a function on $\mathbf{Z}$ by putting $\chi(n) = \chi(n \bmod N)$ if $n \bmod N$ is in $(\mathbf{Z}/N\mathbf{Z})^\times$ and $\chi(n) = 0$ if $n \bmod N$ is outside $(\mathbf{Z}/N\mathbf{Z})^\times$ and define the Dirichlet L-function of χ by

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}.$$

Any $x \in (\mathbf{Z}/N\mathbf{Z})^\times$ satisfies $x^r = 1$ and hence $\chi(x)^r = 1$, where $r = \varphi(N)$ is the order of $(\mathbf{Z}/N\mathbf{Z})^\times$. Thus $\chi(n)$ is a root of unity and in particular satisfies $|\chi(n)| \le 1$. It is an algebraic integer of a cyclotomic field. Then we have

$$|L(s,\chi)| \le \sum_{n=1}^{\infty} |\chi(n)n^{-s}| \le \sum_{n=1}^{\infty} n^{-\sigma} = \zeta(\sigma) \text{ for } \sigma = \mathrm{Re}(s).$$

This shows that $L(s,\chi)$ is absolutely convergent if $\mathrm{Re}(s) > 1$ (this convergence is uniform on every compact subset in the region with $\mathrm{Re}(s) > 1$ and hence $L(s,\chi)$ is an analytic function of s in this region).

Exercise 1. Show the following Euler product expansion of $L(s,\chi)$ and its convergence if $\mathrm{Re}(s) > 1$: $L(s,\chi) = \prod_p (1-\chi(p)p^{-s})^{-1}$.

More generally we think of a function $\phi : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$ and consider

$$L(s,\phi) = \sum_{n=1}^{\infty} \phi(n)n^{-s}.$$

To continue this function to the whole complex plane, we rewrite it as

$$L(s,\phi) = \sum_{n=1}^{\infty}\phi(n)n^{-s} = \sum_{a=1}^{N}\phi(a)\sum_{n=0}^{\infty}(Nn+a)^{-s} = \sum_{a=1}^{N}\phi(a)N^{-s}\sum_{n=0}^{\infty}(n+\frac{a}{N})^{-s}.$$

Thus the problem of analytic continuation of $L(s,\phi)$ is reduced to the same problem for $\sum_{n=0}^{\infty}(n+\frac{a}{N})^{-s}$. More generally we consider the following zeta function for all $0 < x \leq 1$:

$$\zeta(s,x) = \sum_{n=0}^{\infty} (n+x)^{-s},$$

which is convergent if $\mathrm{Re}(s) > 1$. This zeta function is called the Hurwitz L-function (and was introduced by Hurwitz in the 1880's). We then have

$$L(s,\phi) = \sum_{a=1}^{N} \phi(a)N^{-s}\zeta(s,\frac{a}{N}). \tag{1}$$

In the same manner as in the case of the Riemann zeta function, we have the following integral expression of $\zeta(s,x)$:

$$\Gamma(s)\zeta(s,x) = \int_0^{\infty} G(y,x)y^{s-1}dy \quad \text{if } \mathrm{Re}(s) > 1, \tag{2}$$

where $G(y,x) = \dfrac{e^{(1-x)y}}{e^y - 1} = \dfrac{e^{-xy}}{1-e^{-y}} = \sum_{n=0}^{\infty} e^{-(n+x)y}$.

Exercise 2. (a) Show that $\zeta(s,x)$ is absolutely convergent if $\mathrm{Re}(s) > 1$.
(b) Show the formula (2) along the lines of the proof of Proposition 2.1.

Note that the zeros of $1-e^{-y}$ are situated at $2\pi i n$ for $n \in \mathbf{Z}$ and are all simple. In particular, $yG(y,x)$ is bounded in any small neighborhood of 0. Thus for sufficiently small $\varepsilon > 0$ (actually, any ε with $0 < \varepsilon < 2\pi$ does the job), the integral $\int_{P(\varepsilon)} G(y,x)y^{s-1}dy$ is convergent for all s and gives an analytic function of s. The same computation as in the proof of Corollary 2.1 gives

Proposition 1. $(e^{2\pi i s}-1)\Gamma(s)\zeta(s,x)$ *can be continued to a holomorphic function on* $\mathbf{C}$ *and has an integral expression:*

$$(e^{2\pi i s}-1)\Gamma(s)\zeta(s,x) = \int_{P(\varepsilon)} G(y,x)y^{s-1}dy \quad \textit{for} \quad 0 < \varepsilon < 2\pi.$$

This combined with the formula (1) yields

Corollary 1. *The function* $(e^{2\pi is}-1)\Gamma(s)L(s,\phi)$ *of* s *can be continued to a holomorphic function on* $\mathbf{C}$ *and has an integral expression:*

$$(e^{2\pi is}-1)\Gamma(s)L(s,\phi) = \int_{P(\varepsilon)}\sum_{a=1}^{N}\frac{\phi(a)e^{-ay}}{1-e^{-Ny}}y^{s-1}dy \quad \textit{for} \quad 0<\varepsilon<2\pi/N.$$

As a byproduct of the analytic continuation, we can compute the value of $\zeta(1\text{-}n,x)$ using the formula

$$\{(e^{2\pi is}-1)\Gamma(s)\,|_{s=1-n}\}\zeta(1\text{-}n,x) = \int_{\partial D(\varepsilon)}G(y,x)y^{-n}dy = (2\pi\sqrt{-1})\mathrm{Res}_{y=0}G(y,x)y^{-n}.$$

By Exercise 2.1, we know that

$$(e^{2\pi is}-1)\Gamma(s)\,|_{s=1-n} = \frac{(-1)^{n-1}(2\pi\sqrt{-1})}{(n-1)!}.$$

Thus we compute $\mathrm{Res}_{y=0}G(y,x)y^{-n}$. Write $F(y,x) = yG(y,1\text{-}x)$ and expand $F(y,x)$ into a power series in y (regarding x as a constant):

$$F(y,x) = \sum_{n=0}^{\infty} B_n(x)\frac{y^n}{n!}.$$

We can interpret this argument in a manner similar to §1 as follows. Writing $t = e^y$, we have $F(y,x) = y\frac{t^x}{t-1}$. Thus $\frac{t^x}{t-1} = \frac{1}{y} + \sum_{n=0}^{\infty}\frac{B_{n+1}(x)}{(n+1)!}y^n$. This shows $\frac{t^x}{t-1} - a\frac{t^{ax}}{t^a-1} = \sum_{n=0}^{\infty}\frac{(B_{n+1}(x)-a^{n+1}B_{n+1}(x))}{(n+1)!}y^n$ for any integer $a>1$, and thus

$$(3a) \qquad (1-a^{n+1})\frac{B_{n+1}(x)}{n+1} = \left(t\frac{d}{dt}\right)^n\left\{\frac{t^x}{t-1}-a\frac{t^{ax}}{t^a-1}\right\}\Big|_{t=1}.$$

Then $B_n(x)$ is a polynomial in x of degree n with rational coefficients. These are called "Bernoulli polynomials". We can make this more explicit as follows:

$$F(y,x) = e^{xy}\left(\frac{y}{e^y-1}\right) = \left(\sum_{n=0}^{\infty}x^n\frac{y^n}{n!}\right)\left(\sum_{m=0}^{\infty}B_m\frac{y^m}{m!}\right).$$

Therefore, equating the coefficients in y^n, we see that

$$\frac{B_n(x)}{n!} = \sum_{j=0}^{n}\frac{B_j}{j!(n-j)!}x^{n-j}.$$

In other words, we have the formula

$$(3b) \qquad B_n(x) = \sum_{j=0}^{n}\binom{n}{j}B_jx^{n-j} \in \mathbf{Q}[x].$$

Thus we know that

$$\begin{aligned}\mathrm{Res}_{y=0}G(y,x)y^{-n} &= \mathrm{Res}_{y=0}F(y,1\text{-}x)y^{-n-1}\\ &= \text{the coefficient of } y^n \text{ in } F(y,1\text{-}x) = \frac{B_n(1-x)}{n!}.\end{aligned}$$

This shows that

$$\frac{(-1)^{n-1}(2\pi\sqrt{-1})}{(n-1)!}\zeta(1-n,x) = (2\pi\sqrt{-1})\frac{B_n(1-x)}{n!}.$$

Thus we conclude that $\zeta(1-n,x) = (-1)^{n-1}\frac{B_n(1-x)}{n}$. Here we note that

$$F(y,1-x) = \frac{ye^{(1-x)y}}{e^y-1} = \frac{ye^{-xy}}{1-e^{-y}} = F(-y,x).$$

This equality yields

$$B_n(1-x) = (-1)^n B_n(x). \tag{4}$$

Thus we obtain

Theorem 1. *We have, for any integers* $a > 1$ *and* $0 < b \le N$,

$$N^m(1-a^{m+1})\zeta(-m,\frac{b}{N}) = \left(t\frac{d}{dt}\right)^m\left(\frac{t^b}{1-t^N} - a\frac{t^{ab}}{1-t^{aN}}\right)\Big|_{t=1} \textit{ for all } m \ge 0, \textit{ and}$$

$$\zeta(1-n,x) = -\frac{B_n(x)}{n} = -(1-a^n)^{-1}\left(t\frac{d}{dt}\right)^{n-1}\left(\frac{t^x}{t-1} - a\frac{t^{ax}}{t^a-1}\right)\Big|_{t=1} \textit{ for all } n > 0.$$

Then the formula (1), $L(s,\phi) = \sum_{a=1}^N \phi(a)N^{-s}\zeta(s,\frac{a}{N})$, combined with Theorem 1, implies

Corollary 2. *Let* $\mathbf{Q}(\chi)$ *denote the cyclotomic field generated by the values of the character* χ. *Then we have*

$$L(1-n,\chi) = -\sum_{a=1}^N \chi(a)N^{n-1}\frac{B_n(a/N)}{n} \in \mathbf{Q}(\chi).$$

Moreover, suppose $\chi(-1) \ne (-1)^n$. *Then we have* $L(1-n,\chi) = 0$ *for* $n > 0$ *if* χ *is non-trivial, and* $\zeta(1-n) = 0$ *if* $n > 1$. *In general, for* $\phi : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$, *we have, if* a *is prime to* N,

$$L(-m,\phi-a^{m+1}\phi_a) = \left(t\frac{d}{dt}\right)^m\left(\sum_{b=1}^N\frac{\phi(b)t^b}{1-t^N} - a\sum_{b=1}^N\frac{\phi_a(b)t^{ab}}{1-t^{aN}}\right)\Big|_{t=1} \textit{ for all } m \ge 0,$$

where $\phi_a(b) = \phi(ab)$.

The vanishing of $L(1-n,\chi)$ follows from (4) if $\chi(-1) \ne (-1)^n$. The number $B_{n,\chi} = \sum_{a=1}^N \chi(a)N^{n-1}B_n(\frac{a}{N})$ is called the generalized Bernoulli number. Using the notation $B_{n,\chi}$, the above formula takes the following form: $L(1-n,\chi) = -B_{n,\chi}/n$.

Examples of Bernoulli polynomials:

$$B_0(x) = 1,\ B_1(x) = x-\frac{1}{2},\ B_2(x) = x^2 - x + \frac{1}{6},\ B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x.$$

Using the above formula, we can get

$$L(0,\chi) = -\frac{1}{N}\sum_{a=1}^{N-1}\chi(a)a \text{ if } \chi \text{ is non-trivial.}$$

Since $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ is a group character and $(-1)^2 = 1$, $\chi(-1)^2 = 1$. Thus $\chi(-1) = \pm 1$.

Now we prove the functional equation of $L(s,\chi)$. We proceed in the same way as in the case of the Riemann zeta function. We consider the integral on the path $\Delta(m)$ for each positive integer m given in §2. By the Cauchy integral formula,

$$\int_{\Delta(m)} G(y,x)y^{s-1}dy = -(2\pi\sqrt{-1})\sum_{w \text{ pole inside } \Delta(m)} \mathrm{Res}_{y=w}(G(y,x)y^{s-1}).$$

The function $G(y,x)$ has a simple pole at $2\pi\sqrt{-1}n$ for integers n and the residues at $2\pi\sqrt{-1}n$ can be computed as

$$\mathrm{Res}_{y=2\pi in}(G(y,x)y^{s-1}) = \begin{cases} e^{-2\pi inx+(s-1)\pi i/2}\,|\,2n\pi\,|^{s-1} & \text{if } n > 0, \\ e^{-2\pi inx+3(s-1)\pi i/2}\,|\,2n\pi\,|^{s-1} & \text{if } n < 0, \end{cases}$$

because as already computed, $\mathrm{Res}_{y=2\pi in}\frac{1}{1-e^{-y}} = 1$ and the value of $e^{-xy}y^{s-1}$ is $e^{-2\pi inx+(s-1)\pi i/2}\,|\,2n\pi\,|^{s-1}$ or $e^{-2\pi inx+3(s-1)\pi i/2}\,|\,2n\pi\,|^{s-1}$ according as $n > 0$ or $n < 0$. Therefore

$$\int_{\Delta(m)} G(y,x)y^{s-1}dy = (2\pi)^s\{-e^{\pi is/2}\sum_{n=1}^{m} e^{-2\pi inx}n^{s-1} + e^{3\pi is/2}\sum_{n=1}^{m} e^{2\pi inx}n^{s-1}\}.$$

This shows, if $\mathrm{Re}(s) < 0$,

$$\lim_{m\to\infty}\int_{\Delta(m)} G(y,x)y^{s-1}dy = (2\pi)^s\{e^{3\pi is/2}\sum_{n=1}^{\infty} e^{2\pi inx}n^{s-1} - e^{\pi is/2}\sum_{n=1}^{\infty} e^{-2\pi inx}n^{s-1}\}.$$

In exactly the same manner as in the case of the Riemann zeta function, the integral on the outer square $Q(m)$ converges to 0 as $m \to +\infty$. Thus we have

$$(e^{2\pi is}-1)\Gamma(s)\zeta(s,x) = \int_{P(\varepsilon)} G(y,x)y^{s-1}dy = \lim_{m\to\infty}\int_{\Delta(m)} G(y,x)y^{s-1}dy$$
$$= (2\pi)^s\{e^{3\pi is/2}\sum_{n=1}^{\infty} e^{2\pi inx}n^{s-1} - e^{\pi is/2}\sum_{n=1}^{\infty} e^{-2\pi inx}n^{s-1}\} \quad \text{if } \mathrm{Re}(s) < 0.$$

Then by the formula $L(s,\phi) = \sum_{a=1}^{N}\phi(a)N^{-s}\zeta(s,\frac{a}{N})$, we see that

$$(e^{2\pi is}-1)\Gamma(s)L(s,\chi)$$
$$= \left(\frac{2\pi}{N}\right)^s\{e^{3\pi is/2}\sum_{n=1}^{\infty}\sum_{a=1}^{N}\chi(a)e(\tfrac{na}{N})n^{s-1} - e^{\pi is/2}\sum_{n=1}^{\infty}\sum_{a=1}^{N}\chi(a)e(\tfrac{-na}{N})n^{s-1}\},$$

where $e(z) = e^{2\pi iz}$.

Now we need to compute $\sum_{a=1}^{N}\chi(a)e(na/N)$. To treat this sum, we insert here a definition. For each proper factor D of N, we have a natural homomorphism $\rho_D : (\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/D\mathbf{Z})^\times$ which satisfies $\rho_D(n \bmod N) = n \bmod D$. If for some D, there exists a character $\chi_0 : (\mathbf{Z}/D\mathbf{Z})^\times \to \mathbf{C}^\times$ such that $\chi(n) = \chi_0(\rho_D(n))$ for all $n \in (\mathbf{Z}/N\mathbf{Z})^\times$, we say χ is imprimitive. A character χ is called primitive or primitive modulo N if χ is not imprimitive. Now we suppose

(5) χ is a primitive character modulo N.

We do not lose much generality by this assumption:

Exercise 3. Let $\chi = \chi_0 \circ \rho_D$ for a proper divisor D of N. Then show

$$L(s,\chi) = \{\Pi_{p|N}(1-\chi_0(p)p^{-s})\}L(s,\chi_0),$$

where p runs over all prime factors of N.

First we prove the following lemma (the orthogonality relation) in group theory:

Lemma 1. *Let* G *be a finite abelian group and* $\chi : G \to \mathbf{C}^\times$ *be a character. If* χ *is not identically equal to* 1, *then* $\sum_{g\in G}\chi(g) = 0$. *Similarly if* $g \neq 1$, $\sum_\chi \chi(g) = 0$, *where* χ *runs over all characters of* G.

Proof. Since χ has values in the group of roots of unity, which is cyclic, we may assume that G is cyclic and χ is injective by replacing G by G/Ker(χ). Let N be the order of G. Then χ induces an isomorphism of G onto the group μ_N of N-th roots of unity. Thus $\sum_{g\in G}\chi(g) = \sum_{\varsigma\in\mu_N}\varsigma = 0$ because $\Pi_{\zeta\in\mu_N}(X-\zeta) = X^N-1$. Let G* be the set of all characters of G. Defining the multiplication on G* by $\chi\psi(g) = \chi(g)\psi(g)$, G* is a group. If G is cyclic of order N, then the character is determined by its value at a generator g_0. Thus $G^* \ni \chi \mapsto \chi(g_0) \in \mu_N = \{\zeta \in \mathbf{C}^\times \mid \zeta^N = 1\}$ defines an injection. For any given $\zeta \in \mu_N$, defining $\chi(g_0{}^m) = \zeta^m$, χ is a character having the value ζ at g_0. Thus $G^* \cong \mu_N$. Then assigning g the character of G* which sends χ to $\chi(g)$, we have a homomorphism: $G \to G^{**}$. Since $\chi(g)$ takes all the N-th roots of unity as its values at some χ, this map is surjective. Then by counting the order of both sides, we conclude that $G \cong G^{**}$. In general, decomposing G into the product of cyclic groups, G* will be decomposed into the product of that character groups of each cyclic component. Thus $G \cong G^{**}$ in general. Then replacing G by G* and applying the first assertion of the lemma, we get the second.

Lemma 2. *Define the Gauss sum* $G(\chi) = \sum_{a=1}^N \chi(a)e(a/N)$. *Suppose that* χ *is primitive modulo* N. *Then* $\sum_{a=1}^N \chi(a)e(na/N) = \chi^{-1}(n)G(\chi)$ *for all integers* n.

Note here that $\chi^{-1}(n) = \chi(n)^{-1}$ is again a character of $(\mathbf{Z}/N\mathbf{Z})^\times$, which is primitive. In particular, this implies $\sum_{a=1}^N \chi(a)e(na/N) = 0$ if $n \notin (\mathbf{Z}/N\mathbf{Z})^\times$ because $\chi^{-1}(n) = 0$ by our way of extending χ^{-1} outside $(\mathbf{Z}/N\mathbf{Z})^\times$.

Proof. Define $\psi : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}^\times$ by $\psi(t) = e(t/N)$. Then, $\psi(t)$ does not depend on the choice of t. In fact, if $t \equiv s \bmod N$, then $t = s+Nn$ for an integer n and thus $e(t/N) = e((s/N)+n) = e(s/N)e^{2\pi i n} = e(s/N)$. Thus ψ gives a homomorphism of the additive group $\mathbf{Z}/N\mathbf{Z}$ into the multiplicative group $\mathbf{C}^\times$. This fact is obvious because

$$\psi(t+s) = e(t+s) = e^{2\pi i(t+s)} = e^{2\pi i t}e^{2\pi i s} = \psi(t)\psi(s).$$

Then $\sum_{a=1}^{N}\chi(a)e(na/N) = \sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\chi(a)\psi(na)$. We first treat the case where $n \bmod N \in (\mathbf{Z}/N\mathbf{Z})^\times$. Then the multiplication of n induces a bijection $x \mapsto nx$ on $(\mathbf{Z}/N\mathbf{Z})^\times$. Thus we can make the variable change in the above summation; so, rewriting na as a, we have

$$\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\chi(a)\psi(na) = \sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\chi(n^{-1}a)\psi(a) = \chi^{-1}(n)\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\chi(a)\psi(a) = \chi^{-1}(n)G(\chi).$$

Now assume that $n \notin (\mathbf{Z}/N\mathbf{Z})^\times$. In this case $\chi^{-1}(n) = 0$ by our way of extending χ^{-1} outside $(\mathbf{Z}/N\mathbf{Z})^\times$. Thus we need to prove that

$$\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\chi(a)\psi(na) = 0.$$

Let p be a prime which is a common divisor of N and n. Write $N = pD$ and $n = pn'$. Then we have

$$\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\chi(a)\psi(na) = \sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\chi(a)e(n'a/D) = \sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}e(n'a/D)\sum_{b\equiv a \bmod D}\chi(b),$$

because $e(n'a/D)$ only depends on the class of $n'a$ modulo D (but not N). We shall show that $\sum_{b\equiv a \bmod D}\chi(b) = 0$. We see that

$$\sum_{b\equiv a \bmod D}\chi(b) = \sum_{b\equiv a \bmod D}\chi(aba^{-1}) = \chi(a)\sum_{b\equiv 1 \bmod D}\chi(b).$$

Let $H = \{x \in (\mathbf{Z}/N\mathbf{Z})^\times \mid x \equiv 1 \bmod D\}$. Since $H = \mathrm{Ker}(\rho_D)$, it is a subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$. If χ is trivial on H, then we define $\chi_0 : (\mathbf{Z}/D\mathbf{Z})^\times \to \mathbf{C}^\times$ by $\chi_0(\rho_D(c)) = \chi(c)$. χ_0 is well defined because if $\rho_D(c) = \rho_D(c')$, then $c = c'h$ for $h \in H = \mathrm{Ker}(\rho_D)$. Thus $\chi(c) = \chi(c'h) = \chi(c')\chi(h) = \chi(c')$ because of the triviality of χ on H. Then $\chi = \chi_0\circ\rho_D$, which contradicts the primitivity of χ. Therefore we can conclude χ is non-trivial on H. Thus the orthogonality relation of characters (Lemma 1) shows that

$$\sum_{b\equiv 1 \bmod D}\chi(b) = \sum_{b\in H}\chi(b) = 0.$$

Now by using this lemma, we finish the computation:

$$\begin{aligned}(e^{2\pi is}-1)\Gamma(s)L(s,\chi)\\ &= \left(\frac{2\pi}{N}\right)^s\{e^{3\pi is/2}\sum_{n=1}^{\infty}\sum_{a=1}^{N}\chi(a)e(\tfrac{na}{N})n^{s-1}-e^{\pi is/2}\sum_{n=1}^{\infty}\sum_{a=1}^{N}\chi(a)e(\tfrac{-na}{N})n^{s-1}\}\\ &= \left(\frac{2\pi}{N}\right)^s G(\chi)\{e^{3\pi is/2}-\chi^{-1}(-1)e^{\pi is/2}\}\sum_{n=1}^{\infty}\chi^{-1}(n)n^{s-1}.\end{aligned}$$

We see easily that

$$\frac{e^{2\pi is}-1}{e^{3\pi is/2}-\chi^{-1}(-1)e^{\pi is/2}} = \begin{cases}2\cos(\pi s/2) & \text{if } \chi(-1) = 1,\\ 2\sqrt{-1}\sin(\pi s/2) & \text{if } \chi(-1) = -1.\end{cases}$$

This shows

Theorem 2. *Suppose that* χ *is primitive modulo* N. *Then we have*

$$L(s,\chi) = \begin{cases}\dfrac{G(\chi)(2\pi/N)^s L(1-s,\chi^{-1})}{2\Gamma(s)\cos(\pi s/2)} & \textit{if } \chi(-1) = 1,\\[2ex] \dfrac{G(\chi)(2\pi/N)^s L(1-s,\chi^{-1})}{2\sqrt{-1}\,\Gamma(s)\sin(\pi s/2)} & \textit{if } \chi(-1) = -1.\end{cases}$$

Exercise 4. Using the above functional equation, show that $L(s,\chi)$ is a holomorphic function on the whole complex plane $\mathbf{C}$ if χ is a primitive character modulo $N > 1$. (The main point is to show that $L(s,\chi)$ is holomorphic at $s = 1$; use also Corollary 2.)

Exercise 5. Suppose that χ is primitive modulo N. By using the functional equation (and also the power series expansion of $L(s,\chi)$ at $s = \frac{1}{2}$), show $G(\chi)G(\chi^{-1}) = \chi(-1)N$ for general primitive χ, and supposing that $L(\frac{1}{2},\chi) \neq 0$, show $G(\chi) = \sqrt{\chi(-1)N}$ if χ has values in $\{\pm 1\}$. (The fact that $G(\chi) = \sqrt{\chi(-1)N}$ (not $-\sqrt{\chi(-1)N}$) if χ has values in $\{\pm 1\}$ is true without the assumption of the non-vanishing of $L(s,\chi)$ at $\frac{1}{2}$. Try to prove it without the non-vanishing assumption.)

§2.4. Shintani L-functions

In this section, we introduce the contour integral of several variables and Shintani L-functions [St1-6] and later, we will relate them with Dedekind and Hecke L-functions of number fields. We now take another branch of *log* different from the one in the previous section; namely, for $z \in \mathbf{C}$, we write it as $z = |z|e^{i\theta}$

with $-\pi \le \theta < \pi$ using the polar coordinate and define $log(z) = \log|z| + i\theta$. Accordingly, we define the complex power $z^s = e^{s\,log(z)}$ by this logarithm function. We put

$H' = \{z \in \mathbf{C} \mid \mathrm{Re}(z) > 0\}$: the right half complex plane,
$\mathbf{R}_\pm = \{x \in \mathbf{R} \mid \pm x > 0\}$: the right or left real line,
$\overline{\mathbf{R}}_\pm = \mathbf{R}_\pm \cup \{0\}$, $\mathbf{N} = \overline{\mathbf{R}}_+ \cap \mathbf{Z}$.

By our choice of log, we have the luxury of

$$(ab)^s = a^s b^s, \quad \overline{a^s} = \overline{a}^{\overline{s}} \quad \text{and} \quad (a^{-1})^s = a^{-s}$$

for any two $a,b \in H'$ and $s \in \mathbf{C}$.

To define the Shintani L-function, we need the following data: (i) a complex $r \times m$ matrix $A = (a_{ij})$; (ii) $\chi = (\chi_1, \ldots, \chi_r) \in \mathbf{C}^r$ with $|\chi_i| \le 1$ for all i; and (iii) $x = (x_1, \ldots, x_r) \in \mathbf{R}^r$ such that $0 \le x_i \le 1$ for all i but not all x_i are 0. We define linear forms L_i on $\mathbf{C}^m$ and L_j^* on $\mathbf{C}^r$ by

$$L_i(z) = \sum_{k=1}^{m} a_{ik} z_k, \quad L_j^*(w) = \sum_{k=1}^{r} a_{kj} w_k \quad (z = (z_1, \ldots, z_m),\ w = (w_1, \ldots, w_r)).$$

We suppose throughout this section that

$$\mathrm{Re}(a_{ij}) > 0 \text{ for all } i \text{ and } j. \tag{1}$$

This assumption guarantees that $L_i(z)$ and $L_j^*(w)$ for $z \in \overline{\mathbf{R}}_+^m - \{0\}$ and $w \in \overline{\mathbf{R}}_+^r - \{0\}$ stay in H', because $H' \supset \overline{\mathbf{R}}_+ H'$ and $H' \supset H' + H'$. Then we formally define the Shintani L-function by

$$\zeta(s,A,x,\chi) = \sum_{n \in \mathbf{N}^r} \chi^n L^*(n+x)^{-s} \quad \text{for } s = (s_1, \ldots, s_m) \in \mathbf{C}^m, \tag{2}$$

where we write $L^*(n+x) = (L_1^*(n+x), \ldots, L_m^*(n+x)) \in \mathbf{C}^m$ and for $w = (w_1, \ldots, w_m) \in H'^m$, we write $w^s = \prod_{j=1}^m w_j^{s_j}$. When A is the scalar 1 and $\chi = 1$, then $\zeta(s,A,x,\chi) = \zeta(s,x) = \sum_{n=0}^{\infty} (n+x)^{-s}$ and thus the Shintani L-function is a direct generalization of the Hurwitz L-function. We leave the proof of the following lemma to the reader as an exercise:

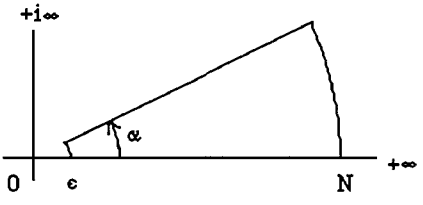
Lemma 1. $\zeta(s,A,x,\chi)$ *converges absolutely and uniformly on any compact subset in the region* $\mathrm{Re}(s_i) > \frac{r}{m}$ *for all* i.

Exercise 1. (a) Prove the above lemma. (Reduce the problem to the case where all entries of A, χ, and x are 1 and use the fact that $\#\{k \in \mathbf{Z}_+^r \mid k_1+\cdots+k_r = n\} \le Cn^{r-1}$ for a constant $C > 0$. Actually, $\zeta(s,A,x,\chi)$ converges if $\mathrm{Re}(s_1+\cdots+s_m) > r$ and $\mathrm{Re}(s_j) > 0$ for all j.)
(b) When all the entries of χ are equal to 1 and A is a real matrix, show that $\zeta(s,A,x,\chi)$ diverges at $s = \frac{r}{m}(1,\ldots,1)$ (actually it diverges if $s_1+\cdots+s_m = r$).

Now we give another exercise which generalizes the fact that

$$\Gamma(s) = \int_0^\infty e^{-y}y^{s-1}dy \quad \text{if } \mathrm{Re}(s) > 0:$$

Exercise 2. If $a \in H'$ and $s \in H'$, then $\int_0^\infty e^{-ay}y^{s-1}dy = a^{-s}\Gamma(s)$, where as already explained, $a^{-s} = |a|^{-s}e^{-i\alpha s}$ writing $a = |a|e^{i\alpha}$ with $-\frac{\pi}{2}<\alpha<\frac{\pi}{2}$. First interpret the integral $\int_0^\infty e^{-ay}y^{s-1}dy$ as a^{-s} times the integral of $e^{-y}y^{s-1}$ on the line in H' from 0 to $+\infty$ with argument α. Then relate this integral with the Γ integral $\int_0^\infty e^{-y}y^{s-1}dy$ by using the following integral path:



and show that the integral on the inner circle of radius ε (resp. the outer circle of radius N) goes to 0 as $\varepsilon \to 0$ (resp. as $N \to +\infty$).

Now we want an integral expression of $\zeta(s,A,x,\chi)$ converging in the domain with sufficiently large real part. We consider the following function $G(y) = G(y,A,x,\chi)$ with variable y in $\mathbf{R}_+^m$ given by

$$G(y) = \sum_{n\in \mathbf{N}^r} \chi^n \exp(-\sum_{j=1}^m L^*_j(n+x)y_j). \tag{3}$$

The convergence of this series can be shown as follows. First of all, we see that

$$\begin{aligned}\sum_{j=1}^m L^*_j(n+x)y_j &= \sum_{j=1}^m\sum_{i=1}^r a_{ij}(n_i+x_i)y_j = \sum_{i=1}^r (n_i+x_i)\sum_{j=1}^m a_{ij}y_j \\ &= \sum_{i=1}^r (n_i+x_i)L_i(y) = \sum_{i=1}^r x_iL_i(y) + \sum_{i=1}^r n_iL_i(y).\end{aligned}$$

This shows that

$$\begin{aligned}G(y) &= \exp(-\sum_{i=1}^r x_iL_i(y))\sum_{n\in \mathbf{N}^r}\chi^n\exp(-\sum_{i=1}^r n_iL_i(y)) \\ &= \exp(-\sum_{i=1}^r x_iL_i(y))\prod_{i=1}^r\{\sum_{n_i=0}^\infty \chi_i^{n_i}\exp(-n_iL_i(y))\}.\end{aligned}$$

Since $L_i(y) \in H'$ as already remarked, $|\chi_i \exp(-L_i(y))| < 1$ and the geometric series in the inside summation converges absolutely. We then have

$$(4) \qquad G(y,A,x,\chi) = \prod_{i=1}^{r} \frac{\exp(-x_i L_i(y))}{1-\chi_i \exp(-L_i(y))}.$$

Now writing $y^s = \prod_{i=1}^m y_i^{s_i}$ for $s \in \mathbf{C}^m$, $\mathbf{1} = (1,1,\dots,1) \in \mathbf{C}^m$, $dy = dy_1 dy_2 \cdots dy_m$ and $\Gamma_m(s) = \prod_{i=1}^m \Gamma(s_i)$, we have, by Exercise 2,

$$\begin{aligned}(5)\ \iint\cdots\int_0^\infty G(y,A,x,\chi)y^{s-\mathbf{1}}dy &= \iint\cdots\int_0^\infty \sum_{n\in N^r}\chi^n \exp(-\textstyle\sum_{j=1}^m L^*_j(n+x)y_j)y^{s-\mathbf{1}}dy \\ &\overset{?}{=} \sum_{n\in N^r}\iint\cdots\int_0^\infty \chi^n \exp(-\textstyle\sum_{j=1}^m L^*_j(n+x)y_j)y^{s-\mathbf{1}}dy \\ &= \sum_{n\in N^r}\chi^n \prod_{j=1}^m \int_0^\infty \exp(-L^*_j(n+x)y_j)y_j^{s_j-1}dy_j \\ &= \Gamma_m(s)\sum_{n\in N^r}\chi^n L^*(n+x)^{-s} = \Gamma_m(s)\zeta(s,A,x,\chi).\end{aligned}$$

As in the case of the Riemann zeta function (Proposition 2.1), we can justify the interchange of the integral $\iint\cdots\int_0^\infty$ and the summation $\sum_{n\in N^r}$ marked by "?" if $\mathrm{Re}(s_i) > \frac{r}{m}$ for all i, thus (5) is valid (if $\mathrm{Re}(s_i) > \frac{r}{m}$ for all i). In fact, if A is a real matrix and $\chi = \mathbf{1}$, the convergence of $\sum_{n\in N^r}\exp(-\sum_{j=1}^m L^*_j(n+x)y_j)$ to $G(y,A,x,\mathbf{1})$ is monotone on $\mathbf{R}_+^r$ and hence we can interchange the integral and the summation at the equality marked by "?". We also know from this that $G(y,A,x,\mathbf{1})y^{\mathrm{Re}(s)-\mathbf{1}}$ is an integrable function if $\mathrm{Re}(s_i) > \frac{r}{m}$ for all i. In general, we know that

$$|G(y,A,x,\chi)y^{s-\mathbf{1}}| \le G(y,\mathrm{Re}(A),x,\mathbf{1})y^{\mathrm{Re}(s)-\mathbf{1}}$$

and using the dominated convergence theorem of Lebesgue,

If a sequence of continuous (actually integrable) functions $f_n(x)$ *(on an interval* $[a,b]$ *in* $\mathbf{R}$; a *and* b *can be* $\pm\infty$*) is dominated by a continuous and integrable function and* $f(x) = \lim_{n\to\infty} f_n(x)$ *at every point* x, *then*

$$\int_a^b \lim_{n\to\infty} f_n(x)dx = \lim_{n\to\infty}\int_a^b f_n(x)dx,$$

we can justify the interchange.

Things have worked in exactly the same way so far, but we encounter a serious difficulty in converting the above integral into the contour integral convergent for all $s \in \mathbf{C}^m$. Probably, many people before Shintani considered the zeta function of type (2) and tried to get its analytic continuation, but because of this difficulty, we had to wait until 1976 [St1] to get the analytic continuation of $\zeta(s,A,x,\chi)$.

First, we explain why the naive conversion to the contour integral does not work. For simplicity, we only treat the case where $\chi = \mathbf{1}$ and $x = \mathbf{1}$. As already seen, $\frac{e^{-z}}{1-e^{-z}}$ has a simple pole at $z = 0$ whose residue is equal to 1; in other words, $\frac{ze^{-z}}{1-e^{-z}}$ is holomorphic at $z = 0$. Thus each factor of

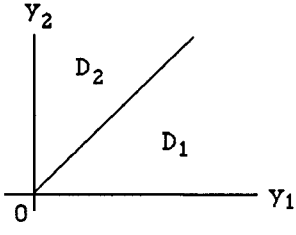
$$G(y) = \prod_{i=1}^{r} \frac{\exp(-L_i(y))}{1-\exp(-L_i(y))}$$

has a simple pole at the hyperplane $S_i = \{y \in \mathbf{C}^m \mid L_i(y) = 0\}$ if $m \geq 2$ (if $m = 1$, then $S_i = \{0\}$). On the other hand, if we denote $D(\varepsilon) = \{y \in \mathbf{C} \mid |y| \leq \varepsilon\}$, then $D(\varepsilon)^m$ gives a neighborhood of 0 in $\mathbf{C}^m$ and thus $D(\varepsilon)^m \cap S_i \neq \emptyset$ if $m \geq 2$. This implies that we cannot avert the singularity by taking the path $\partial D(\varepsilon)^m$.

Shintani's idea is to convert the integral (5) into a contour integral by means of an ingenious variable change. We divide $\mathbf{R}_+^m$ into the following m regions:

$$\mathbf{R}_+^m = \bigcup_{k=1}^m D_k, \quad D_k = \{y = (y_1, \ldots, y_m) \mid y_k \geq y_i \text{ for all } i \neq k\}.$$

This decomposition can be illustrated in the case of $m = 2$ as follows:



On each D_k, we shall make the following variable change:

(6) $\quad y = (y_1, y_2, \ldots, y_m) = u(t_1, t_2, \ldots, t_m)$
$\quad (0 < t_i \leq 1 \ (i \neq k) \text{ and } t_k = 1)$.

Thus $y_1 = ut_1$, $y_2 = ut_2$, ..., $y_k = u$, ..., $y_m = ut_m$. Since the computation is all the same for any of the D_k, we assume $k = 1$ and compute the jacobian matrix:

$$\begin{pmatrix} \frac{\partial y_1}{\partial u} & \frac{\partial y_2}{\partial u} & \cdots & \frac{\partial y_m}{\partial u} \\ \frac{\partial y_1}{\partial t_2} & \frac{\partial y_2}{\partial t_2} & \cdots & \frac{\partial y_m}{\partial t_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial y_1}{\partial t_m} & \frac{\partial y_2}{\partial t_m} & \cdots & \frac{\partial y_m}{\partial t_m} \end{pmatrix} = \begin{pmatrix} 1 & t_2 & t_3 & \cdots & t_m \\ 0 & u & 0 & \cdots & 0 \\ 0 & 0 & u & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & u \end{pmatrix}$$

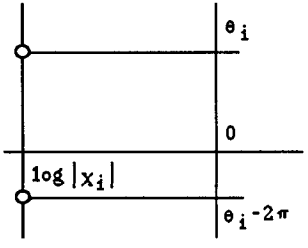
Thus we know that $dy = u^{m-1}dudt$ and $y^{s-1} = u^{Tr(s)-m}t^{s-1}$ for $Tr(s) = s_1+s_2+\cdots+s_m$. On the other hand, we see that

(7) $\quad L_i(y) = \sum_{j=1}^m a_{ij}y_j = uL_i(t)$ and $L_i(t) = \sum_{j=1}^{k-1} a_{ij}t_j + \sum_{j=k+1}^m a_{ij}t_j + a_{ik}$.

Thus we have

$$\iint\cdots\int_0^\infty G(y,A,x,\chi)y^{s-1}dy = \sum_{k=1}^{m} \int_{D_k} G(y,A,x,\chi)y^{s-1}dy$$
$$= \sum_{k=1}^{m} \int_0^\infty\int_0^1\cdots\int_0^1 G_k(u,t,A,x,\chi)u^{Tr(s)-1}t^{s-1}dtdu,$$

where $G_k(u,t,A,x,\chi) = \prod_{i=1}^{r}\frac{\exp(-x_iuL_i(t))}{1-\chi_i\exp(-uL_i(t))}$. This integral expression can be converted into a contour integral convergent everywhere. First let us examine the singularities, i.e., the zeros of $1-\chi_i\exp(-uL_i(t))$. Write $\chi_i = |\chi_i|e^{i\theta_i}$ with $0 \le \theta_i < 2\pi$. Then writing $z = uL_i(t)$, we see that the zeros of $1-\chi_i\exp(-z)$ are located as follows (note that $log|\chi_i| \le 0$ because $|\chi_i| \le 1$):



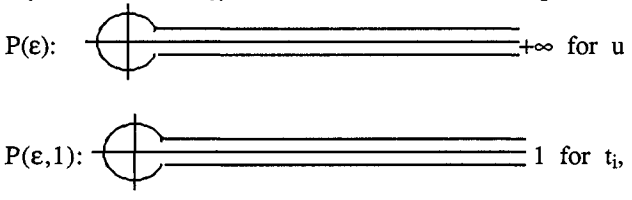
The small circles in the figure at left indicate zeros. Therefore we can take $\delta > 0$ so that

$$\prod_{i=1}^{r}\{1-\chi_i\exp(-uL_i(t))\} \neq 0$$

if $0 < |uL_i(t)| < \delta$ for all i. We fix such a δ. Then we can find $0 < \delta'$ so that if $|u| < \delta'$ and $|t_i| \le 1$ for all i, then $|uL_i(t)| < \delta$. We also fix such a δ'. On the other hand, we know from (7) that $\lim_{t\to 0}\mathrm{Re}(L_i(t)) = \mathrm{Re}(a_{ik}) > 0$. Put $a = \mathrm{Min}\{\mathrm{Re}(a_{ik}) \mid i = 1,\ldots, r\}$. Thus we can find $1 \ge \delta'' > 0$ so that if $|t_i| < \delta''$ for all $i \neq k$, then $\mathrm{Re}(L_i(t)) > \frac{a}{2}$. Thus the only possible zeros of $\prod_{i=1}^{r}\{1-\chi_i\exp(-uL_i(t))\}$ in the neighborhood

$$U = \{(u,t_1, \ldots, t_{k-1},t_{k+1}, \ldots, t_m) \mid |u| < \delta', |t_i| < \delta'' \text{ for } i \neq k\}$$

are at $U\cap\{u = 0\}$. On the other hand, if $\mathbf{R} \ni u \ge \delta'$ and $|t_i| < \delta''$, $\mathrm{Re}(uL_i(t)) > a\delta'/2$ (i.e. $|\chi_i\exp(-uL_i(t))| < 1$), and hence no poles are expected in this remaining case. Thus on the following integral path, we do not have any singularity of $G_k(u,t,A,x,\chi)$ for $0 < \varepsilon < \min(\delta',\delta'')$ independent of t and u:



where the circle is of radius ε centered at 0. Note that if t is on the real line, $\mathrm{Re}(L_i(t)) \ge a$ always because $a_{ij} \in H'$ for all i and j. Thus $|G_k(u,t,A,x,\chi)|$ decreases exponentially as u goes to infinity when $t \in P(\varepsilon,1)^{m-1}$. Thus the integral of u on the real line from ε to $+\infty$ always converges. On the other hand $P(\varepsilon,1)^{m-1}$ is compact and therefore the integral on this path also converges always. Thus

$$\int_{P(\varepsilon)}\int_{P(\varepsilon,1)^{m-1}} G_k(u,t,A,x,\chi)u^{Tr(s)-1}t^{s-1}dtdu$$

gives an analytic function of m variables on the whole complex space $\mathbf{C}^m$. Thus we have the following result:

Theorem 1. $\zeta(s,A,x,\chi)$ *can be continued to the whole space* $\mathbf{C}^m$ *as a meromorphic function and has the following integral expression valid for all* $s \in \mathbf{C}^m$:

$$\Gamma_m(s)\zeta(s,A,x,\chi) = \frac{\sum_{k=1}^m (e^{2\pi i s_k}-1)\int_{P(\varepsilon)}\int_{P(\varepsilon,1)^{m-1}} G_k(u,t,A,x,\chi)u^{Tr(s)-1}t^{s-1}dtdu}{(e^{2\pi i Tr(s)}-1)\prod_{j=1}^m (e^{2\pi i s_j}-1)}$$

Here we insert a general formula. We assume that $\chi_i \neq 1$ for all i. Then $G(y,A,x,\chi)$ has no singularity on a neighborhood $\{y \mid |y_i| < \varepsilon \text{ for all } i\}$ for sufficiently small ε and therefore has a power series expansion in y around 0. We look at the expansion

$$\text{(8a)}\quad G(y,A,x,\chi) = \prod_{i=1}^r \frac{\exp(-x_i L_i(y))}{1-\chi_i \exp(-L_i(y))} = \sum_{n\in N^m} \frac{B_{n+\mathbf{1}}(x)}{(n+\mathbf{1})!} y^n \quad (x = (x_1,\ldots,x_r))$$

for $G(y,A,x,\chi)$ in (4), where $(n+\mathbf{1})! = \prod_{i=1}^m (n_i+1)!$ and $y^n = \prod_{i=1}^m y_i^{n_i}$. We also write the coefficient of $u^{m(l-1)}\prod_{i\neq k} t_i^{l-1}$ in $G_k(u,t,A,x,\chi)$ as $\frac{B_l^{(k)}(x)}{(l!)^m}$ for $l \in \mathbf{N}$. If $\chi_i \neq 1$ for all i, then $G(y,A,x,\chi)$ is holomorphic at $y = 0$ and $G_k(u,t,A,x,\chi)$ is holomorphic at $u = 0$ and $t = 0$. Thus we can compute the expansion of $G_k(u,t,A,x,\chi)$ using that of $G(y,A,x,\chi)$, simply replacing y_i by ut_i $(i \neq k)$ and y_k by u. Then, we have

$$\text{(8b)}\qquad B_{n\mathbf{1}}(x) = m^{-1}\sum_k B_n^{(k)}(x) \quad \text{for } \mathbf{1} = (1,\ldots,1).$$

Thus we conclude, if $\chi_i \neq 1$ for all i, that

$$\text{(8c)}\qquad \zeta((1-n)\mathbf{1},A,x,\chi) = (-1)^{m(n-1)}\frac{B_{n\mathbf{1}}(x)}{n^m} \quad \text{for all } 0 < n \in \mathbf{Z}.$$

This formula will be used later to get a p-adic interpolation of this type of L-function and can be proven without using the variable change $y \mapsto (u,t)$.

Exercise 3. When A is a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\chi = (1,1)$, get the explicit formula of $\zeta((1-n,1-n),A,x,\chi)$ for positive integers n in terms of Bernoulli polynomials given in (3.3b).

§2.5. L-functions of real quadratic fields and Eisenstein series

In this section, we interpret the Shintani zeta function in terms of Dedekind zeta functions and Hecke L-functions of quadratic fields and later introduce Eisenstein series in this context. Although we are ready to do the same thing for general fields, the detailed exposition in the case of quadratic fields helps demonstrate what is going on. First we treat the quadratic field $F = \mathbf{Q}(\sqrt{d})$ for a square-free integer d. We take the standard basis $\{\omega_1, \omega_2\}$ of the integer ring $\mathcal{O}$ of F ([N-Z, 9.5]); i.e.,

$$\omega_1 = 1 \quad \text{and} \quad \omega_2 = \begin{cases} \sqrt{d} & \text{if } d \equiv 2 \text{ or } 3 \bmod 4, \\ (1+\sqrt{d})/2 & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Let I be the ideal group of F and $I(m)$ the subgroup of I consisting of ideals prime to a given integral ideal m. Similarly, let $\mathcal{P}_+(m)$ be the subgroup of I made of principal ideals $\alpha\mathcal{O}$ with $\alpha \equiv 1 \bmod m$ and $\alpha^\sigma > 0$ for all real embeddings σ of F into $\mathbf{R}$. Then as seen in Theorem 1.2.1 (see also Exercise 1.2.1), the (strict) ray class group $\mathrm{Cl}(m) = I(m)/\mathcal{P}_+(m)$ is finite. We consider a character $\chi : \mathrm{Cl}(m) \to \mathbf{C}^\times$. Such a character is called a (finite order) Hecke character modulo m. Then the Hecke L-function of χ is defined by

$$L(s,\chi) = \sum_{n \in I(m),\ \mathcal{O} \supset n} \chi(n) N(n)^{-s} \quad (s \in \mathbf{C}).$$

Exercise 1. (a) Show that $L(s,\chi)$ is absolutely convergent if $\mathrm{Re}(s) > 1$.
(b) Show that $L(s,\chi)$ has the following Euler product expansion:

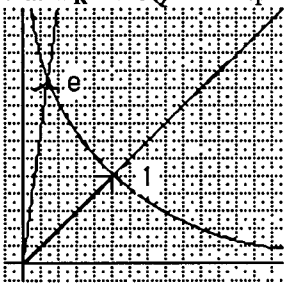
$$L(s,\chi) = \prod_p (1-\chi(p)N(p)^{-s})^{-1},$$

where p runs through all prime ideals prime to m.

Now suppose $d > 0$. Then $F = \mathbf{Q}(\sqrt{d})$ is a real quadratic field and there are two real places. Let σ be the non-trivial field automorphism of F, so that $(\sqrt{d})^\sigma = -\sqrt{d}$. Now $\mathcal{O}^\times = \{\pm 1\} \times \{\varepsilon_0^n \mid n \in \mathbf{Z}\}$ for a fundamental unit ε_0 by Dirichlet's theorem (Theorem1.2.3). Let $E = \{\delta \in \mathcal{O}^\times \mid \delta > 0,\ \delta^\sigma > 0\}$, which is a subgroup of finite index of $\mathcal{O}^\times$ (in fact $E \supset (\mathcal{O}^\times)^2$ and hence $(\mathcal{O}^\times : E) \mid 4$). Then we can find a generator ε of E and $E = \{\varepsilon^n \mid n \in \mathbf{Z}\}$. We may assume that $\varepsilon < 1 < \varepsilon^\sigma$. The following fact is very important to express the Hecke L-function as a sum of Shintani L-functions.

Lemma 1. *Let* $F_+ = \{\alpha \in F \mid \alpha > 0 \text{ and } \alpha^\sigma > 0\}$. *Then each* $\alpha \in F_+$ *can be uniquely written as* $\alpha = \varepsilon^n(r+s\varepsilon)$ *for* $0 < r \in \mathbf{Q}$, $0 \le s \in \mathbf{Q}$ *and* $n \in \mathbf{Z}$.

Proof. We embed F into $\mathbf{R}^2$ by $x \mapsto (x,x^\sigma) \in \mathbf{R}^2$. It is clear from the figure that $F_{\mathbf{R}} = F \otimes_{\mathbf{Q}} \mathbf{R} = \mathbf{R}$-span of $\{1,e\} = \mathbf{R}^2$, where $e = (\varepsilon,\varepsilon^\sigma)$ and $1 = (1,1)$. The



curve in the figure is defined by $xy = 1$. Multiplication by ε (as a map of $F_{\mathbf{R}}$ into itself) takes the line passing through 0 and 1 to that passing through 0 and e. We denote by V the cone $\{s\cdot e+r\cdot 1 \mid r > 0,\ s \geq 0\}$. Then we see easily from the figure that $(\mathbf{R}_+)^2 = \bigcup_{n\in \mathbf{Z}} \varepsilon^n V$ which is a disjoint union. Thus any $\alpha \in F_+$ falls in a unique $\varepsilon^n V$, namely $\alpha = \varepsilon^n(s\cdot e+r\cdot 1)$ for unique $r > 0$ and $s \geq 0$. Since 1 and ε form a basis of F over $\mathbf{Q}$, we can find r' and s' in $\mathbf{Q}$ such that $\varepsilon^{-n}\alpha = s'\varepsilon+r'$ in F. This in particular means that $\varepsilon^{-n}\alpha = s'\cdot e+r'\cdot 1 = s\cdot e+r\cdot 1$. Since 1 and e form a basis of $\mathbf{R}^2$, we now know that $s = s' \in \mathbf{Q}$ and $r = r' \in \mathbf{Q}$. This finishes the proof of the lemma.

Now let $\chi : \mathrm{Cl}(m) \to \mathbf{C}^\times$ be a Hecke character and consider the Hecke L-function

$$L(s,\chi) = \sum_{n\in I(m),\ \mathcal{O}\supset n} \chi(n)N(n)^{-s}.$$

Let $h = \#\mathrm{Cl}(\mathcal{O})$ and let us fix a representative set $\{a_1, \ldots, a_h\}$ for $\mathrm{Cl}(\mathcal{O})$ consisting of integral ideals (i.e. ideals of $\mathcal{O}$). Then for any fractional ideal b, we can find a unique a_i such that $b = \alpha a_i$ for $\alpha \in F_+$. Applying this to bm^{-1}, we can find $\beta \in F_+$ such that $bm^{-1} = \beta a_j$, namely, $b = \beta a_j m$. Thus $\{a_1 m,\ldots,a_h m\}$ forms another representative set.

Exercise 2. Show that we can take the representative set $\{a_1,\ldots,a_h\}$ so that each a_i is prime to the given ideal m.

Hereafter we extend χ to the whole ideal group I so that $\chi(b) = 0$ for $b \in I\text{-}I(m)$. Then we can write

$$\begin{aligned} L(s,\chi) &= \sum_{i=1}^{h} \sum_{\alpha\in (a_i^{-1}m^{-1}\cap F_+)/E} \chi(\alpha a_i m)N(\alpha a_i m)^{-s} \\ &= \sum_{i=1}^{h} N(a_i m)^{-s} \sum_{\alpha\in (a_i^{-1}m^{-1}\cap F_+)/E} \chi(\alpha a_i m)N(\alpha)^{-s}. \end{aligned}$$

Therefore to express the Hecke L-function as a finite sum of Shintani L-functions, it is sufficient to do so for the partial L-function

$$L_i(s,\chi) = \sum_{\alpha\in (a_i^{-1}m^{-1}\cap F_+)/E} \chi(\alpha a_i m)N(\alpha)^{-s}.$$

Let

$$R_i = \{\alpha \in a_i^{-1}m^{-1} \mid \alpha = x_1 + x_2\varepsilon,\ 0 < x_1 \leq 1 \text{ and } 0 \leq x_2 < 1\}.$$

This is a finite set. In fact, $W = \{[0,1]+[0,1]\varepsilon\}$ is a compact subset of $\mathbf{R}^2$. On the other hand, $a_i^{-1}m^{-1} = a\mathbf{Z}+b\mathbf{Z}$ for a $\mathbf{Z}$-basis $\{a,b\}$ since $a_i^{-1}m^{-1}$ is a fractional ideal. Since $\{a,b\}$ forms a basis of $\mathbf{R}^2$ via the embedding $F \to \mathbf{R}^2$ which takes $\alpha \mapsto (\alpha,\alpha^\sigma)$, $a_i^{-1}m^{-1}$ is a discrete submodule of $\mathbf{R}^2$. Thus the subset $W\cap a_i^{-1}m^{-1}$ is discrete and compact and hence is finite. Then R_i is finite since $W \supset R_i$. The shadowed area is W and the dots indicate points in R_i. Now for any $\alpha \in a_i^{-1}m^{-1}\cap F_+$, by Lemma 1, we can uniquely write $\alpha = \varepsilon^n(r+s\varepsilon)$ with $0 < r \in \mathbf{Q}$ and $0 \le s \in \mathbf{Q}$. Let $[s]$ denote the largest integer not exceeding s and $\langle s\rangle = s-[s]$. Thus $0 \le \langle s\rangle < 1$. Similarly we define

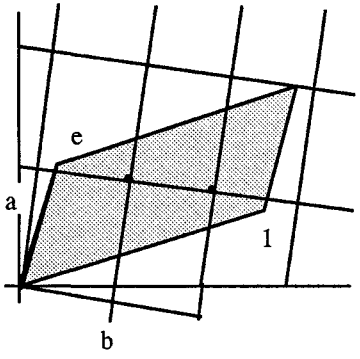


Diagram of W and R_i:

$$(r) = \begin{cases} \langle r\rangle & \text{if } 0 < \langle r\rangle < 1, \\ 1 & \text{if } \langle r\rangle = 0, \end{cases} \quad \text{and} \quad \{r\} = r-(r) \in \mathbf{Z}.$$

Then $r+s\varepsilon = (r)+\langle s\rangle\varepsilon + \{r\}+[s]\varepsilon$ and $(r)+\langle s\rangle\varepsilon \in R_i$. Since $\mathcal{O} \supset a_i m$, we have $a_i^{-1}m^{-1} \supset \mathcal{O}$. This shows especially that $\{r\}+[s]\varepsilon \in a_i^{-1}m^{-1}$ and hence $(r)+\langle s\rangle\varepsilon \in (0,1]+[0,1)\varepsilon\cap a_i^{-1}m^{-1} = R_i$. Thus, we see that

$$a_i^{-1}m^{-1}\cap F_+ = \coprod_{k\in\mathbf{Z}}\varepsilon^k\coprod_{x_1+x_2\varepsilon\in R_i}\{x_1+x_2\varepsilon+m+n\varepsilon \mid (m,n) \in \mathbf{N}^2\}.$$

This shows that

$$\begin{aligned} L_i(s,\chi) &= \sum_{\alpha\in(a_i^{-1}m^{-1}\cap F_+)/E}\chi(\alpha a_i m)N(\alpha)^{-s} \\ &= \sum_{x_1+x_2\varepsilon\in R_i}\sum_{(m,n)\in\mathbf{N}^2}\chi((x_1+x_2\varepsilon+m+n\varepsilon)a_i m)N(x_1+x_2\varepsilon+m+n\varepsilon)^{-s}, \end{aligned}$$

where $N(x_1+x_2\varepsilon+m+n\varepsilon) = (x_1+x_2\varepsilon+m+n\varepsilon)(x_1+x_2\varepsilon^\sigma+m+n\varepsilon^\sigma)$. Now we shall show that

$$\chi((x_1+x_2\varepsilon+m+n\varepsilon)a_i m) = \chi((x_1+x_2\varepsilon)a_i m).$$

Exercise 3. Show that there exist $\gamma \in \mathcal{O}$ and an integral ideal $\mathfrak{b}$ prime to m such that $\gamma\mathcal{O} = m\mathfrak{b}$.

We can write $(x_1+x_2\varepsilon+m+n\varepsilon)a_i m = \gamma(x_1+x_2\varepsilon+m+n\varepsilon)\gamma^{-1}a_i m$. Since $\gamma\mathcal{O} = m\mathfrak{b}$, $\gamma^{-1}a_i m = a_i\mathfrak{b}^{-1}$, which is prime to m, and hence $\chi(\gamma^{-1}a_i m) \neq 0$. On the other hand, $\gamma(x_1+x_2\varepsilon+m+n\varepsilon) = \gamma(x_1+x_2\varepsilon)+\gamma(m+n\varepsilon) \equiv \gamma(x_1+x_2\varepsilon) \bmod m$ because

$\gamma(m+n\varepsilon) \in \gamma O = m\mathfrak{b}$. Thus $\chi(\gamma(x_1+x_2\varepsilon)) = \chi(\gamma(x_1+x_2\varepsilon+m+n\varepsilon))$. (Actually we should remark the fact that $\gamma(x_1+x_2\varepsilon+m+n\varepsilon)/\gamma(x_1+x_2\varepsilon) \in F_+$ to assure this equality). This shows that

$$\chi((x_1+x_2\varepsilon+m+n\varepsilon)a_i m) = \chi((x_1+x_2\varepsilon)a_i m).$$

Thus finally we know that

$$\begin{aligned} L_i(s,\chi) &= \sum_{\alpha\in(a_i^{-1}m^{-1}\cap F_+)/E}\chi(\alpha a_i m)N(\alpha)^{-s} \\ &= \sum_{x_1+x_2\varepsilon\in R_i}\chi((x_1+x_2\varepsilon)a_i m)\sum_{(m,n)\in N^2}N(x_1+x_2\varepsilon+m+n\varepsilon)^{-s} \\ &= \sum_{x_1+x_2\varepsilon\in R_i}\chi((x_1+x_2\varepsilon)a_i m)\zeta((s,s),\begin{pmatrix}1 & 1\\ \varepsilon & \varepsilon^\sigma\end{pmatrix},(x_1,x_2),\mathbf{1}). \end{aligned}$$

This combined with the analytic continuation of the Shintani zeta function yields

Theorem 1. *Let* F *be a real quadratic field and* $\chi : \mathrm{Cl}(m) \to \mathbf{C}^\times$ *be a Hecke character. Then the Hecke L-function* $L(s,\chi)$ *can be continued to a meromorphic function on the whole s-plane. Moreover, it has the following expression in terms of Shintani zeta functions:*

$$L(s,\chi) = \sum_{i=1}^{h} N(a_i m)^{-s}\sum_{x_1+x_2\varepsilon\in R_i}\chi((x_1+x_2\varepsilon)a_i m)\zeta((s,s),\begin{pmatrix}1 & 1\\ \varepsilon & \varepsilon^\sigma\end{pmatrix},(x_1,x_2),\mathbf{1}),$$

where $\mathbf{1} = (1,1)$ *and* ε *is a totally positive fundamental unit of* F.

The analytic continuation of $L(s,\chi)$ was first shown by Hecke in 1917. Actually, one can show, by Hecke's method, that $L(s,\chi)$ is entire if χ is non-trivial and only has a simple pole at $s = 1$ even when χ is trivial. Here the word "entire" means that the function is analytic everywhere on the s-plane. We will come back to this question later in Chapter 8.

Corollary 1(Siegel-Klingen). *For a positive integer* n, $L(1-n,\chi) \in \mathbf{Q}(\chi)$.

Proof. We here give a proof due to Shintani. We will come back later to this problem and give a proof due to Siegel and another proof due to Shimura (see Corollary 5.2.2 and Theorem 5.2.2). What we need to prove is that for a positive integer n,

$$\zeta((1-n,1-n),\begin{pmatrix}1 & 1\\ \varepsilon & \varepsilon^\sigma\end{pmatrix},(x_1,x_2),\mathbf{1}) \in \mathbf{Q}.$$

By the study of the Shintani L-function, we know that

$$\begin{aligned} &\left\{(e^{4\pi is}-1)(e^{2\pi is}-1)\Gamma(s)^2\big|_{s=1-n}\right\}\zeta((1-n,1-n),\begin{pmatrix}1 & 1\\ \varepsilon & \varepsilon^\sigma\end{pmatrix},(x_1,x_2),\mathbf{1}) \\ &\qquad = \int_{\partial D(\varepsilon)}\int_{\partial D(\varepsilon)}\{G(u,t)+G_\sigma(u,t)\}u^{1-2n}t^{-n}du\,dt, \end{aligned}$$

where
$$G(u,t) = \frac{\exp(-x_1u(1+t))}{1-\exp(-u(1+t))} \times \frac{\exp(-x_2u(\varepsilon+\varepsilon^\sigma t))}{1-\exp(-u(\varepsilon+\varepsilon^\sigma t))} \quad \text{and}$$
$$G_\sigma(u,t) = \frac{\exp(-x_1u(t+1))}{1-\exp(-u(t+1))} \times \frac{\exp(-x_2u(\varepsilon t+\varepsilon^\sigma))}{1-\exp(-u(\varepsilon t+\varepsilon^\sigma))}.$$

Writing $(n!)^{-2}B'_n(x_1,x_2)$ for the coefficient of $u^{2(n-1)}t^{n-1}$ in the power series expansion of $G(u,t)$, we see that $B'_n(x_1,x_2)$ is a polynomial with coefficients in F. Moreover if we denote by $B'^{\sigma}_n(x_1,x_2)$ the polynomial obtained by applying σ to all coefficients of $B'_n(x_1,x_2)$, then $(n!)^{-2}B'^{\sigma}_n(x_1,x_2)$ gives the coefficient of $u^{2(n-1)}t^{n-1}$ in $G_\sigma(u,t)$. Thus by the Cauchy integral formula and the fact that $(e^{4\pi is}-1)(e^{2\pi is}-1)\Gamma(s)^2\big|_{s=1-n} = \frac{2(2\pi\sqrt{-1})^2}{(n-1)!^2}$, we have, noting the fact that $x_i \in \mathbf{Q}$,
$$\zeta((1-n,1-n),\begin{pmatrix}1 & 1\\ \varepsilon & \varepsilon^\sigma\end{pmatrix},(x_1,x_2),\mathbf{1}) = 2^{-1}n^{-2}\mathrm{Tr}_{F/\mathbf{Q}}(B'_n(x_1,x_2)) \in \mathbf{Q}.$$

We now want to introduce Eisenstein series which will be studied in detail in Chapters 5 and 9 and which is one of the simplest examples of modular forms. First let us give a brief definition of modular forms. We write $H = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$ for the upper half complex plane. Then the group $GL_2^+(\mathbf{R}) = \{\alpha \in M_2(\mathbf{R}) \mid \det(\alpha) > 0\}$ acts on H via $z \mapsto \alpha(z) = \frac{az+b}{cz+d}$ for $\alpha = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ ($cz+d \neq 0$ because z is not real). We see easily that $(\alpha\beta)(z) = \alpha(\beta(z))$. To see $\alpha(z)$ stays in H, we use the following identity: for $z' = \alpha(z)$,
$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}z & w\\ 1 & 1\end{pmatrix} = \begin{pmatrix}\alpha(z) & \alpha(w)\\ 1 & 1\end{pmatrix}\begin{pmatrix}cz+d & 0\\ 0 & cw+d\end{pmatrix}.$$

Then replacing w by the complex conjugate of z and taking the determinant, we see that $\det(\alpha)\mathrm{Im}(z) = \mathrm{Im}(\alpha(z))\,|cz+d|^2$ and hence if $\det(\alpha) > 0$ and $z \in H$, then $\alpha(z) \in H$. For any discrete subgroup Γ of $GL_2^+(\mathbf{R})$, a modular form on Γ of weight (s,k) ($s \in \mathbf{C}$ and $k \in \mathbf{Z}$) is a function $f: H \to \mathbf{C}$ such that
$$f(\gamma(z)) = j(\gamma,z)^k\,|j(\gamma,z)|^{2s}f(z) \quad \text{for all } \gamma \in \Gamma,$$
where $j(\gamma,z) = \det(\gamma)^{-1/2}(cz+d)$ if $\gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$. We see easily that
$$j(\gamma\delta,z) = j(\gamma,\delta(z))j(\delta,z) \quad \text{(a cocycle relation).}$$
Then we see that
$$\begin{aligned} f(\gamma\delta(z)) &= j(\gamma\delta,z)^k\,|j(\gamma\delta,z)|^{2s}f(z) = j(\gamma,\delta(z))^k\,|j(\gamma,\delta(z))|^{2s}j(\delta,z)^k\,|j(\delta,z)|^{2s}f(z)\\ &= j(\gamma,\delta(z))^k\,|j(\gamma,\delta(z))|^{2s}f(\delta(z)) = f(\gamma(\delta(z))) \end{aligned}$$

and hence the definition is at least consistent. When f is holomorphic (resp. C^∞-class), then f is called a holomorphic (resp. C^∞-class) modular form. The importance of modular forms lies in the fact that it is a non-abelian replacement of Dirichlet and Hecke characters (see Chapter 9 for more details about this fact). This point will be clarified later in Chapters 8 and 9. We will study modular forms in detail in later chapters: Chapters 5 to 10. Here we introduce an example of modular forms: the Eisenstein series. Take a positive integer N, integers $0 \le a < N$, $0 < b \le N$ (so that $(a,b) \neq 0$), and $k \ge 0$. Put as a function of $z \in H$ and $s \in \mathbf{C}$

$$E'_{k,N}(z,s;a,b) = \sum_{(m,n)\in \mathbf{Z}^2-\{0\},\ (m,n)\equiv(a,b) \bmod N} (mz+n)^{-k} \,|\, mz+n \,|^{-2s}.$$

One can easily verify that this series is absolutely and locally uniformly (with respect to s and z) convergent if $\mathrm{Re}(s) > 1-\frac{k}{2}$. We can write

$$\begin{aligned} E'_{k,N}(z,s;a,b) &= \sum_{(m,n)\in \mathbf{Z}^2-\{0\},\ (m,n)\equiv(a,b) \bmod N} (mz+n)^{-k} \,|\, mz+n \,|^{-2s} \\ &= \sum{}'_{(m,n)\in \mathbf{Z}^2} ((a+Nm)z+(b+Nn))^{-k} \,|\, (a+Nm)z+(b+Nn) \,|^{-2s} \\ &= N^{-k-2s} \sum{}'_{(m,n)\in \mathbf{Z}^2} ((\tfrac{a}{N}+m)z+(\tfrac{b}{N}+n))^{-k} \,|\, (\tfrac{a}{N}+m)z+(\tfrac{b}{N}+n) \,|^{-2s}, \end{aligned}$$

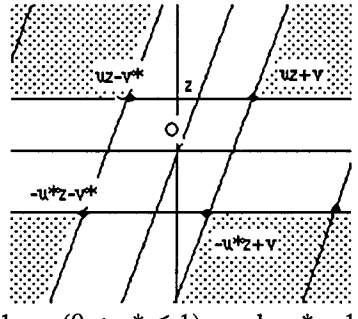
where $\sum'$ means the summation over all $(m,n) \in \mathbf{Z}^2$ for which $(\frac{a}{N}+m)z+(\frac{b}{N}+n) \neq 0$. To relate this series with Shintani L-functions, we consider, for $0 \le u < 1$ and $0 < v \le 1$,

$$\varphi_k(z,s;u,v) = \sum{}'_{(m,n)\in \mathbf{Z}^2} (uz+v+mz+n)^{-k} \,|\, uz+v+mz+n \,|^{-2s}.$$

Then we have

$$E'_{k,N}(z,s;a,b) = N^{-2s-k} \varphi_k(z,s;\tfrac{a}{N}, \tfrac{b}{N}). \tag{1}$$

We now split the summation of φ_k into four pieces:



Here we write $u^* = 1-u$ $(0 < u^* \le 1)$ and $v^* = 1-v$ $(0 \le v^* < 1)$. We consider the function summed on a cone:

$$\xi(\omega_1,\omega_2;s;u,v) = \sum_{(m,n)\in \mathbf{N}^2} (u\omega_1+v\omega_2+m\omega_1+n\omega_2)^{-k} \,|\, u\omega_1+v\omega_2+m\omega_1+n\omega_2 \,|^{-2s}$$

for $\omega_1, \omega_2 \in \mathbf{C}$ and for u, v not both 0. Then it is easy to see from the above figure that, except when $(u,v) = (0,1)$,

$$\varphi_k(z,s;u,v) = \xi(z,1;s;u,v)+\xi(-z,1;s;u^*,v)+\xi(z,-1;s;u,v^*)+\xi(-z,-1;s;u^*,v^*).$$

When $(u,v) = (0,1)$, we have

$$\varphi_k(z,s;0,1) = \xi(z,1;s;0,1) + \xi(-z,1;s;1,0) + \xi(z,-1;s;1,0) + \xi(-z,-1;s;0,1).$$

We can choose $\alpha,\beta \in \mathbf{C}^\times$ so that $\alpha,\alpha z \in H'$ and $\beta,\beta\bar{z} \in H'$ for any given $z \in \mathbf{C}-\mathbf{R}$. The choice of $\beta = \bar{\alpha}$ works well, but we keep the freedom of choosing β differently. Then we see that $u\alpha z+v\alpha+n\alpha z+m\alpha \in H'$ and $u\beta\bar{z}+v\beta+n\beta\bar{z}+m\beta \in H'$ for any $(m,n) \in \mathbf{N}^2$. Recall that $(xy)^s = x^s y^s$ if $x,y \in H'$, where we define x^s by $|x|^s e^{i\theta s}$ for $x = |x|e^{i\theta}$ with $-\frac{\pi}{2}<\theta<\frac{\pi}{2}$.
Thus we have

$$\begin{aligned}(u\alpha z+v\alpha+m\alpha z+n\alpha)^{-s}&(u\beta\bar{z}+v\beta+m\beta\bar{z}+n\beta)^{-s}\\ &= \{(u\alpha z+v\alpha+m\alpha z+n\alpha)(u\beta\bar{z}+v\beta+m\beta\bar{z}+n\beta)\}^{-s}\\ &= \{\alpha\beta\,|uz+v+mz+n|^2\}^{-s} = (\alpha\beta)^{-s}|uz+v+mz+n|^{-2s}.\end{aligned}$$

From this, we conclude that

$$\begin{aligned}&\alpha^{-k}(\alpha\beta)^{-s}\xi(z,1;s;u,v)\\ &= \sum_{(m,n)\in N^2}(u\alpha z+v\alpha+m\alpha z+n\alpha)^{-k-s}(u\beta\bar{z}+v\beta+m\beta\bar{z}+n\beta)^{-s}\\ &\qquad = \zeta((k+s,s),\begin{pmatrix}\alpha z & \beta\bar{z}\\ \alpha & \beta\end{pmatrix},(u,v),\mathbf{1}).\end{aligned}$$

In the above argument, replacing (u,v) by (u^*,v^*), $(z,1)$ by $(-z,-1)$ and (α,β) by $(-\alpha,-\beta)$, we obtain

$$(-\alpha)^{-k}(\alpha\beta)^{-s}\xi(-z,-1;s;u^*,v^*) = \zeta((k+s,s),\begin{pmatrix}\alpha z & \beta\bar{z}\\ \alpha & \beta\end{pmatrix},(u^*,v^*),\mathbf{1}).$$

Similarly choosing $\alpha',\beta' \in \mathbf{C}^\times$ so that $\alpha'(-z),\alpha' \in H'$ and $\beta'(-\bar{z}),\beta' \in H'$, we have

$$(\alpha')^{-k}(\alpha'\beta')^{-s}\xi(-z,1;s;u^*,v) = \zeta((k+s,s),\begin{pmatrix}\alpha'(-z) & \beta'(-\bar{z})\\ \alpha' & \beta'\end{pmatrix},(u^*,v),\mathbf{1}),$$

and

$$(-\alpha')^{-k}(\alpha'\beta')^{-s}\xi(z,-1;s;u,v^*) = \zeta((k+s,s),\begin{pmatrix}-\alpha' z & -\beta'\bar{z})\\ \alpha' & \beta'\end{pmatrix},(u,v^*),\mathbf{1}).$$

Thus we have a theorem of Shintani ([St6, §4]):

Theorem 2. *The Eisenstein series* $E'_{k,N}(z,s;a,b)$ *can be continued to a meromorphic function of* s *to the whole plane and is real analytic with respect to* z. *Moreover writing* $\mathbf{u} = (\frac{a}{N}, \frac{b}{N})$ *and supposing* $\mathbf{u} \neq (0,N)$ *if* $N > 1$ *and* $\mathbf{u} = (0,1)$ *if* $N = 1$, *we have the following expression in terms of the Shintani L-function:*

$$\begin{aligned} E'_{k,N}(z,s;a,b) = N^{-2s-k}\{&(\alpha\beta)^s\alpha^k\zeta((k+s,s),\begin{pmatrix}\alpha z & \beta\bar{z}\\ \alpha & \beta\end{pmatrix},\mathbf{u},\mathbf{1}) \\ &+ (\alpha'\beta')^s\alpha'^k\zeta((k+s,s),\begin{pmatrix}\alpha'(-z) & \beta'(-\bar{z})\\ \alpha' & \beta'\end{pmatrix},(u^*,v),\mathbf{1}) \\ &+ (\alpha'\beta')^s(-\alpha')^k\zeta((k+s,s),\begin{pmatrix}-\alpha' z & -\beta'\bar{z})\\ \alpha' & \beta'\end{pmatrix},\mathbf{u}^*,\mathbf{1}) \\ &+ (\alpha\beta)^s(-\alpha)^k\zeta((k+s,s),\begin{pmatrix}\alpha z & \beta\bar{z}\\ \alpha & \beta\end{pmatrix},\mathbf{u}_*,\mathbf{1})\}, \end{aligned}$$

where $\mathbf{u}^* = \begin{cases}(u,v^*) & \text{if } N > 1\\ (1,0) & \text{if } N = 1\end{cases}$ *and* $\mathbf{u}_* = \begin{cases}(u^*,v^*) & \text{if } N > 1\\ (0,1) & \text{if } N = 1\end{cases}$ *and* $\alpha,\beta,\alpha',\beta'$ *are taken so that* $\alpha z,\alpha \in H'$, $\beta\bar{z},\beta \in H'$, $\alpha'(-z)$, $\alpha' \in H'$ *and* $\beta'(-\bar{z}),\beta' \in H'$.

The analytic continuation of Eisenstein series was first proven by Hecke in the 1920's.

Exercise 4. (a) Show that the following subset of $SL_2(\mathbf{Z})$ is a subgroup of finite index: $\Gamma(N) = \{\alpha \in SL_2(\mathbf{Z}) \mid \alpha \equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \bmod NM_2(\mathbf{Z})\}$.

(b) Show that $E'_{k,N}(z,s;a,b)$ is a modular form of weight (k,s) on the subgroup $\Gamma(N)$.

Now we compute the residue of $E'_{0,N}(z,s;a,b)$ at $s = 1$, which is a key to proving the class number formula for imaginary quadratic fields. We first deal with the residue at $s = 1$ of the Shintani zeta function. For each matrix $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ with $a,b,c,d \in H'$, we have seen the following integral expression:

$$\begin{aligned} &(e^{4\pi is}-1)(e^{2\pi is}-1)\Gamma(s)^2\zeta((s,s),A,x,(1,1)) \\ &\quad = \int_{P(\varepsilon)}\int_{P(\varepsilon,1)} G_1(u,t)u^{2s-1}t^{s-1}dtdu + \int_{P(\varepsilon)}\int_{P(\varepsilon,1)} G_2(u,t)u^{2s-1}t^{s-1}dtdu, \end{aligned}$$

where

$$G_1(u,t) = \left\{\frac{\exp(-x_1u(a+bt))}{1-\exp(-u(a+bt))}\right\} \times \left\{\frac{\exp(-x_2u(c+dt))}{1-\exp(-u(c+dt))}\right\},$$

$$G_2(u,t) = \left\{\frac{\exp(-x_1u(at+b))}{1-\exp(-u(at+b))}\right\} \times \left\{\frac{\exp(-x_2u(ct+d))}{1-\exp(-u(ct+d))}\right\}.$$

Even if t moves around the interval $[0,1]$, $G_j(u,t)u$ is finite provided that $u \neq 0$ ($G_j(u,t)$ has a pole of order 2 at $u = 0$). Thus if $\mathrm{Re}(s) > 0$, we do not have to make the contour integral with respect to t; that is, we have if $\mathrm{Re}(s) > 0$

$$(e^{4\pi is}-1)\Gamma(s)^2\zeta((s,s),A,x,(1,1))$$
$$= \int_{P(\varepsilon)}\int_0^1 G_1(u,t)u^{2s-1}t^{s-1}dtdu + \int_{P(\varepsilon)}\int_0^1 G_2(u,t)u^{2s-1}t^{s-1}dtdu.$$

Note that the expansion of $G_1(u,t)$ at $u=t=0$ is, for the Bernoulli polynomial $B_j(x)$ introduced in §3,

$$\sum_{j=0}^{\infty} (-1)^j B_j(x_1)\frac{(u(a+bt))^{j-1}}{j!} \times \sum_{k=0}^{\infty} (-1)^k B_k(x_2)\frac{(u(c+dt))^{k-1}}{k!}.$$

In particular, the coefficient of u^{-2} is $(a+bt)^{-1}(c+dt)^{-1}$. Now we compute the value

$$\int_{P(\varepsilon)}\int_0^1 G_1(u,t)udtdu = \int_0^1 \int_{\partial D(\varepsilon)} G_1(u,t)ududt = (2\pi\sqrt{-1})\int_0^1 \frac{1}{(a+bt)(c+dt)}dt$$
$$= (2\pi\sqrt{-1})\times\begin{cases} \det(A)^{-1}\{-log(a+b)+log(c+d)+log(a)-log(c)\} & \text{if } \det(A)\neq 0, \\ \dfrac{1}{c(a+b)} & \text{if } \det(A)=0. \end{cases}$$

We can compute similarly the integral: $\int_{P(\varepsilon)}\int_0^1 G_2(u,t)u^{2s-1}t^{s-1}dtdu$ and have

$$\int_{P(\varepsilon)}\int_0^1 G_2(u,t)u^{2s-1}t^{s-1}dtdu$$
$$= (2\pi\sqrt{-1})\times\begin{cases} -\det(A)^{-1}\{log(b)-log(a+b)+log(c+d)-log(d)\} & \text{if } \det(A)\neq 0, \\ \dfrac{1}{d(a+b)} & \text{if } \det(A)=0. \end{cases}$$

Exercise 5. Explain how one can compute $\int_0^1 \frac{1}{(a+bt)(c+dt)}dt$.

Now we start the computation of the residue of $E'_{0,N}(z,s;a,b)$. We have

$$\mathrm{Res}_{s=1}(\alpha\beta)^s\zeta((s,s),\begin{pmatrix}\alpha z & \beta\bar{z}\\ \alpha & \beta\end{pmatrix},(x,x'),\mathbf{1})$$
$$= 2^{-1}(\bar{z}-z)^{-1}\{log(\beta\bar{z})-log(\alpha z)+log(\alpha)-log(\beta)\},$$

$$\mathrm{Res}_{s=1}(\alpha'\beta')^s\zeta((s,s),\begin{pmatrix}-\alpha' z & -\beta'\bar{z})\\ \alpha' & \beta'\end{pmatrix},(x,x'),\mathbf{1})$$
$$= -2^{-1}(z-\bar{z})^{-1}\{log(-\alpha' z)-log(-\beta'\bar{z})+log(\beta')-log(\alpha')\}.$$

If $z\in H'$, then $\bar{z}\in H'$, and α and β can be taken in H'. Hence

$$log(\alpha z) = log(\alpha)+log(z) \text{ and } log(\beta\bar{z}) = log(\beta)+log(\bar{z}).$$

On the other hand, if we write $\alpha' = |\alpha'|e^{ia}$ and $z = |z|e^{i\theta}$, then $-\frac{\pi}{2}<\theta<\frac{\pi}{2}$ and $-\frac{\pi}{2}<\theta-\pi+a<\frac{\pi}{2}$ and $-\frac{\pi}{2}<a<\frac{\pi}{2}$. This shows

$$log(-\alpha' z) = log(|\alpha' z|)+(a+\theta-\pi)i = log(\alpha')+log(z)-\pi i.$$

Similarly, if $\beta' = |\beta'|e^{ib}$, then $-\frac{\pi}{2}<\pi-\theta+b<\frac{\pi}{2}$ and $-\frac{\pi}{2}<b<\frac{\pi}{2}$. This shows that

$$log(-\beta'\bar{z}) = log(|\beta' z|)+(b+\pi-\theta)i = log(\beta')+log(\bar{z})+\pi i.$$

Thus we have

$$\mathrm{Res}_{s=1}(\alpha\beta)^s\zeta((s,s),\begin{pmatrix}\alpha z & \beta\bar{z}\\ \alpha & \beta\end{pmatrix},(x,x'),\mathbf{1}) = 2^{-1}(z-\bar{z})^{-1}\{log(z)-log(\bar{z})\},$$

$$\mathrm{Res}_{s=1}(\alpha'\beta')^s\zeta((s,s),\begin{pmatrix}-\alpha' z & -\beta'\bar{z}\\ \alpha' & \beta'\end{pmatrix},(x,x'),\mathbf{1}) = -\frac{\{log(z)-log(\bar{z})-2\pi i\}}{2(z-\bar{z})}.$$

Thus $\mathrm{Res}_{s=1}E'_{0,N}(z,s;a,b) = \dfrac{\pi}{N^2\mathrm{Im}(z)}$. One can easily verify the same formula even if $\mathrm{Re}(z) \le 0$ and we can conclude with

Corollary 2. $$\mathrm{Res}_{s=1}E'_{0,N}(z,s;a,b) = \frac{\pi}{N^2\mathrm{Im}(z)}.$$

Exercise 6. Prove the above formula when $\mathrm{Re}(z) \le 0$.

§2.6. L-functions of imaginary quadratic fields

In this section, we interpret special values of Eisenstein series as the values of L-functions of imaginary quadratic fields and later prove the class number formula. Let $F = \mathbf{Q}(\sqrt{-D})$ be the imaginary quadratic field with discriminant $-D$ and m be an integral ideal of O. We consider a quasi-character $\chi : I(m) \to \mathbf{C}^\times$ such that $\chi((\alpha)) = \alpha^k\alpha^{cm}$ for $\alpha \equiv 1 \bmod m$, where c denotes complex conjugation, $\alpha^{cm} = (\alpha^c)^m$, $(\alpha) = \alpha O$ is the principal ideal generated by α and (k,m) is a pair of integers. Such a character is called a Hecke character (of ∞-type (k,m)). When $(k,m) = (0,0)$, χ gives a character of the ideal class group $\mathrm{Cl}(m) = I(m)/\mathcal{P}(m)$. The Hecke L-function is then defined by

$$L(s,\chi) = \sum_{n\in I(m),\ O\supset n} \chi(n)N(n)^{-s} \quad (s \in \mathbf{C}).$$

Note that $\chi(\alpha) = \alpha^k\alpha^{cm} = \alpha^{k-m}N(\alpha)^m = \alpha^{c(m-k)}N(\alpha)^k$. Thus writing $N : I(O) \to \mathbf{C}^\times$ for the Hecke character given by $N(a) = N_{F/Q}(a)$ for all ideals a, $L(s,\chi) = L(s-m,\chi_1) = L(s-k,\chi_2)$ for $\chi_1 = \chi N^{-m}$ and $\chi_2 = \chi N^{-k}$. Note that χ_1 is of type $(k-m,0)$ and χ_2 is of type $(0,m-k)$. Thus without loss of generality, we may assume that χ is of type $(k,0)$ or $(0,k)$ for $k \ge 0$. Since the argument is the same in either case, hereafter we assume that χ is of type $(0,k)$ with $k \ge 0$.

Exercise 1. Assume $F = \mathbf{Q}(\sqrt{d})$ for a square-free integer $d > 0$. Let $\chi : I(m) \to \mathbf{C}^\times$ be a quasi-character such that $\chi((\alpha)) = \alpha^k\alpha^{\sigma m}$ whenever $\alpha \equiv 1 \bmod m$ for a pair of integers (k,m) and the unique non-trivial field automorphism σ of F. Show that $k = m$. (Use the existence of non-trivial units.)

By Exercise 1, we do not lose generality by assuming $k = m = 0$, i.e. χ is of finite order, when F is real quadratic.

As in the case of real quadratic fields F, we take a representative set $\{a_1, \ldots, a_h\}$ of $\mathrm{Cl}(m)$ consisting of integral ideals. Then we see that

$$\begin{aligned} L(s,\chi) &= \sum_{n\in I(m),\, \mathcal{O}\supset n} \chi(n)N(n)^{-s} \\ &= \sum_{i=1}^{h} \chi(a_i)N(a_i)^{-s}\,|\mu(m)|^{-1}\sum_{\alpha\in a_i^{-1},\alpha\equiv 1 \bmod a_i^{-1}m}\alpha^{ck}N(\alpha)^{-s}, \end{aligned}$$

where $\mu(m) = \{\zeta \in \mathcal{O}^\times \mid \zeta \equiv 1 \bmod m\}$, which is a finite group and trivial if m is sufficiently small. To express $\sum_{\alpha\in a_i^{-1},\alpha\equiv 1 \bmod a_i^{-1}m}\alpha^{ck}N(\alpha)^{-s}$ as a sum of special values of Eisenstein series, we pick a basis $(\omega_1,\omega_2) = (\omega_{1,i},\omega_{2,i})$ of a_i^{-1} and a positive integer N such that $N \in m$. We may assume that a_i is prime to N and $z_i = \omega_1/\omega_2$. By changing ω_2 to $-\omega_2$ if necessary, we may assume that $z_i = \omega_1/\omega_2 \in H$. Let

$$R_i = \{(a,b) \in \mathbf{Z}^2 \mid 0 \le a < N,\ 0 < b \le N \text{ and } a\omega_1+b\omega_2 \equiv 1 \bmod a_i^{-1}m\}.$$

Then R_i is a finite set, and we have

$$\begin{aligned} &\sum_{\alpha\in a_i^{-1},\alpha\equiv 1 \bmod a_i^{-1}m}\alpha^{ck}N(\alpha)^{-s} \\ &\quad= \sum_{(a,b)\in R_i}\sum_{\alpha\in a_i^{-1},\alpha\equiv a\omega_1+b\omega_2 \bmod a_i^{-1}N}\alpha^{ck}N(\alpha)^{-s} \\ &\quad= \sum_{(a,b)\in R_i}\ \sum_{(m,n)\in \mathbf{Z}^2} \frac{(a\omega_1+b\omega_2+Nm\omega_1+Nn\omega_2)^{-k}}{|(a\omega_1+b\omega_2+Nm\omega_1+Nn\omega_2)|^{2s-2k}} \\ &\quad= \sum_{(a,b)\in R_i}\omega_2^{-k}\,|\omega_2|^{-2s+2k}E'_{k,N}(\omega_1/\omega_2,s-k;a,b). \end{aligned}$$

Thus we have

$$\begin{aligned} L(s,\chi) &= \sum_{n\in I(m),\, \mathcal{O}\supset n} \chi(n)N(n)^{-s} \\ &= \sum_{i=1}^{h}\chi(a_i)N(a_i)^{-s}\,|\mu(m)|^{-1}\sum_{(a,b)\in R_i}\omega_{2,i}^{-k}\,|\omega_{2,i}|^{-2s+2k}E'_{k,N}(z_i,s-k;a,b). \end{aligned}$$

Theorem 1. *$L(s,\chi)$ can be continued to a meromorphic function on the whole s-plane.*

In particular, when $k = 0$, and $m = \mathcal{O}$, and χ is trivial, then

$$\zeta_F(s) = w^{-1}\sum_{i=1}^{H} N(a_i)^{-s}|\omega_{2,i}|^{-2s}E'_{0,1}(z_i,s;0,1),$$

where H is the class number of F and $w = |\mathcal{O}^\times|$. Note that

$$\left|\det\begin{pmatrix}\omega_1 & \omega_2\\ \overline{\omega}_1 & \overline{\omega}_2\end{pmatrix}\right| = \sqrt{D}\,N(a_i)^{-1}.$$

On the other hand, we see that

$$\det\begin{pmatrix}\omega_1 & \omega_2\\ \overline{\omega}_1 & \overline{\omega}_2\end{pmatrix} = \omega_1\overline{\omega}_2-\omega_2\overline{\omega}_1 = \omega_2\overline{\omega}_2(z_i-\overline{z}_i) = |\omega_2|^2 2\sqrt{-1}\,\mathrm{Im}(z_i).$$

By the residue formula of $E'_{0,1}(z_i,s;0,1)$ (Corollary5.2):

$$\mathrm{Res}_{s=1}E'_{0,1}(z,s;0,1) = \frac{\pi}{\mathrm{Im}(z)},$$

we have Dirichlet's residue formula:

Theorem 2. *Let* H *be the class number of the imaginary quadratic field of discriminant* -D. *Then we have*

$$\mathrm{Res}_{s=1}\zeta_F(s) = \frac{2\pi H}{w\sqrt{D}}.$$

Let $R = \mathbf{Z}[\sqrt{-D}] \supset \mathbf{Z}$. Thus R is a subring of the integer ring $\mathcal{O}$ and $R \cong \mathbf{Z}[X]/(X^2+D)$. Let p be an odd prime in $\mathbf{Z}$ prime to D. Then we see easily that X^2+D mod p is reducible if and only if -D is a quadratic residue mod p. In fact, if $\left(\frac{-D}{p}\right) = 1$, then we can find $\alpha \in \mathbf{Z}$ such that $\alpha^2 \equiv -D \bmod p$ and $R/pR \cong \mathbf{F}[X]/(X-\alpha)(X+\alpha) \cong \mathbf{F}\oplus\mathbf{F}$ for $\mathbf{F} = \mathbf{Z}/p\mathbf{Z}$. Thus $pR = \mathfrak{p}'_1\cap\mathfrak{p}'_2$ in R for two distinct prime ideals $\mathfrak{p}'_1$ and $\mathfrak{p}'_2$. If $D \equiv 0 \bmod 2$, then $\mathcal{O} = R$ and thus

(1) $$p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2 \text{ for } \mathfrak{p}_1 \neq \mathfrak{p}_2 \text{ if and only if } \left(\frac{-D}{p}\right) = 1.$$

If D is odd, then for $\omega = \frac{1+\sqrt{-D}}{2}$, the minimal polynomial of ω: $X^2-X+N(\omega) = 0$ is reducible over $\mathbf{F}$ if and only if there is $\alpha \in \mathbf{Z}$ such that $\alpha^2 \equiv -D \bmod p$, because 2 is invertible in $\mathbf{F}$. Thus (1) is still true. For example, if D is a prime, then $D \equiv 3 \bmod 4$ (i.e. $\left(\frac{-1}{D}\right) = (-1)^{(D-1)/2} = -1$), and we know from the quadratic reciprocity law that

$$\left(\frac{-D}{p}\right) = \left(\frac{p}{D}\right) = \chi_D(p).$$

Thus the map $p \mapsto \left(\frac{-D}{p}\right)$ is a Dirichlet character modulo D. More generally, we have the following fact:

Exercise 2. Using the quadratic reciprocity law, show that the map: $p \mapsto \left(\frac{-D}{p}\right)$ is induced by a Dirichlet character $\chi_D : (\mathbf{Z}/D\mathbf{Z})^\times \to \{\pm 1\}$.

Thus we see that $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$ if and only if $\chi_D(p) = 1$. Now we look at the Euler factor of the Dedekind zeta function of F. We see

	Euler factor at prime ideals dividing p
$\chi_D(p) = 1$	$(1-N(p_1)^{-s})(1-N(p_2)^{-s}) = (1-p^{-s})(1-\chi_D(p)p^{-s})$
$\chi_D(p) = -1$	$1-N(p)^{-s} = (1+p^{-s})(1-p^{-s}) = (1-p^{-s})(1-\chi_D(p)p^{-s})$
$\chi_D(p) = 0$	$1-N(p)^{-s} = (1-p^{-s})(1-\chi_D(p)p^{-s})$

Thus we have

$$\zeta_F(s) = \prod_p(1-N(p)^{-s})^{-1} = \prod_p(1-p^{-s})^{-1}(1-\chi_D(p)p^{-s})^{-1} = \zeta(s)L(s,\chi_D).$$

Thus we know that

$$L(1,\chi_D) = \mathrm{Res}_{s=1}\zeta(s)L(s,\chi_D) = \mathrm{Res}_{s=1}\zeta_F(s) = \frac{2\pi H}{w\sqrt{D}}.$$

On the other hand, by the functional equation, we can relate $L(1,\chi_D)$ with the value $L(0,\chi_D) = -D^{-1}\sum_{a=1}^{D-1}\chi_D(a)a$ (see §3). Thus we have

Theorem 3 (Dirichlet's class number formula). $H = -\frac{w}{2D}\sum_{a=1}^{D-1}\chi_D(a)a$.

Exercise 3. Using the above class number formula, show
(i) For a prime $p > 3$ with $p \equiv 3 \bmod 4$, the number a of quadratic residues in $[0, \frac{p}{2}]$ exceeds the number b of quadratic non-residues in the same interval;
(ii) If $p > 3$ and $p \equiv 3 \bmod 8$, then $a-b \equiv 0 \bmod 3$.

§2.7. Hecke L-functions of number fields

Let F be a general number field and let I be the set of all embeddings of F into $\mathbf{C}$. Let $I(\mathbf{R})$ be the subset of I consisting of real embeddings and put $I(\mathbf{C}) = I-I(\mathbf{R})$. Then the number of real places of F is given by $r = \#I(\mathbf{R})$ and the number of complex places is given by $t = \#I(\mathbf{C})/2$. We start with the study of the fundamental domain of F_+/E, where

$$E = \{\varepsilon \in \mathcal{O}^\times \mid \varepsilon^\sigma > 0 \text{ for all } \sigma \in I(\mathbf{R})\},$$
$$F_+ = \{\alpha \in F^\times \mid \alpha^\sigma > 0 \text{ for all } \sigma \in I(\mathbf{R})\}.$$

Thus if $I(\mathbf{R}) = \varnothing$, then we simply put $F_+ = F^\times$. The result we want to prove first is

Theorem 1 (Shintani [St1, St5]). *Let* E' *be a subgroup of finite index in* E. *Then there are finitely many open simplicial cones* $C_i = C(v_{i1},\ldots,v_{im_i})$ *with* $v_{ij} \in F_+$ *such that* $C = \bigcup_i C_i$ *and* $F_+ = \bigcup_{\varepsilon\in E'}\varepsilon C$ *are both disjoint unions. We can take the* C_i*'s so that there exists* $u_{\sigma,i} \in \mathbf{C}^\times$ *for each* $\sigma \in I$ *and* i *such that* $\mathrm{Re}(u_{\sigma,i}v_{ij}^\sigma) > 0$ *for all* $j = 1, \ldots, m_i$.

Here an open simplicial cone $C(v_1, \ldots, v_m)$ in an $\mathbf{R}$-vector space or $\mathbf{Q}$-vector space V with generators $v_i \in V$ is by definition

$$C(v_1, \ldots, v_m) = \{x_1v_1+\cdots+x_mv_m \mid x_i > 0 \text{ for all } i\},$$

where the m vectors v_i are supposed to be linearly independent. We divide $I(\mathbf{C}) = \Sigma(\mathbf{C})\cup\Sigma(\mathbf{C})c$ into a disjoint union of two subsets $\Sigma(\mathbf{C})$ and its complex conjugate $\Sigma(\mathbf{C})c$ for complex conjugation c and write Σ for $I(\mathbf{R})\cup\Sigma(\mathbf{C})$. In the theorem, we regard C_i as an open simplicial cone in the real vector space $V = F_\infty = F\otimes_{\mathbf{Q}}\mathbf{R} = \mathbf{R}^{I(\mathbf{R})}\times\mathbf{C}^{\Sigma(\mathbf{C})}$. We then embed F into V by $\alpha \mapsto (\alpha^\sigma)_{\sigma\in\Sigma} \in V$. Then F is a $\mathbf{Q}$-vector-subspace of V which is dense in V. We put

$$V_+ = \mathbf{R}_+^{I(\mathbf{R})}\times(\mathbf{C}^\times)^{\Sigma(\mathbf{C})},$$

where $\mathbf{R}_+ = \{x \in \mathbf{R} \mid x > 0\}$. Then $F_+ = V_+\cap F$.

Proof of Theorem 1. Since the proof is the same for any E', we simply treat only the case $E' = E$. Consider the hypersurface X in V_+ defined by

$$X = \{(x_\sigma)_{\sigma\in\Sigma} \mid N(x) = \prod_{\sigma\in I(\mathbf{R})}x_\sigma\prod_{\sigma\in\Sigma(\mathbf{C})}|x_\sigma|^2 = 1\}.$$

Then, for $S = \{x \in \mathbf{C} \mid |x| = 1\}$, we have $\rho : X \cong S^t\times\mathbf{R}^{r+t-1}$. In fact the projection to S^t can be given by $x \mapsto (x_\sigma/|x_\sigma|)_{\sigma\in\Sigma(\mathbf{C})} \in S^t$ and the projection to $\mathbf{R}^{r+t-1}$ is given by $x \mapsto l(x) = (l_\sigma(x_\sigma))_{\Sigma-\{\tau\}}$, where we exclude one embedding $\tau \in \Sigma$ and $l_\sigma(x_\sigma) = log(|x_\sigma|)$ or $2log(|x_\sigma|)$ according as σ is real or complex. By definition E acts on X by componentwise multiplication. The image of E in $\mathbf{R}^{r+t-1}$ is a lattice by Dirichlet's theorem (Theorem 1.2.3) and hence X/E is a compact set. Thus we can find a compact subset K of X such that $X = \bigcup_{\varepsilon\in E}\varepsilon K$. We can project V_+ to X via $x \mapsto N(x)^{-1/d}x$ for $d = [F:\mathbf{Q}]$, which will be denoted by π. This is obviously continuous and surjective and hence takes the dense subset F_+ to a dense subset of X. We can find a small neighborhood U of 1 in the multiplicative group X such that $\varepsilon U\cap U = \varnothing$ if $\varepsilon \neq 1$ in E. We may assume that $U = C_0\cap X$ for an open simplicial cone C_0 in V_+ with generators in F_+. Thus $\bigcup_{x\in K\cap\pi(F_+)}xC_0 \supset K$. Since K is compact, we can choose finitely many $x_i \in \pi(F_+)\cap K$ such that $\bigcup_{i=1}^n x_iC_0 \supset K$. We write $F_+\cap x_iC_0 = C_{0,i}$. Note that $\varepsilon C_{0,i}\cap C_{0,i} = \varnothing$ if $\varepsilon \neq 1$ because $\varepsilon U\cap U = \varnothing$ if $\varepsilon \neq 1$ in E and C_0 is the $\mathbf{R}_+$-span of U. Moreover $C_{0,i}$ is a cone with generators in F_+. In fact, taking $y_i \in F_+$ such that $\pi(y_i) = x_i$, then $C_{0,i} = x_iC_0 = y_iC_0$. Since $C_0 = C(v_1, \ldots, v_d)$ with $v_i \in F_+$, we see that $C_{0,i} = C(y_iv_1, \ldots, y_iv_d)$ is a cone generated by vectors in F_+. Now admitting the following lemma, we finish the proof of the theorem:

Lemma 1. *Let* C *and* C' *be two polyhedral cones whose generators are in* F *(where a polyhedral cone means a disjoint union of finitely many open simplicial cones). Then* $C\cap C'$, $C\cup C'$ *and* $C-C'$ *are all polyhedral cones whose generators are in* F.

We have $F_+ = \bigcup_{i=1}^n \bigcup_{\varepsilon\in E} \varepsilon C_{0,i}$ and $C_{0,i}\cap \varepsilon C_{0,i} = \varnothing$ if $\varepsilon \neq 1$. If $n = 1$, $C_{0,1}$ is the desired cone. When $n > 1$, we define $C_{1,1} = C_{0,1}$ and for $i \geq 2$, $C_{1,i} = C_{0,i} - \bigcup_{\varepsilon\in E} \varepsilon C_{0,1}$. Since $C_{0,i}$ $(i > 1)$ intersects with $\varepsilon C_{0,1}$ for only finitely many ε, $C_{1,i}$ is a polyhedral cone by the lemma. We now have $C_{1,i}\cap\{\bigcup_{\varepsilon\in E}\varepsilon C_{1,1}\} = \varnothing$ $(i \geq 2)$ and $F_+ = \bigcup_{i=1}^n \bigcup_{\varepsilon\in E}\varepsilon C_{1,i}$ and $C_{1,i}\cap\varepsilon C_{1,i} = \varnothing$ if $\varepsilon \neq 1$. We now construct inductively (on j) polyhedral cones $C_{j,i}$ with generators in F_+ for each $0 < j \leq n$ by $C_{j,i} = C_{j-1,i}$ if $i \leq j$ and $C_{j,i} = C_{j-1,i} - \bigcup_{\varepsilon\in E}\varepsilon C_{j-1,j}$ $(C_{j,j} = C_{j-1,j})$ for $j < i$. Then we see that

$$C_{j,i}\cap\bigcup_{\varepsilon\in E}\varepsilon C_{j,k} = \varnothing \quad \text{for } i > j \geq k, \quad F_+ = \bigcup_{i=1}^n \bigcup_{\varepsilon\in E}\varepsilon C_{j,i},$$
$$\text{and } C_{j,i}\cap\varepsilon C_{j,i} = \varnothing \text{ if } \varepsilon \neq 1.$$

Then $C_{n,i}$ is a disjoint union of finitely many simplicial cones which give the desired simplicial cones. This proves the first assertion of the theorem. We can subdivide the cones C_j so that the last assertion follows.

Exercise 1. Give a detailed proof of the last assertion of Theorem 1.

Proof of Lemma 1. We may assume that C and C' are open simplicial cones. Write $C = C(v_1, \ldots, v_m)$, where the v_i's are linearly independent. By adding $v_{m+1}, \ldots, v_d$, we have a basis $v_1, \ldots, v_d$ of V. Let V^* be the dual vector space of V and v_i^* be the dual basis of the v_i's, i.e., $v_i^*(v_j) = \delta_{ij}$. In particular, for $v = x_1v_1+\cdots+x_dv_d$, $x_i = v_i^*(v)$. Thus, we see that

$$C = \{v \in V \mid v_i^*(v) > 0 \text{ for } 1 \leq i \leq m \text{ and } v_i^*(v) = 0 \text{ for } i > m\}.$$

Since the v_i are in F, v_i^* induces $\mathbf{Q}$-linear forms on F. (We call such a form a $\mathbf{Q}$-linear form.) Similarly, there are d linearly independent $\mathbf{Q}$-linear forms w_i^* on F and an integer n between 1 and d such that

$$C' = \{v \in V \mid w_i^*(v) > 0 \text{ for } 1 \leq i \leq n \text{ and } w_i^*(v) = 0 \text{ for } i > n\}.$$

Thus $C-C$ and $C\cap C'$ are disjoint unions of sets of the following form for finitely many $\mathbf{Q}$-linear forms L_i on a vector subspace W of V (W may not be a proper subspace but W is an $\mathbf{R}$-span of a $\mathbf{Q}$-vector subspace of F):

$$X = \{w \in W \mid L_i(w) > 0 \text{ for } i = 1, \ldots, l\}.$$

We may assume that $\{L_i\}$ is a minimum set of linear forms to define X. For example, when $X = C \cap C'$, then we take W to be

$$\{x \in V \mid v_i^*(x) = 0 \text{ and } w_j^*(x) = 0 \text{ if } i > m \text{ and } j > n\}.$$

Since $C \cup C' = (C \cap C') \cup (C - C') \cup (C' - C)$ is a disjoint union, it is sufficient to show that X is a polyhedral cone with generators in F. When $\dim(W) = 1$ or 2, the assertion is obvious. Thus we shall prove the assertion by induction on $\dim(W)$. Let

$$X_j = \{w \in W \mid L_i(w) \geq 0 \text{ for } i \neq j \text{ and } L_j(w) = 0\} - \{0\},$$
$$\overline{X} = \{w \in W \mid L_i(w) \geq 0 \text{ for } i = 1, \ldots, l\} - \{0\}.$$

Since X_j is contained in $\mathrm{Ker}(L_j)$ which has dimension less than $\dim(W)$, by the induction hypothesis, X_j is a disjoint union of open simplicial cone. Moreover, $X_j - \bigcup_{i \neq j} X_i$ is a disjoint union of open simplicial cones, and hence it is easy to see that $\overline{X} - X = \bigcup_j X_j$ is also a disjoint union of open simplicial cones. Write these cones as $\bigcup_j X_j = \bigcup_k C(v_{k1}, \ldots, v_{ki_k})$. Let u be a point in $X \cap F$, which exists because X is open in W and $F \cap W$ is dense as already remarked. Since $v_{k1}, \ldots, v_{ki_k}$ are in a proper subspace of W and u is not in the subspace spanned by $v_{k1}, \ldots, v_{ki_k}$, $u, v_{k1}, \ldots, v_{ki_k}$ are linearly independent. Write $C_k(u)$ for $C(u, v_{k1}, \ldots, v_{ki_k})$. Then we claim that

$$X = \bigcup_k C_k(u) \cup \mathbf{R}_+ u \quad \text{(disjoint)}.$$

By definition, $L_i(x) > 0$ for all i if $x \in X$. Thus in particular, if $x = \lambda u$ for $\lambda \in \mathbf{R}$, then $L_i(x) = \lambda L_i(u) > 0$, $L_i(x) > 0$ and $L_i(u) > 0$. Thus, $\mathbf{R}u \cap X = \mathbf{R}_+ u$. Suppose that $x \in X$ is not a scalar multiple of u. Let s be the minimum of $L_i(x)/L_i(u)$ for $i = 1, \ldots, l$. Then $s > 0$. There is an index i (maybe several) such that $s = L_i(x)/L_i(u)$. Then $L_j(x - su) = L_j(x) - sL_j(u) \geq 0$ and $L_i(x - su) = 0$. Thus $x - su \in \overline{X} - X$. Therefore $x - su \in C_k$ for a unique k (because $\overline{X} - X$ is a disjoint union of the C_k's) and thus $x \in C_k(u)$. This shows the desired assertion.

Exercise 2. Write down the proof of $\overline{X} - X = \bigcup_j X_j$ explaining every detail.

Let $\mathbf{Z}[I]$ be the free module generated by embeddings of F into $\mathbf{C}$. We can think of each element $\xi \in \mathbf{Z}[I]$ as a quasi-character of $F^\times$ which takes $\alpha \in F^\times$ to $\alpha^\xi = \prod_{\sigma \in I} \alpha^{\sigma\xi\sigma} \in \mathbf{C}^\times$. A quasi-character $\lambda : I(m) \to \mathbf{C}^\times$ for an ideal m of O is called an arithmetic Hecke character if there exists $\xi \in \mathbf{Z}[I]$ such that $\lambda((\alpha)) = \alpha^\xi$ for all $\alpha \in P(m)$, where

$$P(m) = \{\alpha \in F_+ \mid \beta(\alpha - 1) \in m \text{ for some } \beta \in O \text{ prime to } m\}.$$

Theorem 2 (Hecke). *If λ is an arithmetic Hecke character modulo $\mathfrak{m}$, then $L(s,\lambda) = \sum_{\mathfrak{n}\in I(\mathfrak{m}),\, \mathcal{O}\supset\mathfrak{n}} \lambda(\mathfrak{n})N(\mathfrak{n})^{-s}$ can be continued to a meromorphic function on the whole complex s-plane* $\mathbf{C}$.

Proof. Let $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\}$ be a representative set of ideal classes for $I/\mathcal{P}_+$ (see Exercise 1.2.1). We may assume that $\mathfrak{a}_i$ are all prime to $\mathfrak{m}$. Since $\{\mathfrak{a}_i\mathfrak{m}\}_{i=1,\ldots,h}$ still gives a representative set, we can write

$$\begin{aligned} L(s,\lambda) &= \sum_{i=1}^{h} \sum_{\alpha\in(\mathfrak{a}_i^{-1}\mathfrak{m}^{-1}\cap F_+)/E} \lambda(\alpha\mathfrak{a}_i\mathfrak{m})N(\alpha\mathfrak{a}_i\mathfrak{m})^{-s} \\ &= \sum_{i=1}^{h} N(\mathfrak{a}_i\mathfrak{m})^{-s} \sum_{\alpha\in(\mathfrak{a}_i^{-1}\mathfrak{m}^{-1}\cap F_+)/E} \lambda(\alpha\mathfrak{a}_i\mathfrak{m})N(\alpha)^{-s}. \end{aligned}$$

Now we take the fundamental domain $C = \bigcup_{j=1}^{a} C_j$ for F_+/E with disjoint open simplicial cones C_j. Here note that for a positive rational number u, $C_j = uC_j$ by definition. In particular, $NC_j = C_j$ for any positive integer N. Thus we may assume that C_j is generated by totally positive integers in $\mathcal{O}$. Fix a set of generators $\{v_1, \ldots, v_b\}$ of C_j in $\mathcal{O}$ and consider the Shintani L-function

$$\zeta_j(s,x) = \sum_{n\in N^b} \prod_{\sigma\in I} (x^\sigma + n\cdot v^\sigma)^{-s_\sigma},$$

where $v^\sigma = (v_1^\sigma, \ldots, v_b^\sigma) \in \mathbf{C}^b$, $x = x_1v_1 + \cdots + x_bv_b$ with $x_i \in (0,1]$, $x^\sigma = v_1^\sigma x_1 + \cdots + v_b^\sigma x_b$ and $n\cdot v^\sigma = v_1^\sigma n_1 + \cdots + v_b^\sigma n_b$. By Theorem 1, we also have $u_\sigma \in \mathbf{C}^\times$ such that all the entries of $u_\sigma v^\sigma$ have positive real parts. Then

$$\begin{aligned} \zeta_j(s,x) &= \sum_{n\in N^b} \prod_{\sigma\in I} (x\cdot v^\sigma + n\cdot v^\sigma)^{-s_\sigma} \\ &= \{\prod_{\sigma\in I} u_\sigma^{s_\sigma}\} \sum_{n\in N^b} \prod_{\sigma\in I} (x\cdot u_\sigma v^\sigma + n\cdot u_\sigma v^\sigma)^{-s_\sigma} = \{\prod_{\sigma\in I} u_\sigma^{s_\sigma}\} \zeta(s, A, (x_i), \mathbf{1}), \end{aligned}$$

where we have to choose the branch of $\log(u_\sigma)$ suitably and $A = ({}^t(u_\sigma v^\sigma))_{\sigma\in I}$ is a $b\times d$ matrix with coefficients in H'. Thus by Theorem 2.4.1, $\zeta_j(s,x)$ can be continued to an analytic function of s. Now we try to express $L(s,\lambda)$ as a sum of $\zeta_j(s,x)$. Let

$$\begin{aligned} R_{ij} &= \mathfrak{a}_i^{-1}\mathfrak{m}^{-1} \cap \{x_1v_1 + \cdots + x_bv_b \mid 0 < x_k \le 1 \quad \text{for} \quad k = 1, \ldots, b\}, \\ C_j(\mathbf{Z}) &= \{n_1v_1 + \cdots + n_bv_b \mid 0 \le n_k \in \mathbf{Z} \quad \text{for all } k\}. \end{aligned}$$

Then R_{ij} is a finite set and any $\alpha \in \mathfrak{a}_i^{-1}\mathfrak{m}^{-1}\cap F_+$ can be written as $\alpha = \varepsilon(x+\beta)$ for unique $\varepsilon \in E$, $x \in R_{ij}$ for a unique j and $\beta \in C_j(\mathbf{Z})$. Thus we have

$$\begin{aligned} L(s,\lambda) &= \sum_{i=1}^{h} \sum_{\alpha\in(\mathfrak{a}_i^{-1}\mathfrak{m}^{-1}\cap F_+)/E} \lambda(\alpha\mathfrak{a}_i\mathfrak{m})N(\alpha\mathfrak{a}_i\mathfrak{m})^{-s} \\ &= \sum_{i=1}^{h} N(\mathfrak{a}_i\mathfrak{m})^{-s} \sum_{j=1}^{a} \sum_{x\in R_{ij}} \lambda(x\mathfrak{a}_i\mathfrak{m})x^{-\xi}\zeta_j((s-\xi_\sigma)_{\sigma\in I}, x) \quad \text{for } s \in \mathbf{C}. \end{aligned}$$

In fact, choosing $\gamma \in \mathcal{O}$ such that $\gamma\mathcal{O} = \mathfrak{m}\mathfrak{b}$ and $\mathfrak{b}$ is prime to $\mathfrak{m}$, we can write $(x+\beta)\mathfrak{a}_i\mathfrak{m} = \gamma(x+\beta)\gamma^{-1}\mathfrak{a}_i\mathfrak{m}$. Since $\gamma\mathcal{O} = \mathfrak{m}\mathfrak{b}$, $\gamma^{-1}\mathfrak{a}_i\mathfrak{m} = \mathfrak{a}_i\mathfrak{b}^{-1}$, which is prime to

m and hence $\lambda(\gamma^{-1}a_i m) \neq 0$. On the other hand, $\gamma(x+\beta) = \gamma x+\gamma\beta \equiv \gamma x \bmod^{\times} m$ because $\gamma\beta \in \gamma O = mb$. Thus $\lambda(\gamma(x+\beta)/\gamma x) = (\gamma(x+\beta)/\gamma x)^{\xi}$. (Actually we should remark the fact that $\gamma(x+\beta)/\gamma x \in F_+$ to assure this equality.) This shows that

$$\begin{aligned}\lambda((x+\beta)a_i m) &= \lambda(((x+\beta)\gamma/\gamma x)a_i m)\lambda(x)\\ &= (\gamma(x+\beta)/\gamma x)^{\xi}\lambda(x a_i m) = (x+\beta)^{\xi}x^{-\xi}\lambda(x a_i m),\end{aligned}$$

which finishes the proof of Theorem 2.

Exercise 3. Write down every detail of the proof of the equality $\lambda((x+\beta)a_i m) = (x+\beta)^{\xi}x^{-\xi}\lambda(x a_i m)$, because in the proof we implicitly assumed that $x a_i m$ is prime to m.

Corollary 1. *If* $n \in \mathbf{Z}$ *with* $n \leq \xi_\sigma$ *for all* σ, *then* $L(n,\lambda) \in \mathbf{Q}(\lambda)$.

This has meaning only when F is totally real, because we will see in Chapter 8 that $L(n,\lambda)$ is zero otherwise.

Now we briefly discuss Hilbert modular Eisenstein series. We will take up this topic in adelic language later in Chapter 9 in more detail. Here we suppose that F is totally real, i.e. $I = I(\mathbf{R})$. Consider $SL_2(O)$ and its congruence subgroup for each integral ideal m

$$\Gamma(m) = \{\alpha \in SL_2(O) \mid \alpha \equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \bmod mM_2(O)\}.$$

We consider the product H^I of d copies of the upper half complex plane H indexed by the set I of embeddings of F into $\mathbf{R}$. Then we let $SL_2(O)$ act on H^I so that $\alpha((z_\sigma)) = (\alpha^\sigma(z_\sigma))$, where $\begin{pmatrix}a & b\\ c & d\end{pmatrix}^\sigma = \begin{pmatrix}a^\sigma & b^\sigma\\ c^\sigma & d^\sigma\end{pmatrix} \in SL_2(\mathbf{R})$ acts on each component H via the linear fractional transformation. To define modular forms in a weak sense, we consider not only weights in $\mathbf{Z}[I]$ but also those which are formal linear combinations of symbols σ and σc with $\sigma \in I$, where c denotes complex conjugation. We denote by $\mathbf{Z}[I \cup Ic]$ for $Ic = \{\sigma c \mid \sigma \in I\}$ the module of weights. A function $f : H^I \to \mathbf{C}$ is called a Hilbert modular form on $\Gamma(m)$ of weight (k,s) if

$$f(\gamma(z)) = j(\gamma,z)^k \,|\, j(\gamma,z)\,|^{2s} f(z) \quad \text{for all } \gamma \in \Gamma(m),$$

where $k = \sum_{\sigma \in I \cup Ic} k_\sigma \sigma \in \mathbf{Z}[I \cup Ic]$, $s \in \mathbf{C}$ and for $\gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$,

$$j(\gamma,z)^k = \prod_{\sigma \in I}\{(c^\sigma z_\sigma + d^\sigma)^{k_\sigma}(c^\sigma \bar{z}_\sigma + d^\sigma)^{k_{\sigma c}}\}, \quad |j(\gamma,z)|^{2s} = \prod_{\sigma \in I}|(c^\sigma z_\sigma + d^\sigma)|^{2s}.$$

Then, for $(a,b) \in (O/m)^2$, the Eisenstein series of weight (k,s) is defined by

$$E'_{k,m}(z,s;a,b)$$
$$= \sum{}'_{(m,n)\equiv(a,b) \bmod m}\{\prod_{\sigma\in I}(m^\sigma z_\sigma+n^\sigma)^{-k_\sigma}\}\{\prod_{\sigma\in I}(m^\sigma \bar{z}_\sigma+n^\sigma)^{-k_{\sigma c}}\}\,|N(mz+n)|^{-2s},$$

where the summation runs over

$$\{(m,n) \in \mathcal{O}^2-(0,0) \mid (m,n) \equiv (a,b) \bmod m\}/E(m)$$

and

$$N(mz+n) = \prod_{\sigma\in I}(m^\sigma z_\sigma+n^\sigma).$$

Here $E(m) = \{\varepsilon \in E \mid \varepsilon \equiv 1 \bmod m\}$, which is a subgroup of E of finite index, and $E(m)$ acts on $\mathcal{O}^2$ by $(m,n)\varepsilon = (m\varepsilon,n\varepsilon)$. Then $E'_{k,m}(z,s;a,b)$ is convergent if s has sufficiently large real part. We now fix finitely many simplicial cones C_j so that $C = \bigcup_i C_i$ gives a representative set of $F^\times/E(m)$.

Exercise 4. Show that $(F^\times)^2 = \bigcup_{\varepsilon\in E(m)}\varepsilon(C\times F^\times)$ is a disjoint union.

By dividing $F^\times$ as a disjoint union of finitely many simplicial cones C'_j, we know from Exercise 5 that $(F^\times)^2 = \bigcup_{\varepsilon\in E(m)}\varepsilon\{\bigcup_{i,j}C_i\times C'_j\}$. Note that $C_i \times C'_j$ is again an open simplicial cone $C(\{(v_i,0),(0,w_j)\})$ for $v_i \in C_i$ and $w_j \in C'_j$. We define, for $x = x_1v_1+\cdots+x_\alpha v_\alpha$ with $x_i \in (0,1]$ and $y = y_1w_1+\cdots+y_\beta w_\beta$ with $y_i \in (0,1]$,

$$\zeta_{ij}(s,x,y) = \sum_{(m,n)\in N^a\times N^b}\prod_{\sigma\in I}(x^\sigma z_\sigma+y^\sigma+m\cdot v^\sigma z_\sigma+n\cdot w^\sigma)^{-s_\sigma}.$$

Then in exactly the same manner as in the proof of Theorem 2, we can express $E'_{k,m}(z,s;a,b)$ as a finite sum of $\zeta_{ij}((s+k_\sigma)_{\sigma\in I\cup I^c},x,y)$ for $s \in \mathbf{C}$. Since $\zeta_{ij}(s,x,y)$ can be continued to a meromorphic function on the whole s-plane and gives a real analytic function of z for a fixed s, we have

Theorem 3 (Hecke). *The Eisenstein series has a meromorphic continuation to the whole s-plane. When $E'_{k,m}(z,s;a,b)$ is finite at $s \in \mathbf{C}$, then $E'_{k,m}(z,s;a,b)$ gives a real analytic Hilbert modular form of weight (k,s) on $\Gamma(m)$.*

We will return to the study of Eisenstein series in more detail later in Chapters 5 and 9.

Chapter 3. p-adic Hecke L-functions

In this chapter, we first construct p-adic Dirichlet L-functions for $\mathbf{Q}$ using Euler's method of computing the values $L(n,\chi)$. We follow Katz's article [K2] in this part. Then we generalize the result for Hecke L-functions of totally real fields using the method in [K6]. Roughly speaking, a p-adic L-function is a p-adic analytic function whose values coincide with those of its complex counterpart at enough integer points to guarantee its uniqueness. Here we mean by a p-adic analytic function on an open set U of $\mathbf{Z}_p$ a function on U having values in a finite extension F of $\mathbf{Q}_p$ which can be expanded into a power series in $(z-u)$ (with coefficients in F) for each $u \in U$ convergent on an open neighborhood of u in U. A p-adic meromorphic function on U is a quotient of two p-adic analytic functions on U. The p-adic L-function we discuss was first constructed for $\mathbf{Q}$ by Kubota and Leopoldt [KL] as a continuous function and later shown to be p-adic analytic by Iwasawa [Iw1]. The result was generalized to totally real fields independently by Deligne and Ribet [DR], Cassou-Nogues [CN] and Barsky [Ba]. Katz's method in [K6] is an interpretation of the methods of [CN] and [Ba] in terms of formal groups.

§3.1. Interpolation series

We recall the definition of the binomial polynomial: as a rational polynomial with variable x, for a non-negative integer n,

$$\binom{x}{n} = \begin{cases} \dfrac{x(x-1)\cdot\cdots\cdot(x-n+1)}{n!} & \text{if } n \geq 1, \\ 1 & \text{if } n = 0. \end{cases}$$

Then it is obvious that this polynomial has integer values on the set $\mathbf{N}$ of non-negative integers. For negative integers $-m$ $(m \in \mathbf{N})$, we have $\binom{-m}{n} = (-1)^n\binom{m+n-1}{n} \in \mathbf{Z}$. Thus in fact, $\binom{x}{n}$ has integer value on $\mathbf{Z}$. Such a polynomial is called *numerical*. By the binomial theorem, we have a formal identity in the formal power series ring

$$(1+X)^x = \sum_{n=0}^{\infty} \binom{x}{n} X^n.$$

When $x \in \mathbf{N}$ $(= \{n \in \mathbf{Z} \mid n \geq 0\})$, this power series is actually a polynomial of degree x and the identity holds for any value of X. Thus, for $x \in \mathbf{N}$,

$$\text{(1a)} \qquad \sum_{k=0}^{x-j}(-1)^k\binom{x-j}{k} = (1-1)^{x-j} = \begin{cases} 1 & \text{if } j = x, \\ 0 & \text{if } 0 \leq j < x. \end{cases}$$

By comparing the coefficients of X^m of $(1+X)^x(1+X)^y = (1+X)^{x+y}$, we have

(1b) $$\binom{x+y}{m} = \sum_{n=0}^{m} \binom{x}{n}\binom{y}{m-n}.$$

Let K be a field extension of $\mathbf{Q}$ and A be a subring of K. Let $f : \mathbf{N} \to A$ be any function. We define the n-th coefficient $a_n(f)$ of f by

(2) $$a_n = a_n(f) = \sum_{k=0}^{n}(-1)^k\binom{n}{k}f(n-k) = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(k) \in A.$$

Using these coefficients, we define a new function $f^* : \mathbf{N} \to A$ by

$$f^*(x) = \textstyle\sum_{n=0}^{\infty} a_n(f)\binom{x}{n} \quad \text{for } x \in \mathbf{N}.$$

This is actually a finite sum $\sum_{n=0}^{x} a_n(f)\binom{x}{n}$ because $\binom{x}{n} = 0$ when $n > x$. We now compute the value of f^*. By definition, we have

$$f^*(x) = \sum_{n=0}^{x} a_n(f)\binom{x}{n} = \sum_{n=0}^{x}\left\{\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(k)\right\}\binom{x}{n}$$

$$= \sum_{k=0}^{x} f(k)\sum_{j=0}^{x-k}(-1)^j\binom{j+k}{j}\binom{x}{j+k} = \sum_{k=0}^{x} f(k)\sum_{j=0}^{x-k}(-1)^j\binom{x}{k}\binom{x-k}{j}$$

$$= \sum_{k=0}^{x} f(k)\binom{x}{k}\sum_{j=0}^{x-k}(-1)^j\binom{x-k}{j} = f(x).$$

The last equality follows from (1a). This shows that

(3) $$f(x) = \textstyle\sum_{n=0}^{\infty} a_n(f)\binom{x}{n} \quad \text{on } \mathbf{N}.$$

Exercise 1. Let $(a_1, \ldots, a_r)$ be an r-tuple of non-negative distinct integers and $(b_1, \ldots, b_r)$ be an r-tuple of real numbers. Show the existence of a polynomial P with coefficients in $\mathbf{R}$ such that $P(a_i) = b_i$ for all $i = 1, \ldots, r$.

We now prove the uniqueness of the expansion (3). We suppose the existence of coefficients $\{a'_n \in K\}_{n\in\mathbf{N}}$ such that

$$f(x) = \textstyle\sum_{n=0}^{\infty} a'_n\binom{x}{n} \quad \text{on } \mathbf{N}.$$

Then by (3), putting $b_n = a_n - a'_n$, we see that

$$\textstyle\sum_{n=0}^{\infty} b_n\binom{x}{n} = 0 \quad \text{on } \mathbf{N}.$$

Supposing the existence of coefficients b_n, not all zero, we take the smallest n with $b_n \neq 0$. By the minimality of n, $b_m = 0$ for all $0 \le m < n$. Thus $\sum_{m=0}^{n-1} b_m\binom{x}{m} = 0$ and in particular $\sum_{m=n+1}^{\infty} b_m\binom{n}{m} = 0$. Since $\binom{n}{m} = 0$ if $n < m$, we conclude from this that $b_n = \binom{n}{n}b_n = 0$, which contradicts our

choice of n. Thus $b_n = 0$ for all n and the expansion as in (3) is unique. Summarizing this, we have

Proposition 1. *For a given function* $f : \mathbf{N} \to A$, *there exists a unique sequence of elements* $\{a_n(f)\}_{n\in\mathbf{N}}$ *in* A *such that* $f(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}$ *for all* $x \in \mathbf{N}$. *Moreover* $\{\binom{x}{n}\}_{n\in\mathbf{N}}$ *gives a basis of the ring of numerical polynomials.*

§3.2. Interpolation series in p-adic fields

We are now able to describe, using interpolation series, the space $\mathcal{C}(\mathbf{Z}_p;A)$ of continuous functions on $\mathbf{Z}_p$ having values in any closed subring A of the p-adic completion F_p of a number field F. A continuous function $f : \mathbf{Z}_p \to \mathcal{O}_p$ is in fact determined by its restriction to the natural numbers $\mathbf{N}$ by the density of $\mathbf{N}$ in $\mathbf{Z}_p$ (see (1.3.3)). Thus f is uniquely determined by the interpolation series of its restriction to $\mathbf{N}$:

$$(1) \qquad f(x) = \sum_{n=0}^{\infty} a_n(f)\binom{x}{n} \quad \text{on } \mathbf{N}.$$

We are going to show that the right-hand side of the above identity converges in $\mathcal{O}_p$ uniformly for any $x \in \mathbf{Z}_p$. After showing this, we will know that the right-hand side gives a continuous function which coincides with f on $\mathbf{N}$ and hence is equal to f on all $\mathbf{Z}_p$. What we need to show is $\lim_{n\to\infty} a_n(f) = 0$. Then the convergence of (1) and the uniformity of the convergence follow from the strong triangle inequality (1.3.1) and the fact (see (2) below) that $|\binom{x}{n}|_p \le 1$ for all $x \in \mathbf{Z}_p$.

Exercise 1. Show the convergence of (1) and the uniformity of the convergence assuming $\lim_{n\to\infty} a_n(f) = 0$.

Let us now show that $\lim_{n\to\infty} a_n(f) = 0$. For any given polynomial $P(X)$ $(= a_0+a_1X+\cdots+a_dX^d)$ with coefficients in $\mathbf{Q}_p$, we see that

$$\begin{aligned} |P(x)-P(y)|_p &\le \max_{0\le n\le d}(|a_n|_p|x-y|_p|x^{n-1}+x^{n-2}y+\cdots+y^{n-1}|_p) \\ &\le \max_{0\le n\le d}(|a_n|_p)|x-y|_p \text{ on } \mathbf{Z}_p. \end{aligned}$$

Thus $x \mapsto P(x)$ is continuous on $\mathbf{Z}_p$. In particular, the function $x \mapsto \binom{x}{n}$ is continuous on $\mathbf{Z}_p$. Since this function has values in $\mathbf{N}$ on the dense subset $\mathbf{N}$ of $\mathbf{Z}_p$, its continuity shows that it takes $\mathbf{Z}_p$ into $\mathbf{Z}_p$. Thus

$$(2) \qquad |\binom{x}{n}|_p \le 1 \quad \text{for all } x \in \mathbf{Z}_p \text{ and } n \in \mathbf{N}.$$

Since $\mathbf{Z}_p$ is compact (because it is a projective limit of compact (even finite) sets $\mathbf{Z}/p^n\mathbf{Z}$ [Bour2, I.9.6]), any continuous function $f : \mathbf{Z}_p \to \mathcal{O}_p$ is uniformly continuous [Bour2, II.4.1]; thus, for any given positive ε, we can find a small positive δ such that $|x-y|_p < \delta \Rightarrow |f(x)-f(y)|_p < \varepsilon$. Now assuming $x,y \in \mathbf{N}$, we take ε to be p^{-s} and write $\delta = p^{-t}$ $(t = t(s))$ for this ε. We may of course assume that $t > 0$. Then $|f(x+p^t)-f(x)|_p \le p^{-s}$. If we let $f_y(x) = f(x+y)$, then by definition, we have

$$a_n(f_y) = \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k} f(k+y).$$

Using the identity (1.1b), $\binom{x+y}{m} = \sum_{n=0}^{m}\binom{x}{n}\binom{y}{m-n}$, we have

$$f_y(x)=f(x+y)=\sum_{m=0}^{\infty} a_m(f)\sum_{n=0}^{m}\binom{x}{n}\binom{y}{m-n}.$$

Now we are going to interchange the summation with respect to m and n in the above formula. Since $x,y \in \mathbf{N}$, m (resp. n) actually runs from 1 (resp. 0) to $x+y$ (resp. m), the summation is in fact finite and thus the interchange of the two sums is legitimate. Thus we have

$$f_y(x) = \sum_{n=0}^{\infty}\binom{x}{n}\sum_{m=n}^{\infty} a_m(f)\binom{y}{m-n} = \sum_{n=0}^{\infty}\binom{x}{n}\sum_{k=0}^{\infty} a_{n+k}(f)\binom{y}{k}.$$

In particular, we have, by the definition in §1 of $a_n(f_y)$,

$$\sum_{k=0}^{\infty} a_{n+k}(f)\binom{y}{k} = a_n(f_y) = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k} f(k+y). \tag{3}$$

Now replacing y by p^t $(= \delta^{-1})$, we see that

$$\begin{aligned} a_{n+p^t}(f) &= -\sum_{j=1}^{p^t-1}\binom{p^t}{j} a_{n+j}(f) + \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k} f(k+p^t) - a_n(f) \qquad (4)\\ &\overset{(3.1.2)}{=} -\sum_{j=1}^{p^t-1}\binom{p^t}{j} a_{n+j}(f) + \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\{f(k+p^t)-f(k)\}. \end{aligned}$$

Since $|f(k+p^t)-f(k)|_p < p^{-s}$ for all k, $\left|\binom{p^t}{j}\right|_p \le p^{-1}$ for $j = 1, \ldots, p^t-1$ and $|a_n(f)|_p \le 1$, the strong triangle inequality shows that

$$|a_{n+p^t}(f)|_p \le \max(p^{-1}|a_{n+1}(f)|_p,\ldots,p^{-1}|a_{n+p^{t(s)}-1}(f)|_p, p^{-s}). \tag{5}$$

In particular, $|a_n(f)|_p \le p^{-1}$ for $n \ge p^{t(1)}$. Using this inequality for $n \ge p^{t(1)}$, we have $|a_{n+p^{t(2)}}(f)|_p \le p^{-2}$ if $n \ge p^{t(1)}$. In other words, $|a_n(f)|_p \le p^{-2}$ if $n \ge p^{t(1)}+p^{t(2)}$. Repeating this process m times, we have

$$|a_n(f)|_p \le p^{-m} \text{ if } n \ge p^{t(1)}+p^{t(2)}+\cdots+p^{t(m)}.$$

This shows the desired assertion: $|\lim_{n\to\infty} a_n(f)|_p = \lim_{n\to\infty} |a_n(f)|_p = 0$. We have proven the following theorem due to Mahler [Ma] for $A = \mathcal{O}_p$:

Theorem 1. *Let* A *be a closed subring of* F_p. *Then we have*
(i) For each function $f : \mathbf{Z}_p \to A$, $a_n(f) \in A$;
(ii) A function $f : \mathbf{Z}_p \to A$ *is continuous if and only if* $\lim_{n\to\infty} a_n(f) = 0$. *In this case, the interpolation series* $\sum_{n=0}^{\infty} a_n(f)\binom{x}{n}$ *converges to* $f(x)$ *for all* $x \in \mathbf{Z}_p$.

Proof. We have already proved the assertion (i) and the sufficiency in the assertion (ii) for $A = \mathcal{O}_p$. The necessity for (ii) is obvious because the interpolation series converges uniformly on $\mathbf{Z}_p$ and coincides with f on the dense subset $\mathbf{N}$ in $\mathbf{Z}_p$. The sufficiency for arbitrary A can be shown as follows. Since $\mathbf{Z}_p$ is compact and f is continuous, f is bounded. Thus we can find a sufficiently large integer $\alpha > 0$ such that $p^\alpha f$ has values in $\mathcal{O}_p$ on $\mathbf{Z}_p$. Then we apply the result already proven for $A = \mathcal{O}_p$ to $p^\alpha f$ and recover the result for general A.

We write $\mathcal{C}(\mathbf{Z}_p;A)$ for the space of continuous functions on $\mathbf{Z}_p$ having values in A. Since $\mathbf{Z}_p$ is compact, for $f \in \mathcal{C}(\mathbf{Z}_p;A)$, $f(\mathbf{Z}_p)$ is a compact subset of A [Bour2, I.9.4] and hence is bounded. Thus the uniform norm $|f|_p = \mathrm{Sup}_{x\in \mathbf{Z}_p}|f(x)|_p$ is a well defined real number. This norm satisfies the strong triangle inequality. Since the uniform limit of continuous functions is again continuous, the A-module $\mathcal{C}(\mathbf{Z}_p;A)$ is complete under this norm (i.e. it is a Banach A-module).

Corollary 1. *We have* $|f|_p = \mathrm{Sup}_n |a_n(f)|_p$ *for* $f \in \mathcal{C}(\mathbf{Z}_p;A)$.

Proof. By definition of $a_n(f)$, we have

$$|a_n(f)|_p = \left|\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(k)\right|_p \le |f|_p.$$

On the other hand, for each $x \in \mathbf{Z}_p$

$$|f(x)|_p = \left|\lim_{m\to\infty}\sum_{n=0}^{m} a_n(f)\binom{x}{n}\right|_p = \lim_{m\to\infty}\left|\sum_{n=0}^{m} a_n(f)\binom{x}{n}\right|_p \le \mathrm{Sup}_n |a_n(f)|_p.$$

This shows that $|f|_p \le \mathrm{Sup}_n |a_n(f)|_p$ and the result.

§3.3. p-adic measures on $\mathbf{Z}_p$

In this section, we introduce the theory of p-adic measures supported on $\mathbf{Z}_p$. In later sections, we generalize this notion to measures on arbitrary profinite groups. The theory of p-adic measures was initiated by B. Mazur in the 70's in order to construct p-adic standard L-functions for the algebraic group GL(2) ([Mz1] and [MzS]). Increasingly the usefulness of the theory is recognized by every mathematician working with p-adic L-functions because of its conciseness and its relevance to the Iwasawa theory.

Let A be a closed subring of F_p. An A-linear map $\varphi : \mathcal{C}(\mathbf{Z}_p;A) \to A$ is called a bounded p-adic measure if there exists a constant $B \geq 0$ such that $|\varphi(\phi)|_p \leq B|\phi|_p$ for all $\phi \in \mathcal{C}(\mathbf{Z}_p;A)$. Let $\mathcal{M}eas(\mathbf{Z}_p;A)$ be the space of all bounded p-adic measures on $\mathbf{Z}_p$ having values in A. Then we can define the uniform norm on $\mathcal{M}eas(\mathbf{Z}_p;A)$ by

$$|\varphi|_p = \mathrm{Sup}_{|\phi|_p=1}|\varphi(\phi)|_p = \mathrm{Sup}_{\phi\neq 0}(|\varphi(\phi)|_p/|\phi|_p).$$

Obviously, $\mathcal{M}eas(\mathbf{Z}_p;A)$ is a p-adic Banach A-module under this norm. In particular, if ϕ_m converges uniformly to ϕ as $m \to \infty$, we see that

$$|\varphi(\phi_m)-\varphi(\phi)|_p \leq |\varphi|_p|\phi_m-\phi|_p$$

and thus $\lim_{n\to\infty}\varphi(\phi_m) = \varphi(\phi)$. We sometimes write $\varphi(\phi)$ as $\int\phi d\varphi = \int_{Z_p}\phi d\varphi$. Since each continuous function ϕ has a unique expansion into an interpolation series $\phi(x) = \sum_{n=0}^{\infty}a_n(\phi)\binom{x}{n}$ by Mahler's theorem (Theorem 2.1) with $a_n(\phi) \in A$ satisfying $\lim_{n\to\infty}a_n(\phi) = 0$ and since $\phi_m = \sum_{n=0}^{m}a_n(\phi)\binom{x}{n}$ converges to ϕ uniformly, we know that

$$\int\phi d\varphi = \lim_{m\to\infty}\int\phi_m d\varphi = \lim_{m\to\infty}\sum_{n=0}^{m}a_n(\phi)\int\binom{x}{n}d\varphi = \sum_{n=0}^{\infty}a_n(\phi)\int\binom{x}{n}d\varphi.$$

Thus the measure φ is determined by the sequence of numbers

$$\{\int\binom{x}{n}d\varphi \mid n \in \mathbf{N}\} \subset A.$$

This sequence of numbers is bounded because

$$|\int\binom{x}{n}d\varphi|_p \leq |\varphi|_p|\binom{x}{n}|_p \leq |\varphi|_p.$$

Conversely if a sequence of bounded p-adic numbers b_n in A is given, the infinite sum $\sum_{n=0}^{\infty}b_na_n(\phi)$ converges absolutely because of the strong triangle inequality (1.3.1) and $\lim_{n\to\infty}a_n(\phi) = 0$. Thus we can define a measure φ by

$$\int \phi d\varphi = \sum_{n=0}^{\infty} b_n a_n(\phi).$$

Note that

$$\left|\int \phi d\varphi\right|_p = \left|\sum_{n=0}^{\infty} b_n a_n(\phi)\right|_p = \lim_{m\to\infty} \left|\sum_{n=0}^{m} b_n a_n(\phi)\right|_p$$
$$\leq \max_n |b_n a_n(\phi)|_p \leq (\mathrm{Sup}_n |b_n|_p)|\phi|_p \text{ by Corollary 2.1.}$$

Thus φ is a bounded measure having values in A and

$$|\varphi|_p \leq \mathrm{Sup}_n |b_n|_p.$$

Since $\binom{n}{n} = 1$, $\left|\binom{x}{n}\right|_p = 1$, and thus we conclude from $\int \binom{x}{n} d\varphi = b_n$ that $|\varphi|_p \geq |b_n|_p$ for all n. This shows that $|\varphi|_p = \mathrm{Sup}_n |b_n|_p$. We have proven the following fact noted by Katz:

Theorem 1. *Given a bounded sequence* $\{b_n\}$ *of numbers in* A, *we can define uniquely a bounded* p-*adic measure* φ *satisfying* $\int \binom{x}{n} d\varphi = b_n$ *for all* n *by*

$$\int \phi d\varphi = \sum_{n=0}^{\infty} b_n a_n(\phi)).$$

All bounded measures on $\mathbf{Z}_p$ *are obtained in this way. Moreover we have*

$$|\varphi|_p = \mathrm{Sup}_n |b_n|_p.$$

Since $\binom{x}{n}$ is a polynomial of x with coefficients in $\mathbf{Q}$, the value $\int \binom{x}{n} d\varphi$ is uniquely determined by the values of $\int x^m d\varphi$ for all $m \geq 0$. Thus we record

Corollary 1. *Each bounded* p-*adic measure having values in* A *is uniquely determined by its values at all monomials* x^m $(m = 0,1,2,\cdots)$.

We should remark that the measure corresponding to an arbitrarily assigned bounded sequence of b_n is not necessarily bounded: for example, if we assign the value of a measure φ by

$$\int x^m d\varphi = \begin{cases} 1 & \text{if } m = 1, \\ 0 & \text{otherwise,} \end{cases}$$

then we see easily that $\int \binom{x}{p^n} d\varphi = \dfrac{(-1)^{p^n-1}}{p^n}$ and thus, φ is no longer bounded.

Exercise 1. Give a detailed proof of the above fact.

If we assign the value a^m to $\int x^m d\varphi$ for $a \in \mathbf{Z}_p$, then naturally $\int \binom{x}{n} d\varphi = \binom{a}{n} \in$ A, whose absolute value is bounded by 1. Thus in this case, the desired bounded measure exists and is called the Dirac measure at a (i.e. the evaluation of functions at a).

Exercise 2. Suppose that $\int f(x+y)d\varphi(x) = \int f(x)d\varphi(x)$ for all $y \in \mathbf{Z}_p$ and $f \in \mathcal{C}(\mathbf{Z}_p;A)$. Show that $\varphi = 0$ if φ is a bounded measure.

§3.4. The p-adic measure of the Riemann zeta function

Let $\zeta(s)$ ($s \in \mathbf{C}$) be the Riemann zeta function defined in §2.1. We already know that $\zeta(-m) \in \mathbf{Q}$ for $m \in \mathbf{N}$. In this section, for each positive integer $a \geq 2$ prime to p, we show the existence of a p-adic bounded measure ζ_a on $\mathbf{Z}_p$ having values in $\mathbf{Z}_p$ such that

$$\int x^m d\zeta_a = (1-a^{m+1})\zeta(-m) \quad \text{for all } m \in \mathbf{N}.$$

If such a measure exists, it is unique by Corollary 3.1.

As in §2.1, for the function $\xi : \mathbf{Z} \to \mathbf{Z}$ given by

$$\xi(n) = \begin{cases} 1 & \text{if } n \not\equiv 0 \bmod a, \\ 1-a & \text{if } n \equiv 0 \bmod a, \end{cases}$$

we consider the function

$$\text{(1a)} \qquad \Psi(t) = \frac{-\sum_{b=1}^{a}\xi(b)(1+t+t^2+\cdots+t^{b-1})}{1+t+t^2+\cdots+t^{a-1}} = \frac{\sum_{b=1}^{a}\xi(b)t^b}{1-t^a}$$

Then by Theorem 2.1.1, we have

$$\text{(1b)} \qquad (1-a^{m+1})\zeta(-m) = \left(t\frac{d}{dt}\right)^m \Psi(t)\Big|_{t=1}.$$

In order to show the existence of the measure ζ_a, writing $\binom{x}{n} = \sum_{k=0}^{n} c_{n,k}x^k$ with $c_{n,k} \in \mathbf{Q}$, we need to prove that, for all $n \in \mathbf{N}$,

$$\left|\int\binom{x}{n}d\zeta_a\right|_p = \left|\sum_{m=0}^{n} c_{n,m}(1-a^{m+1})\zeta(-m)\right|_p = \left|\partial_n\Psi(t)\Big|_{t=1}\right|_p \leq 1,$$

where we write, as a differential operator,

$$\partial_n = \sum_{m=0}^{n} c_{n,m}\left(t\frac{d}{dt}\right)^m = \binom{t\frac{d}{dt}}{n}.$$

To show this boundedness, we prepare with two lemmas:

Lemma 1. *We have* $\partial_n = \frac{t^n}{n!}\frac{d^n}{dt^n}$.

Proof. The assertion is clear for $n = 0$ and 1. We prove the assertion in general by induction on n. Thus, assuming the above formula is true for n, we compute ∂_{n+1}. An easy computation using the definition of the binomial polynomial shows that

$$\binom{x}{n+1} = \frac{(x-n)}{(n+1)!}n!\binom{x}{n}.$$

Then we see that

$$\partial_{n+1}f = \frac{1}{(n+1)!}(t\frac{d}{dt} - n)(t^n\frac{d^nf}{dt^n}) = \frac{1}{(n+1)!}(t^{n+1}\frac{d^{n+1}f}{dt^{n+1}}),$$

which proves the assertion.

By Leibniz's formula, we see that

$$\frac{d^n(fg)}{dt^n} = \sum_{r=0}^{n} \binom{n}{r}\frac{d^rf}{dt^r}\frac{d^{n-r}g}{dt^{n-r}}.$$

Multiplying both sides of the above formula by $t^n/n!$, we get

$$\partial_n(fg) = \sum_{r=0}^{n} (\partial_r f)(\partial_{n-r}g). \tag{2}$$

Lemma 2. *Let* $R' = \{\frac{P(t)}{Q(t)} \mid P(t), Q(t) \in \mathbf{Z}_p[t]$ and $|Q(1)|_p = 1\}$. *Then* R' *is a ring and is stable under* ∂_n *for all* n.

Proof. Taking $\frac{P}{Q}$ and $\frac{P'}{Q'}$ from R', we have

$$\frac{P}{Q} \pm \frac{P'}{Q'} = \frac{PQ' \pm P'Q}{QQ'} \in R' \text{ and } \frac{P}{Q} \times \frac{P'}{Q'} = \frac{PP'}{QQ'} \in R',$$

which shows that R' is a ring. We now show $R' \supseteq \partial_n R'$ by induction on n. When $n = 1$, we see that

$$\partial_1\frac{P}{Q} = \frac{t\frac{dP}{dt}Q - Pt\frac{dQ}{dt}}{Q^2},$$

which shows the result. Now assuming the result is true for ∂_m for $m \leq n-1$, we shall show $R' \supseteq \partial_n R'$. Applying (2) for $f = Q$ and $g = Q^{-1}$ with $P/Q \in R'$, we have $\sum_{r=0}^{n}(\partial_r Q)(\partial_{n-r}Q^{-1}) = 0$. Since $\partial_0 Q = Q$, we have

$$\partial_n(Q^{-1}) = -Q^{-1}\sum_{r=1}^{n}\partial_r Q\partial_{n-r}(Q^{-1}).$$

By the induction hypothesis, $\partial_{n-r}(Q^{-1}) \in R'$ for $r \geq 1$. Since R' is a ring containing $\mathbf{Z}_p[t] \ni \partial_r Q$, the above formula shows that $\partial_n(Q^{-1}) \in R'$. Then again by (2), we have

$$\partial_n(\frac{P}{Q}) = \frac{\partial_n P}{Q} + \partial_{n-1}P\partial_1(Q^{-1}) + \cdots + \partial_1 P\partial_{n-1}(Q^{-1}) + P\partial_n(Q^{-1}).$$

Since $\partial_n(Q^{-1}) \in R'$, again by induction assumption, we see that $\partial_n(\frac{P}{Q}) \in R'$.

We are now ready to prove

Theorem 1. *Let* $a \in \mathbf{N}$ *with* $a \geq 2$ *and* $(a,p) = 1$. *Then there exists a unique bounded* p*-adic measure* ζ_a *on* $\mathbf{Z}_p$ *having values in* $\mathbf{Z}_p$ *such that*

$$\int x^m d\zeta_a = (1-a^{m+1})\zeta(-m) \text{ for all } m \in \mathbf{N}.$$

Proof. As already remarked, we only need to prove

$$\left|\int \binom{x}{n} d\zeta_a\right|_p = \left|\partial_n \Psi(t)|_{t=1}\right|_p \leq 1.$$

By definition, we see that

$$\Psi(t) = \frac{-\sum_{b=1}^{a} \xi(b)(1+t+t^2+\cdots+t^{b-1})}{1+t+t^2+\cdots+t^{a-1}}$$

and hence $\Psi \in R'$. Thus by Lemma 2, we see that $\partial_n \Psi \in R'$. This implies $\partial_n \Psi = \frac{P}{Q}$ for $P, Q \in \mathbf{Z}_p$ with $|Q(1)|_p = 1$. Thus we see that $P(1) \in \mathbf{Z}_p$ and

$$\left|\int \binom{x}{n} d\zeta_a\right|_p = \left|\partial_n \Psi(t)|_{t=1}\right|_p = \frac{|P(1)|_p}{|Q(1)|_p} \leq 1.$$

§3.5. p-adic Dirichlet L-functions

Since the absolute value $|\ |_p$ is an ultra metric (i.e. a metric satisfying the strong triangle inequality (1.3.1)), $\mathbf{Z}_p$ is totally disconnected (i.e. $\mathbf{Z}_p$ is a disjoint union of arbitrarily small open sets). In fact, if we write

$$D(x,p^{-r}) = \{y \in \mathbf{Z}_p \mid |y-x|_p \leq p^{-r}\} = \{y \in \mathbf{Z}_p \mid |y-x|_p < p^{-r+1}\},$$

this is an open set and $\mathbf{Z}_p = \coprod_{x=1}^{p^r} D(x,p^{-r})$ (disjoint union), because

$$D(x,p^{-r}) = \{y \in \mathbf{Z}_p \mid y \equiv x \bmod p^r\mathbf{Z}_p\}.$$

By this, there exist locally constant but non-constant continuous functions. We compute in this section the integral of such functions with respect to $d\zeta_a$.

It is clear from the argument in §3.4 that to each $F(t) \in R'$, we can associate a p-adic measure μ_F on $\mathbf{Z}_p$ with values in $\mathbf{Z}_p$ in the same way:

(1a) $$\int\binom{x}{n}d\mu_F = (\partial_n F)(1) = \frac{1}{n!}\frac{d^nF}{dt^n}(1) \quad \text{for all } n \in \mathbf{N}.$$

Now expanding F into its Taylor expansion around $t = 1$, we see that

$$F(t) = \sum_{n=0}^{\infty} \frac{1}{n!}\frac{d^nF}{dt^n}(1)T^n = \sum_{n=0}^{\infty} \left(\int\binom{x}{n}d\mu_F(x)\right)T^n \quad (\text{for } T = t-1).$$

In this way, we can embed R' into $\mathbf{Z}_p[[T]]$. Conversely if a p-adic measure φ on $\mathbf{Z}_p$ having values in $\mathbf{Z}_p$ is given, then we can define the corresponding power series $\Phi_\varphi(t)$ by

$$\Phi_\varphi(t) = \sum_{n=0}^{\infty} \left(\int\binom{x}{n}d\varphi(x)\right)T^n \quad (T = t-1).$$

By Theorem 4.1, the measure φ is determined by the power series Φ_φ. Thus the map $\varphi \mapsto \Phi_\varphi$ induces an isomorphism: $\mathcal{M}eas(\mathbf{Z}_p;\mathbf{Z}_p) \cong \mathbf{Z}_p[[T]]$. Choosing a basis $\{w_1,\ldots, w_r\}$ of $\mathcal{O}_p$ over $\mathbf{Z}_p$, for each measure φ in $\mathcal{M}eas(\mathbf{Z}_p,\mathcal{O}_p)$ and for $\phi \in \mathcal{C}(\mathbf{Z}_p;\mathcal{O}_p)$, we can write $\varphi(\phi) = \varphi_1(\phi)w_1+\cdots+\varphi_r(\phi)w_r$. Then it is plain that $\varphi_i \in \mathcal{M}eas(\mathbf{Z}_p;\mathbf{Z}_p)$. Thus we know that

$$\mathcal{M}eas(\mathbf{Z}_p;\mathcal{O}_p) \cong \mathcal{M}eas(\mathbf{Z}_p;\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathcal{O}_p.$$

Thus we know that

(1b) the map $\varphi \mapsto \Phi_\varphi$ induces an isomorphism: $\mathcal{M}eas(\mathbf{Z}_p;\mathcal{O}_p) \cong \mathcal{O}_p[[T]]$.

Exercise 1. Show $\int x^m d\varphi = (t\frac{d}{dt})^m\Phi_\varphi|_{T=0}$ $(T = t-1)$ for all $m \in \mathbf{N}$.

When $|y|_p < 1$ $(y \in \mathcal{O}_p)$, the following infinite sum is convergent:

$$(1+y)^x = \sum_{n=0}^{\infty} \binom{x}{n}y^n \quad \text{for } x \in \mathbf{Z}_p.$$

Thus we define the p-adic power y^x $(x \in \mathbf{Z}_p)$, when $|y-1|_p < 1$, by

(2a) $$y^x = \sum_{n=0}^{\infty} \binom{x}{n}(y-1)^n \quad \text{for } x \in \mathbf{Z}_p.$$

This definition coincides with the definition given in §1.3 because the two definitions coincide with each other if x is a positive integer. It is easy to check that the usual exponent rules hold: $y^{x+z} = y^xy^z$, $y^xz^x = (yz)^x$ and $y^0 = 1$ because of the density of $\mathbf{N}$ in $\mathbf{Z}_p$. Using this trick, we know that

(2b) $$\int y^x d\varphi(x) = \sum_{n=0}^{\infty} \int\binom{x}{n}d\varphi(y-1)^n = \Phi_\varphi(y) \quad \text{for } y \in \mathcal{O}_p \text{ if } |y-1|_p < 1.$$

Exercise 2. For two measures φ and ψ in $\mathcal{M}eas(\mathbf{Z}_p;\mathcal{O}_p)$, define the convolution product $\varphi*\psi \in \mathcal{M}eas(\mathbf{Z}_p;\mathcal{O}_p)$ of φ and ψ by

$$\int f d(\varphi * \psi) = \iint f(x+y) d\varphi(x) d\psi(y).$$

Show $\Phi_{\varphi*\psi} = \Phi_\varphi \Phi_\psi$ in $\mathcal{O}_p[[T]]$.

The space of measures $\mathcal{M}eas(\mathbf{Z}_p;\mathcal{O}_p)$ is naturally a module over the ring $\mathcal{C}(\mathbf{Z}_p;\mathcal{O}_p)$ in the following way: for $f \in \mathcal{C}(\mathbf{Z}_p;\mathcal{O}_p)$ and $\varphi \in \mathcal{M}eas(\mathbf{Z}_p;\mathcal{O}_p)$,

$$\int \phi d f\varphi = \int \phi(x) f(x) d\varphi(x).$$

We want to determine $\Phi_{f\varphi}$ for some special f supposing the knowledge of Φ_φ. First let us deal with the function $f(x) = z^x$ for $z \in \mathcal{O}_p$ with $|z-1|_p < 1$. By (2b), we see that

$$\Phi_{f\varphi}(y) = \int y^x d f\varphi(x) = \int y^x z^x d\varphi(x) = \int (yz)^x d\varphi(x) = \Phi_\varphi(yz).$$

Thus

(3) *For* $z \in \mathcal{O}_p$ *with* $|z-1|_p < 1$, *we have* $\Phi_{z^x \bullet \varphi}(t) = \Phi_\varphi(zt)$ *in* $\mathcal{O}_p[[t-1]]$.

Let μ_{p^n} be the group of p^n-th roots of unity in an algebraic closure of F_p. Let $K = F_p[\mu_{p^n}]$ be the field extension of F_p obtained by adding all elements in μ_{p^n}. Let R be the integral closure of $\mathcal{O}_p$ in K. Then, as seen in §1.3, there is a unique norm $|\ |_p$ on K extending that on F. Since there are no p power roots of unity except 1 in characteristic p, $\zeta \bmod \mathcal{P} = 1$ for the maximal ideal $\mathcal{P}$. Thus $|\zeta-1|_p < 1$ for any $\zeta \in \mu_{p^n}$ and hence we can think of ζ^x for $x \in \mathbf{Z}_p$. If $x \equiv k \bmod p^n$ for $k \in \mathbf{N}$, we have $\zeta^x = \zeta^k$ because $\zeta^{p^n} = 1$. If $\phi : \mathbf{Z}_p/p^n\mathbf{Z}_p = \mathbf{Z}/p^n\mathbf{Z} \to K$, then

$$\phi(x) = p^{-n} \sum_{\zeta \in \mu_{p^n}} \zeta^x \sum_{b \in \mathbf{Z}/p^n\mathbf{Z}} \phi(b) \zeta^{-b}. \tag{4}$$

This follows from the orthogonality relation

$$\sum_{\zeta \in \mu_{p^n}} \zeta^{x-b} = \begin{cases} p^n & \text{if } x \equiv b \bmod p^n\mathbf{Z}_p, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, applying (3) for $z = \zeta$ and writing

$$[\phi]\Phi(t) = p^{-n} \sum_{b \in \mathbf{Z}/p^n\mathbf{Z}} \phi(b) \sum_{\zeta \in \mu_{p^n}} \zeta^{-b} \Phi(\zeta t) \text{ for } \Phi(t) \in \mathcal{O}_p[[t-1]],$$

we see that, for a locally constant function $\phi \in \mathcal{C}(\mathbf{Z}_p;\mathcal{O}_p)$ factoring through $\mathbf{Z}/p^n\mathbf{Z}$ (i.e. $\phi = \phi' \circ \rho$ for the projection $\rho : \mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$ with $\phi' : \mathbf{Z}/p^n\mathbf{Z} \to \mathcal{O}_p$),

$$\Phi_{\phi\varphi} = [\phi]\Phi_\varphi \text{ for } \varphi \in \mathcal{M}eas(\mathbf{Z}_p;\mathcal{O}_p) \text{ and} \tag{5}$$
$$\int \phi(x) x^m d\varphi(x) = (t\frac{d}{dt})^m ([\phi]\Phi_\varphi)|_{t=1}.$$

Here note that $[\phi]\Phi_\varphi$ actually belongs to $\mathcal{O}_p[[t-1]]$ because of (5), although this fact is not *a priori* clear from the definition of $[\phi]\Phi_\varphi$. Note that

(6a) $$[\phi](t^m) = \phi(m)t^m \text{ and } [\phi]t\frac{d}{dt}\Phi = t\frac{d}{dt}[\phi]\Phi$$

(6b) if $\Phi(\zeta t) = \Phi(t)$ for all $\zeta \in \mu_{p^n}$, then $[\phi](\Phi\Theta) = ([\phi]\Theta)\Phi$,

where Φ, $\Theta \in \mathcal{O}_p[[t-1]]$. In fact,

$$\begin{aligned}[\phi]t^m &= p^{-n}\sum_{b\in \mathbf{Z}/p^n\mathbf{Z}}\phi(b)\sum_{\zeta\in\mu_{p^n}}\zeta^{-b}(\zeta t)^m \\ &= p^{-n}\sum_b\phi(b)t^m\sum_{\zeta\in\mu_{p^n}}\zeta^{m-b} = \phi(m)t^m,\end{aligned}$$

where we have again used the orthogonality relation. Since $t\frac{d}{dt}t^m = mt^m$, the second formula of (6a) is obvious from the first. As for (6b), we compute

$$\begin{aligned}[\phi](\Phi\Theta) &= p^{-n}\sum_{b\in \mathbf{Z}/p^n\mathbf{Z}}\phi(b)\sum_{\zeta\in\mu_{p^n}}\zeta^{-b}\Phi(\zeta t)\Theta(\zeta t) \\ &= \Phi(t)p^{-n}\sum_{b\in \mathbf{Z}/p^n\mathbf{Z}}\phi(b)\sum_{\zeta\in\mu_{p^n}}\zeta^{-b}\Theta(\zeta t) = \Phi(t)[\phi]\Theta(t).\end{aligned}$$

Exercise 3. Let $R = \left\{ \frac{P(t)}{Q(t)} \,\middle|\, P(t), Q(t) \in \mathbf{Z}_p[t] \text{ and } |Q(1)|_p = 1 \right\}$. Then show that $R \supseteq [\phi]R$ for a locally constant function $\phi : \mathbf{Z}_p \to \mathbf{Z}_p$.

We know from the definition (4.1a) that

(7) $$\Psi(t) = \Phi_{\zeta_a}(t) = \frac{\sum_{b=1}^{a}\xi(b)t^b}{1-t^a} = \frac{t}{1-t} - \frac{at^a}{1-t^a} = t\frac{d}{dt}\left\{\log\frac{1-t^a}{1-t}\right\}.$$

Using the geometric series, we see that $\frac{1}{1-t^a} = 1+t^a+t^{2a}+\cdots+t^{na}+\cdots$. Therefore

$$\Psi(t) = \sum_{m=1}^{\infty}\xi(m)t^m = \sum_{b=1}^{ap^n}\xi(b)t^b\sum_{m=0}^{\infty}t^{ap^n m} = \frac{\sum_{b=1}^{ap^n}\xi(b)t^b}{1-t^{ap^n}}.$$

We put $\Theta(t) = \sum_{b=1}^{ap^n}\xi(b)t^b$ and $\Phi = 1/(1-t^{ap^n})$. Then we have $\Psi = \Phi\Theta$ and

$$[\phi]\Theta = \sum_{b=1}^{ap^n}\xi(b)\phi(b)t^b \text{ by (6a).}$$

By (6b)

$$[\phi]\Psi = \Phi[\phi]\Theta = \sum_{m=1}^{\infty}\xi(m)\phi(m)t^m = \sum_{m=1}^{\infty}\phi(m)t^m - a\sum_{m=1}^{\infty}\phi(am)t^{am}.$$

Writing $\phi_a(m) = \phi(am)$ and supposing ϕ actually has values in $F\cap\mathcal{O}_p$ (and hence has values in $\mathbf{C} \supset F$), we can consider the complex L-function

$$L(s,\phi\text{-}a^{k+1}\phi_a) = \sum_{n=1}^{\infty} (\phi(n)\text{-}a^{k+1}\phi_a(n))n^{-s}.$$

As seen in §§2.1-3, this sum is convergent in $\mathbf{C}$ if $\mathrm{Re}(s) > 1$ and has a meromorphic continuation to the whole complex plane, and

$$L(-m,\phi\text{-}a^{m+1}\phi_a) = (t\tfrac{d}{dt})^m([\phi]\Psi)\,|_{t=1} = \int\phi(x)x^m d\zeta_a.$$

If χ is a character of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ having values in $F^\times$, extending χ by 0 on $\mathbf{Z}_p\text{-}\mathbf{Z}_p^\times$ and denoting this function by the same symbol χ, we have a locally constant function χ on $\mathbf{Z}_p$. Then

$$L(-m,\chi\text{-}a^{m+1}\chi_a) = (1\text{-}a^{m+1}\chi(a))(1\text{-}\chi_0(p)p^m)L(-m,\chi_0),$$

where $\chi_0 = \chi$ if χ is non-trivial and χ_0 is the constant function on $\mathbf{Z}_p$ having value 1 if χ is trivial. Thus we have proven the first part of

Theorem 1. *If* $\chi : (\mathbf{Z}/p^n\mathbf{Z})^\times \to F^\times$ *is a primitive character (when* χ *is trivial, we agree to put* $n = 0$*), then*

$$\int\chi(x)x^m d\zeta_a(x) = (1\text{-}a^{m+1}\chi(a))(1\text{-}\chi_0(p)p^m)L(-m,\chi_0) \text{ for all } m \in \mathbf{N}.$$

If χ *is an even character* χ *(i.e.* $\chi(-1) = 1$*),*

$$\int\chi(x)x^{-1}d\zeta_a(x) = \begin{cases} (1-p^{-1})\log(a) & \text{if } \chi = \mathrm{id}, \\ -(1\text{-}\chi(a))p^{-n}G(\chi)\Sigma_{b\in(\mathbf{Z}/p^n\mathbf{Z})^\times}\chi^{-1}(b)\log(1\text{-}\zeta^b) & \text{if } \chi \neq \mathrm{id}, \end{cases}$$

where $G(\chi) = \Sigma_{b=1}^{p^n}\chi(b)\zeta^b$ (the formula is independent of the choice of ζ).

To finish the proof of the above theorem, we need to compute $\int\chi(x)x^{-1}d\zeta_a(x)$. By Corollary 2.3.2, if $\chi(-1) = -1$, the integral is identically 0 and is not included in the theorem. Thus we assume that χ is even. We first assume that $|a\text{-}1|_p < 1$. Writing $\Phi(t) = \log\left\{\frac{1-t^a}{1-t}\right\}$, we can expand it formally as a power series in $T = t\text{-}1$ in $\mathbf{Q}_p[[T]]$ because $\left\{\frac{1-t^a}{1-t}\right\}\Big|_{t=1} = a$, which is in the domain of convergence of the p-adic logarithm. Write this power series as Φ. Then inside $\mathbf{Q}_p[[t\text{-}1]]$, we have from (6a) and (7) that $[\chi]\Psi = t\frac{d}{dt}[\chi]\Phi = (1+T)\frac{d}{dT}[\chi]\Phi$. On the other hand, since χ is supported on $\mathbf{Z}_p^\times$, the function $x \mapsto x^{-1}\chi(x)$ is a continuous function on $\mathbf{Z}_p$. Thus we may consider the measure φ given by

$$\int\phi d\varphi = \int\phi(x)x^{-1}\chi(x)d\zeta_a(x) \text{ for all } \phi \in C(\mathbf{Z}_p;O_p).$$

By the definition of $\Phi_\varphi \in O_p[[T]]$, we know that $\Phi_{x\varphi} = t\frac{d\Phi_\varphi}{dt}$. Therefore we see that $(1+T)\frac{d}{dT}\Phi_\varphi = [\chi]\Psi$. Thus $\Phi_\varphi - [\chi]\Phi \in F_p$ because $\mathrm{Ker}((1+T)\frac{d}{dT})$ in $F_p[[T]]$ consists of constants. By (6a), the operation $[\chi]$ kills constant functions, and for the identity character id, $[\mathrm{id}]\Phi_\varphi = \Phi_\varphi$ and $[\mathrm{id}][\chi] = [\chi]$. This implies $\Phi_\varphi = [\chi]\Phi$. Therefore

$$\int x^{-1}\chi(x)d\zeta_a(x) = [\chi]\Phi(1) = p^{-n}\sum_{b\in \mathbf{Z}/p^n\mathbf{Z}}\chi(b)\sum_{\zeta\in\mu_{p^n}}\zeta^{-b}\Phi(\zeta).$$

Now suppose that $\chi|_{1+p^{n-1}\mathbf{Z}_p} \neq 1$ (i.e. χ is primitive modulo p^n). Then by Lemma 2.3.2, we see, writing $\zeta = e(\frac{-c}{p^n})$, that

$$\sum_{b\in \mathbf{Z}/p^n\mathbf{Z}}\chi(b)\zeta^{-b} = \chi^{-1}(c)G(\chi).$$

Therefore $[\chi]\Phi(1) = p^{-n}G(\chi)\sum_{c\in(\mathbf{Z}/p^n\mathbf{Z})^\times}\chi^{-1}(c)\Phi(\zeta^{-c})$ for $\zeta = e(\frac{1}{p^n})$. When χ is the trivial character, we see that

$$\sum_{b\in \mathbf{Z}/p\mathbf{Z}}\chi(b)\zeta^{-b} = \begin{cases} p-1 & \text{if } \zeta = 1, \\ -1 & \text{if } \zeta \neq 1. \end{cases}$$

Using the extended log in (1.3.9b), we can obtain the formula in the theorem when $|a-1|_p < 1$. The formula holds for general a because the p-adic L-function defined below is independent of a.

Let us define p-adic Dirichlet L-functions. Since $\chi(x)$ is only supported on $\mathbf{Z}_p^\times$, we may write

$$\int_{\mathbf{Z}_p^\times}\chi(x)x^m d\zeta_a(x) = (1-a^{m+1}\chi(a))(1-\chi_0(p)p^m)L(-m,\chi_0) \quad \text{for all } m\in \mathbf{N}.$$

We can decompose $\mathbf{Z}_p^\times = \mu \times W$ where

$$W = 1+\mathbf{p}\mathbf{Z}_p \quad \text{for } \mathbf{p} = \begin{cases} 4 & \text{if } p = 2, \\ p & \text{otherwise,} \end{cases}$$

and μ is the maximal torsion subgroup of $\mathbf{Z}_p^\times$. Fixing an element $u \in W-(1+p\mathbf{p}\mathbf{Z}_p)$, we have an isomorphism of topological groups $\mathbf{Z}_p \cong W$ given by $\mathbf{Z}_p \ni s \mapsto u^s \in W$. Let $\omega : \mathbf{Z}_p^\times \to \mu$ be the projection map. Thus $\omega(x) = \lim_{n\to\infty} x^{p^n}$ if $p > 2$ and $\omega(x) = \pm 1$ according as $x \equiv \pm 1 \bmod 4\mathbf{Z}_2$ if $p = 2$. This character ω is called tha Teichmüller character. Then we define $\langle x\rangle$ for $x \in \mathbf{Z}_p^\times$ by $\langle x\rangle = \omega(x)^{-1}x$. Then $x \mapsto \langle x\rangle$ is the projection of $\mathbf{Z}_p^\times$ onto W. We then fix a character χ of $(\mathbf{Z}/p^r\mathbf{Z})^\times$ and define the p-adic Dirichlet L-function with character χ by

$$L_p(s,\chi) = (1-\chi(a)\langle a\rangle^{1-s})^{-1}\int_{Z_p^\times}\chi\omega^{-1}(x)\langle x\rangle^{-s}d\zeta_a(x).$$

Then $L_p(s,\chi)$ is a continuous function on $\mathbf{Z}_p$ except when $\chi = \mathrm{id}$, and in this special case, $\zeta_p(s) = L_p(s,\mathrm{id})$ is a continuous function defined on $\mathbf{Z}_p-\{1\}$. Moreover we have the following evaluation formula:

(8) $\quad L_p(-m,\chi) = (1-(\chi\omega^{-m-1})_0(p)p^m)L(-m,(\chi\omega^{-m-1})_0)$ for all $m \in \mathbf{N}$,

where the right-hand side is the value of the complex L-function while the left-hand side is the value of the p-adic L-function and the values are equal in the field F common to F_p and $\mathbf{C}$. Since the right-hand side is independent of the choice of a, we conclude from the density of $\mathbf{N}$ in $\mathbf{Z}_p$ that $L_p(s,\chi)$ is independent of a.

We now show that $L_p(s,\chi)$ is a p-adic analytic function on $\mathbf{Z}_p$ when $\chi \neq \mathrm{id}$ and a p-adic meromorphic function on $\mathbf{Z}_p-\{1\}$ when $\chi = \mathrm{id}$. We can define a p-adic measure $\zeta_{a,\chi}$ on $W\ (\cong \mathbf{Z}_p)$ in the following way. For any given continuous function $\phi : W \to O_p$, we define

$$\int_W\phi(\gamma)d\zeta_{a,\chi}(\gamma) = \int_{Z_p^\times}\chi\omega^{-1}(x)\phi(\langle x\rangle)d\zeta_a(x).$$

Then we can write $L_p(s,\chi) = (1-\chi(a)\langle a\rangle^{1-s})^{-1}\int_W\gamma^s d\zeta_{a,\chi}(\gamma)$. Identifying W with $\mathbf{Z}_p$ via $\iota : \mathbf{Z}_p \ni s \mapsto u^s \in W$, we can associate with χ a power series $\Phi_{a,\chi}(t) \in O_p[[t-1]]$ as in (3) in the following way:

$$(1-\chi(a)\langle a\rangle^{1-s})L_p(s,\chi) = \int_W\gamma^s d\zeta_{a,\chi}(\gamma) = \int_{Z_p}u^{-sx}d(\iota^*\zeta_{a,\chi})(x) = \Phi_\varphi(u^{-s}).$$

We define $\Phi_{a,\chi}(t)$ by $\Phi_\varphi(u^{-1}t)$. Then $L_p(1-s,\chi) = (1-\chi(a)\langle a\rangle^s)^{-1}\Phi_{a,\chi}(u^s)$. By (1.3.6a,b), the exponential (resp. the logarithm) function converges on $\mathbf{p}\mathbf{Z}_p$ (resp. W). Thus we can write $u^s = \exp(s\log(u))$. This shows that $L_p(s,\chi)$ is a meromorphic function on $\mathbf{Z}_p$ whose pole comes from the possible zero of $(1-\chi(a)\langle a\rangle^{1-s})$ at $s = 1$. When $\chi(a) \neq 1$, this function $(1-\chi(a)\langle a\rangle^{1-s})$ does not have a zero at $s = 1$ and hence $L_p(s,\chi)$ is an analytic function. Here note that $L_p(s,\chi)$ itself does not depend on the choice of a because of the density of $\mathbf{N}$ in $\mathbf{Z}_p$ and the evaluation formula (8). Since $\mathbf{Z}_p^\times = \mu\times W$ and W is topologically generated by u and μ is cyclic (When $p = 2$, $\mu = \{\pm 1\}$, and when $p > 2$, μ is the group of (p-1)-th roots of unity), we can take a so that $\omega(a)$ generates μ and $\langle a\rangle$ topologically generates W. Then $\chi(a) = 1 \Leftrightarrow \chi = \mathrm{id}$. Thus if $\chi \neq \mathrm{id}$, $L_p(s,\chi)$ is analytic on $\mathbf{Z}_p$. We see that $\langle a\rangle^s = 1+\log(\langle a\rangle)s+$higher terms of s by (1.3.8a,b). This shows that $\zeta_p(s)$ has a simple pole at $s = 1$ whose residue is $(1-p^{-1})$.

Summing up these considerations, we have

Theorem 2. *For each Dirichlet character* $\chi : (\mathbf{Z}/p^r\mathbf{Z})^\times \to F^\times$ *with* $\chi(-1) = 1$, *there exists a* p-*adic analytic function* $L_p(s,\chi)$ *on* $\mathbf{Z}_p$-$\{1\}$ *such that*

$$L_p(-m,\chi) = (1-(\chi\omega^{-m-1})_0(p)p^m)L(-m,(\chi\omega^{-m-1})_0) \text{ for all } m \in \mathbf{N}.$$

When χ *is non-trivial,* $L_p(s,\chi)$ *is analytic even at* $s = 1$ *and*

$$L_p(1,\chi) = -p^{-n}G(\chi)\textstyle\sum_{b\in(\mathbf{Z}/p^n\mathbf{Z})^\times}\chi^{-1}(b)\log(1-\zeta^b).$$

On the other hand, $\zeta_p(s) = L_p(s,\mathrm{id})$ *has a simple pole at* $s = 1$ *whose residue is* $(1-p^{-1})$.

When χ is an odd character (i.e. $\chi(-1) = -1$), then $\chi\omega^{m-1}(-1) = (-1)^m$ because of $\omega(-1) = -1$, and thus $L_p(-m,\chi) = 0$ for all $m \in \mathbf{N}$ by Exercise 2.3.3. This shows that $L_p(s,\chi)$ is identically zero if χ is odd. This is why we excluded the case of odd characters χ. Although non-trivial $L_p(s,\chi)$ exists only for even χ, the values of complex L-functions with odd characters show up as the special values of the p-adic L-function $L_p(s,\chi)$. In fact, when m is even, $\chi\omega^{m-1}$ is an odd character.

§3.6. Group schemes and formal group schemes

In order to give an interpretation of p-adic measure theory on $\mathbf{Z}_p$ using formal multiplicative groups in the next section, we recall here briefly the properties of affine schemes and affine group schemes. For details of the theory, see Mumford's book [Mm1, §11]. Let A be a commutative algebra with identity and R be an A-algebra. We consider the affine scheme $G_{/A} = \mathrm{Spec}(R)_{/A}$. Thus G is a covariant functor from the category $\mathcal{Alg}_{/A}$ of A-algebras to the category of sets given by $G(S) = \mathrm{Hom}_{A\text{-alg}}(R,S)$ for any A-algebra S. For any algebra homomorphism $\varphi : S \to T$, the functorial map $G(\varphi) : G(S) \to G(T)$ is given by $G(\varphi)(\phi) = \varphi\circ\phi$. The set G(S) is called the set of S-valued points (or simply S-points) of G. For two affine schemes G_A and $G'_{/A} = \mathrm{Spec}(R')_{/A}$, a morphism of schemes $f : G \to G'$ is a set of maps $f(S) : G(S) \to G'(S)$ such that for every A-algebra homomorphism $\varphi : S \to T$, the following diagram is commutative:

$$\begin{array}{ccc} G(S) & \xrightarrow{f(S)} & G'(S) \\ \downarrow G(\varphi) & & \downarrow G'(\varphi) \\ G(T) & \xrightarrow[f(T)]{} & G'(T). \end{array}$$

Let $\mathcal{Sch}_{/A}$ be the category of schemes over A [Ha, II]. If $\eta : R' \to R$ is an A-algebra homomorphism, then $\eta^* : G \to G'$ given by $\eta^*(S)(\phi) = \phi\circ\eta$ is obviously a morphism of affine schemes. Conversely if $f : G \to G'$ is a morphism of affine schemes, we in particular have a map $f(R) : G(R) \to G'(R)$. We have two natural maps:

$$\iota : \mathrm{Hom}_{A\text{-alg}}(R',R) \to \mathrm{Hom}_{\mathcal{Sch}}(G,G') \text{ given by } \eta \mapsto \eta^* \text{ and}$$
$$\pi : \mathrm{Hom}_{\mathcal{Sch}}(G,G') \to \mathrm{Hom}_{A\text{-alg}}(R',R) \text{ given by } \pi(f) = f(R)(\mathrm{id}).$$

By definition $\eta^*(R)(\mathrm{id}) = \mathrm{id}\circ\eta = \eta$. Thus $\pi\circ\iota = \mathrm{id}$. Let $\eta = f(R)(\mathrm{id})$ for the identity map $\mathrm{id} \in G(R)$. We want to show $f = \eta^*$ (i.e. $\iota\circ\pi = \mathrm{id}$). We have a commutative diagram (for any map $\phi : R \to S$ of A-algebras):

$$\begin{array}{ccc} G(S) & \xrightarrow{f(S)} & G'(S) \\ \uparrow{\scriptstyle G(\phi)} & & \uparrow{\scriptstyle G'(\phi)} \\ G(R) & \xrightarrow[f(R)]{} & G'(R). \end{array}$$

This implies

$$\eta^*(S)(\phi) = \phi\circ\eta = \phi\circ f(R)(\mathrm{id}) = G'(\phi)\circ f(R)(\mathrm{id}) = f(S)\circ G(\phi)(\mathrm{id}) = f(S)(\phi\circ\mathrm{id}).$$

This shows that

(1) $\qquad \pi : \mathrm{Hom}_{\mathcal{Sch}}(G,G') \cong \mathrm{Hom}_{A\text{-alg}}(R',R)$ by $\pi(f) = f(R)(\mathrm{id})$.

Let $G = \mathrm{Spec}(R)$, $G' = \mathrm{Spec}(R')$ and $S = \mathrm{Spec}(B)$ be (affine) A-schemes and $f : G \to S$ and $g : G' \to S$ be two morphisms of A-schemes. We consider the following universal property for an A-scheme X. Whenever we have a commutative diagram

$$\begin{array}{ccc} T & \xrightarrow{\phi} & G \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle f} \\ G' & \xrightarrow[g]{} & S, \end{array}$$

we have a unique morphism of schemes $h : X \to T$ such that $f\circ\phi\circ h = g\circ\varphi\circ h$ and $p = \phi\circ h$ and $p' = \varphi\circ g$ are independent of φ and ϕ. This universality is the contravariant version of the universal property defining the tensor product $R\otimes_B R'$ (see §1.1). Thus such a universal object X is given by $\mathrm{Spec}(R\otimes_B R')$. We write $X = G\times_S G'$.

Now we suppose that R has the structure of an A-bialgebra; that is, there are three A-algebra homomorphisms

$$m : R \to R\otimes_A R, \quad e : R \to A \quad \text{and} \quad i : R \to R$$

satisfying

(G1) The diagram $\begin{array}{ccc} R & \xrightarrow{m} & R\otimes_A R \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle \mathrm{id}\otimes m} \\ R\otimes_A R & \xrightarrow[m\otimes\mathrm{id}]{} & R\otimes_A R\otimes_A R \end{array}$ is commutative;

(G2) The diagrams
$$\begin{tikzcd} R \arrow[r, "m"] \arrow[dr, "id"'] & R\otimes_A R \arrow[d, "id\otimes e"] \\ & R \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} R \arrow[r, "m"] \arrow[dr, "id"'] & R\otimes_A R \arrow[d, "e\otimes id"] \\ & R \end{tikzcd}$$
are commutative;

(G3) The diagrams
$$\begin{tikzcd} R \arrow[r, "m"] \arrow[d, "e"] & R\otimes_A R \arrow[d, "id\otimes i"] \\ A \arrow[r] \arrow[d] & R\otimes_A R \arrow[d, "\mu"] \\ R \arrow[r, equal] & R \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} R \arrow[r, "m"] \arrow[d, "e"] & R\otimes_A R \arrow[d, "i\otimes id"] \\ A \arrow[r] \arrow[d] & R\otimes_A R \arrow[d, "\mu"] \\ R \arrow[r, equal] & R \end{tikzcd}$$
are commutative,

where $\mu : R\otimes_A R \to R$ is the multiplication: $a\otimes b \mapsto ab$;

(G4) The diagram
$$\begin{tikzcd} R \arrow[r, "m"] \arrow[dr, "m"'] & R\otimes_A R \arrow[d] & \ni x\otimes y \arrow[d, mapsto] \\ & R\otimes_A R & \ni y\otimes x \end{tikzcd}$$
is commutative.

Since
$G\times_A G(S) = \mathrm{Hom}_{A\text{-alg}}(R\otimes_A R,S) = \mathrm{Hom}_{A\text{-alg}}(R,S)\times\mathrm{Hom}_{A\text{-alg}}(R,S) = G(S)\times G(S)$, the morphism m (resp. i) induces $m^* : G(S)\times G(S) \to G(S)$ (resp. $i^* : G(S) \to G(S)$), and $e : R \to A$ induces $e \in G(S)$ by composing the original e with the A-algebra structure: $A \to S$. Writing $x\bullet y \in G(S)$ for $m^*(x,y)$ $(x,y \in G(S))$ and x^{-1} for $i^*(x)$, we know that

$$\text{(i)}\ (x\bullet y)\bullet z = x\bullet(y\bullet z)\ \text{(G1)},\ \text{(ii)}\ x\bullet e = e\bullet x = x\ \text{(G2)},$$
$$\text{(iii)}\ x^{-1}\bullet x = x\bullet x^{-1} = e\ \text{(G3) and (iv)}\ x\bullet y = y\bullet x\ \text{(G4)}.$$

This shows that $G(S)$ is an abelian group. In particular, we have $e = e^{-1} = i^*e = e\circ i$. Thus if R is an A-bialgebra, then G is a functor on $\mathcal{Sch}_{/A}$ having values in the category $\mathcal{Ab}$ of abelian groups. In this case, G is called a commutative group scheme defined over A. When R only satisfies G1-3 but not G4, $G(S)$ is a group (which may not be commutative). In this case, we just call G a group scheme. A morphism of group schemes G and G' is a morphism of schemes which induces a group homomorphism between $G(S)$ and $G'(S)$ for all S. It is easy to check under the isomorphism (1) that such a morphism corresponds to a homomorphism φ of A-bialgebras, i.e., $\varphi : R' \to R$ is a homomorphism of A-algebras which makes the following diagrams commutative: for the morphisms of bialgebras m', e' and i' (resp. m, e and i) for R' (resp. R)

$$\begin{tikzcd} R' \arrow[r, "m'"] \arrow[d, "\varphi"] & R'\otimes_A R' \arrow[d, "\varphi\otimes\varphi"] \\ R \arrow[r, "m"'] & R\otimes_A R, \end{tikzcd} \quad \begin{tikzcd} R' \arrow[r, "e'"] \arrow[d, "\varphi"] & A \arrow[d, equal] \\ R \arrow[r, "e"'] & A \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} R' \arrow[r, "i'"] \arrow[d, "\varphi"] & R' \arrow[d, "\varphi"] \\ R \arrow[r, "i"'] & R. \end{tikzcd}$$

Conversely if a functor $T : \mathcal{Sch}_{/A} \to \mathcal{Ab}$ is given and if $T(S) = \mathrm{Hom}_{A\text{-alg}}(R,S)$ for every A-algebra S, we can define an A-bialgebra structure on R by (1) using the group laws (i)-(iv) above. Thus *any functor from* $\mathcal{Sch}_{/A}$ *to* $\mathcal{Ab}$ *represented by an* A-*bialgebra* R *is in fact a commutative group scheme.* Let $\varphi^* : G \to G'$ be the homomorphism of group schemes induced by $\varphi : R' \to R$. We then consider $R_\varphi = R \otimes_{R'} A = R/\varphi(\mathrm{Ker}(e'))R$, where we regard R (resp. A) as an R'-algebra via φ (resp. e'). Then by the above compatibility of φ with the bialgebra structure, the bialgebra structure (m,e,i) of R induces the bialgebra structure $(m_\varphi, e_\varphi, i_\varphi)$ of R_φ. Thus we have a commutative group scheme $\mathrm{Ker}(\varphi^*) = \mathrm{Spec}(R_\varphi)$. We now have an exact sequence of groups for all S:

$$1 \to \mathrm{Ker}(\varphi^*)(S) \to G(S) \xrightarrow{\varphi^*} G'(S).$$

Exercise 1. (i) Give a detailed proof of the fact that R_φ is an A-bialgebra.
(ii) Prove the above sequence is exact.

Let us now give some of the most important examples of commutative group schemes. Let $A = \mathbf{Z}$ and $R = \mathbf{Z}[t,t^{-1}]$ for an indeterminate t. We define $m : \mathbf{Z}[t,t^{-1}] \to \mathbf{Z}[x,y,x^{-1},y^{-1}] \cong R \otimes_A R$ by $m(t) = xy$, $i : R \to R$ by $i(t) = t^{-1}$ and $e : R \to \mathbf{Z}$ by $e(t) = 1$. Then it is easy to check properties G1-4 and thus R gives a group scheme defined over $\mathbf{Z}$. We write this scheme as $\mathbf{G}_m$ (or GL_1). Any algebra homomorphism of R to a ring S is determined by its value at t. Thus $\mathbf{G}_m(S)$ can be embedded into S. If $x \in \mathbf{G}_m(S)$, then $x(t^{-1}) = x(t)^{-1} \in S$ and therefore $\mathbf{G}_m(S) = S^\times$. If $x,y \in \mathbf{G}_m(S)$, then $x \cdot y(t) = x(t)y(t)$ by definition, and thus $\mathbf{G}_m(S)$ is the multiplicative group $S^\times$ as a group. We consider the endomorphism $[N]_S$ of $\mathbf{G}_m(S)$ given by $[N]_S(s) = s^N$. This is induced by an endomorphism [N] of R taking t to t^N. Then $\mu_N = \mathrm{Ker}([N]) = \mathrm{Spec}(\mathbf{Z}[t]/(t^N-1))$ and hence

$$\mu_N(S) = \{\zeta \in S^\times \mid \zeta^N = 1\}.$$

Let $G_{/A} = \mathrm{Spec}(R)_{/A}$ be a commutative group scheme. We may regard $\phi \in R \otimes_A S$ as a function on G(S) having values in S for any A-algebra S in the following way:

$$\phi(s) = s(\phi) \quad \text{for} \quad s \in G(S) = \mathrm{Hom}_{A\text{-alg}}(R,S) = \mathrm{Hom}_{S\text{-alg}}(R \otimes_A S, S).$$

We then consider the space $\mathrm{Der}_A(G)$ of derivations on R over A having values in R. Thus $\mathrm{Der}_A(G)$ is an R-module of A-linear maps $D : R \to R$ satisfying $D(fg) = fD(g) + gD(f)$. The A-linearity of D is equivalent to the fact that D annihilates A in R. The composition of two derivations is no longer a derivation, but we still can think of the algebra Diff(G) generated by derivations over A in $\mathrm{End}_A(R)$. An element of Diff(G) is called a differential operator on G. A dif-

ferential operator $D : R \to R$ is called invariant if the following diagram commutes:

(2a)
$$\begin{array}{ccc} R & \xrightarrow{D} & R \\ \downarrow m & & \downarrow m \\ R\otimes_A R & \xrightarrow[D\otimes id]{} & R\otimes_A R. \end{array}$$

We write $\mathcal{D}(G)$ for the A-algebra of invariant differential operators. A differential operator D is invariant if and only if for any $\phi \in R$, defining $\phi_x = (id\otimes x)\circ m(\phi) \in R\otimes_A S$ for $x \in G(S) = \mathrm{Hom}_{A\text{-alg}}(R,S)$, we have

(2b) $$D(\phi_x) = (D\phi)_x \text{ for all } x \in G(S) \text{ and all } S_{/A}.$$

In fact, for $y \in G(S)$,

$$\phi_x(y) = (y\otimes id)\circ(id\otimes x)\circ m(\phi) = (y\otimes x)\circ m(\phi) = \phi(y\cdot x).$$

Thus ϕ_x as a function on $G(S)$ is the right translation of ϕ. Thus it is legitimate to call D invariant if (2b) holds for all S and all x. Let us prove the equivalence of the conditions (2a) and (2b). The commutativity of (2a) implies

$$D(\phi_x) = (D\otimes id)((id\otimes x)\circ m(\phi)) = (id\otimes x)\circ(D\otimes id)\circ m(\phi) = (id\otimes x)\circ m(D\phi) = (D\phi)_x.$$

Conversely if the above identity (2b) is true for all x, then it is obvious from (1) that the diagram (2a) is commutative and D is invariant. We write $\mathcal{L}ie_A(G)$ for the space of invariant derivations on $G_{/A}$. If D is a derivation on $\mathbf{G}_{m/\mathbf{Z}}$ over $\mathbf{Z}$, it is determined by its value at t (because $R = \mathbf{Z}[t,t^{-1}]$). On the other hand, $D' = D(t)\frac{d}{dt}$ is a derivation satisfying $D'(t) = D(t)$. This shows

$$\mathrm{Der}_{\mathbf{Z}}(\mathbf{G}_m) = R\frac{d}{dt} \text{ and } \mathrm{Der}_{\mathbf{Z}}(\mathbf{G}_{m/\mathbf{Z}})\otimes_{\mathbf{Z}}\mathbf{C} = \mathrm{Der}_{\mathbf{C}}(\mathbf{G}_{m/\mathbf{C}}),$$

and thus $\mathcal{L}ie_{\mathbf{Z}}(\mathbf{G}_m)$ injects into $\mathcal{L}ie_{\mathbf{C}}(\mathbf{G}_m)$. Since a $\mathbf{G}_m$-invariant first order differential operator on $\mathbf{G}_m(\mathbf{C}) = \mathbf{C}^\times$ in $\mathbf{C}[t,t^{-1}]\frac{d}{dt}$ is, by (2b), a constant multiple of $t\frac{d}{dt} = \frac{d}{d\log(t)}$, we know that $\mathcal{L}ie_{\mathbf{Z}}(\mathbf{G}_m) = \mathbf{Z}t\frac{d}{dt}$. Thus

(3a) $$\mathrm{Der}_{\mathbf{Z}}(\mathbf{G}_m) = R\frac{d}{dt},\ \mathcal{L}ie_{\mathbf{Z}}(\mathbf{G}_m) = \mathbf{Z}t\frac{d}{dt} \text{ and } \mathcal{D}(\mathbf{G}_m)\otimes_{\mathbf{Z}}\mathbf{Q} = \mathbf{Q}[t\tfrac{d}{dt}].$$

A polynomial on $\mathbf{Z}$ is called *numerical* if $P(n) \in \mathbf{Z}$ for all $n \in \mathbf{N}$. We know from Proposition 1.1 that the binomial polynomial gives a basis over $\mathbf{Z}$ of the ring of numerical polynomials. Thus we have by (3a) that

(3b) $$\mathcal{D}(\mathbf{G}_m) = \{P(t\tfrac{d}{dt}) \mid P(T) \text{ is a numerical polynomial}\} = \mathbf{Z}[\partial_n]_{n\in\mathbf{Z}},$$

where ∂_n is the differential operator in Lemma 4.1. Writing $D_P = P(t\frac{d}{dt})$, we see easily that D_P is characterized by the fact $D_P(t^m) = P(m)t^m$.

We consider in this note a group scheme a little more general than $\mathbf{G}_m$. Let M be a free $\mathbf{Z}$-module of finite rank. We consider the group algebra $R = \mathbf{Z}[M]$. Thus R is a commutative ring generated by a $\mathbf{Z}$-free basis t^α for $\alpha \in M$ ($t^0 = 1$) and $t^\alpha t^\beta = t^{\alpha+\beta}$. When $M = \mathbf{Z}$ as an additive group, $R = \mathbf{Z}[t,t^{-1}]$. Note that any algebra homomorphism $\lambda : \mathbf{Z}[M] \to S$ is determined by its value at t^{α_i} for a basis $\{\alpha_i\}$ of M. Since t^{α_i} is invertible in $\mathbf{Z}[M]$, $\lambda(t^{\alpha_i})$ has to have values in $S^\times$. Thus, writing T for $\mathrm{Spec}(\mathbf{Z}[M])$, we know that

(3c) $\quad T(S) = \mathrm{Hom}_{A\text{-alg}}(\mathbf{Z}[M],S) = \mathrm{Hom}_{gr}(M,S^\times) = \mathrm{Hom}_{gr}(M,\mathbf{G}_m(S))$.

Thus as a functor, we know that $T = \mathrm{Hom}_{gr}(M,\mathbf{G}_m)$. Since T is a group functor, by (1), T is an affine group scheme.

Exercise 2. Make explicit the bialgebra structure of $\mathbf{Z}[M]$.

If we identify M with $\mathbf{Z}^r$ choosing a basis $\{\alpha_i\}$, we have an isomorphism

$$\mathbf{Z}[M] \cong \mathbf{Z}[t^{\alpha_1},t^{-\alpha_1},\ldots,t^{\alpha_r},t^{-\alpha_r}] \cong \otimes_i \mathbf{Z}[t^{\alpha_i},t^{-\alpha_i}].$$

This shows that $T \cong \mathbf{G}_m{}^r$ non-canonically. We call a rational polynomial P on M *numerical* if $P(\alpha) \in \mathbf{Z}$ for all $\alpha \in M$. Then by (3b), we see that

(3d) $$\mathcal{D}(T) \cong \{D_P \mid P \text{ is a numerical polynomial on } M\},$$

where D_P is the invariant differential operator on T given by

$$D_P(t^\alpha) = P(\alpha)t^\alpha \quad \text{for all } \alpha \in M.$$

Let K be a finite extension of $\mathbf{Q}_p$, and assume A to be the p-adic integer ring of K. Hereafter, we always consider T to be defined over A. Thus we change the notation and write hereafter R for the coordinate ring $A[M]$ of T over A. For each integer N, we define the endomorphism $[N]$ which takes $x \in T(S)$ to $x^N \in T(S)$. Then as a group subscheme of T, we define $T_N = \mathrm{Ker}[N]$ in T. Then $T_N = \mathrm{Spec}(R_N)$ for $R_N = \mathbf{Z}[M/NM] = \otimes_i A[t^{\alpha_i},t^{-\alpha_i}]/(t^{N\alpha_i}-1)$, and we see that

(4) $\quad T_N(S) = \mathrm{Hom}_{A\text{-alg}}(A[M/NM],S) = \mathrm{Hom}_{\mathbf{Z}}(M/NM,\mu_N(S))$ for all S.

We now restrict the category on which the group functor T is defined. Let $\mathcal{A}d = \mathcal{A}d_{/A}$ be the category of A-algebras $S = \varprojlim_\alpha (S/p^\alpha S)$ for the maximal ideal p of A. Let $\mathcal{N}il_{/A}$ be the subcategory of $\mathcal{A}d$ consisting of A-algebras in

which p is nilpotent. Thus we may regard the category $\mathcal{A}d$ of p-adic algebras as the category obtained from $\mathcal{N}il$ adding projective limits of its objects. Let $F = \mathrm{Spec}(R')_{/A}$ for an A-algebra R'. We consider the restriction of F to $\mathcal{N}il$. Then for any $S \in \mathrm{Ob}(\mathcal{N}il)$, every $x \in F(S) = \mathrm{Hom}_{A\text{-alg}}(R',S)$ has to factor through $R'/p^{\alpha}R'$ for sufficiently large α (such that p^{α} kills S). Thus

$$F(S) = \mathrm{Hom}_{A\text{-alg}}(R',S) = \mathrm{Hom}_{A\text{-alg}}(\hat{R}',S),$$

where $\hat{R}' = \varprojlim_{\alpha} (R'/p^{\alpha}R') = \varprojlim_{\alpha} (R'/p^{\alpha}R')$ is the p-adic completion of R'. Thus considering the restriction of F to $\mathcal{N}il$ is studying the p-adic completion of R' algebraically and is studying the germs (with infinitesimals) along the special fiber at p of Spec(R'). For $S \in \mathrm{Ob}(\mathcal{N}il)$, we write S^{red} for the reduced part of S, i.e., the residue ring of S modulo its nilradical n_S. Returning to the original $R = A[M]$, we define a new functor $\hat{T} : \mathcal{N}il \to \mathcal{A}b$ by

(5) $$\hat{T}(S) = \text{Kernel of the natural map } T(S) \to T(S^{\mathrm{red}}).$$

Since $T(S) = \mathrm{Hom}_{gr}(M,S^{\times})$ for any S, $\hat{T}(S) = \mathrm{Hom}_{gr}(M,1+n_S)$. Since p is nilpotent in S, for any $x \in n_S$, taking N so that $x^N = 0$, we see that $(1+x)^{p^n} = 1+\sum_{i=1}^{N}\binom{p^n}{i}x^i$ if $p^n \geq N$. Since $\left|\binom{p^n}{i}\right|_p \to 0$ as $n \to \infty$ if $|i| \leq N$, we see that $1+n_S$ is contained in $\mu_{p^n}(S)$ for large n. On the other hand, if $\zeta \in \mu_{p^n}(S)$,

$$(\zeta-1)^{p^n} = (-1)^{p^n}\left\{1+(-1)^{p^n}+\sum_{i=1}^{p^n-1}(-1)^i\binom{p^n}{i}\zeta^i\right\}$$

is divisible by p, because $1+(-1)^{p^n}$ and $\binom{p^n}{i}$ for $1 \leq i < p^n$ are both divisible by p. Thus $(\zeta-1)$ is nilpotent in S. Thus

(6) $$\text{If p is nilpotent in S, } \mu_{p^\infty}(S) = \varinjlim_{\alpha} \mu_{p^\alpha}(S) = 1+n_S.$$

This shows that, because p is nilpotent in S,

$$\hat{T}(S) = \mathrm{Hom}_{gr}(M,\mu_{p^\infty}(S)) = \mathrm{Hom}_{conti}(M_p,S^{\times}),$$

where $M_p = \varprojlim_{\alpha} (M/p^{\alpha})$ and $S^{\times}$ is supposed to have the discrete topology, while M_p is equipped with the p-adic topology. Then the last equality follows from (4) because any continuous homomorphism of M_p to $S^{\times}$ factors through $M/p^{\alpha}M$ for some α. Now we can extend this functor to $\mathcal{A}d$ by

(7a) $$\hat{T}(S) = \varprojlim_{\alpha} \hat{T}(S/p^{\alpha}S) = \mathrm{Hom}_{conti}(M_p,S^{\times}),$$

where $\hat{T}(S/p^{\alpha}S) = \mathrm{Hom}_{\mathrm{conti}}(M_p,(S/p^{\alpha}S)^{\times})$. Thus, by (4), on $\mathcal{Ad}$, we see that $\hat{T}(S) = \mathrm{Hom}_{A\text{-alg}}(R_{p^\infty},S)$ for

$$\text{(7b)}\quad R_{p^\infty} = \varprojlim_n R_{p^n} \cong \varprojlim_n \otimes_i A[t^{\alpha_i},t^{-\alpha_i}]/(t^{p^n\alpha_i}-1) \cong A[[t^{\alpha_1}-1,\dots,t^{\alpha_r}-1]].$$

In this sense, we may write $\hat{T} = \mathrm{Spf}(R_{p^\infty})$, which is the formal completion of T along the ideal $(t^{\alpha_1}-1, \dots, t^{\alpha_r}-1)$ (see [Ha, II.9]). We thus call this functor the formal group (scheme) of T. To complete the proof of (7b), we need to show

$$\varprojlim_n A[t,t^{-1}]/(t^{p^n}-1) \cong A[[t-1]] \text{ as compact algebras.}$$

Since $A[t,t^{-1}]/(t^{p^n}-1) \cong A[t]/(t^{p^n}-1) \cong A[T]/((T+1)^{p^n}-1)$ for $T = t-1$, we first show that $(T+1)^{p^n}-1 \in (p,T)^{n+1}$. When $n = 0$, this is obvious. We proceed by induction on n. We see that

$$(T+1)^{p^{n+1}}-1 = ((T+1)^{p^n}-1)(1+(T+1)+\cdots+(T+1)^{p-1}) = ((T+1)^{p^n}-1)(p+TQ(T))$$

for an integral polynomial Q of T, and hence by the induction hypothesis, $(T+1)^{p^{n+1}}-1 \in (p,T)^{n+2}$ because $(p+TQ(T)) \in (p,T)$. Thus there is a natural map $\varprojlim_n A[t,t^{-1}]/(t^{p^n}-1) \to \varprojlim_n A[T]/(p,T)^{n+1} = A[[T]]$. This map is continuous under the projective limit of the natural topology on both sides. By compactness, the image of the map is closed and contains a dense subset $A[T]$. Thus the map is surjective. The injectivity of the map is obvious because $\bigcap_n (p,T)^n = \{0\}$. This shows the isomorphism.

§3.7. Toroidal formal groups and p-adic measures

We study here the relation between the space of p-adic measures on M_p and the coordinate ring R_{p^∞} of the formal group $\hat{T}$. We will get a natural isomorphism $R_{p^\infty} \cong \mathcal{Meas}(M_p;A)$ generalizing the isomorphism $A[[t-1]] \cong \mathcal{Meas}(\mathbf{Z}_p;A)$ given in (5.1b). Here we keep the notaion of the previous section. In particular, the base algebra A is the p-adic integer ring (with the maximal ideal p) of a finite extension $K/\mathbf{Q}_p$. We continue to use the notation introduced in the previous section. For $S \in \mathrm{Ob}(\mathcal{Ad}_{/A})$, we can write

$$\mathcal{Meas}(M_p;S) = \{\varphi : \mathcal{C}(M_p;S) \to S \mid \varphi \text{ is S-linear and continuous}\},$$

where we use the topology of uniform convergence in the space $\mathcal{C}(M_p;S)$ of continuous functions on M_p with values in S, while S is equipped with the p-adic topology. By definition, we have

$$R_{p^\infty} = \varprojlim_n R_{p^n} = \varprojlim_n A[M/p^nM] \cong A[[t^{\alpha_1}-1,\ldots,t^{\alpha_r}-1]]$$

and

$$R_{p^\infty}\hat{\otimes}_A S = \varprojlim_\alpha (R_{p^\infty}\otimes_A S/p^\alpha S) = \varprojlim_n S[M/p^nM] \cong S[[t^{\alpha_1}-1,\ldots,t^{\alpha_r}-1]] .$$

For any finite group G, the group algebra $A[G]$ has the obvious universal property: for any given group homomorphism $\xi : G \to S^\times$ for $S \in \mathcal{A}lg_{/A}$, there is a unique A-algebra homomorphism $\xi^* : A[G] \to S$ making the following diagram commutative:

$$\begin{array}{ccc} A[G] & \xrightarrow{\xi^*} & S \\ \uparrow & & \uparrow \\ G & \xrightarrow[\xi]{} & S^\times \end{array}$$

The algebra $R_{p^\infty}\hat{\otimes}_A S$ has a similar universal property for continuous homomorphisms $\xi : M_p \to S^\times$ (i.e. $\xi \in \hat{T}(S) = \mathrm{Hom}_{\mathrm{cont}}(M_p,S^\times)$). Thus, for any given $\xi \in \hat{T}(S)$, by continuity, $\xi_\alpha : x \mapsto \xi(x) \bmod p^\alpha S$ factors through $M/p^\alpha M$. Therefore, by the universality characterizing group algebras, we have the S-algebra homomorphism

$$\xi_\alpha{}^* : S[M/p^\alpha M] = R_{p^\alpha}\otimes_A S \to S/p^\alpha S$$

extending ξ_α. By construction, $\{\xi_\alpha{}^*\}$ forms a projective system yielding

$$\xi^* = \varprojlim_\alpha \xi_\alpha{}^* : R_{p^\infty}\hat{\otimes}_A S \to S,$$

which extends ξ. Thus $R_{p^\infty}\hat{\otimes}_A S$ is sometimes written as $S[[M]]$ and is called the continuous group algebra of M. Anyway we have recovered the canonical isomorphism proved in the previous section:

$$\hat{T}(S) \cong \mathrm{Hom}_{A\text{-alg}}(R_{p^\infty},S) = \mathrm{Hom}_{S\text{-alg}}(R_{p^\infty}\hat{\otimes}_A S,S) \quad (\xi \mapsto \xi^*).$$

In naive geometric terms, the evaluation at an S-rational point ξ of a variety gives an algebra homomorphism from its coordinate ring into S. Reversing this process, in modern algebraic geometry, we define S-rational points to be algebra homomorphisms from the coordinate ring (given without any reference to geometric objects) into S. From this point of view, the value $f(\xi)$ of an element f in the coordinate ring as a function of S-rational points ξ is nothing but the value of the algebra homomorphism ξ at f. Following this convention in algebraic geometry, we regard an element $f = f(t^{\alpha_1}-1,\ldots,t^{\alpha_r}-1)$ in the coordinate ring $R_{p^\infty}\hat{\otimes}_A S = S[[t^{\alpha_1}-1,\ldots,t^{\alpha_r}-1]]$ of $\hat{T}$ as a function of $\xi \in \hat{T}(S)$ by putting

$$f(\xi) = \xi^*(f) = f(\xi(\alpha_1)-1,\ldots,\xi(\alpha_r)-1).$$

We now want to prove the following result of Katz [K6]:

Theorem 1. *Let* S *be an object in* $\mathcal{Ad}_{/A}$. *Then there is a functorial isomorphism of A-algebras between* $R_{p^\infty}\hat{\otimes}_A S$ $(= \varprojlim_\alpha (R_{p^\infty}\otimes_A S/p^\alpha S))$ *and* $\mathcal{M}eas(M_p;S)$ *characterized by the following properties. Writing the correspondence as* $R_p\hat{\otimes}_A S \ni f \leftrightarrow \mu_f \in \mathcal{M}eas(M_p;S)$, *we have*

(i) for each point $\xi \in \hat{T}(S) = \mathrm{Hom}_{\mathrm{cont}}(M_p,S^\times)$, $\int \xi(x)d\mu_f(x) = f(\xi)$;
(ii) for any numerical polynomial $P : M \to \mathbf{Z}$ *regarded as a continuous function on* M_p,

$$\int P(x)\xi(x)d\mu_f(x) = D_P f(\xi),$$

where D_P *is the differential operator in (6.3b);*
(iii) for ξ *and* P *as above, and for any locally constant function* $\phi : M_p \to S$,

$$\int \phi(x)\xi(x)d\mu_f(x) = \int d\mu_F(x)$$

for $F(t) = ([\phi]f)$ *for the operator* $[\phi]$ *on* $R_{p^\infty}\hat{\otimes}_A S$ *satisfying* $[\phi]t^\alpha = \phi(\alpha)t^\alpha$.

Before proving the theorem, we recall briefly the isomorphism (5.1a), its construction and its properties. By Mahler's theorem (Theorem 2.1), to each measure $\varphi \in \mathcal{M}eas(\mathbf{Z}_p;S)$, we assign a power series

$$(*) \qquad \Phi(t-1) = \sum_{n=0}^{\infty} \int \binom{x}{n} d\varphi (t-1)^n = \int t^x d\varphi \in S[[t-1]],$$

where in the last equality, we regard $d\mu$ as a measure having values in $S[[t-1]]$ in an obvious manner, using the expansion $t^x = \sum_{n=0}^{\infty} \binom{x}{n}(t-1)^n$. Write $\Phi = \Phi_\varphi$ and $\varphi = \varphi_\Phi$. Then we have verified

(1a) for each $\xi \in \hat{G}_m(S)$, $\int \xi(x)d\varphi = \Phi_\varphi(\xi(1)-1) = \Phi_\varphi(\xi)$,

where in the last equality, we have used the convention described above the theorem. Since $\mathbf{Z}_p$ is topologically generated by 1, we see that $\xi(x) = \xi(x1) = \xi(1)^x$. Thus replacing y in $(*)$ by $\xi(1)$, we know that

$$\int \xi(x)d\varphi = \Phi_\varphi(\xi(1)-1).$$

We already know from (6.3a) that any invariant differential operator of $\mathbf{G}_{m/Z}$ is given by $D_P = P(t\frac{d}{dt})$ for a numerical polynomial P. Then we see from Exercise 5.1 and (1a) that

(1b) $$\int P(x)\xi(x)d\varphi(x) = D_P\Phi_\varphi(\xi).$$

Finally, for any locally constant function $\phi : \mathbf{Z}_p \to S$, we have

(1c) $$\int \phi(x)P(x)\xi(x)d\varphi(x) = D_P[\phi]\Phi_\varphi(\xi),$$

where $[\phi]$ is the operator defined in (5.6a,b) satisfying $[\phi]t^m = \phi(m)t^m$.

Proof. We may identify $\hat{T} = \hat{G}_m{}^r$ and $M = \mathbf{Z}^r$ by fixing a basis $\{\alpha_i\}$ of M. Writing t_i for t^{α_i}, we already know that $R_{p^\infty} = A[[t_1-1,\ldots,t_r-1]]$ (6.7b). Then writing $n = (n_i)$ for an r-tuple of natural numbers (i.e. $n \in \mathbf{N}^r$) and defining $\binom{x}{n} = \prod_{i=1}^r \binom{x_i}{n_i}$ for $x = (x_i) \in \mathbf{Z}_p{}^r = M_p$, we see in the same manner as in §3.3 that

(2) *Any* $f \in \mathcal{C}(\mathbf{Z}_p{}^r;S)$ *can be expressed uniquely as an interpolation series:* $f(x) = \sum_{n\geq 0} a_n(f)\binom{x}{n}$ *with* $a_n(f) \in S$ *satisfying* $\lim_{|n|\to\infty} a_n = 0$, *where* $\sum_{n\geq 0}$ *means* $\sum_{n_1=0}^\infty \cdots \sum_{n_r=0}^\infty$ *and* $|n| = \sum_i |n_i|$. *Conversely, if a sequence* $\{a_n\}$ *satisfying* $\lim_{|n|\to\infty} a_n = 0$ *is given in* S, *then the infinite sum* $\sum_{n\geq 0} a_n\binom{x}{n}$ *converges in* S *giving a continuous function on* $\mathbf{Z}_p{}^r$ *having values in* S.

In fact, if we write $\mathcal{LC}(M_p;S)$ for the space of locally constant functions on M_p with values in S, it is plain that $\mathcal{LC}(\mathbf{Z}_p{}^r;S) = \mathcal{LC}(\mathbf{Z}_p;S)\otimes_S\cdots\otimes_S\mathcal{LC}(\mathbf{Z}_p;S)$. Since $\mathcal{LC}(\mathbf{Z}_p;S)$ is dense in $\mathcal{C}(\mathbf{Z}_p;S)$ under the topology of uniform convergence, we see that $\mathcal{C}(\mathbf{Z}_p{}^r;S) = \mathcal{C}(\mathbf{Z}_p;S)\hat{\otimes}_S\cdots\hat{\otimes}_S\mathcal{C}(\mathbf{Z}_p;S)$. Then (2) follows from Mahler's theorem. Then all the assertions of the theorem are easy consequences of (1a,b,c).

§3.8. p-adic Shintani L-functions of totally real fields

We fix an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$ and $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. We also fix embeddings of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_p$ and $\mathbf{C}$ so that any algebraic number can be regarded both as a complex number and as a p-adic number. We extend the absolute value $|\ |_p$ as assured in (2.5). Let F be a number field of degree d in $\overline{\mathbf{Q}}$. We write I for the set of all embeddings of F into $\mathbf{C}$. We assume that all the embeddings of F into $\mathbf{C}$ actually fall in $\mathbf{R}$, i.e., that F is totally real. We write $\mathbf{R}_+$ for the strictly positive real line. We write $F_\mathbf{R} = F\otimes_\mathbf{Q}\mathbf{R}$, which is canonically isomorphic to $\mathbf{R}^I$ via $F \ni \xi \mapsto (\xi^\sigma)_{\sigma\in I}$. We put $F_{\mathbf{R}+} = \mathbf{R}_+{}^I$. For any subset X of $F_\mathbf{R}$, we

write X_+ for $X \cap F_{\mathbf{R}+}$. We write E for $\mathcal{O}_+^\times = \mathcal{O}^\times \cap F_{\mathbf{R}+}$. Let $v = \{v_1, \ldots, v_r\}$ be a set of $\mathbf{Q}$-linearly independent element in F_+. We write $C(v)$ for the open simplicial cone spanned by v, i.e., $C(v) = \sum_i \mathbf{R}_+ v_i$ in $F_{\mathbf{R}+}$. As shown in §2.7 (Theorem 2.7.1), there exists a finite set V of the v's as above such that

$$F_{\mathbf{R}+} = \bigcup_{\varepsilon \in E} \bigcup_{v \in V} v\varepsilon C(v) \quad \text{(disjoint union).}$$

Let $\mathcal{O}$ be the integer ring of F. We fix an ideal $\mathfrak{a} \neq \{0\}$ in $\mathcal{O}$. For any $\lambda \in F_+$, we can replace V by $\lambda V = \{\lambda v \mid v \in V\}$ without affecting the above property. In particular, we may assume that v is contained in $\mathfrak{a}$ for all $v \in V$. We consider the torus $T_{/\mathbf{Z}}$ associated with $M = \mathfrak{a}$ defined in (6.3c). Let R be the coordinate ring of T. Then R is a group algebra of $\mathfrak{a}$, i.e., $R = \mathbf{Z}[t^\alpha \mid \alpha \in \mathfrak{a}]$. Let $\overline{\mathbf{Z}}_p$ be the integral closure of $\mathbf{Z}_p$ in $\overline{\mathbf{Q}}_p$. We define

$$R'_p = \{\frac{P(t)}{Q(t)} \mid P(t), Q(t) \in R \otimes_{\mathbf{Z}} \overline{\mathbf{Z}}_p \text{ and } |Q(1)|_p = 1\}.$$

Similarly, we define

$$R'_\infty = \{\frac{P(t)}{Q(t)} \mid P(t), Q(t) \in R \otimes_{\mathbf{Z}} \mathbf{C} \text{ and } |Q(1)| \neq 0\}.$$

We put $R(v) = \mathfrak{a}_+ \cap \{\sum_{v_i \in v} x_i v_i \mid 0 < x_i \leq 1\}$. For each $v \in V$, $x \in R(v)$ and for $\xi \in T(\mathbf{C}) = \mathrm{Hom}(\mathfrak{a}, \mathbf{C}^\times)$, we define

(1a) $$f_{v,\xi,x}(t) = \frac{\xi(x)t^x}{\prod_{v_i \in v}(1 - \xi(v_i)t^{v_i})}.$$

(1b) When $\xi(v_i) \neq 1$ and $|\xi(v_i)| \leq 1$ for all $v_i \in v$, we see that
$$f_{v,\xi,x} \in R'_\infty.$$

(1c) If $\xi(v_i)$ is a non-trivial l^m-th root of unity for a prime l prime to p $(m > 0)$, then $|\xi(v_i) - 1|_p = 1$ and hence $f_{v,\xi,x} \in R'_p$.

For the coordinate ring $R_{p\infty}$ of the formal group $\hat{T}$, the argument which proves Lemma 4.2 combined with (6.3b) shows that, for every numerical polynomial P on $\mathfrak{a}$,

(2) $$R'_p \supset D_P(R'_p) \text{ and } R'_p \text{ is embedded into } R_{p\infty} \otimes_{\mathbf{Z}_p} \overline{\mathbf{Z}}_p.$$

Numbering the elements in I, writing the i-th conjugate of $\alpha \in F$ as $\alpha^{(i)}$ and replacing t^α by $\exp(-\sum_i \alpha^{(i)} y_i)$, we see that

(3) $$f_{v,\xi,x}(t) \text{ corresponds to } \xi(x)G(y, A, \underline{x}, \chi) \text{ (see (2.4.3)),}$$

where $L_i(y) = \sum_j v_i^{(j)} y_j$, $\chi_i = \xi(v_i)$ and $\underline{x} = (x_i)$ given by $x = \sum_i x_i v_i$. Finally note that the norm map $N : \mathfrak{a} \to \mathbf{Z}$ is a numerical polynomial on $\mathfrak{a}$ and

hence we have an invariant differential operator $D_N \in \mathcal{D}(T_{/\mathbf{Z}})$ $(D_N(t^\alpha) = N(\alpha)t^\alpha)$. Then, directly from (2.4.8c), we get

Proposition 1. *For each* $\xi \in \mathrm{Hom}(a,\mathbf{C}^\times)$ *satisfying* $|\xi(v_i)| \le 1$ *and* $\xi(v_i) \ne 1$ *for all* v_i *in* v, *we have*

$$\xi(x)\zeta((-n)\mathbf{1},A,x,\chi) = (D_N)^n(f_{v,\xi,x})|_{t=1} \text{ for all } n \in \mathbf{N}.$$

Write $\mathcal{R}_a = \{\bigcup_{v\in v} C(v)\} \cap a$. Then $a_+ = \bigcup_{\varepsilon\in E} \varepsilon\mathcal{R}_a$ (disjoint union). For any function ϕ on a having values in $\mathbf{C}$, we put

$$\zeta_{a,\phi}(s) = \sum_{\alpha\in\mathcal{R}_a} \phi(\alpha)N(\alpha)^{-s}.$$

Let $\phi : a/\mathfrak{l}a \to \mathbf{C}$ be a function for an ideal $\mathfrak{l}$ of O. Then ϕ is a linear combination of additive characters $\psi \in \mathrm{Hom}(a/\mathfrak{l}a,\mathbf{C}^\times)$. In fact, for any given $a \in a/\mathfrak{l}a$, we have

$$\chi_a(x) = \sum_\psi \psi(x-a) = \begin{cases} \#(a/\mathfrak{l}a) = N(a) & \text{if } x = a, \\ 0 & \text{otherwise,} \end{cases}$$

by the orthogonality relation (Lemma 2.3.1). Since $\phi = N(a)^{-1}\sum_\psi \phi(a)\chi_a$, ϕ is a linear combination of additive characters ψ. Write $\phi = \sum_\psi c_\phi \psi$ and put

$$f_{a,\phi\xi}(t) = \sum_\psi c_\phi \sum_{v\in V} \sum_{x\in R(v)} \psi\xi(x) f_{v,\psi\xi,x}(t) = [\phi] f_{a,\xi}(t).$$

This is legitimate because $\psi\xi \in \mathrm{Hom}(a,\mathbf{C}^\times)$ with $|\psi\xi(v_i)| \le 1$ if $|\xi(v_i)| \le 1$. Then, noting

$$\zeta_{a,\phi\xi}(s) = \sum_{\alpha\in\mathcal{R}_a} \sum_\psi c_\phi \psi\xi(\alpha)N(\alpha)^{-s} = \sum_{\alpha\in\mathcal{R}_a} \sum_\psi c_\phi \zeta_{a,\psi\xi}(s),$$

we have with the notation of Theorem 7.1

(4) $\zeta_{a,\phi\xi}(s)$ has an analytic continuation to the whole complex s-plane and satisfies $(D_N)^n f_{a,\phi\xi}(1) = (D_N)^n[\phi]f_{a,\xi}(1) = \zeta_{a,\phi\xi}(-n)$ for all $n \in \mathbf{N}$ and for each function $\phi : a/\mathfrak{l}a \to \mathbf{C}$.

Now we fix a prime ideal $\mathfrak{l}$ of F with $O/\mathfrak{l} \cong \mathbf{Z}/l\mathbf{Z}$ for a prime $l \ne p$. The additive group $a/\mathfrak{l}a$ is a cyclic group of order l. We consider the function $\phi : a/\mathfrak{l}a \to \mathbf{C}$ given by $\phi(x) = \sum_{\psi\ne \mathrm{id}} \psi(x)$, where ψ runs over all non-trivial additive characters $\psi : a/\mathfrak{l}a \to \overline{\mathbf{Q}}^\times$. By the orthogonality relation (Lemma 2.3.1), we see that

(5a) $$\phi(x) = -\sum_{\psi\neq id}\psi(x) = \begin{cases} 1 & \text{if } x \notin a\mathfrak{l}, \\ 1-l & \text{if } x \in a\mathfrak{l}. \end{cases}$$

Then

(5b) $$f_{a,\phi}(t) = -\sum_{\psi\neq id}\sum_{v\in V}\sum_{x\in R(v)} f_{v,\psi,x}(t),$$

where ψ runs over all non-trivial characters $\psi : a/\mathfrak{l}a \to \overline{\mathbf{Q}}^{\times}$. We assume that $v_i \notin a\mathfrak{l}$ for all $v = (v_i) \in V$ and for all i. This is possible because there are only finitely many ideals which violate this condition (such an ideal is a factor of $v_i a^{-1}$ for some i). Then by (1c), $f_{a,\phi} \in R'_p$. Thus we have from Theorem 7.1

Theorem 1. *Let the notation and the assumption be as above. Then there exists a* p*-adic measure* $\mu_{a,\mathfrak{l}} \in \mathcal{M}eas(a_p;\mathbf{Z}_p[\mu_l])$ *such that for all locally constant functions* $f : a_p = \varprojlim_{\alpha} a/p^{\alpha}a \to \overline{\mathbf{Q}}$ *and* $n \in \mathbf{N}$,

$$\int f(x)N(x)^n d\mu_{a,\mathfrak{l}}(x) = \zeta_{a,f\phi}(-n),$$

where $\phi(x) = -\sum_{\psi\neq id}\psi(x) = \begin{cases} 1 & \text{if } x \notin a\mathfrak{l}, \\ 1-l & \text{if } x \in a\mathfrak{l}. \end{cases}$

§3.9. p-adic Hecke L-functions of totally real fields

We consider the ray class group $Cl_F(p^{\alpha})$ defined in §1.2. If $\alpha > \beta > 0$, we see from the definition that $\mathcal{P}_+(p^{\beta}) \supseteq \mathcal{P}_+(p^{\alpha})$ and thus we have a natural map $Cl_F(p^{\alpha}) = I(p)/\mathcal{P}_+(p^{\alpha}) \to I(p)/\mathcal{P}_+(p^{\beta}) = Cl_F(p^{\beta})$, where

$$I(p) = \{ \mathfrak{b} = \frac{n}{d} \mid n \text{ and } d \text{ are integral and prime to } p\},$$

$$\mathcal{P}_+(p^{\alpha}) = \mathcal{P}_+ \cap \{ a\mathcal{O} \mid a \in F^{\times}, a \equiv 1 \bmod^{\times} p^{\alpha}\} \quad \text{(see Exercise 1.2.1).}$$

Thus we may consider the projective limit

(1a) $$Cl_F(p^{\infty}) = \varprojlim_{\alpha} Cl_F(p^{\alpha}),$$

which is a compact group. By definition, we have a natural group homomorphism

$$i_{\alpha} : (\mathcal{O}/p^{\alpha}\mathcal{O})^{\times} \to Cl_F(p^{\alpha}) \text{ given by } a \bmod p^{\alpha} \mapsto \text{the class of } a\mathcal{O}.$$

Here we have implicitly assumed that a is totally positive. Let E be the subgroup of totally positive units in $\mathcal{O}^{\times}$. Then it is obvious that $\mathrm{Ker}(i_{\alpha})$ = the image of E in $(\mathcal{O}/p^{\alpha}\mathcal{O})^{\times}$. The cokernel of i_{α} is just $Cl_F(1) = I/\mathcal{P}_+$. Taking the projective limit, we have an exact sequence

(1b) $$1 \to \overline{E} \to \mathcal{O}_p^\times \to \mathrm{Cl}_F(p^\infty) \to \mathrm{Cl}_F(1) \to 1,$$

where $\mathcal{O}_p^\times = \varprojlim_\alpha (\mathcal{O}/p^\alpha\mathcal{O})^\times$ and $\overline{E} = \varprojlim_\alpha \mathrm{Ker}(i_\alpha)$ is the closure of E in $\mathcal{O}_p^\times$. Note that $\mathcal{O}_p = \prod_{\mathfrak{p}|p}\mathcal{O}_\mathfrak{p}$ for prime ideals $\mathfrak{p}$ and as seen in §3, we have for sufficiently large α that

$$log : 1+p^\alpha\mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}$$

induces an isomorphism from the multiplicative group $1+p^\alpha\mathcal{O}_\mathfrak{p}$ to an open additive subgroup (of finite index) in $\mathcal{O}_\mathfrak{p}$. Since $\mathrm{rank}_{\mathbf{Z}_p}\mathcal{O}_\mathfrak{p} = [F:\mathbf{Q}]$, we have $\mathcal{O}_p^\times \cong \mu\times\mathbf{Z}_p^{[F:\mathbf{Q}]}$ as topological groups with a finite group μ. Since $\overline{E}$ is a $\mathbf{Z}_p$-submodule of $\mathcal{O}_p^\times$, it is of finite rank over $\mathbf{Z}_p$. Since $\mathrm{rank}_{\mathbf{Z}}E = [F:\mathbf{Q}]-1$ by Dirichlet's unit theorem (Theorem 1.2.3), we know that

$$\mathrm{rank}_{\mathbf{Z}_p}\overline{E} \le [F:\mathbf{Q}]-1, \text{ i.e. } \mathcal{O}_p^\times/\overline{E} \cong \mu'\times\mathbf{Z}_p^{1+\delta}$$

for a non-negative integer δ and a finite group μ'. Although the equality of the ranks, $\mathrm{rank}_{\mathbf{Z}_p}\overline{E} = \mathrm{rank}_{\mathbf{Z}}E$, is conjectured by Leopoldt, this is still an open question except when $F/\mathbf{Q}$ is an abelian extension (a theorem of Brumer confirms this conjecture when $F/\mathbf{Q}$ is abelian [Wa, Th.5.25]). Anyway, $G = \mathrm{Cl}_F(p^\infty)$ is a compact group, and we can decompose $G = G_{tor}\times W$ non-canonically so that G_{tor} is a finite subgroup and $W \cong \mathbf{Z}_p^{1+\delta}$. The group $I(\mathfrak{p})$ of fractional ideals prime to $\mathfrak{p}$ can be naturally regarded as a dense subgroup of G. On $I(\mathfrak{p})$, we have the norm map $N : I(\mathfrak{p}) \to \mathbf{Z}_{(p)} = \mathbf{Z}_p\cap\mathbf{Q}$. This map N coincides with the usual norm map on $\mathcal{P}_+$ and hence a polynomial map. Thus $N : I(\mathfrak{p}) \to \mathbf{Z}_p$ is continuous with respect to the topology induced from G. Thus N extends to a continuous character $N : G \to \mathbf{Z}_p^\times$. Now take the completion Ω of $\overline{\mathbf{Q}}_p$ and denote by A the p-adic integer ring of Ω. (Note that Ω is substantially larger than $\overline{\mathbf{Q}}_p$; see [BGR, 3.4.3].) The space $\mathcal{C}(G;A)$ of all continuous functions on G with values in A is naturally equipped with the uniform norm $|f|_p = \mathrm{Sup}_{x\in G}|f(x)|_p$. Let $\mathcal{M}eas(G;A)$ denote the space of bounded p-adic measures on G with values in A:

$$\mathcal{M}eas(G;A) = \mathrm{Hom}_A(\mathcal{C}(G;A),A).$$

We can define the uniform norm on $\mathcal{M}eas(G;A)$ by

$$|\varphi|_p = \mathrm{Sup}_{|f|_p=1}\left|\int_G f d\varphi\right|_p.$$

Theorem 1. *For each element* $a \in G = \mathrm{Cl}_F(p^\infty)$, *there exists a unique* p-*adic measure* ζ_a *on* G *such that for any character* $\chi : \mathrm{Cl}_F(p^\alpha) \to \overline{\mathbf{Q}}^\times$ *and any* $n \in \mathbf{N}$, *we have*

$$\int_G \chi(x)N(x)^n d\zeta_a(x) = (1-\chi(a)N(a)^{n+1})\prod_{\mathfrak{p}|p}(1-\chi_0(\mathfrak{p})N(\mathfrak{p})^n)L(-n,\chi_0),$$

where we denote by $L(s,\chi)$ *the primitive L-function (i.e. the L-function of primitive character* χ_0 *associated with* χ*) and hence the factor* $(1-\chi_0(\mathfrak{p})N(\mathfrak{p})^n)$ *is non-trivial if the primitive character* χ *has conductor prime to* p.

Proof. For each ray class c in $\mathrm{Cl}_F(1)$, we choose a representative $\mathfrak{a} = \mathfrak{a}_c$ which is prime to p. Then we choose V as in the previous section so that v is contained in $\mathfrak{a}$ for all $v \in V$. We then choose a prime ideal $\mathfrak{l}$ with $\mathfrak{a}/\mathfrak{a}\mathfrak{l} \cong \mathbf{Z}/l\mathbf{Z}$ for a prime l in $\mathbf{Z}$ such that $v_i \notin \mathfrak{a}\mathfrak{l}$ for all i and all $v \in V$. Among the prime ideals $\mathfrak{l}$ with $\mathfrak{a}/\mathfrak{l}\mathfrak{a} \cong \mathbf{Z}/l\mathbf{Z}$ for a prime l in $\mathbf{Z}$, there are only finitely many which do not satisfy the above condition for a fixed V. Thus by changing $\mathfrak{l}$ if necessary, we have the measure $\mu_{\mathfrak{a}_c,\mathfrak{l}}$ on $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ as in Theorem 8.1 for all $c \in \mathrm{Cl}_F(1)$. Since $G = \bigcup_c \mathfrak{a}_c^{-1}(\mathcal{O}_\mathfrak{p}^\times/\overline{E})$ (disjoint union), to each function $\phi \in \mathcal{C}(G;A)$, we can associate a continuous function ϕ_c ($c \in \mathrm{Cl}_F(1)$) on $\mathcal{O}_\mathfrak{p}$ by $\phi_c(x) = \begin{cases} \phi(\mathfrak{a}_c^{-1}x) & \text{if } x \in \mathcal{O}_\mathfrak{p}^\times, \\ 0 & \text{otherwise.} \end{cases}$ Then we define

$$\int_G \phi d\zeta_\mathfrak{l} = \sum_{c \in \mathrm{Cl}_F(1)} \int_{\mathcal{O}_\mathfrak{p}} \phi_c d\mu_{\mathfrak{a}_c,\mathfrak{l}}.$$

This certainly defines a measure on G. We now compute

$$(2) \qquad \int_G \chi(x)N(x)^n d\zeta_\mathfrak{l}(x) = \sum_{c \in \mathrm{Cl}_F(1)} \chi(\mathfrak{a}_c)^{-1}N(\mathfrak{a}_c)^{-n}\int_{\mathcal{O}_\mathfrak{p}} \chi(x)N(x)^n d\mu_{\mathfrak{a}_c,\mathfrak{l}}(x).$$

By Theorem 8.1, we see that

$$\begin{aligned} \int_{\mathcal{O}_\mathfrak{p}} \chi(x)N(x)^n d\mu_{\mathfrak{a},\mathfrak{l}}(x) &= \zeta_{\mathfrak{a},\chi\xi}(-n) \\ &= \sum_{\alpha \in \mathcal{R}_\mathfrak{a}} \chi(\alpha)N(\alpha)^{-s} - N(\mathfrak{l})\sum_{\alpha \in \mathcal{R}_\mathfrak{a} \cap \mathfrak{a}\mathfrak{l}} \chi(\alpha)N(\alpha)^{-s}\,|_{s=-n} \\ &= \sum_{\alpha \in \mathfrak{a}_+/E} \chi(\alpha)N(\alpha)^{-s} - N(\mathfrak{l})\sum_{\alpha \in \mathfrak{a}\mathfrak{l}_+/E} \chi(\alpha)N(\alpha)^{-s}\,|_{s=-n}, \end{aligned}$$

since $\mathfrak{a}_+ = \bigcup_{\varepsilon \in E} \varepsilon\mathcal{R}_\mathfrak{a}$ and the integrand is invariant under multiplication by E. Thus

$$\begin{aligned} \int_{\mathfrak{a}_\mathfrak{p}} \chi(x)N(x)^n d\mu_{\mathfrak{a},\mathfrak{l}}(x) = \chi(\mathfrak{a})N(\mathfrak{a})^n\{&\sum_{\alpha \in \mathfrak{a}_+/E} \chi(\alpha\mathfrak{a}^{-1})N(\alpha\mathfrak{a}^{-1})^{-s} \\ &-\chi(\mathfrak{l})N(\mathfrak{l})^{n+1}\sum_{\alpha \in \mathfrak{a}\mathfrak{l}_+/E} \chi(\alpha(\mathfrak{a}\mathfrak{l})^{-1})N(\alpha(\mathfrak{a}\mathfrak{l})^{-1})^{-s}\}\,|_{s=-n}, \end{aligned}$$

where αa^{-1} runs over all integral ideals prime to p which are in the same class as a^{-1} in $\mathrm{Cl}_F(1)$. This combined with (2) shows the desired formula when $a = \mathfrak{l}$. The uniqueness follows from the fact that the polynomial functions and locally constant functions are dense in $\mathcal{C}(G;A)$. Now the ideals $\mathfrak{l}$ for which the measures $\zeta_{\mathfrak{l}}$ are constructed are dense in G by Chebotarev's density theorem (see §1.2). Thus for general $a \in G$, we can choose a sequence $\{\mathfrak{l}_n\}$ of such ideals converging to a. Then by the evaluation formula, $\zeta_n = \zeta_{\mathfrak{l}_n}$ converges to ζ_a in $\mathcal{M}eas(G;A)$, which finishes the proof.

Using the notation of §5, we now define the p-adic Hecke L-function with character $\chi : \mathrm{Cl}_F(p^\alpha) \to \overline{\mathbf{Q}}^\times$ by

$$L_p(s,\chi) = L_{F,p}(s,\chi) = (1-\chi(a)\langle N(a)\rangle^{1-s})^{-1}\int_G \chi(x)\omega^{-1}(N(x))\langle N(x)\rangle^{-s}d\zeta_a(x),$$

where ω is the Teichmüller character of $\mathbf{Z}_p^\times$. Then $L_p(s,\chi)$ is a p-adic analytic function on $\mathbf{Z}_p$ except when $\chi = \mathrm{id}$, and in this special case, $\zeta_p(s) = \zeta_{F,p}(s) = L_{F,p}(s,\mathrm{id})$ is a p-adic meromorphic function defined on $\mathbf{Z}_p-\{1\}$ and having at most a simple pole at $s = 1$. Moreover we have the following evaluation formula:

$$(3)\ L_p(-m,\chi) = \prod_{p|p}(1-(\chi\omega^{-m-1})_0(p)N(p)^m)L(-m,(\chi\omega^{-m-1})_0) \text{ for all } m \in \mathbf{N},$$

where we write simply ω for $\omega\circ N$, and the right-hand side is the value of the complex L-function while the left-hand side is the value of the p-adic L-function and the values are equal in $\overline{\mathbf{Q}}$.

The value of the p-adic L-function at positive integers are unknown except the value at 1 for F abelian over $\mathbf{Q}$ (see §5). When F is abelian over $\mathbf{Q}$, $\zeta_{F,p}(s) = \prod_\chi L_{Q,p}(s,\chi)$ by class field theory for Dirichlet characters associated with the field F. (For class field theory, we refer to [N] and [W1].) Thus we know the residue at $s = 1$ of $\zeta_{F,p}$ by the result in §5. In fact, for general F not necessarily abelian, Colmez [Co] proved the following p-adic residue formula:

$$(4)\qquad \mathrm{Res}_{s=1}\zeta_{F,p}(s) = \frac{2^{[F:Q]}h(F)R_p}{w\sqrt{D_F}}\prod_{p|p}(1-N(p)^{-1}),$$

where $h(F) = (I:\mathcal{P})$ is the class number of F, w is the number of roots of unity in $\mathcal{O}$ (thus $w = 2$) and choosing a basis $\{\varepsilon_1,\ldots,\varepsilon_r\}$ of the unit group $\mathcal{O}^\times$, $R_p = \pm\det(log(\varepsilon_i^{(j)}))_{i,j=1,\ldots,r-1}$ and D_F is the discriminant of F. Here $\varepsilon^{(j)}$ is the j-th conjugate of ε in $\overline{\mathbf{Q}}_p$ and "log" is the p-adic logarithm defined in a neighborhood of 1 in $\overline{\mathbf{Q}}_p$. For the choice of the sign of $\frac{R_p}{\sqrt{D_F}}$ and the proof of

the formula, see [Co]. The Leopoldt conjecture for F and p is equivalent to the non-vanishing of R_p. This formula is a generalization of Theorem 5.2 and is an interesting p-adic analogue of Theorem 2.6.2 and Corollary 8.6.2.

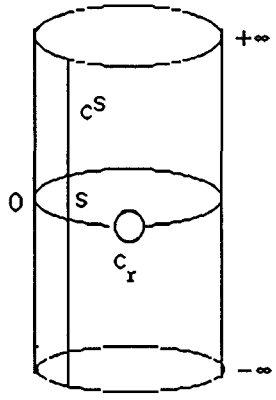
Although we have only discussed p-adic abelian L-functions over totally real fields, we can also construct abelian p-adic L-functions over CM fields. We refer to [K3], [K5], [dS] and [HT2] for the various constructions of such p-adic Hecke L-functions. The existence of abelian p-adic L-functions is the starting point of Iwasawa theory, which studies a subtle but deep interaction between such p-adic L-functions and the arithmetic of abelian extensions of the base field F. We refer to [Wa], [L] and [dS] for basics of Iwasawa theory. The so-called "main conjectures" in the Iwasawa theory have been proven recently in many instances. Although there are no books written on this subject yet, we refer for recent developments to the following research articles: [MW], [Wi2], [MT], [R] and [HT1-3].

Chapter 4. Homological Interpretation

In this chapter, we will give a homological interpretation of the theory of the special values of Dirichlet L-functions over $\mathbf{Q}$ and will reconstruct p-adic Dirichlet L-functions by a homological method (called the "modular symbol" method). A similar theory might exist for arbitrary fields, but here we restrict ourselves to $\mathbf{Q}$. The modular symbol method was introduced by Mazur [MzS] in the context of modular forms on GL(2) as we will construct later, in §6.5, p-adic L-functions of modular forms (on GL(2)) by his original method. Basic facts from cohomology theory we use in this section are summarized in Appendix at the end of this book. We use standard notations for cohomology groups introduced in Appendix without further warning and quote, for example, Theorem 1 in the appendix as Theorem A.1. If the reader is not familiar with cohomology theory, it is better to have a look at Appendix before reading this chapter.

§4.1. Cohomology groups on $\mathbf{G}_m(\mathbf{C})$

We consider the space $T = \mathbf{C}/\mathbf{Z}$, which is isomorphic to $\mathbf{G}_m(\mathbf{C})$ via $z \mapsto \mathbf{e}(z) = \exp(2\pi iz)$. Thus $T \cong \mathbf{P}^1(\mathbf{C})-\{0,\infty\}$, where $\mathbf{P}^1(\mathbf{C})$ is the projective line. We apply the theory developed in Appendix to $X = \mathbf{P}^1(\mathbf{C})$ and $Y = T$. With the notation of Proposition A.5, S is first $\{0,\infty\}$ and later will be $\mu_N \cup \{0,\infty\}$, and S_0 will be $\{0,\infty\}$. We have $\pi_1(T) \cong \mathbf{Z}$. Let A be any commutative algebra. Let $L(n;A)$ for $0 \le n \in \mathbf{Z}$ be the subspace of the polynomial ring $A[X,Y]$ consisting of homogeneous polynomials of degree n. We let the additive group $\mathbf{Z}$ act on $L(n;A)$ by $vP(X,Y) = P(X-vY,Y)$ for $v \in \mathbf{Z}$. Then we define a sheaf $\mathcal{L}(n;A) = \underline{L(n;A)}$ on T (with the notation in Theorem A.1) by the sheaf of locally constant sections of the projection $(\mathbf{C}\times L(n;A))/\mathbf{Z} \to T$, where $n \in \mathbf{Z}$ acts on $\mathbf{C}\times L(n;A)$ by $n(z,P) = (z+n,nP)$. We identify $\mathbf{C}/\mathbf{Z}$ with $(-i\infty,i\infty)\times\mathbf{R}/\mathbf{Z}$ and compactify it as $T^* = [-i\infty,i\infty]\times\mathbf{R}/\mathbf{Z}$ $(i = \sqrt{-1})$. With the notation of Appendix, we have $T^* = T^{S_0}$ for $S_0 = \{0,\infty\} \cong \{\pm i\infty\}$. Let N be a positive integer, and take out N small open disks around $\frac{r}{N}$ $(r \in \mathbf{Z})$ from T^*. The resulting space we write as T_N^S for $S = N^{-1}\mathbf{Z}/\mathbf{Z}\cup\{\pm\infty\} \cong \mu_N\cup\{0,\infty\}$. We also consider $T_N^{S-S_0}$ (resp. $T_N^{S_0}$), removing the boundaries from T_N^S around $s \in S_0 = \{\pm\infty\}$ (resp. $s \in S-S_0$). This notation fits well with Proposition A.5. We write the boundary around $s \in S$ of T_N^S as $\partial_s T_N^S$. Note that $T_N^{S-S_0}$ is no longer compact. We want to study $H^q(T_N^S,\mathcal{L}(n;A))$ and the compact support cohomology group $H_c^q(T_N^{S-S_0},\mathcal{L}(n;A))$ on $T_N^{S-S_0}$. We first compute the homology group $H_1(T_N^{S_0},\partial T_N^{S_0},A)$ for $\partial T_N^{S_0} = T_\infty\cup T_{-\infty}$, where $T_{\pm\infty} = \pm\infty\times(\mathbf{R}/\mathbf{Z})$. Let c_r be a small circle centered at $r \in S$ inside $T_N^{S_0}$ and



c^r be the vertical line passing through $r \in \mathbf{R}$. We write c_∞ for the circle added at ∞. Then we see easily that

$$\text{(1a)} \quad \begin{cases} H_1(T_N^{S_0}, \partial T_N^{S_0}, A) = Ac^0 \oplus \{\oplus_{r \in (Z/NZ)} Ac_r\} \\ H_1(T_N^S, A) = Ac_\infty \oplus \{\oplus_{r \in (Z/NZ)} Ac_r\}. \end{cases}$$

We now compute $\pi_1(T_N^{S-S_0})$. Fixing a base point x, we draw the line from x to c_r ($r \in \mathbf{Z}$ or $\pm\infty$) and turn around the circle in the positive direction and return to x. This path will be denoted by π_r. Then $\Gamma = \pi_1(T_N^{S-S_0})$ is generated by π_r ($r = \pm\infty$ and $r \in \mathbf{Z}/N\mathbf{Z}$), and there is only one relation among them: $\pi_\infty\{\prod_{r \in (Z/NZ)} \pi_r\}\pi_{-\infty} = 1$, where the product is taken in the increasing order for the index $0 \le r < N$. By using the exponential map $\mathbf{e}(z) = \exp(2\pi i z)$, we can identify T_N-S with

$$\mathbf{G}_m\text{-}\mu_N \text{ for } \mu_N = \{\zeta \in \mathbf{C}^\times \mid \zeta^N = 1\}.$$

Identifying $\mathbf{G}_m\text{-}\mu_N$ with $\mathbf{P}^1\text{-}\mu_N\text{-}\{0,\infty\}$, we can identify Γ with $\pi_1(\mathbf{G}_m\text{-}\mu_N)$. Anyway we have a natural action of Γ on $L(m;A)$. Of course this action factors through $\pi_1(T) = \pi_\infty{}^{\mathbf{Z}} = \{\pi_\infty{}^m \mid m \in \mathbf{Z}\}$. We write Γ_ζ for the stabilizer of $\zeta \in \mu_N$. Then $\Gamma_\zeta \cong \pi_\zeta{}^{\mathbf{Z}}$ (where $\pi_\zeta = \pi_r$ for $\zeta = \mathbf{e}(r/N)$) acts trivially on $L(m;A)$. We have a natural map

$$\text{res: } H^1(\Gamma, L(m;A)) \to H^1(\Gamma_\zeta, L(m;A)) = H^1(c_{r/N}, L(m;A)) = L(m;A),$$

which fits into the following exact sequence (Corollary A.2):

$$\text{(1b)} \quad 0 \to H^0(\partial T_N^{S_0}, \mathcal{L}(m;A)) \xrightarrow{\partial} H_c^1(T_N^{S-S_0}, \mathcal{L}(m;A)) \to H^1(T_N^{S-S_0}, \mathcal{L}(m;A))$$
$$\to H^1(\partial T_N^{S_0}, \mathcal{L}(m;A)) \to H_c^2(T_N^{S-S_0}, \mathcal{L}(m;A)) \to H^2(T_N^{S-S_0}, \mathcal{L}(m;A)).$$

Let $T_N = \mathbf{G}_m(\mathbf{C})\text{-}\mu_N \cong T_N^S\text{-}\partial T_N^S = T_N^\emptyset$. Then

$$H^1(T_N^S, \mathcal{L}(m;A)) \cong H^1(T_N^{S-S_0}, \mathcal{L}(m;A)) \cong H^1(T_N, \mathcal{L}(m;A)),$$

because they are of the same homotopy type. Moreover T_N does not have any boundary and hence $H_c^2(T_N, A) \cong A$. By Proposition A.6, $H^2(T_N, \mathcal{L}(m;A))$ is dual to $H_c^0(T_N, \mathcal{L}(m;A)) = 0$ as long as A is a $\mathbf{Q}$-algebra, because there are no compactly supported (locally constant) global sections except 0. This shows $H^2(T_N, \mathcal{L}(m;A)) = 0$. We give a different proof of this fact: We first prove $H_{DR}^2(T, \mathbf{C}) = 0$. We need to show that for any $\omega = f dx \wedge dy$ for $z = x+iy$,

$\omega = d\eta$ for some η. Defining $F(z) = \int_0^y f(x+it)dt$, we have $\frac{\partial F}{\partial y} = f$, and F is a function on T. This shows that $d(Fdx) = \{\frac{\partial F}{\partial x}dx + \frac{\partial F}{\partial y}dy\}\wedge dx = -fdx\wedge dy$. Thus $d(-Fdx) = fdx\wedge dy$, which shows the result in this case. For general T_N, we take a small neighborhood U of each hole $x = \frac{j}{N}$ isomorphic to a punctured disk D at the origin. Then D is isomorphic to a cylinder by $z \mapsto \log(z)$. Thus any differential 2-form ω can be considered to be a 2-form on a cylinder and therefore is of the form $d\eta$. Thus by pulling η back to U, locally any differential 2 form ω is equal to $d\eta$ on U for some η. Taking a C^∞-function on T which is equal to 1 on a smaller open disk in U and vanishes outside U, we know that the support of ω-$d\eta$ does not meet the hole. Thus by changing a representative ω of the cohomology class in $H^2_{DR}(T_N,\mathbf{C})$, we may assume that ω is well defined on T (i.e. ω does not have singularities at the holes). Then as already seen, $\omega = d\eta$ and hence $H^2_{DR}(T_N,\mathbf{C}) = \{0\}$. Since $\mathbf{C}$ is faithfully flat over $\mathbf{Q}$, we see that $H^2(T_N;\mathbf{Q})\otimes_{\mathbf{Q}}\mathbf{C} = H^2(T_N,\mathbf{C}) = \{0\}$. Thus $H^2(T_N,\mathbf{Q}) = 0$, and hence we see that $H^2(T_N,A) = H^2(T_N,\mathbf{Q})\otimes_{\mathbf{Q}}A = \{0\}$. Now we prove $H^2(T_N,\mathcal{L}(m,A)) = \{0\}$ by induction on m. We consider the exact sequence of Γ-modules

$$0 \to L(m;A) \xrightarrow{\times Y} L(m+1;A) \xrightarrow{\pi} A \to 0,$$

where $\pi(P(X,Y)) = P(1,0)$. This induces an exact sequence of sheaves

$$(*) \qquad 0 \to \mathcal{L}(m;A) \xrightarrow{\times Y} \mathcal{L}(m+1;A) \xrightarrow{\pi} A \to 0$$

from which we get another exact sequence

$$0 = H^2(T_N,\mathcal{L}(m;A)) \xrightarrow{\times Y} H^2(T_N,\mathcal{L}(m+1;A)) \xrightarrow{\pi} H^2(T_N,A) = 0.$$

The vanishing of $H^2(T_N,\mathcal{L}(m;A))$ follows from the induction assumption. This shows $H^2(T_N,\mathcal{L}(m+1;A)) = 0$.

We see easily that $H^0(T_N,\mathcal{L}(m;A)) = L(m;A)^\Gamma \cong AY^m$. Thus we have from $(*)$ an exact sequence

$$0 \to A \to H^1(T_N,\mathcal{L}(m;A)) \xrightarrow{\times Y} H^1(T_N,\mathcal{L}(m+1;A)) \xrightarrow{\pi} H^1(T_N,A) \to 0.$$

Thus if A is a $\mathbf{Q}$-algebra,

$$\dim_A H^1(T_N,A) + \dim_A H^1(T_N,\mathcal{L}(m;A)) - 1 = \dim_A H^1(T_N,\mathcal{L}(m+1;A)).$$

Since $\dim_A H^1(T_N,A) = N+1$, we see that

$$\dim_A H^1(T_N,\mathcal{L}(m;A)) + N = \dim_A H^1(T_N,\mathcal{L}(m+1;A)).$$

In particular, we get

$$(2) \qquad \mathrm{rank}_A(H^1(T_N,\mathcal{L}(m;A))) = \mathrm{rank}_A(H^1(T_N^S,\mathcal{L}(m;A))) = N(m+1)+1.$$

Each inhomogeneous 1-cocycle u of Γ is determined by its values $u(\pi_\zeta)$ for $\zeta \in \mu_N \cup \{\infty\}$ because of the relation: $\pi_\infty \prod_{r\in(\mathbf{Z}/N\mathbf{Z})} \pi_r \pi_{-\infty} = 1$. Thus we can embed the module of 1-cocycle $Z^1(\Gamma, L(m;A))$ into copies of $L(m;A)$

$$\mathrm{res} : Z^1(\Gamma, L(m;A)) \hookrightarrow L(m;A)[\mathbf{Z}/N\mathbf{Z}] \oplus L(m;A)$$
$$u \mapsto \{\textstyle\sum_{r\in(\mathbf{Z}/N\mathbf{Z})} u(\pi_r) r\} \oplus u(\pi_\infty),$$

where $L(m;A)[\mathbf{Z}/N\mathbf{Z}]$ denotes the module of a formal linear combination of elements in $\mathbf{Z}/N\mathbf{Z}$ with coefficients in $L(m;A)$, which is in turn isomorphic to $L(m;A[\mathbf{Z}/N\mathbf{Z}])$ for the group algebra $A[\mathbf{Z}/N\mathbf{Z}]$. On the other hand, since π_ζ for $\zeta \in \mu_N$ acts trivially on $L(m;A)$, res brings the submodule $B^1(\Gamma, L(m;A))$ of coboundaries into $(\pi_\infty - 1)L(m;A)$

$$\mathrm{res}(B^1(\Gamma, L(m;A))) = (\pi_\infty - 1)L(m;A).$$

Thus we have

(3a) $H^1(T_N, \mathcal{L}(m;A)) \cong H^1(\Gamma, L(m;A) \cong L(m;A)[\mathbf{Z}/N\mathbf{Z}] \oplus L(m;A)/(\pi_\infty - 1)L(m;A).$

We define $H^1_P(T_N, \mathcal{L}(m;A))$ by the kernel of the natural restriction map

(3b) $\mathrm{res} : H^1(T_N, \mathcal{L}(m;A)) \cong H^1(T_N^{S_0}, \mathcal{L}(m;A)) \to H^1(\partial T_N^{S_0}, \mathcal{L}(m;A)).$

Then we see from the relation that $\pi_\infty \prod_{r\in(\mathbf{Z}/N\mathbf{Z})} \pi_r \pi_{-\infty} = 1$

(3c) $H^1_P(T_N, \mathcal{L}(m;A)) \cong \{u \in L(m;A[\mathbf{Z}/N\mathbf{Z}]) \mid \{u\} \in (\pi_\infty - 1)L(m;A)\},$

where $\{\sum_{r\in \mathbf{Z}/N\mathbf{Z}} u_r r\} = \sum_{r\in \mathbf{Z}/N\mathbf{Z}} u_r$, and from (2)

(3d) $\mathrm{rank}_A H^1_P(T_N, \mathcal{L}(m;A)) = N(m+1)-1$, if A is a $\mathbf{Q}$-algebra.

We now define Hecke operators $T(n)$ for each integer $n \neq 0$ acting on the cohomology groups. We consider the projection map $\pi : \mathbf{C}/n\mathbf{Z} \to \mathbf{C}/\mathbf{Z}$. We put

$$V = \pi^{-1}(T_N) \text{ and } \pi_1(V) = \Phi \text{ as a subgroup of } \Gamma.$$

Since the projection map $\pi : V \to T_N$ is a local isomorphism, we have two natural maps:

$$\pi^* : H^1(T_N, \mathcal{L}(m;\mathbf{Q})) \to H^1(V, \mathcal{L}(m;\mathbf{Q})) \text{ and}$$
$$\mathrm{Tr} : H^1(V, \mathcal{L}(m;\mathbf{Q})) \to H^1(T_N, \mathcal{L}(m;\mathbf{Q})).$$

The existence of the morphism π^* is obvious. We explain the construction of the trace operator Tr. Since the projection $\pi : V \to T_N$ is a local homeomorphism, for each small open set U in a simply connected open set in T_N, $\pi^{-1}(U)$ is isomorphic to a disjoint union of open sets each isomorphic to U. Write simply $M = L(m;A)$. We write π_* for the direct image functor, i.e. $\pi_*\underline{M}$ is the sheaf on T_N generated by the presheaf $U \mapsto \underline{M}(\pi^{-1}(U))$. We take an open subset U_0 in $\pi^{-1}(U)$ so that π induces $U_0 \cong U$. Then by definition, we know that

$\pi_*\underline{M}(U) \cong M(U_0)^d$ for the degree d of π. This isomorphism is explicitly given as follows. We may identify $\pi^{-1}(U)$ with the image of the disjoint union $\bigcup_i \delta_i(U_0)$ in V, where $\{\delta_i\}$ is a complete representative set for $\Phi\backslash\Gamma$. Here we have a commutative diagram for the universal covering H of T_N:

$$\begin{array}{ccccccc} H & \xrightarrow{\pi_0} & \mathbf{C}-N^{-1}\mathbf{Z}/n\mathbf{Z} & \xrightarrow{\pi_1} & V & \xrightarrow{\pi} & T_N \\ \downarrow\delta_i & & \downarrow\delta_i & & \| & & \\ H & \xrightarrow[\pi_0]{} & \mathbf{C}-N^{-1}\mathbf{Z}/n\mathbf{Z} & \xrightarrow[\pi_1]{} & V & & \end{array}$$

in which $\delta_i : H \cong H$ naturally induces $\delta_i : \mathbf{C}^\times\text{-}\mu_N \cong \mathbf{C}^\times\text{-}\mu_N$. Then we identify $\underline{M}(\delta_i(U_0)) = M$ with $\underline{M}(U_0) = M$ via the map:

$$\underline{M}(\delta_i(U_0)) \ni x \mapsto \delta_i^{-1}x \in \underline{M}(U_0) = \underline{M}(U).$$

Now it is clear that $\pi_*\underline{M}_{/S} = \underline{\mathrm{Ind}_{\Gamma/\Phi}(M)}$ on T_N, where $\mathrm{Ind}_{\Gamma/\Phi}(M)$ is the induced module $M\otimes_{\mathbf{Z}[\Phi]}\mathbf{Z}[\Gamma]$ and the Γ-action is given by $\gamma(m\otimes a) = m\otimes a\gamma^{-1}$. Note that the direct image of a flabby sheaf is flabby by definition and that π_* is an exact functor by (A.5a), because π is a local homeomorphism. Therefore any flabby resolution of $\underline{M}_{/S}$ gives rise to a flabby resolution of $(\pi_*\underline{M})_{/T_N}$ just by applying π_*. Thus we know that

$$H^i_*(T_N,\pi_*\underline{M}) = H^i_*(V,\underline{M}) \text{ (Shapiro's lemma).}$$

Now we define $\mathrm{Tr} : \pi_*\underline{M}_{/T_N}(U) \to \underline{M}(U)_{/T_N}$ by $\mathrm{Tr}(x) = \sum_i \delta_i^{-1}x$. This induces a morphism of sheaves. Obviously this is induced from the trace map of algebras $\mathrm{Tr} : \mathbf{Z}[\Gamma] \to \mathbf{Z}[\Phi]$

$$\mathrm{id}\otimes\mathrm{Tr} : \mathrm{Ind}_{\Gamma/\Phi}(M) = M\otimes_{\mathbf{Z}[\Phi\alpha]}\mathbf{Z}[\Gamma] \to M.$$

Then Tr induces a map of cohomology groups

$$\mathrm{Tr} : H^i_*(V,\underline{M}) = H^i_*(T_N{}^*,\pi_*\underline{M}) \to H^i_*(T_N,\underline{M}).$$

For $\alpha_n = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$, we define $\alpha_n(z) = z/n$. Then α_n induces a morphism of sheaves $\alpha_n : \mathcal{L}(m;A)_{/V} \to \mathcal{L}(m;A)_{/T_N}$ by $(z,P(X,Y)) \mapsto (z/n,P((X,Y)^t\alpha_n))$, which in turn induces a morphism of sheaves $\alpha_n{}^*\mathcal{L}(m;A) \to \mathcal{L}(m;A)_{/V}$, where the inverse image $\alpha_n{}^*\mathcal{L}(m;A)$ is the sheaf on V generated by the presheaf $U \mapsto \mathcal{L}(m;A)(\alpha_n(U))$. Then we have a natural pull back map

$$\alpha_n{}^* : H^i(T_N,\mathcal{L}(m;A)) \to H^i(V,\mathcal{L}(m;A)).$$

Then we put

$$T(n) = \mathrm{Tr}\circ\alpha_n{}^*. \tag{4}$$

Note that the action of α_n preserves boundaries at $\pm\infty$. Therefore we can define the operator $T(n)$ in the same manner on $H^i(T_{\pm\infty},\mathcal{L}(m;A))$, $H^i(\partial T_N^{S_0},\mathcal{L}(m;A))$

and $H^1_c(T_N^{S-S_0},\mathcal{L}(m;A))$. Then the boundary exact sequence is compatible with the action of $T(n)$. More generally, we can let an upper triangular matrix $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbf{Z})$ $(ad \neq 0)$ act on $\mathbf{C}$ and $L(m;A)$ by

$$\alpha(z) = (az+b)/d \quad \text{and} \quad \alpha P(X,Y) = P((X,Y)^t\alpha^\iota),$$

where $\alpha^\iota = \det(\alpha)\alpha^{-1}$.

We insert here a computation of the Fourier transform on finite abelian groups which will be used later. Let $\phi : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$ be a function. We define the Fourier transform $\hat{\phi} = \mathcal{F}(\phi) : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$ by

$$\mathcal{F}(\phi)(x) = \mathcal{F}_N(\phi)(x) = \sum_{y\in \mathbf{Z}/N\mathbf{Z}}\phi(y)e(\tfrac{xy}{N}).$$

Then we see from Lemma 2.3.1 that, for $\mathcal{F}(\phi)\,|\,t(x) = \mathcal{F}(\phi)(tx)$,

$$\text{(5a)} \quad \mathcal{F}(\mathcal{F}(\phi)\,|\,t)(-z) = \sum_{x\in \mathbf{Z}/N\mathbf{Z}}\sum_{y\in \mathbf{Z}/N\mathbf{Z}}\phi(y)e(\tfrac{txy}{N})e(\tfrac{-zx}{N})$$
$$= \sum_{y\in \mathbf{Z}/N\mathbf{Z}}\phi(y)\sum_{x\in \mathbf{Z}/N\mathbf{Z}}e(\tfrac{x(ty-z)}{N}) = \begin{cases} N\phi(z/t) & \text{if } t\,|\,z, \\ 0 & \text{otherwise.} \end{cases}$$

Now we apply this Fourier transform to a primitive Dirichlet character $\chi : (\mathbf{Z}/C\mathbf{Z})^\times \to \mathbf{C}^\times$ for a divisor $C \neq 1$ of N. We write $N = N'C$. We extend the character χ to a function $\chi : (\mathbf{Z}/C\mathbf{Z}) \to \mathbf{C}$ just defining its value to be 0 outside $(\mathbf{Z}/C\mathbf{Z})^\times$. Then we compute

$$\text{(5b)} \quad \hat{\chi}(x) = \sum_{y\in \mathbf{Z}/N\mathbf{Z}}\chi(y)e(\tfrac{xy}{N}) = \sum_{y\in \mathbf{Z}/N\mathbf{Z}}\chi(y)\sum_{m \bmod N'}e(\tfrac{x(y+mC)}{N'C})$$
$$= \sum_{y\in \mathbf{Z}/N\mathbf{Z}}\chi(y)e(\tfrac{xy}{N})\sum_{m \bmod N'}e(\tfrac{xm}{N'}) = \begin{cases} \chi^{-1}(x/N')G(\chi)N' & \text{if } N'\,|\,x, \\ 0 & \text{otherwise.} \end{cases}$$

In other words, $\hat{\chi}(tx)$ with $0 < t\,|\,N'$ is supported on $(N'/t)(\mathbf{Z}/N\mathbf{Z})^\times$.

We now compute the action of $T(n)$ on $H^1(T_N,\mathcal{L}(m;\mathbf{C}))$ using differential forms (see Theorem A.2). We consider differential forms with values in $\mathcal{L}(m;\mathbf{C})$ of the following type. For an integer $0 \le j \le m$

$$\text{(6a)} \quad \omega_j(f) = f(z)(X-zY)^{m-j}Y^j dz \text{ for any meromorphic function } f \text{ on } T.$$

In particular, we study the following explicitly defined meromorphic functions. Let $\mu : \mathbf{Z} \to \{\pm 1, 0\}$ be the Möbius function and χ be a primitive Dirichlet character modulo C. Then we put

(6b) $f(z) = f_{id}(z) = \frac{e(z)}{1-e(z)}$,

$$f_{s,id}(z) = \sum_{0<t|s} \mu(t)f(tz) = \sum_{n=1,(n,s)=1}^{\infty} e(nz) \quad \text{for } 0 < s \mid N,$$

(6c) $$f_\chi(z) = \sum_{n=0}^{\infty} \chi(n)e(nz) = \chi(-1)C^{-1}\sum_{n=1}^{\infty} e(nz)\mathcal{F}_C(\mathcal{F}_C(\chi))(n)$$

$$= \chi(-1)C^{-1}\sum_{n=1}^{\infty} e(nz)\sum_{j=0}^{C-1} G(\chi)\chi^{-1}(j)e(\tfrac{nj}{C}) = G(\chi^{-1})^{-1}\sum_{j=0}^{C-1}\chi^{-1}(j)f(z+\tfrac{j}{C}).$$

Since $\Gamma_\infty\alpha_n\Gamma_\infty = \bigcup_{j=0}^{n-1} \Gamma_\infty\alpha_{n,j}$ for $\alpha_{n,i} = \begin{pmatrix} 1 & i \\ 0 & n \end{pmatrix}$, it is easy to see from definition that the action $\omega \mapsto \sum_j(\alpha_{n,j}{}^*\omega) \mid \alpha_{n,j}$ on differential forms induces the operator $T(n)$ on de Rham cohomology groups with coefficients in $\mathcal{L}(m;A)$ (see Theorem A.2), where $\omega \mid \alpha_{n,j}(x) = \alpha_{n,j}{}^\iota\omega(x)$ ($\alpha^\iota = \det(\alpha)\alpha^{-1}$) for the action of $\alpha_{n,j}{}^\iota$ on $L(m;\mathbf{C})$ and $\alpha_{n,j}{}^*\omega$ is the pullback of ω under the action of $\alpha_{n,j}$ on $\mathbf{C}$. We now compute the action of the operator $T(n)$ acting on $\omega_j(f_\chi)$:

$$\omega_j(g) \mid T(n) = \sum_{i=0}^{n-1}\alpha_{n,i}{}^*\omega_j(g) \mid \alpha_{n,i}$$
$$= n^{j-1}\sum_{i=0}^{n-1}(X+iY-\tfrac{z+i}{n}\cdot nY)^{m-j}g(\tfrac{z+i}{n})dz = \omega(n^{j-1}\sum_{i=0}^{n-1}g(\tfrac{z+i}{n})).$$

Then it is easy to see that $\omega_j(g) \mid T(n) = \omega_j(g \mid_j T(n))$ for $g \mid_j T(n)$ given by

(7a) $$g \mid_j T(n) = n^{j-1}\sum_{i=0}^{n-1} g(\tfrac{z+i}{n}).$$

If g has a Fourier expansion $g(z) = \sum_{m=-\infty}^{\infty} a(m,g)e(mz)$ ($a(m,g) \in \mathbf{C}$), then we see that

(7b) $$a(m,g \mid_j T(n)) = n^j a(mn,g).$$

Since $\omega_j(f_\chi)$ gives a closed form, we have its de Rham cohomology class $[\omega_j(f_\chi)]$ in $H^1_{DR}(T_N,\mathcal{L}(m;\mathbf{C}))$ (see Theorem A.2). Then we have

$$[\omega_j(g)] \mid T(n) = [\omega_j(g) \mid T(n)] = [\omega_j(g \mid_j T(n))].$$

We compute the action of $T(n)$ on f_χ using the formula (7b). The functions in (6b) have two Fourier expansions: one at ∞ and the other at $-\infty$, which are given as follows. Since $f(z) = \frac{e(z)}{1-e(z)}$, we may expand it into the geometric series $f(z) = \sum_{n=1}^{\infty} e(nz)$ if $\mathrm{Im}(z) > 0$. Writing the same function as $f(z) = \frac{1}{e(-z)-1}$, we have the expansion valid on the lower half plane:

$$f(z) = -1-\sum_{n=1}^{\infty} e(-nz) \quad \text{if } \mathrm{Im}(z) < 0.$$

We now list the two expansions of f_χ for $\chi \neq \mathrm{id}$, which are computed using the above expansion of f and the definition of f_χ:

(8a) $$f_\chi(z) = \begin{cases} \sum_{n=1}^{\infty}\chi(n)e(nz) & \text{if } \mathrm{Im}(z) > 0, \\ -\sum_{n=1}^{\infty}\chi(-n)e(-nz) & \text{if } \mathrm{Im}(z) < 0. \end{cases}$$

We define $g\,|\,t(z) = g(tz)$ for each divisor t of N. Since the Fourier expansion of f_χ with $\chi \neq \mathrm{id}$ and $f\,|\,t\text{-}f$ with $1 < t\,|\,N$ has no constant terms, the cohomology classes $[\omega_j(f_\chi\,|\,t)]$ and $[\omega_j(f\text{-}f\,|\,t)]$ actually fall in the parabolic cohomology group; that is,

(8b) $$[\omega_j(f_\chi\,|\,t)] \in H^1_P(T_N,\mathcal{L}(m;\mathbf{C})) \text{ for } \chi \neq \mathrm{id} \text{ and } 0 < t\,|\,N',$$
$$[\omega_j(f\text{-}f\,|\,t)] \in H^1_P(T_N,\mathcal{L}(m;\mathbf{C})) \text{ for } 1 < t\,|\,N.$$

By (7b), we have

(8c) $\omega_j(f_\chi\,|\,t)\,|\,T(n) = n^j\chi(n)\omega_j(f_\chi\,|\,t)$, $\omega_0(1)\,|\,T(n) = \omega_0(1)$ for n prime to N.

Theorem 1. *The set of cohomology classes*
$$\{[\omega_j(f_\chi\,|\,t)]\,|\,0 \le j \le m,\ 0 < t\,|\,N'\}\cup\{[\omega_0(1)]\} \quad (= \{[(X\text{-}zY)^m dz]\})$$
forms a basis of $H^1(T_N,\mathcal{L}(m;\mathbf{C}))$, *where* χ *runs over primitive characters* mod C *including the trivial character* mod 1, *and we have written* $N = N'C$.

Proof. Let $\Omega_\chi = \{[\omega_j(f_\chi\,|\,t)]\,|\,0 \le j \le m,\ 0 < t\,|\,N'\}$. Writing W_χ for the subspace of $H^1(T_N,\mathcal{L}(m;\mathbf{C}))$ spanned by Ω_χ, we see from (8c) that $W_\chi \cap \sum_{\xi\neq\chi} W_\xi = \{0\}$. When $\chi \neq \mathrm{id}$, $f_\chi\,|\,t$ has non-trivial simple poles at $P_t = \{x \in N^{-1}\mathbf{Z}\,|\,Ctx \in (\mathbf{Z}/C\mathbf{Z})^\times\}$ by definition, where C is the conductor of χ. Here we understand $C = 1$ for $\chi = \mathrm{id}$ and $(\mathbf{Z}/1\mathbf{Z})^\times = \{0\}$. This shows $\int_{c_x}\omega_j(f_\chi\,|\,t)$ is non-zero if and only if $x \in P_t$. Therefore Ω_χ is linearly independent in W_χ. Thus writing the number of positive divisors of N as $d(N)$, we see that $\dim_{\mathbf{C}} W_\chi = d(N')(m+1)$. Moreover by computation, we know that $\int_{c_\infty}\omega_0(1) \notin (\pi_\infty\text{-}1)L(m;\mathbf{C})$ (see (9b) below) and hence $\omega_0(1) \notin \sum_\chi W_\chi$. Since we know that $\dim_{\mathbf{C}} H^1(T_N,\mathcal{L}(m;\mathbf{C}))$ by (2), what we need to show is $\sum_\chi \dim_{\mathbf{C}} W_\chi = N(m+1)$. Writing $\varphi_{pr}(C)$ for the number of primitive characters modulo C, we have an obvious identity: $\sum_{0<C\,|\,N}\varphi_{pr}(C)d(N/C) = N$ for the Euler function φ. This shows the desired dimension formula.

Exercise 1. Give a detailed proof of the fact that $\sum_{0<C\,|\,N}\varphi_{pr}(C)d(N/C) = N$.

We note that $\omega_j(f_\chi)$ only has poles at reduced fractions $x = \frac{r}{C}$ and

(9a) $$\int_{c_x}\omega_j(f_\chi) = -G(\chi^{-1})^{-1}\chi^{-1}(-j)Y^j(X\text{-}xY)^{m-j}.$$

Similarly the value of $\int_z^{z+1}\omega_0(1)$ at $(X,Y) = (1,0)$ is

(9b) $$(\int_z^{z+1}\omega_0(1))(1,0) = 1.$$

Noting that $H^1_{DR}(c_\infty,\underline{M}) \cong M/(\pi_\infty-1)M$ via $\omega \mapsto \int_z^{z+1}\omega(1,0)$ for $M = L(m;\mathbf{C})$, (9b) shows that the cocycle $\gamma \mapsto \int_z^{\gamma(z)}\omega_0(1)$ is rational. Thus we have

Corollary 1. *Let* K *be the field generated over* $\mathbf{Q}$ *by the values of all characters of* $(\mathbf{Z}/N\mathbf{Z})^\times$. *Then the following elements form a basis of* $H^1(T_N,\mathcal{L}(m;K))$: $\{G(\chi^{-1})\omega_j(f_\chi\,|\,t)\}_{j,t,\chi}\cup\{\omega_0(1)\}$ *in the notation of Theorem 1. Moreover we have* $N^{m-j}G(\chi^{-1})\omega_j(f_\chi) \in H^1(T_N,\mathcal{L}(m;\mathbf{Z}[\chi]))$ *for primitive* χ.

Since Γ_ζ $(\zeta = e(\frac{r}{N}))$ acts trivially on $L(m;A)$, we have a natural restriction map

$$\mathrm{res}_r : H^1(T_N, \mathcal{L}(m;A)) \to H^1(c_{r/N}, \mathcal{L}(m;A)) \cong L(m;A).$$

For each closed form ω, this map is realized by $\omega \mapsto \int_{c_{r/N}}\omega$. Then we define

$$\varphi_m = \varphi : H^1(T_N,\mathcal{L}(m;A)) \to L(m;A[\mathbf{Z}/N\mathbf{Z}]) \text{ by } \varphi(x) = \sum_{r=0}^{N-1}\begin{pmatrix}1 & -\frac{r}{N}\\ 0 & 1\end{pmatrix}\mathrm{res}_r(x)r.$$

By definition φ is injective on $H^1_P(T_N, \mathcal{L}(m;A))$ and

$$\varphi : H^1_P(T_N,\mathcal{L}(m;A)) \cong \{x = \textstyle\sum_r x_r r \in L(m;A[\mathbf{Z}/N\mathbf{Z}]) \,|\, \sum_r x_r \in (\pi_\infty-1)L(m;A)\}.$$

We define the action of $T(n)$ for n prime to N on $L(m;A[\mathbf{Z}/N\mathbf{Z}])$ by

$$T(n)(\textstyle\sum_r x_r r) = \sum_r \alpha_n x_r (rn^{-1}),$$

where $rn^{-1} \in \mathbf{Z}/N\mathbf{Z}$ is such that $(rn^{-1})n \equiv r \bmod N$.

Proposition 1. *We have* $\varphi\circ T(n) = T(n)\circ\varphi$ *for all* n *prime to* N.

Proof. Since $H_1(T_N, A)$ is dual to $H^1(T_N, A)$, the operator $T(n)$ on $H^1(T_N, A)$ induces its dual operator on $H_1(T_N, A)$, which we still denote by $T(n)$. We first compute the action of $T(n)$ on $c_{r/N} \in H_1(T_N, A)$. By definition

$$T(n)(c_{r/N}) = \alpha_n(\pi^*(c_{r/N})) \text{ for } \pi : V \to T_N.$$

Then we see that

$$T(n)(c_{r/N}) = \sum_{i=1}^{|n|-1} c_{(r/Nn)+(i/n)}.$$

Note that $c_{(r/Nn)+(i/n)} = 0$ in the homology group except when $r+Ni \equiv 0 \bmod n$. If $r+Ni \equiv 0 \bmod n$, $c_{(r+Ni)/Nn} = c_{n^{-1}r/N}$ for $n^{-1}r \in \mathbf{Z}/N\mathbf{Z}$. This shows

(10) $$T(n)(c_{r/N}) = c_{n^{-1}r/N}.$$

Note that $H^1(T_N,\mathcal{L}(m;A))/\mathrm{Ker}(\varphi_m) \cong \{H^1(T_N,A)/\mathrm{Ker}(\varphi_0)\}\otimes L(m;A)$, because π_ζ acts trivially on $L(m;A)$. This isomorphism at the level of differential forms is

given by $\omega_j(f) \mapsto fdz \otimes X^{m-j}Y^j = \begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix}\omega_j(f)(z)$. Then it is clear that when $A = \mathbf{C}$, the action of $T(n)$ is interpreted on the right-hand side of the above identity by $T(n)\otimes\alpha_n$ for $T(n)$ on $H^1(T_N,\mathbf{C})$. Then the above formula (10) shows the desired result for $A = \mathbf{C}$. The result for general $\mathbf{Q}$-algebras A then follows from the result over $\mathbf{C}$ because $H^1(T_N,\mathcal{L}(m;A))\otimes_A\mathbf{C} = H^1(T_N,\mathcal{L}(m;\mathbf{C}))$.

Let $\mathbf{H}_m(N;A)$ be the A-subalgebra of $\mathrm{End}_A(H^1(T_N,\mathcal{L}(m;A)))$ generated by $T(n)$ for all n prime to N. For any A-algebra homomorphism $\lambda : \mathbf{H}_m(N;A) \to \mathbf{C}$, we define

$$H^1_P(T_N,\mathcal{L}(m;A))[\lambda] = \{x \in H^1_P(T_N,\mathcal{L}(m;A)) \mid x \mid h = \lambda(h)x\}.$$

All the λ's are explicitly given by $\lambda(T(n)) = n^j\chi(n)$ for Dirichlet characters $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to A^\times$ and integers $0 \le j \le m$. We call λ primitive if the associated Dirichlet character is primitive modulo N. Then we get from Proposition 1

Corollary 2. *(i)* $\mathbf{H}_m(N;A)$ *is isomorphic to the A-subalgebra in* $\mathrm{End}_A(L(m;A))\otimes A[\mathbf{Z}/N\mathbf{Z}]$ *generated over* A *by* $\alpha_n\otimes(n^{-1} \bmod N)$ *for all* n *prime to* N. *In particular,* $\mathbf{H}_0(N;A) \cong A[(\mathbf{Z}/N\mathbf{Z})^\times]$.
We now suppose that A *is a* $\mathbf{Q}$*-algebra. Then we have*
(ii) $H^1_P(T_N,\mathcal{L}(m;A))[\lambda] \cong L(m;A[\mathbf{Z}/N\mathbf{Z}])[\lambda]$ *is free of rank one over* A *if* λ *is primitive;*
(iii) Suppose N *is a prime. Then* $H^1_P(T_N,\mathcal{L}(m;A))[\lambda]$ *is free of rank one over* A *if* $\lambda(T(n)) = 1$ *for all* n *prime to* N*;*
(iv) $H^1_P(T_N,\mathcal{L}(m;\mathbf{C}))[\lambda] = \mathbf{C}\omega_j(f_\chi)$ *if* λ *is primitive and* $\lambda(T(n)) = n^j\chi(n)$ *for all* n *prime to* N;
(v) Suppose N *is a prime. Then* $H^1_P(T_N,\mathcal{L}(m;\mathbf{C}))[\lambda] = \mathbf{C}\omega_0(f\text{-}f \mid N)$ *if* $\lambda(T(n)) = 1$ *for all* n *prime to* N.

Now we consider the natural projection map

$$\rho : H^1_c(T_N^{S-S_0},\mathcal{L}(m;A)) \to H^1_P(T_N,\mathcal{L}(m;A)).$$

We analyze $\mathrm{Ker}(\rho)$ as a Hecke module. By the boundary exact sequence (1b), $\mathrm{Ker}(\rho)$ is the image of

$$H^0(\partial T_N^{S_0},\mathcal{L}(m;A)) = H^0(T_\infty,\mathcal{L}(m;A))\oplus H^0(T_{-\infty},\mathcal{L}(m;A)) \cong H^0(\mathbf{R}/\mathbf{Z},\mathcal{L}(m;A))^2.$$

We see easily that $H^0(\mathbf{R}/\mathbf{Z},\mathcal{L}(m;A)) \cong H^0(\mathbf{Z},\mathcal{L}(m;A)) \cong AY^m$ if A is a ring of characteristic 0. Then it is easy to see from the definition of $T(n)$ that

$$Y^m \mid T(n) = \textstyle\sum_{i=0}^{n-1}\alpha^\iota_{n,i}Y^m = n^{m+1}Y^m.$$

Thus $T(n)$ acts on the one dimensional space $\mathrm{Ker}(\rho)$ via the multiplication by n^{m+1}. The eigenvalue n^{m+1} of $T(n)$ does not appear in $\mathrm{Im}(\rho)$. Thus we have

$$H^1_c(T_N^{S-S_0},\mathcal{L}(m;A)) \cong \mathrm{Im}(T(n)\text{-}n^{m+1})\oplus\mathrm{Ker}(\rho)$$

as long as A is a $\mathbf{Q}$-algebra, and therefore we have a unique section

$$(11) \qquad \iota : H^1_P(T_N,\mathcal{L}(m;A)) \to H^1_c(T_N^{S-S_0},\mathcal{L}(m;A))$$

satisfying $\iota\circ T(n) = T(n)\circ\iota$ for all n. Since $[G(\chi^{-1})N^{m-j}\omega_j(f_\chi)]$ for a primitive χ is an integral element which is an eigenform of all T(n) and is cohomologous to a compactly supported form, we see that

$$\iota([G(\chi^{-1})N^j\omega_j(f_\chi)]) \in H^1_c(T_N^{S-S_0},\mathcal{L}(m;\mathbf{Q}[\chi])).$$

Since $T(a)-a^{m+1}$ is well defined over $H^1_c(T_N^{S-S_0},\mathcal{L}(m;\mathbf{Z}[\chi]))$, we have for any integer $a > 1$ prime to N

(12) $(T(a)-a^{m+1})\iota$ bring the image of $H^1_P(T_N,\mathcal{L}(m;A))$ in $H^1_P(T_N,\mathcal{L}(m;A\otimes_{\mathbf{Z}}\mathbf{Q}))$ into the image of $H^1_c(T_N^{S-S_0},\mathcal{L}(m;A))$ in $H^1_c(T_N^{S-S_0},\mathcal{L}(m;A\otimes\mathbf{Q}))$ for any subalgebra A in $\mathbf{C}$.

§4.2. Cohomological interpretation of Dirichlet L-values

We fix a primitive character $\chi \neq \mathrm{id}$ mod. N. We write $\lambda : \mathbf{H}_m(N;\mathbf{Z}[\chi]) \to \mathbf{Z}[\chi]$ for the $\mathbf{Z}[\chi]$-algebra homomorphism given by $\lambda(T(n)) = \chi(n)$. We fill the hole at 0 of $T_N = T\text{-}N^{-1}\mathbf{Z}$ (resp. $T_N^{S_0}$) and call the new space Y_N (resp. X_N). By (1.10), T(n) for n prime to N still acts on $H^1(Y_N, \mathcal{L}(m;A))$. Since $\omega_j(f_\chi)$ does not have a pole at 0, we may consider $[\omega_j(f_\chi)] \in H^1_P(Y_N,\mathcal{L}(m;\mathbf{C}))$. Let $\delta_\chi = G(\chi^{-1})[\omega_0(f_\chi)]$. By (1.9a) combined with Corollary 1.2, $N^m\delta_\chi$ generates the λ-eigenspace $H^1_P(Y_N, \mathcal{L}(m;A))[\lambda]$ defined in Corollary 1.2. We consider the integral $\int_{c^0}\delta_\chi$ on the vertical line c^0 passing the origin. By (1.8a), we have

$$(1) \qquad \int_{c^0}\delta_\chi = -G(\chi^{-1})\sum_{j=0}^{m}(2\pi i)^{-j-1}(1-\chi(-1)(-1)^j)j!\binom{m}{j}L(1+j,\chi)X^{m-j}Y^j.$$

The embedding $\mathbf{R} \to Y_N$ given by $y \mapsto iy$ induces a morphism

$$\mathrm{Int} : H^1_c(Y_N, \mathcal{L}(m;A)) \to H^1_c(\mathbf{R},\mathcal{L}(m;A)) \cong L(m;A) \quad (\omega \mapsto \int_{-\infty}^{\infty} \omega).$$

Here $\mathcal{L}(m;A)$ on $\mathbf{R}$ is a constant sheaf. By Corollary 1.1, for each integer a prime to N, the cohomology class $(a^{m+1}-\chi(a))[N^mG(\chi^{-1})\omega_0(f_\chi)]$ for primitive χ is integral (i.e. is contained in the image of $H^1(X_N, \mathcal{L}(m;\mathbf{Z}[\chi]))$); moreover, by (1.12), it can be regarded as being contained inside the image of $H^1_c(X_N, \mathcal{L}(m;\mathbf{Z}[\chi]))$ in $H^1_c(X_N, \mathcal{L}(m;\mathbf{Q}[\chi]))$. Then by a theorem of de Rham (Theorem A.2), we see that

$$(a^{m+1}-\chi(a))N^m\int_{c^0}\delta_\chi = \mathrm{Int}(N^m(a^{m+1}-\chi(a))\delta_\chi) \in \mathbf{Z}[\chi].$$

To include the identity character $\chi = \mathrm{id}$, we modify a little the cycle c^0. Instead of c^0, we take a small real number $\varepsilon > 0$ and put $\tilde{c}^0 = c^\varepsilon$. Since $\tilde{c}^0$ and c^0 are homologous in $H_1(X_N,\partial X_N;\mathbf{Z})$, we get the same result: $\int_{c^0}\omega = \int_{c^\varepsilon}\omega$ as long as ω is holomorphic at 0. We define Int' on $H^1_c(T_N^{S-S_0},\mathcal{L}(m;A))$ using $\tilde{c}^0$ in place of c^0 in the same manner as Int. The map $\rho_m : L(m;A) \to YL(m-1;A)$ given by $\rho_m(\sum_i a_i X^{m-i}Y^i) = \sum_{i\geq 1} a_i X^{m-i}Y^i$ combined with Int' gives

$$\mathrm{Int}_m : H^1_c(Y_N, \mathcal{L}(m;A)) \to H^1_c(\mathbf{R}, YL(m-1;A)) \cong YL(m-1;A).$$

The power z^i of z of the coefficient of $X^{n-i}Y^i$ in $(X-zY)^m$ kills the pole at $z = 0$ if $i > 0$, and thus we can compute the map Int_m in the same way as Int even for $\omega_0(f\text{-}f\,|\,q)$. Then for a prime to q,

$$\begin{aligned}&(a^{m+1}-T(a))\mathrm{Int}_m(q^m\omega_0(f\text{-}f\,|\,q))\\ &= -q^m(a^{m+1}-1)\sum_{j=1}^m j!(2\pi i)^{-j-1}(1-(-1)^j)\binom{m}{j}(1-q^{-j-1})\zeta(j+1)X^{n-j}Y^j \in YL(m-1;\mathbf{Z}).\end{aligned}$$

Thus this proves again the result we obtained as Corollary 2.3.2:

Theorem 1. *Let* $\chi \neq \mathrm{id}$ *be a primitive Dirichlet character modulo* N *and* a *be any integer prime to* N. *Then*

$$j!N^jG(\chi^{-1})(2\pi i)^{-j-1}(1-\chi(-1)(-1)^j)(a^{m+1}-\chi(a))L(1+j,\chi) \in \mathbf{Z}[\chi] \text{ and}$$
$$(2\pi i)^{-j-1}(1-(-1)^j)(a^{j+1}-1)q^j(1-q^{-j-1})j!\zeta(1+j) \in \mathbf{Z} \text{ for all primes } q.$$

By the functional equation, we have for $j \in \mathbf{N}$,

$$L(-j,\chi^{-1}) = j!(1-\chi(-1)(-1)^j)N^jG(\chi^{-1})(2\pi i)^{-j-1}L(1+j,\chi). \tag{2}$$

§4.3. p-adic measures and locally constant functions

In §3.3, we studied the structure of the space of p-adic measures on $\mathbf{Z}_p$ in terms of interpolation series. Here we describe the space via locally constant functions. Let p be a prime and G be a topological group of the form $G = \mu\times\mathbf{Z}_p^r$ for a finite group μ. We put $G_i = (p^i\mathbf{Z}_p)^r$. We fix a finite extension $K/\mathbf{Q}_p$ and write A for its p-adic integer ring. We equip K a normalized p-adic norm $|\ |_p$ such that $|p|_p = p^{-1}$. For any topological space X, we write $\mathcal{LC}(G;X)$ for the space of locally constant functions on G with values in X. Thus a function $\phi : G \to X$ is in $\mathcal{LC}(G;X)$ if and only if for any point $g \in G$, there exists an open neighborhood V_g of g in G such that the restriction of ϕ to V is a constant function. By definition, it is obvious that for any locally constant function ϕ and for any subset S of X, $\phi^{-1}(S) = \bigcup_{g\in\phi^{-1}(S)}V_g$ is open; in particular, ϕ is

continuous. Since G is compact, $G = \bigcup_{g\in G} V_g$ implies that we can find finitely many points $g_1, \ldots, g_s$ on G such that $G = \bigcup_{j=1}^{s} V_{g_j}$. By the definition of the topology of G, a basis of open sets of G is given by $\{g+G_i \mid g \in G, i = 0,1,\cdots\}$. Thus for large i, $V_{g_j} \supset g_j+G_i$, that is, ϕ induces a function

$$\phi_i : G/G_i \to X \quad \text{and} \quad \phi = \phi_i \circ \pi_i$$

for the projection $\pi_i : G \to G/G_i$. The space $\mathcal{C}(G/G_i;X)$ is made of all functions on the finite group G/G_i with values in X and is isomorphic to the set $X[G/G_i]$ of formal linear combinations $\sum_{g\in G/G_i} x_g g$ with $x_g \in X$ via $\phi \mapsto \sum_{g\in G/G_i} \phi(g)g$. Thus we see that

$$(1) \qquad \mathcal{LC}(G;X) = \varinjlim_i \mathcal{C}(G/G_i;X) = \varinjlim_i X[G/G_i].$$

For a topological ring R, we define the space of distributions $\mathcal{D}ist(G;R)$ by

$$(2) \qquad \mathcal{D}ist(G;R) = \mathrm{Hom}_R(\mathcal{LC}(G;R), R).$$

If $\varphi \in \mathcal{D}ist(G;R)$ and if χ_S is the characteristic function of an open set S of G, we write $\varphi(S)$ for $\varphi(\chi_S)$. Since $\chi_{h+G_i} = \sum_{g\in G_i/G_j} \chi_{h+g+G_j}$ for $j \geq i$, we have the following distribution relation:

$$(3) \qquad \varphi(h+G_i) = \sum_{g\in G_i/G_j} \varphi(h+g+G_j) \quad \text{for all } h \in G \text{ and } j \geq i.$$

On the other hand, if we are given a system φ assigning a value $\varphi(g+G_i) \in R$ for all $g \in G/G_i$ and for all i sufficiently large satisfying (3), we can extend φ to a distribution as follows. For a given $\phi \in \mathcal{LC}(G;R)$, taking sufficiently large i so that $\varphi(g+G_i)$ is well defined and $\phi = \phi_i \circ \pi_i$ with $\phi_i : G/G_i \to R$, we define $\varphi(\phi) = \sum_{g\in G/G_i} \phi_i(g)\varphi(g+G_i)$. This is well defined because for any other choice $j \geq i$ of the index, we have

$$\varphi(\phi) = \sum_{h\in G/G_i} \phi_i(g)\varphi(h+G_i) = \sum_{h\in G/G_i} \phi_i(g) \sum_{g\in G_i/G_j} \varphi(h+g+G_j)$$
$$= \sum_{g\in G/G_j} \phi_j(g)\varphi(g+G_j) \quad \text{because } \phi_j(g) = \phi_i(g) \text{ for all } g \in G.$$

Thus we have

Proposition 1. *Let* R *be a topological ring. Then a function* $\varphi : \{g+G_i \mid i \geq M, \text{ and } g \in G\} \to R$ *is induced from a distribution if and only if* φ *satisfies (3) for all* $j \geq i \geq M$.

Let R be a closed subring of K. For any measure $\varphi \in \mathcal{M}eas(G;R)$, φ induces a distribution, again denoted by φ, by $\varphi(\phi) = \int \phi d\varphi$. Then $|\varphi(\phi)|_p \leq |\varphi|_p |\phi|_p$. Thus $|\varphi|_p = \mathrm{Sup}_{0\neq\phi\in \mathcal{LC}(G;R)} |\varphi(\phi)|_p / |\phi|_p$ is finite. Now we want to show the converse. For any continuous function $\phi : G \to R$, we can find for each

positive $\varepsilon > 0$ and $g \in G$ a small open neighborhood V_g of g such that $|\phi(h)-\phi(h')|_p < \varepsilon$ for all h and $h' \in V_g$. Thus $G = \bigcup_{g\in G} V_g$. Since G is compact, we can choose finitely many $g_1,\ldots, g_s \in G$ such that $\bigcup_{j=1}^{s} V_{g_j}$ and i large such that $V_{g_j} \supset g+G_i$ for all $g \in V_{g_j}$. Then choosing a complete representative set R for G/G_i and defining $\phi_\varepsilon : G/G_i \to R$ by $\phi_\varepsilon(h) = \phi(g)$ if $h \in g+G_i$, we see that $\phi_\varepsilon \in \mathcal{LC}(G;R)$ and $|\phi_\varepsilon-\phi|_p < \varepsilon$. Thus $\mathcal{LC}(G;R)$ is dense in $\mathcal{C}(G;R)$ and

(4) $|\phi_{\varepsilon'}-\phi_\varepsilon|_p < |(\phi_{\varepsilon'}-\phi)+(\phi-\phi_\varepsilon)|_p \le \max(|\phi_{\varepsilon'}-\phi|_p, |\phi-\phi_\varepsilon|_p) < \max(\varepsilon,\varepsilon')$.

Let φ is a distribution with bounded norm $|\varphi|_p$. This is equivalent to saying that $|\varphi(g+G_i)|_p$ is bounded by $|\varphi|_p$ for all $i \ge M$ and all $g \in G$. Then (4) implies

$$|\varphi(\phi_\varepsilon)-\varphi(\phi_{\varepsilon'})|_p \le |\varphi|_p |\phi_{\varepsilon'}-\phi_\varepsilon|_p < |\varphi|_p \max(\varepsilon,\varepsilon')$$

and $\{\varphi(\phi_{1/n})\}$ is a Cauchy sequence in R. We then define

$$\varphi(\phi) = \lim_{n\to\infty} \varphi(\phi_{1/n}) \in R.$$

Then it is easy to verify that $\varphi \in \mathcal{Meas}(G;R)$. Thus we have

Proposition 2. *For any closed subring* R *of* K, $\mathcal{LC}(G;R)$ *is dense in* $\mathcal{C}(G;R)$. *Any bounded distribution on* G *with values in* R *can be uniquely extended to a bounded measure with values in* R. *In particular,*

$$\mathcal{Meas}(G;A) \cong \mathcal{Dist}(G;A) \text{ via the restriction to } \mathcal{LC}(G;A)$$

for the p-adic integer ring A *of* K.

§4.4. Another construction of p-adic Dirichlet *L*-functions

We reconstruct the p-adic measure which interpolates the values of Dirichlet *L*-functions via cohomology theory. This type of formalism (the formalism of modular symbols) was found by Mazur in [Mz1] and [MzS] where he applied it to *L*-functions of elliptic modular forms (see §6.5).

We fix a prime p. Let $K/\mathbf{Q}_p$ be a finite extension and A be the p-adic integer ring of K. Let $N > 1$ be a positive integer prime to the fixed prime p. Let X_N be the space obtained from $T_N^{S_0}$ by filling the hole around 0. The inclusion: $c^r \to T_N^{S_0}$ induces an A-linear map: $H_c^1(X_N,\mathcal{L}(m;A)) \to L(m;A)$, which we write as $\xi \mapsto \int_{c^r} \xi$. Then we consider a map

(1) $$c : p^{-\infty}\mathbf{Z} = \bigcup_{i=1}^{\infty} p^{-i}\mathbf{Z} \to \mathrm{Hom}_A(H_c^1(X_N,\mathcal{L}(m;A)), L(m;K))$$
$$\textit{given by } c(r)(\xi) = \int_{c^r} \xi.$$

For $\xi \in H^1_c(X_N,\mathcal{L}(m;K))$, we write $c_\xi(r) = \begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix}\int_{c^r}\xi$. Here we let the multiplicative semi-group $M_2(\mathbf{Z})\cap GL_2(\mathbf{Q})$ act on $L(m;K)$ by $\alpha P(X,Y) = P((X,Y)^t\alpha^\iota)$ $(\alpha \in M_2(\mathbf{Z}))$, where $\alpha^\iota = \det(\alpha)\alpha^{-1}$. Then $c_\xi(r+1) = c_\xi(r)$ by definition, and c_ξ factors through $\mathbf{Q}_p/\mathbf{Z}_p = p^{-\infty}\mathbf{Z}/\mathbf{Z}$. Supposing $\xi \,|\, T(p) = a_p\xi$ with $|a_p|_p = 1$, we define a distribution Φ_ξ on $\mathbf{Z}_p^\times$ by

$$(2) \qquad \Phi_\xi(z+p^m\mathbf{Z}_p) = a_p^{-m}\begin{pmatrix} p^m & 0 \\ 0 & 1 \end{pmatrix}c_\xi(\tfrac{z}{p^m}) \text{ for } z = 1, 2, \ldots \text{ prime to } p.$$

This is well defined because $c_\xi(r+1) = c_\xi(r)$. We take $G = \mathbf{Z}_p^\times$ and fix an isomorphism $G \cong \mu\times\mathbf{Z}_p$ for a finite group μ. Then $\mu = \{\zeta \in \mathbf{Z}_p^\times \,|\, \zeta^{\varphi(p)} = 1\}$, where φ is the Euler function and $\mathbf{p} = 4$ or p according as $p = 2$ or not. Then the subgroup $G_i = 1+p^i\mathbf{Z}_p$ corresponds to $p^i\mathbf{Z}_p$. To show that Φ_ξ actually gives a distribution, we need to check the distribution relation (3.3). We compute

$$\begin{aligned}
&\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\sum_{j=1}^{p-1} c_\xi(\tfrac{j+x}{p}) = \sum_j \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -(j+x)/p \\ 0 & 1 \end{pmatrix}c(\tfrac{j+x}{p})(\xi) \\
&= \sum_j \begin{pmatrix} p & -x-j \\ 0 & 1 \end{pmatrix}c(\tfrac{j+x}{p})(\xi) \\
&= \sum_j \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}^\iota c(\tfrac{j+x}{p})(\xi) = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}c(x)(\xi \,|\, T(p)) = a_p c_\xi(x).
\end{aligned}$$

This shows

$$\sum_{j=1}^{p-1} \Phi_\xi(x+jp^m+p^{m+1}\mathbf{Z}_p) = \Phi_\xi(x+p^m\mathbf{Z}).$$

The general distribution relation (3.3) then follows from the iteration of this relation. By a similar argument, we see that

$$(3) \quad |\Phi_\xi(z+p^m\mathbf{Z}_p)|_p = |a_p^{-m}\begin{pmatrix} p^m & 0 \\ 0 & 1 \end{pmatrix}c_\xi(\tfrac{z}{p^m})|_p = |\begin{pmatrix} p^m & -z \\ 0 & 1 \end{pmatrix}c(\tfrac{z}{p^m})(\xi)|_p \le |\xi|_p,$$

where $|\xi|_p = \mathrm{Sup}_{x,j}|\xi_j(x)|_p$ for the coefficient $\xi_j(x)$ in $X^{m-j}Y^j$ of $c(x)(\xi)$ with x running over $p^{-\infty}\mathbf{Z}$. Thus Φ_ξ is bounded and, by Proposition 3.2, we have a unique measure Φ_ξ extending the distribution Φ_ξ. Projecting down to the coefficient in $\binom{m}{j}X^{m-j}Y^j$ of Φ_ξ, we get a measure $\varphi_{\xi,j}$. Now we want to show $d\varphi_{\xi,j}(x) = x^j d\varphi_{\xi,0}$. To show this, we may assume that $|\xi|_p \le 1$ by multiplying by a constant if necessary. We follow the argument given in [Ki] which originates with Manin [Mn1] and [Mn2]. For $\phi \in \mathcal{C}(\mathbf{Z}_p^\times;A)$, take a locally constant function $\phi_k : (\mathbf{Z}/p^{n(k)}\mathbf{Z})^\times \to A$ such that $|\phi_k-\phi|_p < p^{-k}$ and $n(k) \ge k$. Then we know that $|\Phi_\xi(\phi_k)-\Phi_\xi(\phi)|_p < |\Phi_\xi|_p p^{-k} < p^{-k}$ and

$$\begin{aligned}
\Phi_\xi(\phi_k) &= \sum_{z=1,(p,z)=1}^{p^{n(k)}-1} \phi_k(z)a_p^{-n(k)}\begin{pmatrix} p^{n(k)} & 0 \\ 0 & 1\end{pmatrix} c_\xi\left(\tfrac{z}{p^{n(k)}}\right) \\
&= \sum_{z=1,(p,z)=1}^{p^{n(k)}-1} \phi_k(z)a_p^{-n(k)}\begin{pmatrix} p^{n(k)} & -z \\ 0 & 1\end{pmatrix} c\left(\tfrac{z}{p^{n(k)}}\right)(\xi) \\
&= a_p^{-n(k)}\sum_{j=0}^{m} \sum_{z=1,(p,z)=1}^{p^{n(k)}-1} \phi_k(z)(X+zY)^{m-j}(p^{n(k)}Y)^j\xi_j\left(\tfrac{z}{p^{n(k)}}\right) \\
&\equiv a_p^{-n(k)} \sum_{z=1,(p,z)=1}^{p^{n(k)}-1} \phi_k(z)(X+zY)^m\xi_0\left(\tfrac{z}{p^{n(k)}}\right) \mod p^k \\
&\equiv \textstyle\sum_{j=0}^{m} \int\phi(z)z^j d\varphi_{\xi,0}(z)\binom{m}{j}X^{m-j}Y^j \mod p^k,
\end{aligned}$$

where $\xi_j(x)$ is the coefficient of $c(x)(\xi)$ in $X^{n-j}Y^j$. Thus taking the limit making $k \to \infty$, we see that

$$\int\phi d\varphi_{\xi,j} = \int\phi(z)z^j d\varphi_{\xi,0}(z) \quad \text{for all} \quad \phi \in \mathcal{C}(\mathbf{Z}_p^\times;K). \tag{4}$$

Let N be a positive integer prime to p. We take $\xi = \delta_{\chi^{-1}}$ for each primitive character χ modulo N ($\delta_{\chi^{-1}}$ may not be p-integral but is bounded because $(a^{m+1}-\chi^{-1}(a))\delta_{\chi^{-1}}$ is p-integral as seen in §1). Then we write Φ_ξ as Φ_χ and compute for any primitive character ϕ of $(\mathbf{Z}/p^r\mathbf{Z})^\times$ the integral $\int\phi d\Phi_\chi$. For each triangular matrix $\alpha = \begin{pmatrix} a & b \\ 0 & d\end{pmatrix}$, we let α act on $\mathbf{C}$ by $\alpha(z) = (az+b)/d$, and for any differential form ω on $\mathbf{C}$, we write $\alpha^*\omega$ for the pullback of ω by the action of α. We see that, if $\phi \neq 1$, then $\chi\phi$ is primitive and

$$\begin{aligned}
&\int\phi d\Phi_\chi = \textstyle\sum_{x\in(\mathbf{Z}/p^r\mathbf{Z})^\times}\phi(x)\chi(p)^r\begin{pmatrix} p^r & 0 \\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & -x/p^r \\ 0 & 1\end{pmatrix} c\left(\tfrac{x}{p^r}\right)(\delta_{\chi^{-1}}) \qquad (5) \\
&= \chi(p)^r\begin{pmatrix} p^r & 0 \\ 0 & 1\end{pmatrix}\int_{c_0}\textstyle\sum_{x\in(\mathbf{Z}/p^r\mathbf{Z})^\times}\phi(x)\begin{pmatrix} 1 & -x/p^r \\ 0 & 1\end{pmatrix}\left\{\begin{pmatrix} 1 & x/p^r \\ 0 & 1\end{pmatrix}^*\delta_{\chi^{-1}}\right\} \\
&= \chi(p)^r\begin{pmatrix} p^r & 0 \\ 0 & 1\end{pmatrix}G(\chi)G(\phi)\int_{c_0}f_{(\chi\phi)^{-1}}(X-zY)^m dz \\
&= -\chi(p)^rG(\chi)G(\phi)\sum_{j=0}^{m}(2\pi i)^{-j-1}(1-\chi\phi(-1)(-1)^j)j!p^{rj}L(1+j,(\chi\phi)^{-1})\binom{m}{j}X^{m-j}Y^j \\
&= -\chi(p)^rG(\chi)G(\phi)G(\phi\chi)^{-1}\sum_{j=0}^{m}N^{-j}L(-j,\chi\phi)\binom{m}{j}X^{m-j}Y^j \quad \text{(see (2.2))} \\
&= -\phi^{-1}(N)\sum_{j=0}^{m}N^{-j}L(-j,\chi\phi)\binom{m}{j}X^{m-j}Y^j.
\end{aligned}$$

Here we have used the formula

$$(6)\qquad G(\chi)G(\phi) = \sum_{u \bmod N,\ v \bmod p^r}\chi(u)\phi(v)e(\tfrac{u}{N}+\tfrac{v}{p^r})$$
$$= \sum_{u \bmod N,\ v \bmod p^r}\chi(u)\phi(v)e(\frac{p^r u+Nv}{Np^r})$$
$$= \chi^{-1}(p^r)\phi^{-1}(N)\sum_{u \bmod N,\ v \bmod p^r}\chi\phi(p^r u+Nv)e(\frac{p^r u+Nv}{Np^r})$$
$$= \chi^{-1}(p^r)\phi^{-1}(N)G(\chi\phi).$$

Now assume that ϕ is trivial. Then we see that

$$\sum_{x\in(\mathbf{Z}/Np\mathbf{Z})^\times}\phi(x)\begin{pmatrix}1 & -x/p\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & x/p\\ 0 & 1\end{pmatrix}^*\delta_{\chi^{-1}} = -(f_{\chi^{-1}}-p\chi^{-1}(p)f_{\chi^{-1}}\,|\,p)(X-zY)^m dz.$$

This shows that

$$(7)\qquad \int d\Phi_\chi = \chi(p)\sum_{j=0}^{m}(1-\chi^{-1}(p)p^{-j})p^j L(-j,\chi)\binom{m}{j}X^{m-j}Y^j$$
$$= -\sum_{j=0}^{m}N^{-j}(1-\chi(p)p^j)L(-j,\chi)\binom{m}{j}X^{m-j}Y^j.$$

Now we assume that $\chi = \mathrm{id}$ and $N = q \neq p$ is a prime. Then we take $\xi = \iota(\omega_0(f\text{-}f\,|\,q))$ and write φ_{id} for ϕ_ξ. Replacing c^0 by $\tilde{c}^0$ introduced in §2 to avoid singularity at 0, we see from (1.12) that φ_χ is bounded and

$$(8)\qquad -\int\phi d\Phi_\chi = \begin{cases}\sum_{j=0}^{m}(1-\phi^{-1}(q)q^{-j-1})L(-j,\phi)\binom{m}{j}X^{m-j}Y^j & \text{if } \phi \neq \mathrm{id},\\ \alpha X^m+\sum_{j=1}^{m}(1-q^{-j-1})(1-\chi(p)p^j)\zeta(-j)\binom{m}{j}X^{m-j}Y^j & \text{if } \phi = \mathrm{id},\end{cases}$$

for a suitable $\alpha \in \mathbf{Q}$. Thus projecting down to the coefficient of $\binom{m}{j}X^m$ in Φ_χ, we get by (4) a measure φ_χ satisfying, for all characters $\phi : (\mathbf{Z}/p^r\mathbf{Z})^\times \to K^\times$,

$$(9)\qquad -\int\phi(z)z^j d\varphi_\chi(z) = \begin{cases}\phi(N)^{-1}N^{-j}(1-\chi\phi(p)p^j)L(-j,\chi\phi) & \text{if } \chi \neq \mathrm{id},\\ (1-\phi^{-1}(q)q^{-1-j})(1-\phi(p)p^j)L(-j,\phi) & \text{if } \chi = \mathrm{id}.\end{cases}$$

Here at first sight, the measure φ_χ looks to depend on $L(m;A)$ or m. However the evaluation formula (9) does not depend on m. Note that every function on $f : (\mathbf{Z}/p^r\mathbf{Z})^\times \to K$ can be written by Lemma 2.3.1 as

$$f(g) = \varphi(p^r)^{-1}\sum_x f(x)\sum_\phi\phi(x^{-1}g) = \varphi(p^r)^{-1}\sum_\phi\phi(g)\{\sum_x f(x)\phi(x^{-1})\}.$$

Thus every locally constant function is a linear combination of finite order characters by (3.1). Since the space of locally constant functions is dense in the space of continuous functions (Proposition 3.2), each measure is determined by its value on finite order characters. This shows the independence of φ_χ with respect to m. Summing up all these discussions, we get

Theorem 1. *Let* p *be a prime and* N *be a positive integer prime to* p. *For each primitive Dirichlet character* $\chi \neq \mathrm{id}$ *modulo* N, *we have a unique p-adic measure* φ_χ *on* $\mathbf{Z}_p^\times$ *such that for all finite order characters* ϕ *of* $\mathbf{Z}_p^\times$ *and* $j \in \mathbf{N}$, *we have*

$$\int \phi(z) z^j d\varphi_\chi(z) = -\phi(N)^{-1} N^{-j} (1-\chi\phi(p)p^j) L(-j,\chi\phi).$$

As for the identity character, fixing a prime q *prime to* p, *we have a unique p-adic measure* φ_q *on* $\mathbf{Z}_p^\times$ *such that for all finite order characters* ϕ *of* $\mathbf{Z}_p^\times$ *and* $j \in \mathbf{N}$, *we have*

$$\int \phi(z) z^j d\varphi_q(z) = -(1-\phi^{-1}(q)q^{-1-j})(1-\phi(p)p^j) L(-j,\phi).$$

By the evaluation formula in the above theorem, we conclude that $\varphi_q = -\zeta_{q^{-1}}$ on $\mathbf{Z}_p^\times$ for the measure ζ_a defined in Theorems 3.5.1 and 3.9.1. We now define the p-adic Dirichlet L-function for each primitive character $\chi : (\mathbf{Z}/Np^r\mathbf{Z})^\times \to K^\times$, writing χ_N (resp. χ_p) for the restriction of χ to $(\mathbf{Z}/N\mathbf{Z})^\times$ (resp. $(\mathbf{Z}/p^r\mathbf{Z})^\times$), by

$$L_p(s,\chi) = \begin{cases} -\chi_p\omega^{-1}(N)\langle N\rangle^{-s}\int_{\mathbf{Z}_p^\times}\chi_p\omega^{-1}(x)\langle x\rangle^{-s}d\varphi_{\chi_N}(x) & \text{if } \chi_N \neq \mathrm{id}, \\ -(1-\chi_p^{-1}(q)\langle q\rangle^{s-1})^{-1}\int_{\mathbf{Z}_p^\times}\chi_p\omega^{-1}(x)\langle x\rangle^{-s}d\varphi_{\chi_N}(x) & \text{if } \chi_N = \mathrm{id}. \end{cases}$$

Thus we get a generalization of Theorem 3.5.2:

Theorem 2. *For each primitive Dirichlet character* $\chi : (\mathbf{Z}/Np^r\mathbf{Z})^\times \to K^\times$ *with* $\chi(-1) = 1$, *there exists a* p*-adic analytic function* $L_p(s,\chi)$ *on* $\mathbf{Z}_p$ *if* $\chi \neq \mathrm{id}$ *and on* $\mathbf{Z}_p - \{1\}$ *if* $\chi = \mathrm{id}$ *such that*

$$L_p(-m,\chi) = (1-\chi\omega^{-m-1}(p)p^m) L(-m,\chi\omega^{-m-1}) \text{ for all } m \in \mathbf{N}.$$

Chapter 5. Elliptic modular forms and their L-functions

A modular form of weight k with respect to $SL_2(\mathbf{Z})$ is a holomorphic function on the upper half complex plane

$$\mathcal{H} = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$$

satisfying the functional equation

$$f\left(\frac{az+b}{cz+d}\right) = f(z)(cz+d)^k \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}).$$

Thus it is invariant under the translation $z \mapsto z+1$ and has Fourier expansion:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e(nz) \quad \text{for} \quad \mathbf{e}(z) = \exp(2\pi\sqrt{-1}z).$$

We always assume that $a_n = 0$ if $n < 0$. A typical example of such a modular form is given by absolutely convergent Eisenstein series

$$E'_k(z) = \sum{}'_{(m,n)} (mz+n)^{-k} \text{ for every even integer } k > 2,$$

where Σ' means that the summation is taken over all ordered pairs of integers (m,n) but $(0,0)$. The Fourier expansion of $E'_k(z)$ is well known (we will verify the expansion later):

$$E_k(z) = \left(\frac{2(2\pi\sqrt{-1})^k}{(k-1)!}\right)^{-1} E'_k(z) = 2^{-1}\zeta(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n,$$

where $\sigma_m(n) = \Sigma_{0<d\,|\,n} d^m$ is the sum of m-th powers of divisors of n. In this section, we study the complex analytic theory of modular forms. To each holomorphic modular form $f = \sum_{n=0}^{\infty} a_n q^n$, we associate a Dirichlet series

$$L(s,f) = \sum_{n=1}^{\infty} a_n n^{-s},$$

and with each pair of modular forms f and $g = \sum_{n=0}^{\infty} b_n q^n$, we also associate another Dirichlet series

$$D(s,f,g) = \sum_{n=1}^{\infty} \bar{a}_n b_n n^{-s}.$$

Then, we will study algebraicity properties of these modular L-functions later in this chapter and Chapters 6 and 10.

§5.1. Classical Eisenstein series of $GL(2)_{/\mathbf{Q}}$

A subgroup of $SL_2(\mathbf{Z})$ is called a congruence subgroup if it contains all matrices $\alpha \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod NM_2(\mathbf{Z})$ in $SL_2(\mathbf{Z})$ for an integer $N > 0$. We study here Eisenstein series for congruence subgroups of $SL_2(\mathbf{Z})$. In this book, we are mainly concerned with modular forms with respect to the following type of congruence subgroups: for each positive integer N

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \mid c \in N\mathbf{Z}\right\},$$

$$\Gamma_1(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \mid c \in N\mathbf{Z} \text{ and } d \equiv 1 \bmod N\right\}.$$

In particular, we are interested in the case where $N = p^r$ for a rational prime p. We write Δ for one of these groups. A more detailed study of classical Eisenstein series for general congruence subgroups can be found in [M, Chap.7]. Each matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $\det(\gamma) > 0$ acts on the upper half complex plane

$$\mathcal{H} = \{z \in \mathbf{C} \mid \operatorname{Im}(z) > 0\}$$

via the linear fractional transformation $z \mapsto \gamma(z) = \frac{az+b}{cz+d}$. Then for any given function f on $\mathcal{H}$, we define an action of γ on f by

$$f|_k\gamma(z) = \det(\gamma)^{k-1} f(\gamma(z))(cz+d)^{-k}.$$

For each positive integer k, the space of modular forms $\mathcal{M}_k(\Delta)$ of weight k for Δ consists of holomorphic functions f on $\mathcal{H}$ satisfying the following conditions:

(1a) $$f|_k\gamma = f \text{ for all } \gamma \in \Delta;$$

(1b) For each $\alpha \in SL_2(\mathbf{Z})$, $f|_k\alpha$ has the following type of Fourier expansion of the following form: $f|_k\alpha(z) = \sum_{n\geq 0} a(n, f|_k\alpha)e(nz)$, where n runs over a fractional ideal $a\mathbf{Z}$ in $\mathbf{Q}$.

A modular form f is called a cusp form if $a(0, f|_k\alpha) = 0$ for all $\alpha \in SL_2(\mathbf{Z})$. We write as $\mathcal{S}_k(\Delta)$ the subspace of $\mathcal{M}_k(\Delta)$ consisting of cusp forms. Let $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ be a character. Then we write $\mathcal{M}_k(\Gamma_0(N),\chi)$ (resp. $\mathcal{S}_k(\Gamma_0(N),\chi)$) for the subspace of $\mathcal{M}_k(\Gamma_1(N))$ (resp. $\mathcal{S}_k(\Gamma_1(N))$) consisting of functions satisfying the following automorphic property:

$$f|_k\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \chi(d)f \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Since the unipotent matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is contained in Δ, every modular form f in $\mathcal{M}_k(\Delta)$ is invariant under the translation by 1; that is, we have $f(z+1) = f(z)$. Since $\mathbf{e}(z) = \mathbf{e}(w)$ if and only if $z \equiv w \bmod \mathbf{Z}$, we can consider f as a function of $q = \mathbf{e}(z)$. Thus the above condition (1b) means that f as a function of q is analytic at 0 and has the following Taylor expansion $f(q) = \sum_{n=0}^{\infty} a(n,f)q^n$.

A typical example of a modular form of even weight $k > 2$ is given by the Eisenstein series which is defined by the absolutely convergent infinite series

$$E'_k(z) = \sum{}'_{(m,n)} (mz+n)^{-k},$$

where "Σ'" indicates that the summation is taken over all ordered pairs of integers excluding (0,0). By definition, it is clear that $E'_k \in \mathcal{M}_k(SL_2(\mathbf{Z}))$ if the above summation is absolutely convergent, since

$$(m\frac{az+b}{cz+d} + n)(cz+d) = (m,n)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z \\ 1 \end{pmatrix}.$$

We consider slightly more general series for any non-trivial primitive Dirichlet character $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$:

$$E'_k(z;\chi) = \sum{}'_{(m,n)} \chi^{-1}(n)(mNz+n)^{-k}.$$

This series is non-trivial only when $\chi(-1) = (-1)^k$ because

$$\chi^{-1}(-n)(-mNz-n)^{-k} = \chi(-1)(-1)^k\chi^{-1}(n)(mNz+n)^{-k}.$$

One can easily verify that this series is absolutely convergent if $k > 2$. We see that

$$\begin{aligned} E'_k(\tfrac{az+b}{cz+d};\chi) &= \sum{}'_{(m,n)} \chi^{-1}(n)(mN\tfrac{az+b}{cz+d}+n)^{-k} \\ &= \sum{}'_{(m,n)} \chi^{-1}(n)((mN,n)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z \\ 1 \end{pmatrix})^{-k}(cz+d)^k \\ &= \sum{}'_{(m,n)} \chi^{-1}(n)((mNa+cn,mNb+dn)\begin{pmatrix} z \\ 1 \end{pmatrix})^{-k}(cz+d)^k. \end{aligned}$$

Rewriting $(mNa+cn,mNb+dn)$ as (mN,n) for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ (because c is divisible by N), we have

$$E'_k(\tfrac{az+b}{cz+d};\chi) = \chi(d)E'_k(z;\chi)(cz+d)^k.$$

Thus $E'_k(z;\chi)$ satisfies the automorphic property defining the elements of $\mathcal{M}_k(\Gamma_0(p^r),\chi)$. We now compute the Fourier expansion of $E'_k(z;\chi)$. We use the formulas (2.1.5-6):

$$z^{-1}+\sum_{n=1}^{\infty} \{(z+n)^{-1}+(z-n)^{-1}\} = \pi\cot(\pi z) = \pi\sqrt{-1}\,\{-1-2\sum_{n=1}^{\infty} e(nz)\},$$

where $e(z) = \exp(2\pi\sqrt{-1}\,z)$. This series converges absolutely and locally uniformly with respect to z, and hence we can differentiate this series term by term k-times by $(2\pi i)^{-1}\frac{\partial}{\partial z}$, and we get

$$\sum_{n=-\infty}^{\infty} (z+n)^{-k} = \frac{(-2\pi\sqrt{-1})^k}{(k-1)!}\sum_{n=1}^{\infty} n^{k-1}e(nz). \tag{2}$$

Then we have

$$\begin{aligned} E'_k(z;\chi) &= \sum{}'_{(m,n)} \chi^{-1}(n)(mNz+n)^{-k} \\ &= 2L(k,\chi^{-1}) + 2\sum_{r=1}^{N} \chi^{-1}(r)\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty} (mNz+r+nN)^{-k} \\ &= 2L(k,\chi^{-1}) + 2N^{-k}\sum_{m=1}^{\infty}\sum_{j=1}^{N} \chi^{-1}(j)\sum_{n=-\infty}^{\infty} ((mz+\tfrac{j}{N})+n)^{-k} \\ &= 2L(k,\chi^{-1}) + 2N^{-k}\frac{(-2\pi\sqrt{-1})^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{j=1}^{N} \chi^{-1}(j)\sum_{n=1}^{\infty} n^{k-1}e(n(mz+\tfrac{j}{N})) \\ &= 2L(k,\chi^{-1}) + 2N^{-k}\frac{(-2\pi\sqrt{-1})^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{k-1}e(nmz)\sum_{j=1}^{N} \chi^{-1}(j)e(\tfrac{nj}{N}). \end{aligned}$$

We now compute $\sum_{j=1}^{N}\chi^{-1}(j)e(\frac{nj}{N})$. If n is prime to N, then by making the variable change $nj \mapsto j$ in the summation,

$$\sum_{j=1}^{N} \chi^{-1}(j)e(\frac{nj}{N}) = \chi(n)\sum_{j=1}^{N} \chi^{-1}(j)e(\frac{j}{N}) = \chi(n)G(\chi^{-1}),$$

where we write $G(\chi^{-1}) = \sum_{j=1}^{N}\chi^{-1}(j)e(\frac{j}{N})$. (If χ is trivial, then $1+G(\mathrm{id})$ is the sum of all N-th roots of unity and hence 0. Thus $G(\mathrm{id}) = -1$.) If χ is primitive, then as seen in Exercise 2.3.5 and (4.2.5a,b), we have

$$G(\chi)G(\chi^{-1}) = \chi(-1)N.$$

Anyway $G(\chi) \neq 0$. If n is not prime to N, then we have $\sum_{j=1}^{N}\chi^{-1}(j)e(\frac{nj}{N}) = 0$ by Lemma 2.3.2, because χ is primitive. Thus we know, for primitive χ, that

$$E'_k(z;\chi) = 2L(k,\chi^{-1}) + 2N^{-k}G(\chi^{-1})\frac{\{-2\pi\sqrt{-1}\}^k}{(k-1)!}\left\{\sum_{m=0}^{\infty}\sum_{n=0,(n,N)=1}^{\infty}\chi(n)n^{k-1}e(nmz)\right\}.$$

By the functional equation (Theorem 2.3.2), we know that

$$L(1-k,\chi) = \left\{N^{-k}G(\chi^{-1})\frac{(-2\pi\sqrt{-1})^k}{(k-1)!}\right\}^{-1} L(k,\chi^{-1}).$$

We put $E_k(z;\chi) = \left\{2N^{-k}G(\chi^{-1})\frac{(-2\pi\sqrt{-1})^k}{(k-1)!}\right\}^{-1} E'_k(z;\chi)$ and

$$\sigma_{m,\chi}(n) = \sum_{0<d\,|\,n} \chi(d)d^m,$$

where we agree to put $\chi(d) = 0$ if d has some non-trivial common factor with N. Then we have

Proposition 1. *We have* $E_k(z;\chi) = 2^{-1}L(1-k,\chi)+\sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n)e(nz)$ *if* χ *is primitive modulo* N *or* $\chi = \mathrm{id}$.

We note here that $E_k(z)-p^{k-1}E_k(pz)$ has the following Fourier expansion:

$$E_k(z)-p^{k-1}E_k(pz) = 2^{-1}(1-p^{k-1})\zeta(1-k)+\sum_{n=1}^{\infty} \sigma_{k-1,\iota_p}(n)e(nz),$$

where ι_p is the identity character modulo p (therefore, $\iota_p(pn) = 0$ for all n and $\iota_p(n) = 1$ if n is prime to p). Although we have only proved this proposition under the assumption that $k > 2$, the assertion for non-trivial χ is true even for $k = 1$ and 2. We will see this in Chapter 9.

We now want to compute a slightly different series for a Dirichlet character χ modulo N (we allow here χ to be imprimitive):

$$G'_k(z;\chi) = \sum_{(m,n)} \chi(m)(mz+n)^{-k} = 2\sum_{m=1}^{\infty} \chi(m) \sum_{n=-\infty}^{\infty} (mz+n)^{-k}$$

$$= 2\sum_{m=1}^{\infty} \chi(m) \sum_{n=-\infty}^{\infty} \frac{(-2\pi\sqrt{-1})^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1}e(mnz) = 2\frac{(-2\pi\sqrt{-1})^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma'_{k-1,\chi}(n)q^n,$$

where we write $\sigma'_{m,\chi}(n) = \sum_{0<d\,|\,n} \chi(n/d)d^m$. We put

$$G_k(z;\chi) = \sum_{n=1}^{\infty} \sigma'_{k-1,\chi}(n)q^n.$$

For $\tau = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$, we see easily that

$$E'_k(z;\chi)\,|_k\tau = N^{-1}z^{-k}\sum_{(m,n)} \chi^{-1}(n)(mN\frac{-1}{Nz}+n)^{-k} = N^{-1}G'_k(z;\chi^{-1}).$$

We in particular have, for a primitive character χ,

$$E_k(z;\chi)\,|_k\tau = \chi(-1)N^{k-2}G(\chi)G_k(z;\chi^{-1}),$$

where we have used the fact that $G(\chi)G(\chi^{-1}) = \chi(-1)N$. We note this fact as

Proposition 2 (Hecke). *Let* χ *be a Dirichlet character modulo* N *with* $\chi(-1) = (-1)^k$. *We have*

$$E_k(z;\chi) = 2^{-1}L(1-k,\chi) + \sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n)q^n \textit{ for primitive } \chi,$$

$$G_k(z;\chi) = \delta_{k,2}(2\pi y)^{-1}+\delta_{k,1}2^{-1}L(0,\chi) + \sum_{n=1}^{\infty} \sigma'_{k-1,\chi}(n)q^n \textit{ for any } \chi,$$

where $\delta_{k,j} = 1$ *or* 0 *according as* $k = j$ *or not. Unless* $k = 2$ *and* χ *is the identity character, the functions* $E_k(z,\chi)$ *and* $G_k(z;\chi)$ *are elements in* $\mathcal{M}_k(\Gamma_0(N),\chi)$. *Moreover we have* $E_k(z;\chi)\,|_k\tau = \chi(-1)N^{k-2}G(\chi)G_k(z;\chi^{-1})$.

Proof. We only need to prove that $E'_k(z,\chi)$ and $G'_k(z,\chi)$ satisfy (1b). We prove this assuming $k > 2$ and complete the proof in Chapter 9 (see Theorem 9.1.1 and (9.2.4a,b)) dealing with the case where $k = 1$ and 2. We consider a slightly more general series: for a pair (a,b) of integers

$$E'_{k,N}(z;a,b) = \sum{}'_{(m,n)\equiv(a,b) \bmod N}(mz+n)^{-k}.$$

Then it is easy to see that $E'_{k,N}(z;a,b)\,|_k\alpha = E'_{k,N}(z;(a,b)\alpha)$ and

$$E'_k(z;\chi) = \sum_{a \bmod N}\chi^{-1}(a)E'_{k,N}(z;0,a),$$

$$G'_k(z;\chi) = \sum_{b \bmod N}\sum_{a \bmod N}\chi(a)E'_{k,N}(z;a,b).$$

Thus we only need to prove that $E'_{k,N}(z;a,b)$ has no negative terms in its Fourier expansion. We see by definition that $E'_{k,N}(z;a,b)$ is equal to

$$\delta_a \sum_{n\equiv b \bmod N} n^{-k}$$
$$+N^{-k}\left\{\sum_{m\equiv a \bmod N, m>0}\sum_{n=-\infty}^{\infty}\left(\frac{mz+b}{N}+n\right)^{-k}+(-1)^k\sum_{m\equiv a \bmod N, m<0}\sum_{n=-\infty}^{\infty}\left(\frac{|m|z-b}{N}+n\right)^{-k}\right\},$$

where $\delta_a = \begin{cases}1 & \text{if } a \equiv 0 \bmod N,\\ 0 & \text{otherwise.}\end{cases}$

By (2), we have for a constant $c \neq 0$

$$\sum_{n=-\infty}^{\infty}\left(\frac{|m|z\pm b}{N}+n\right)^{-k} = c\sum_{n=1}^{\infty}n^{k-1}e\left(n\left(\frac{|m|z\pm b}{N}\right)\right).$$

This shows that the Fourier expansion of $E'_{k,N}(z;a,b)$ does not have terms in $e(nz)$ with $n < 0$.

As a byproduct of the above calculation, we get

(3) *The constant term of the Fourier expansion of* $G_k(z;\chi)|_k\alpha$ *vanishes for every* $\alpha = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \Gamma_0(p)$, *if* χ *is primitive modulo* p^r *and* $k \geq 2$.

We prove the following facts for our later use

(4a) *If* $k > 2$, *then*
$$|\sigma_{k-1,\chi}(n)| \leq \zeta(k-1)n^{k-1} \text{ and } |\sigma'_{k-1,\chi}(n)| \leq \zeta(k-1)n^{k-1}.$$
(4b) *If* $k = 1$ or 2, *for any* $\varepsilon > 0$, *there is a positive constant* C *such that*
$$|\sigma_{k-1,\chi}(n)| \leq Cn^{k-1+\varepsilon} \text{ and } |\sigma'_{k-1,\chi}(n)| \leq Cn^{k-1+\varepsilon}.$$

We compute

$$|\sigma_{k-1,\chi}(n)| \leq |\sigma_{k-1,\mathrm{id}}(n)| = \sum_{0<d|n}d^{k-1} = \prod_{p|n}(1+p^{k-1}+\cdots+p^{e(p)(k-1)}),$$

where $n = \prod_{p|n}p^{e(p)}$. Then we see that

$$|\sigma_{k-1,\mathrm{id}}(n)| = \prod_{p|n}(1+p^{k-1}+\cdots+p^{e(p)(k-1)}) = \prod_{p|n}\frac{p^{(e(p)+1)(k-1)}-1}{p^{k-1}-1}$$
$$= \{\prod_{p|n}(1-p^{1-k})^{-1}\}\prod_{p|n}(p^{e(p)(k-1)}-p^{1-k}) \leq \zeta(k-1)n^{k-1} \text{ if } k > 2.$$

Since $|\sigma'_{k-1,\chi}(n)| \leq |\sigma'_{k-1,\mathrm{id}}(n)| = |\sigma_{k-1,\mathrm{id}}(n)|$, the assertion is also true for σ'. The above argument yields

$$|\sigma_{s-1,id}(n)| \le \zeta(s-1)n^{s-1} \text{ for } \sigma_{s-1,id}(n) = \sum_{0<d|n} d^{s-1} \text{ if } s > 2.$$

Since

$$|\sigma_{1,id}(n)| \le |\sigma_{1+\varepsilon,id}(n)| \le \zeta(1+\varepsilon)n^{\varepsilon} \text{ for all } \varepsilon > 0.$$

This proves (4b) for $k = 2$. When $k = 1$, we have

$$|\sigma_{0,id}(n)| = \prod_{p|n}(e(p)+1) \text{ if } n = \prod_{p|n} p^{e(p)}.$$

Thus
$$|\sigma_{0,id}(n)n^{-\varepsilon}| \le \prod_{p|n}(1+e(p))/p^{e(p)\varepsilon}.$$

Since $p^{e(p)\varepsilon} > 1$, we see, if $n \ge 2$, that

$$\frac{(1+e(p))}{p^{e(p)\varepsilon}} \le 1 + \frac{e(p)}{p^{e(p)\varepsilon}} \le 1 + \frac{1}{\varepsilon\log 2} \le \exp(\tfrac{\log 2}{\varepsilon}).$$

If $p \ge 2^{1/\varepsilon}$, then $p^{\varepsilon} \ge 2$ and

$$\frac{1+e(p)}{p^{e(p)\varepsilon}} \le \frac{e(p)+1}{2^{e(p)}} \le 1.$$

Combining these two inequalities, we see that

$$|\sigma_{0,id}(n)n^{-\varepsilon}| \le \prod_{p|n,\ p<2^{1/\varepsilon}} \exp(\tfrac{\log 2}{\varepsilon}) \le \exp(2^{1/\varepsilon}/\varepsilon\log 2) \le Cn^{\varepsilon}.$$

§5.2. Rationality of modular forms

We first deal with the rational structure of the space $\mathcal{M}_k(SL_2(\mathbf{Z}))$. We introduce several modular forms with integral Fourier coefficients to study the rational structure in an elementary manner. For $k = 4, 6, 8, 10$ and 14, we put

$$G_k(z) = 2\zeta(1-2k)^{-1}E_k = 1 + C_k \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n \in \mathcal{M}_k(SL_2(\mathbf{Z})).$$

By the actual values of $\zeta(1-2k)$ given after Theorem 2.2.1, we have

k	4	6	8	10	14
C_k	240	-504	480	-264	-24

We could have defined G_{12} in a similar manner, but then it would have had the prime 691 as the denominator of its Fourier coefficients. We further put $G_0(z) = 1$ and $\Delta(z) = g_2^3(z) - 27g_3^2(z)$ for $g_2 = G_4/12$ and $g_3 = G_6/216$. The function Δ is called the Ramanujan's Δ-function (or the discriminant function). Computing the constant term of Δ, we see that $\Delta \in \mathcal{S}_{12}(SL_2(\mathbf{Z}))$. It is known that Δ does not vanish on $\mathcal{H}$ and even has the product expansion

$$\Delta(z) = q\prod_{n=1}^{\infty} (1-q^n)^{24} \quad \text{(see [W2, IV, (36)])}.$$

Let $X = (SL_2(\mathbf{Z})\backslash\mathcal{H})\cup\{\infty\}$ (see [Sh, 1.4, 6.1] and [M, §4.1] for how to give a standard structure of Riemann surface on this space). Put $J = G_4^3/\Delta$. Then J has the q-expansion of the form: $q^{-1} + \sum_{n=0}^{\infty} c_n q^n$ with $c_n \in \mathbf{Z}$. The function J gives an identification of X with the projective J-line $\mathbf{P}^1(J)$ [Sh, Chapter 4]. We define for each positive even integer k

$$r = r(k) = \begin{cases} [k/12], & \text{if } k \equiv 2 \bmod 12, \\ [k/12]+1, & \text{otherwise,} \end{cases}$$

where $[q]$ for a rational number q denotes the largest integer not exceeding q. Put $s(k) = k-12(r(k)-1)$.

Lemma 1. *The equation* $4a+6b = k-12(r(k)-1) = s(k)$ *has one and only one non-negative integer solution for each even integer* k.

Proof. If $k \equiv 2 \bmod 12$, then $k-12(r(k)-1) = 14$; in this case, the unique solution is $(a,b) = (2,1)$, and if $k \not\equiv 2 \bmod 12$, then $k-12(r(k)-1) < 12$ and the uniqueness and the existence of the solution can be checked easily. We list all the solutions in the following table:

k mod 12	0	2	4	6	8	10
s	0	14	4	6	8	10
a	0	2	1	0	2	1
b	0	1	0	1	0	1

We choose the unique solution (a,b) as above for a given k and define

$$h_i = (G_4)^a(G_6)^{b+2(r-1-i)}\Delta^i \in \mathcal{M}_k(SL_2(\mathbf{Z})) \quad \text{for } i = 0, 1, \cdots, r-1 \quad (r = r(k)).$$

Note that $h_i \in \mathcal{M}_k(SL_2(\mathbf{Z}))$, and h_i has the q-expansion $(q = \mathbf{e}(z))$ with coefficients in $\mathbf{Z}$ of the following form:

$$h_i = q^i + \sum_{n=i+1}^{\infty} b_n q^n \quad \text{with } b_n \in \mathbf{Z}.$$

This shows that h_i are linearly independent. For any subring A of $\mathbf{C}$ and each congruence subgroup Γ, we put

$$\mathcal{M}_k(\Gamma;A) = \{f \in \mathcal{M}_k(\Gamma) \mid a(n,f) \in A \text{ for all } n\}, \quad \mathcal{S}_k(\Gamma;A) = \mathcal{M}_k(\Gamma;A)\cap\mathcal{S}_k(\Gamma).$$

Theorem 1. *We have* $\dim_{\mathbf{C}}(\mathcal{M}_k(SL_2(\mathbf{Z})) = \mathrm{rank}_{\mathbf{Z}}(\mathcal{M}_k(SL_2(\mathbf{Z});\mathbf{Z})) = r(k)$ *and for any subring* A *of* $\mathbf{C}$,

$$\mathcal{M}_k(SL_2(\mathbf{Z});A) = \mathcal{M}_k(SL_2(\mathbf{Z});\mathbf{Z})\otimes_{\mathbf{Z}}A, \quad \mathcal{S}_k(SL_2(\mathbf{Z});A) = \mathcal{S}_k(SL_2(\mathbf{Z});\mathbf{Z})\otimes_{\mathbf{Z}}A.$$

Moreover $\{h_0, \cdots, h_{r-1}\}$ *(resp.* $\{h_1, \cdots, h_{r-1}\}$*) form a basis of* $\mathcal{M}_k(SL_2(\mathbf{Z});\mathbf{Z})$ *(resp.* $\mathcal{S}_k(SL_2(\mathbf{Z});\mathbf{Z})$*) over* $\mathbf{Z}$.[1]

[1] I am indebted to Y. Maeda for the construction of the basis $\{h_i\}$.

Proof. If we know that the dimension of the space of modular forms is less than or equal to $r(k)$, then h_i gives a basis of $\mathcal{M}_k(SL_2(\mathbf{Z});A)$ over A and everything will be proven. Let us show the inequality

$$\dim_{\mathbf{C}}(\mathcal{M}_k(SL_2(\mathbf{Z}))) \le r(k).$$

Put $s(k) = k-12(r(k)-1)$. Recall that $s(k) = 0,14,4,6,8,10$ according as $k \equiv 0,2,4,6,8,10 \mod 12$. We put

$$T_k(z) = G_{14-s(k)}(z)\Delta(z)^{-r}.$$

Then T_k is holomorphic everywhere on $\mathcal{H}$ and we have the following q-expansion of T_k $(q = e(z))$:

$$(1) \qquad T_k(z) = c_{k,r}q^{-r} + \cdots + c_{k,0} + \cdots \quad \text{with } c_{k,j} \in \mathbf{Z} \ (c_{k,r} = 1).$$

Since the weight of T_k is given by $14-s(k)-12r(k) = 2-k$, for each $f \in \mathcal{M}_k(SL_2(\mathbf{Z}))$, $fT_k(z)$ is of weight 2. Thus the differential form $\omega = fT_k(z)dz = \frac{1}{2\pi\sqrt{-1}}fT_k dq/q$ satisfies $\gamma^*\omega = \omega$ for all $\gamma \in SL_2(\mathbf{Z})$ and is holomorphic on $\mathcal{H}$. That is, ω has a singularity only at infinity. By construction, the singularity of ω at infinity is a pole of order at most $r+1$. Let $\omega_m = J^m dJ$ which has a pole of order $m+2$ at infinity and which is holomorphic outside infinity. Let δ be a meromorphic differential form on X whose singularity at infinity is a pole of order n and is holomorphic outside infinity. Then $n \ge 2$ since $\deg(\delta) = 2g-2 = -2$ for the genus $g = 0$ of X. In fact, this can be proven as follows. Since X is a Riemann sphere with coordinate J, at any point $x \in X$, $J-J(x)$ is a local parameter at x. Therefore dJ has order 0 at x. On the other hand, at infinity, dJ has order -2 and hence $\deg(dJ) = -2$. For any morphism $f : X \to \mathbf{P}^1(\mathbf{C})$ of algebraic varieties (or Riemann surfaces), the numbers of points in the fiber at 0 and ∞ are equal (counting with multiplicity). Thus

$$\deg(f) = \#(\text{points over } 0) - \#(\text{points over } \infty) = 0$$

and therefore, writing $\delta = fdJ$ for a suitable function $f : X \to \mathbf{P}^1(\mathbf{C})$, we see that $\deg(\delta) = \deg(fdJ) = -2$. Thus, subtracting suitable constant multiples of the ω_i's from δ, we may assume that $\delta-(b_0\omega_0+\cdots+b_{n-2}\omega_{n-2})$ has at most a simple pole at infinity and is everywhere holomorphic outside infinity; that is, $\deg(\delta - b_0\omega_0 + \cdots + b_{n-2}\omega_{n-2}) \ge -1$. This implies $\delta = b_0\omega_0+\cdots+b_{n-2}\omega_{n-2}$. Applying this argument to ω, we know that ω can be written as $b_0\omega_0+\cdots+b_{r-1}\omega_{r-1}$. Via the map $f \mapsto \omega = fT_k dz$, we can embed $\mathcal{M}_k(SL_2(\mathbf{Z}))$ into the space of differential forms generated by $\omega_0, \cdots, \omega_{r-1}$ and thus we get

$$\dim_{\mathbf{C}}(\mathcal{M}_k(SL_2(\mathbf{Z}))) \le r(k).$$

Since $\dim_{\mathbf{C}}(\mathcal{M}_k(SL_2(\mathbf{Z}))) = r(k)$, the first $r(k)+1$ q-expansion coefficients of any $f \in \mathcal{M}_k(SL_2(\mathbf{Z}))$ have to satisfy a non-trivial linear relation. We can make explicit this linear form:

Corollary 1 (Siegel [Si]). *If* $f = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{M}_k(SL_2(\mathbf{Z}))$, *then*

$$c_{k,0}a_0 + \cdots + c_{k,r}a_r = 0 \quad (r = r(k)) \quad \textit{and} \quad c_{k,0} \neq 0,$$

where $c_{k,j}$ *are the Fourier coefficients of* T_k *in (1).*

Proof. Note that $\omega_m = J^m dJ = \frac{1}{m+1}\frac{dJ^{m+1}}{dq}dq$ and $\frac{dJ^{m+1}}{dq} = (2\pi iq)^{-1}\frac{dJ^{m+1}}{dz}$ ($\frac{dq^m}{dz} = 2\pi i m q^m$), and hence the coefficient in q^{-1} of ω_m is always 0. The constant term of $T_k f dq$ is given by $c_{k,0}a_0 + \cdots + c_{k,r}a_r$, which shows $c_{k,0}a_0 + \cdots + c_{k,r}a_r = 0$. Now we prove that $c_{k,0} \neq 0$. Note that

$$\Delta^{-1}(z) = q^{-1}\prod_{n=1}^{\infty}(1-q^n)^{-24} = q^{-1}\prod_{n=1}^{\infty}(\sum_{m=0}^{\infty} q^{nm})^{24}.$$

Therefore the coefficients of Δ^{-r} are all positive. On the other hand, the coefficients of G_0, G_8, G_4 are positive and hence $c_{k,0} \neq 0$ when $k \equiv 2 \bmod 4$. Now suppose that $k \equiv 0 \bmod 4$. Then

$$s(k) = k-12(r(k)-1) \equiv k \bmod 4$$

and we can write $s(k) = 4t$ with $t \in \mathbf{Z}$. Now consider $\omega = (2\pi i)^{-1}G_{14}\Delta^{-1}dq/q = G_{14}\Delta^{-1}dz$ which has a pole of order 2 at infinity and is holomorphic outside infinity. Therefore we can write $\omega = cdJ$ with $c \neq 0$ and thus $G_{14}\Delta^{-1} = c\frac{dJ}{dz}$ or $G_{14} = c\Delta\frac{dJ}{dz}$ because $r(14) = 1$. This shows that $T_k = cG_{14-s(k)}\Delta^{1-r}(G_{14})^{-1}\frac{dJ}{dz}$. Since $\mathcal{M}_{14}(SL_2(\mathbf{Z}))$ is of dimension 1, we know that $G_{14-s(k)}G_{s(k)} = G_{14}$ and $G_{s(k)} = (G_4)^t$, comparing the constant terms. Then, we know that

$$T_k = c(G_{s(k)})^{-1}\Delta^{1-r}\frac{dJ}{dz} = c(G_4)^{-t}\Delta^{1-r}\frac{dJ}{dz}.$$

By replacing G_4 by $(\Delta J)^{1/3}$ in this formula ($G_4{}^3 = \Delta J$ by the definition of J), we have

$$T_k = c\Delta^{1-r-t/3}J^{-t/3}\frac{dJ}{dz} = \frac{3c}{3-t}\Delta^{1-r-t/3}\frac{dJ^{1-(t/3)}}{dz}.$$

Note that $J^{1-(t/3)} = (G_4)^{3-t}\Delta^{(t/3)-1}$. Then we have

$$\Delta^{1-r-t/3}\frac{dJ^{1-(t/3)}}{dz} = \Delta^{1-r-t/3}\frac{d(G_4)^{3-t}\Delta^{(t/3)-1}}{dz},$$

$$\frac{d(G_4)^{3-t}\Delta^{-r}}{dz} = \frac{d(G_4)^{3-t}\Delta^{(t/3)-1}\Delta^{1-r-t/3}}{dz}$$
$$= \Delta^{1-r-t/3}\frac{dJ^{1-(t/3)}}{dz} + (G_4)^{3-t}\Delta^{(t/3)-1}\frac{d\Delta^{1-r-t/3}}{dz},$$

and

$$\Delta^{(t/3)-1}\frac{d\Delta^{1-r-t/3}}{dz} = \frac{r+(t/3)-1}{r}\left(\frac{d\Delta^{-r}}{dz}\right).$$

Therefore, we see that

$$T_k = \frac{3c}{3-t}\frac{d}{dz}(G_4^{3-t}\Delta^{-r}) + \frac{(3r+t-3)c}{(t-3)r}G_4^{3-t}\frac{d\Delta^{-r}}{dz}.$$

Since $\frac{d}{dz}(G_4^{3-t}\Delta^{-r})$ has no constant term, we look at the second term of the above formula. Since the coefficient of q^j in $\frac{d\Delta^{-r}}{dz}$ for $j < 0$ is negative, and the coefficients of G_4^{3-t} are all positive, we know that the constant term of the second term is negative. This shows that $c_{k,0} < 0$.

Applying the linear form in Corollary 1 to $E_k(z)$, we have

Corollary 2. $2^{-1}\zeta(1-k) = -c_{k,0}^{-1}\sum_{j=1}^{r(k)} \sigma_{k-1}(n)c_{k,j}$ *for all* $2 < k \in 2\mathbf{Z}$.

Let me briefly explain how Siegel applied Corollary 1 to show the rationality of the values of the Dedekind zeta function of a totally real field F of degree d. Let a be an ideal of the integer ring $\mathcal{O}$ of F and consider the following Eisenstein series for $z \in \mathcal{H}$ (see Theorem 2.7.3):

$$\mathbf{E}_k(z;a) = N_{F/Q}(a)^k\sum{}'_{(m,n)\in a^2/\mathcal{O}^\times} N(mz+n)^{-k} \text{ for even integer } k.$$

Here $N(mz+n)$ is the product $\prod_\sigma(m^\sigma z+n^\sigma)$ taken over all embeddings σ of F into $\mathbf{R}$, and (m,n) runs over all equivalence classes of ordered pairs of numbers (m,n) in a under the relation $(m,n) \sim (m',n')$ if $m' = \varepsilon m$ and $n' = \varepsilon n$ for $\varepsilon \in \mathcal{O}^\times$. This series is absolutely convergent if $k > 2$. We can verify that $\mathbf{E}_k(z;a)$ is a modular form of weight $k[F:\mathbf{Q}]$ with respect to $SL_2(\mathbf{Z})$, and we can compute its Fourier expansion (see Theorem 9.1.1). Even if one replaces a by λa for $\lambda \in F^\times$, each term of $\mathbf{E}_k(z;a)$

$$N_{F/Q}(a)^k N(mz+n)^{-k} = N_{F/Q}(\lambda a)^k N(\lambda mz+\lambda n)^{-k}$$

does not change, and thus, $\mathbf{E}_k(z;a)$ depends only on the ideal class of a. To simplify a little, we define

$$\mathbf{E}_k(z) = \sum_a \mathbf{E}_k(z;a),$$

where a runs over a set of representatives of ideal classes of F. Then we have

$$\mathbf{E}_k(z) = \zeta_F(k) + \left(\frac{(2\pi\sqrt{-1})^k}{(k-1)!}\right)^d D^{(2k-1)/2} \sum_{n=1}^{\infty} \sum_{\mathrm{Tr}(\xi)=j} \sigma_{k-1}(\xi\vartheta^{-1})q^n,$$

where ϑ is the different of F, ξ runs over all totally positive elements in ϑ^{-1}, $D = N_{F/Q}(\vartheta)$ is the discriminant of F, $\zeta_F(s) = \sum_{\mathfrak{b}} N_{F/Q}(\mathfrak{b})^{-s}$ is the Dedekind zeta function of F and $\sigma_{k-1}(\mathfrak{b}) = \sum_{\mathfrak{a}\supset\mathfrak{b}} N_{F/Q}(\mathfrak{a})^{k-1}$.

Corollary 3 (Siegel). *For each even positive integer* k, *we have*

$$\frac{(k-1)!^d\zeta_F(k)}{(2\pi\sqrt{-1})^{kd}D^{(2k-1)/2}} = -\frac{\sum_{j=1}^{kd}\sum_{\mathrm{Tr}(\xi)=j}\sigma_{kd-1}(\xi\vartheta)}{c_{kd,0}} \in \mathbf{Q} \quad (d = [F:\mathbf{Q}]).$$

This fact also follows from Corollary 2.7.1 proved by Shintani's method by the functional equation of $\zeta_F(s)$ (Corollary 8.6.1).

Now let us note another application of Corollary 1. Let p be an odd prime and consider the Eisenstein series $f = E_k(z;\omega^a) \in \mathcal{M}_k(\Gamma_0(p),\omega^a)$. Let b be the order of ω^a. Then f^b is an element of $\mathcal{M}_{kb}(\Gamma_0(p))$. We choose a complete representative set R for $\Gamma_0(p)\backslash SL_2(\mathbf{Z})$ and define $\mathrm{Tr}(g) = \sum_{\gamma\in R} g\,|_k\gamma$ for $g \in \mathcal{M}_k(\Gamma_0(p))$. Then obviously $\mathrm{Tr}(g) \in \mathcal{M}_k(SL_2(\mathbf{Z}))$. We now want to compute $\mathrm{Tr}(f^b)$.

Lemma 2. *We can take as* R *the set of the following matrices: the identity matrix* 1_2 *and* $\delta_j = \delta\begin{pmatrix}1 & j\\ 0 & 1\end{pmatrix}$ *for* $\delta = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ *with* $j = 1, \cdots, p$. *If* $g(z) = \sum_{n=0}^{\infty} a_n e(nz)$ *and* $g\,|_k\delta = \sum_{n=0}^{\infty} b_n e(\frac{nz}{p})$, *then we have*

$$\mathrm{Tr}(g) = a_0 + pb_0 + \sum_{n=1}^{\infty} (a_n + pb_{np})e(nz).$$

Proof. Take $\gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL_2(\mathbf{Z})$. If c is divisible by p, then γ is in $\Gamma_0(p)$ and in the left coset of 1_2. Thus we may assume that c is prime to p. Take an integer j in the interval [1,p] such that $cj \equiv d \mod p$ and consider $\gamma\delta_j^{-1} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}j & 1\\ -1 & 0\end{pmatrix}$. The entry at the lower left corner of this matrix is cj-d which is divisible by p by definition of j. Thus $\gamma \in \Gamma_0(p)\delta_j$. If γ and $\gamma' = \begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}$ are in the same left coset of $\Gamma_0(p)$, then $cd' \equiv c'd \mod p$ and hence $SL_2(\mathbf{Z}) = \bigcup_j \Gamma_0(p)\delta_j \cup \Gamma_0(p)$ is a disjoint union. Note that $\sum_{j=1}^{p} g\,|_k\delta_j = \sum_{n=0}^{\infty} b_n \sum_{j=1}^{p} e(\frac{njz}{p}) = pb_0 + \sum_{n=1}^{\infty} pb_{np}e(nz)$. From this, the formula in the lemma is obvious.

Recall that for the Eisenstein series $G_k(z;\chi) = \sum_{n=1}^{\infty}\sigma'_{k-1,\chi}(n)e(nz)$ with $\sigma'_{m,\chi}(n) = \sum_{0<d|n}\chi(n/d)d^m$, we proved the following formula in §1:

$$E_k(z;\chi)\,|_k\tau = (-1)^k p^{k-2}G(\chi)G_k(z;\chi^{-1}),$$

where $\tau = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$ and $\chi = \omega^a$ for the Teichmüller character ω. Note that $\tau = \delta\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ and therefore $E_k(z;\chi)\,|_k\delta = (-1)^k p^{-1}G(\chi)G_k(\frac{z}{p};\chi^{-1})$. Thus if we put $f = E_k(z;\chi)$ and $g = (-1)^k p^{-1}G(\chi)G_k(\frac{z}{p};\chi^{-1})$, then $f^b\,|_k\delta = g^b = \sum_{n=1}^{\infty}b_n e(\frac{nz}{p})$ where b_n for all positive n are algebraic numbers. Write f as $X + F(q)$ with $X = 2^{-1}L(1-k,\omega^a)$ and $F(q) \in q\mathbf{Q}(\omega^a)[[q]]$. Then $f^b = X^b + \sum_{n=1}^{\infty}a_n(X)q^n$, where $a_n(X)$ is a polynomial of X of degree strictly less than b with coefficients in $\mathbf{Q}(\omega^a)$. Thus by Siegel's theorem, we have an equation with coefficients in $\mathbf{Q}(\omega^a)$:

$$c_{kb,0}X^b + \sum_{j=1}^{r(kb)} c_{kb,j}(a_j(X)+pb_{jp}) = 0,$$

where the degree of a_j in X is strictly less than b. Thus the above equation is non-trivial, and we get another proof (valid only when $k > 1$) of the following fact:

Proposition 1. *$2^{-1}L(1-k,\omega^a)$ for $k > 0$ is an algebraic number if $\omega^a(-1) = (-1)^k$.*

We now want to show that $2^{-1}L(1-k,\omega^a) \in \mathbf{Q}(\omega^a)$. For that purpose, we introduce the transformation equations. For each modular form f in $\mathcal{M}_k(\Gamma)$, we fix a representative set R for $\Gamma\backslash SL_2(\mathbf{Z})$ and define

$$P(f;X) = \prod_{\gamma\in R}(X-f\,|_k\gamma) = X^d + s_1(f)X^{d-1} + \cdots + s_d(f).$$

Note that $s_j(f) \in \mathcal{M}_{kj}(SL_2(\mathbf{Z}))$ and $P(f;f\,|_k\gamma) = 0$ for any $\gamma \in SL_2(\mathbf{Z})$. For each $f \in \mathcal{M}_k(\Gamma)$, we formally define the conjugate $f^\sigma = \sum_{n=0}^{\infty}a(n,f)^\sigma q^n$ as an element of $\mathbf{C}[[q]]$ for any automorphism σ of $\mathbf{C}$. Since the map

$$\sum_{n=0}^{\infty}a(n,f)q^n \mapsto \sum_{n=0}^{\infty}a(n,f)^\sigma q^n$$

defines a ring automorphism of $\mathbf{C}[[q]]$, if we put

$$P^\sigma(f;X) = X^d + s_1(f)^\sigma X^{d-1} + \cdots + s_d(f)^\sigma, \text{ then } P^\sigma(f;f^\sigma) = 0 \text{ in } \mathbf{C}[[q]].$$

Proposition 2. *For $f \in \mathcal{M}_k(SL_2(\mathbf{Z}))$, we have $f^\sigma \in \mathcal{M}_k(SL_2(\mathbf{Z}))$ for each $\sigma \in \mathrm{Aut}(\mathbf{C})$. In particular, $s_j(g)^\sigma \in \mathcal{M}_{kj}(SL_2(\mathbf{Z}))$ for any $g \in \mathcal{M}_k(\Gamma)$.*

Proof. Write $f = c_0h_0+\cdots+c_{r-1}h_{r-1}$ for the basis h_j as in Theorem 1. Then $f^\sigma = c_0{}^\sigma h_0+\cdots+c_{r-1}{}^\sigma h_{r-1} \in \mathcal{M}_k(SL_2(\mathbf{Z}))$ because $h_j \in \mathbf{Z}[[q]]$.

Let $\mathcal{M}(\mathbf{C}) = \oplus_{k=0}^{\infty}\mathcal{M}_k(SL_2(\mathbf{Z}))$ and for any subring A of $\mathbf{C}$, we put $\mathcal{M}(A) = \mathcal{M}(\mathbf{C})\cap A[[q]]$. Note that $\mathcal{M}(\mathbf{C})$ is a graded algebra and $f = \oplus_k f_k \mapsto f^\sigma = \oplus_k f_k{}^\sigma$ for $\sigma \in \mathrm{Aut}(A)$ is a ring automorphism of $\mathcal{M}(A)$. Let $\mathcal{A}(A)$ be the quotient field of $\mathcal{M}(A)$.

Proposition 3. *If* $f \in \mathcal{M}_k(\Gamma)$ *for a subgroup* Γ *of finite index of* $SL_2(\mathbf{Z})$, *then for any* $\sigma \in \mathrm{Aut}(\mathbf{C})$, $f^\sigma \in \mathcal{M}_k(\Delta)$ *for a normal subgroup* Δ *of finite index in* $SL_2(\mathbf{Z})$.

Proof. Let F (resp. F^σ) be the set of all roots of $P(f;X)$ (resp. $P^\sigma(f;X)$). Each root g of $P^\sigma(f;X)$ is not only a formal Fourier series but it converges on $\mathcal{H}$, because it is a root of a polynomial with function coefficients. Thus for $\gamma \in SL_2(\mathbf{Z})$, we can consider $g|_k\gamma$, which is a root of

$$P^\sigma(f;X)|\gamma = X^d + s_1(f)^\sigma|_k\gamma X^{d-1}+ \cdots + s_d(f)^\sigma|_{kd}\gamma = 0.$$

The left-hand side of this equation is equal to $P^\sigma(f;X)$ because $s_j(f)^\sigma \in \mathcal{M}_{kj}(SL_2(\mathbf{Z}))$. Thus F^σ is stable under $SL_2(\mathbf{Z})$. Let Δ be the subgroup of $SL_2(\mathbf{Z})$ which fixes all elements of F^σ. Then the action of $SL_2(\mathbf{Z})$ on F^σ gives a representation of $SL_2(\mathbf{Z})/\Delta$ into the group of permutations of elements of F^σ, which is a finite group. Thus Δ is a normal subgroup of finite index in $SL_2(\mathbf{Z})$.

The following fact is clear from Corollary 2.3.2, but we shall give another proof of the fact:

Theorem 2. *The value* $L(1\text{-}k,\chi)$ *for* $\chi(-1) = (-1)^k$ *is an element of* $\mathbf{Q}(\chi)$, *and for each* $\sigma \in \mathrm{Aut}(\mathbf{C})$, $L(1\text{-}k,\chi)^\sigma = L(1\text{-}k,\chi^\sigma)$.

Proof. Let σ be an element of $\mathrm{Aut}(\mathbf{C})$. Then for $f = E_k(z;\chi)$, all Fourier coefficients of f^σ but its constant term coincide with those of $g = E_k(z;\chi^\sigma)$. Thus $C = f^\sigma - g$ is a constant, which is a modular form of weight k for a subgroup Δ of finite index in $SL_2(\mathbf{Z})$ (if f^σ is modular with respect to Φ and g with respect to Γ, then $\Phi/\Phi\cap\Gamma \cong \Phi\Gamma/\Gamma$, which is a finite group). Therefore for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta$ with $c \neq 0$, $C|_k\gamma = (cz+d)^{-k}C = C$. Since $cz+d \neq 1$, we know that $C = 0$. Thus $(L(1\text{-}k,\chi))^\sigma = L(1\text{-}k,\chi^\sigma)$. This shows the assertion.

The above proof of the rationality of the Dirichlet L-values using the action of $\sigma \in \mathrm{Aut}(\mathbf{C})$ is due to Shimura.

§5.3. Hecke operators

In this section, we shall introduce the Hecke operator $T(q)$ as an endomorphism of $\mathcal{M}_k(\Gamma_0(p^r),\chi)$. We consider the double coset $\Gamma\begin{pmatrix}1 & 0\\ 0 & q\end{pmatrix}\Gamma$ for primes q with $\Gamma = \Gamma_0(N)$ for a prime power $N = p^r$. Then we can decompose, for $\alpha = \begin{pmatrix}1 & 0\\ 0 & q\end{pmatrix}$, $\Gamma\alpha\Gamma = \bigcup_i \Gamma\alpha_i$ as a disjoint union; actually, an explicit left coset decomposition is given by

$$\text{(1a)}\qquad \Gamma\alpha\Gamma = \begin{cases} \coprod_{u=1}^{q} \Gamma\begin{pmatrix}1 & u\\ 0 & q\end{pmatrix} \amalg \Gamma\begin{pmatrix}q & 0\\ 0 & 1\end{pmatrix} & \text{if } q \text{ is prime to } N, \\ \coprod_{u=1}^{p} \Gamma\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix} & \text{if } q = p. \end{cases}$$

A proof of the above decomposition is given as follows. Take any $\gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in M_2(\mathbf{Z})$ with $ad\text{-}bc = q$. If c is divisible by q, then ad is divisible by q, and thus one of a and d is divisible by q. We have $\gamma = \begin{pmatrix}a/q & b\\ c/q & d\end{pmatrix}\begin{pmatrix}q & 0\\ 0 & 1\end{pmatrix} \in SL_2(\mathbf{Z})\begin{pmatrix}q & 0\\ 0 & 1\end{pmatrix}$ if a is divisible by q. If d is divisible by q but a is prime to q, then by choosing $u \in [1,q]$ such that $ua \equiv b \bmod q$, $\gamma\begin{pmatrix}1 & u\\ 0 & q\end{pmatrix}^{-1} \in SL_2(\mathbf{Z})$. If c is not divisible by q but a is divisible by q, we can interchange a and c by multiplication by $\delta = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ on the left. If both a and c are not divisible by q, then by choosing u so that $ua \equiv -c \bmod q$, we know that the lower left corner of $\begin{pmatrix}1 & 0\\ u & 1\end{pmatrix}\gamma$ is equal to $ua+c$ and is divisible by q. This shows (1a) for $\Gamma = SL_2(\mathbf{Z})$. The case of $\Gamma = \Gamma_0(p^r)$ can be similarly treated (see [M, Lemma 4.5.6]). Note that for any element $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ in $\Gamma_0(p^r)\alpha\Gamma_0(p^r)$, c is divisible by p^r and a is prime to p (because every element of $\Gamma_0(p^r)$ is upper triangular mod p^r).

Exercise 1. Give a detailed proof of (1) when $\Gamma = \Gamma_0(p^r)$.

We define the Hecke operator $T(q)$ on $\mathcal{M}_k(\Gamma_0(N),\chi)$, using the disjoint decompositions $\Gamma\alpha\Gamma = \bigcup_i \Gamma\alpha_i$ and $\Gamma\alpha^\iota\Gamma = \bigcup_i \Gamma\beta_i$ ($\alpha^\iota = \det(\alpha)\alpha^{-1}$), by

$$\text{(1b)}\qquad f\,|\,T(q) = \textstyle\sum_i \chi(\alpha_i) f\,|_k\alpha_i \quad\text{and}\quad f\,|\,T^*(q) = \sum_i \chi(\beta_i^\iota)^{-1} f\,|_k\beta_i,$$

where $\chi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \chi(a)$ (a is always prime to N by (1a)). Here we understand that χ is trivial when $\Gamma = SL_2(\mathbf{Z})$. Then obviously $T(q)$ and $T^*(q)$ gives an operator acting on $\mathcal{M}_k(\Gamma)$ if $\Gamma = SL_2(\mathbf{Z})$. If $\gamma \in \Gamma_0(N)$, then $\Gamma\alpha\Gamma = \coprod_i \Gamma\alpha_i = \coprod_i \Gamma\alpha_i\gamma$ and thus

$$f \mid T(q) \mid_k \gamma = \sum_i \chi(\alpha_i) f \mid_k \alpha_i\gamma = \chi(\gamma)^{-1} \sum_i \chi(\alpha_i\gamma) f \mid_k \alpha_i\gamma = \chi(\gamma)^{-1} f \mid T(q).$$

Here note that $\chi(\gamma)^{-1} = \chi(a)^{-1} = \chi(d)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ because $ad \equiv 1 \bmod N$. This shows that $f \mid T(q) \in \mathcal{M}_k(\Gamma_0(N),\chi)$. Similarly, we can show that $T^*(q)$ preserve $\mathcal{M}_k(\Gamma_0(N),\chi)$. Now we want to compute the Fourier expansion of $f \mid T(q)$. When $f \in \mathcal{M}_k(\Gamma_0(p^r),\chi)$ for $r > 0$, then

$$f \mid T(p) = p^{-1} \sum_{u=1}^{p} f\left(\frac{z+u}{p}\right) = p^{-1} \sum_{n=0}^{\infty} a(n,f) e\left(\frac{nz}{p}\right) \sum_{u=1}^{p} e\left(\frac{nu}{p}\right) = \sum_{n=0}^{\infty} a(np,f) e(nz).$$

As for $T(q)$ for $q \neq p$, we have

$$\Gamma\alpha\Gamma = \coprod_{u=1}^{q} \Gamma\begin{pmatrix} 1 & u \\ 0 & q \end{pmatrix} \coprod \Gamma\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}.$$

As the contribution of the term $\coprod_{u=1}^{q} \Gamma\begin{pmatrix} 1 & u \\ 0 & q \end{pmatrix}$ to the coefficient of $e(nz)$, by the same computation as above, we get $a(nq,f)$. For the remaining term $\Gamma\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$, we get $\chi(q)q^{k-1}a(n/q,f)$. Thus we have for $f \in \mathcal{M}_k(\Gamma_0(N),\chi)$ $(N = p^r)$,

$$a(n, f \mid T(q)) = a(nq,f) + \chi(q)q^{k-1}a(n/q,f), \tag{1c}$$

where we have implicitly assumed that $a(n,f) = 0$ if n is not an integer and $\chi(q) = 0$ if $q \mid N$. If q and r are two distinct primes, then

$$\begin{aligned} a(m, f \mid T(q)T(r)) &= a(mr, f \mid T(q)) + \chi(r)r^{k-1}a(m/r, f \mid T(q)) \\ &= a(mrq,f) + \chi(q)q^{k-1}a(mr/q,f) + \chi(r)r^{k-1}a(mq/r,f) + \chi(rq)(rq)^{k-1}a(m/rq,f), \end{aligned}$$

which is symmetric with respect to r and q and hence

$$T(r)T(q) = T(q)T(r) \text{ if } r \text{ and } q \text{ are different primes.} \tag{2}$$

By the above formula, we have

$$a(m, f \mid T(q)^2) = a(mq^2,f) + 2\chi(q)q^{k-1}a(m,f) + \chi(q)^2 q^{2(k-1)} a(m/q^2,f). \tag{3}$$

We now define the operator $T(q^e)$ for $e \geq 1$ inductively by

$$T(q^{e+1}) = \begin{cases} T(q)^{e+1} & \text{if } q \mid N, \\ T(q)T(q^e) - \chi(q)q^{k-1}T(q^{e-1}) & \text{otherwise,} \end{cases} \tag{4a}$$

where we define $T(1)$ to be the identity map. Then we see from (2) that $T(q^e)T(l^s) = T(l^s)T(q^e)$ for different primes l and q. More generally, we can define $T(n)$ for each positive integer n by

$$\text{(4b)} \qquad T(n) = \prod_q T(q^{e(q)}) \text{ if } n = \prod_q q^{e(q)} \text{ for primes } q.$$

Then we can write down the Fourier expansion of $f|T(n)$ explicitly (see [Sh, (3.5.12)]) as

$$\text{(5)} \qquad a(m,f|T(n)) = \sum_{0<b|(m,n)} \chi(b)b^{k-1}a(mn/b^2,f).$$

Define a semi-group Δ (depending on N) by

$$\text{(6a)} \quad \Delta = \{\alpha \in M_2(\mathbf{Z}) \mid \det(\alpha) > 0\} \text{ if } \Gamma = SL_2(\mathbf{Z}) \text{ and}$$
$$\Delta = \{\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \mid p\nmid a,\ p^r|c \text{ and } ad\text{-}bc > 0\} \text{ if } \Gamma = \Gamma_0(p^r).$$

Let R be a complete representative set for $\Gamma\backslash\{\alpha \in \Delta \mid \det(\alpha) = n\}$. Then it is known that in fact

$$f|T(n) = \sum_{\alpha\in R} \chi(\alpha)f|_k\alpha,$$

which is the original definition of Hecke (see [Sh, III] and [M, IV]). In particular, on $\mathcal{S}_k(\Gamma_0(p^r),\chi)$ $(r > 0)$, we can easily check that

$$\text{(6b)} \qquad f|T(p^s) = \sum_{u=1}^{p^s} f|_k\begin{pmatrix} 1 & u \\ 0 & p^s \end{pmatrix}.$$

Let A be a subalgebra of $\mathbf{C}$. By (5), $\mathcal{M}_k(\Gamma,\chi;A)$ and $\mathcal{S}_k(\Gamma,\chi;A)$ are stable under the Hecke operators $T(n)$ if A contains $\mathbf{Z}[\chi]$. Here we write

$$\mathcal{M}_k(\Gamma,\chi;A) = \mathcal{M}_k(\Gamma,\chi)\cap A[[q]] \text{ and } \mathcal{S}_k(\Gamma,\chi;A) = \mathcal{S}_k(\Gamma,\chi)\cap A[[q]].$$

Let V be an A-submodule of any one of the above spaces stable under $T(n)$ for all positive integers n. Then we define the Hecke algebra $\mathcal{h}(V)$ by the A-subalgebra of $\mathrm{End}_A(V)$ generated by $T(n)$ for all positive n. Note that $T(1)$ gives the identity on V and hence $\mathcal{h}(V)$ is a commutative algebra with identity. Hereafter we suppose that A contains $\mathbf{Z}[\chi]$ if we consider $\mathcal{M}_k(\Gamma_0(N),\chi;A)$ and $\mathcal{S}_k(\Gamma_0(N),\chi;A)$. We define

$$\mathbf{H}_k(\Gamma_0(N),\chi;A) = \mathcal{h}(\mathcal{M}_k(\Gamma_0(N),\chi;A)) \text{ and } \mathbf{h}_k(\Gamma_0(N),\chi;A) = \mathcal{h}(\mathcal{S}_k(\Gamma_0(N),\chi;A)).$$

Lemma 1. *The space* $\mathcal{M}_k(\Gamma_0(N),\chi;\mathbf{C})$ *is of finite dimension over* $\mathbf{C}$.

Proof. By replacing $\Gamma = \Gamma_0(N)$ by the kernel of χ, we may assume that χ is trivial. We fix a representative set R for $\Gamma\backslash SL_2(\mathbf{Z})$ and consider the A-linear map $I_M : \mathcal{M}_k(\Gamma) \to \mathbf{C}^{M*}$ for each positive integer M given by $I_M(f) = (a(n,f|_k\gamma))_{n,\gamma}$, where (n,γ) runs over all possible pairs with $0 \le n < M$ and $\gamma \in R$ for

which we have some modular form f with $a(n,f|_k\gamma) \neq 0$ and M^* is the number of such pairs (n,γ). The number M^* is smaller than $NM[SL_2(\mathbf{Z}):\Gamma]$ because we always have $n \in N^{-1}\mathbf{Z}$ for the pairs (n,γ) as above. Take $M \geq r(k)+1$ and suppose that $I_M(f) = 0$. Let $s_i(f)$ be the coefficient of X^{d-i} in $P(f;X) = \prod_{\gamma\in R}(X-f|_k\gamma)$ for $d = \#R$. Then we have $a(n,s_i(f)) = 0$ if $n < r(ki) < i(r(k)+1)$. Hence by the proof of Theorem 2.1, $s_i(f) = 0$ for $i > 0$. Thus $P(f;X) = X^d$. Since $0 = P(f;f) = f^d$, we know that $f = 0$. In particular, we have

$$\dim_{\mathbf{C}}(\mathcal{M}_k(\Gamma)) \leq (r(k)+1)N[SL_2(\mathbf{Z}):\Gamma].$$

We define for the quotient field K of A

$$m_k(\Gamma_0(N),\chi;A) = \{f \in \mathcal{M}_k(\Gamma_0(N),\chi;K) \mid a(n,f) \in A \text{ if } n > 0\}.$$

Clearly we know that $m_k(\Gamma_0(N),\chi;A) \supset \mathcal{M}_k(\Gamma_0(N),\chi;A)$, but they may not be equal.

Theorem 1 (duality). *Suppose that* A *contains* $\mathbf{Z}[\chi]$. *Define a pairing*

$$\langle\ ,\ \rangle : \mathbf{H}_k(\Gamma_0(N),\chi;A) \times m_k(\Gamma_0(N),\chi;A) \to A \text{ by } \langle h,f\rangle = a(1,f|h) \in A.$$

Then this pairing is perfect on $m_k(\Gamma_0(N),\chi;A)$ *and* $\mathcal{S}_k(\Gamma_0(N),\chi;A)$*; in other words, we have isomorphisms*

$$\mathrm{Hom}_A(\mathbf{H}_k(\Gamma_0(N),\chi;A),A) \cong m_k(\Gamma_0(N),\chi;A),$$
$$\mathrm{Hom}_A(m_k(\Gamma_0(N),\chi;A),A) \cong \mathbf{H}_k(\Gamma_0(N),\chi;A),$$
$$\mathrm{Hom}_A(\mathbf{h}_k(\Gamma_0(N),\chi;A),A) \cong \mathcal{S}_k(\Gamma_0(N),\chi;A),$$
$$\mathrm{Hom}_A(\mathcal{S}_k(\Gamma_0(N),\chi;A),A) \cong \mathbf{h}_k(\Gamma_0(N),\chi;A).$$

Proof. Here we prove this theorem under the assumption that either $N = 1$ or $A = \mathbf{C}$ and later return to this problem for general $N = p^r$ and A. First assume that $A = \mathbf{C}$. Write $\Gamma = \Gamma_0(N)$. Since $\mathbf{H}_k(\Gamma,\chi;\mathbf{C})$ is a subspace of $\mathrm{End}_{\mathbf{C}}(m_k(\Gamma,\chi;\mathbf{C}))$ which is of finite dimension, $\mathbf{H}_k(\Gamma,\chi;\mathbf{C})$ is of finite dimension. Thus we only need to prove the non-degeneracy of the pairing. Since $a(m,f|T(n)) = \sum_{b|(m,n)} \chi(b)b^{k-1}a(mn/b^2,f)$, we see that

$$\langle T(n),f\rangle = a(1,f|T(n)) = a(n,f).$$

If $\langle h,f\rangle = 0$ for all h in the Hecke algebra, then $a(n,f) = \langle T(n),f\rangle = 0$ for all positive n. Thus f is a constant. Since k is positive, f must be 0. Conversely, if $\langle h,f\rangle = 0$ for all f, then

$$a(n,f|h) = \langle T(n),f|h\rangle = a(1,f|hT(n)) = \langle h,f|T(n)\rangle = 0.$$

Thus $f|h = 0$ for all f and hence $h = 0$ as an operator. This proves the assertion for $A = \mathbf{C}$. The above argument is valid as long as A is a field and both $\mathbf{H}_k(\Gamma,\chi;A)$ and $m_k(\Gamma,\chi;A)$ are of finite dimension over A. In particular, the theorem is true for $A = \mathbf{Q}$ when $\Gamma = SL_2(\mathbf{Z})$ by Theorem 2.1. Now we want to show the theorem for $A = \mathbf{Z}$ and $\Gamma = SL_2(\mathbf{Z})$. Since A is a principal ideal domain, it is sufficient to prove one of the following two assertions:

$$\mathrm{Hom}_A(\mathbf{H}_k(\Gamma;\mathbf{Z}),\mathbf{Z}) \cong \mathcal{M}_k(\Gamma;\mathbf{Z}), \qquad \mathrm{Hom}_A(\mathcal{M}_k(\Gamma;\mathbf{Z}),\mathbf{Z}) \cong \mathbf{H}_k(\Gamma;\mathbf{Z}).$$

We shall show that $\mathrm{Hom}_A(\mathbf{H}_k(\Gamma;\mathbf{Z}),\mathbf{Z}) \cong \mathcal{M}_k(\Gamma;\mathbf{Z})$. Since

$$\mathcal{M}_k(\Gamma;\mathbf{Z})\otimes_{\mathbf{Z}}\mathbf{Q} = \mathcal{M}_k(\Gamma;\mathbf{Q}), \qquad \mathbf{H}_k(\Gamma;\mathbf{Z})\otimes_{\mathbf{Z}}\mathbf{Q} = \mathbf{H}_k(\Gamma;\mathbf{Q}).$$

The natural map from $\mathcal{M}_k(\Gamma;A)$ into $\mathrm{Hom}_A(\mathbf{H}_k(\Gamma;A),A)$ is injective, because if $\langle h,f\rangle = 0$ for all h, then $f = 0$ as shown already. If $\varphi : \mathbf{H}_k(\Gamma;A) \to \mathbf{Z}$ is a linear form, we can extend φ to a linear form on $\mathbf{H}_k(\Gamma;\mathbf{Q})$ with values in $\mathbf{Q}$ by linearity. Then we can find $f \in \mathcal{M}_k(\Gamma;\mathbf{Q})$ such that $\langle h,f\rangle = \varphi(h)$ for all h. Then $a(n,f) = \varphi(T(n)) \in \mathbf{Z}$ and hence $f \in \mathcal{M}_k(\Gamma;\mathbf{Z})$. This proves the surjectivity. As for general A, since $\mathcal{M}_k(\Gamma;A) = \mathcal{M}_k(\Gamma;\mathbf{Z})\otimes_{\mathbf{Z}}A$, by definition, we know that $\mathbf{H}_k(\Gamma;A) = \mathbf{H}_k(\Gamma;\mathbf{Z})\otimes_{\mathbf{Z}}A$. Thus

$$\mathrm{Hom}_A(\mathbf{H}_k(\Gamma;A),A) \cong \mathrm{Hom}_{\mathbf{Z}}(\mathbf{H}_k(\Gamma;\mathbf{Z}),\mathbf{Z})\otimes A \cong \mathcal{M}_k(\Gamma;\mathbf{Z})\otimes A \cong \mathcal{M}_k(\Gamma;A),$$
$$\mathrm{Hom}_A(\mathcal{M}_k(\Gamma;A),A) \cong \mathrm{Hom}_{\mathbf{Z}}(\mathcal{M}_k(\Gamma;\mathbf{Z}),\mathbf{Z})\otimes A \cong \mathbf{H}_k(\Gamma;\mathbf{Z})\otimes A \cong \mathbf{H}_k(\Gamma;A),$$

which finishes the proof.

We consider the hermitian product (called Petersson inner product) on $\mathcal{S}_k(\Gamma_0(N),\chi)$ defined by

$$(7) \qquad (f,g)_N = \int_{\Gamma_0(N)\backslash\mathcal{H}} f(z)\,\overline{g(z)}\,\mathrm{Im}(z)^{k-2}dxdy = \int_{\Phi} f(z)\,\overline{g(z)}\,\mathrm{Im}(z)^{k-2}dxdy,$$

where Φ is the fundamental domain of $\Gamma_0(N)$. First of all, we know that $f(\gamma(z)) = f(z)(cz+d)^k$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Thus $\bar{g}f(\gamma(z)) = \bar{g}f(z)|cz+d|^{2k}$. On the other hand,

$$dx\wedge dy = (-2i)^{-1}dz\wedge d\bar{z} \text{ and thus } \gamma^*(dx\wedge dy) = |cz+d|^{-4}(dx\wedge dy).$$

By taking the determinant of the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z & \bar{z} \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \gamma(z) & \gamma(\bar{z}) \\ 1 & 1 \end{pmatrix}\begin{pmatrix} cz+d & 0 \\ 0 & c\bar{z}+d \end{pmatrix},$$

we know that $\mathrm{Im}(\gamma(z)) = \det(\gamma)|cz+d|^{-2}\mathrm{Im}(z)$. Thus $f\bar{g}y^{k-2}dx\wedge dy$ for $y = \mathrm{Im}(z)$ is invariant under the action of Γ, and hence at least formally the above integral is well defined. By the same formula, $|f(z)y^{k/2}|$ for $f \in \mathcal{S}_k(\Gamma_0(N),\chi)$ is a continuous function on $Y = \Gamma_0(N)\backslash\mathcal{H}$. Since as a function of $q = \mathbf{e}(z)$, f vanishes at $q = 0$, on a small relatively compact neighborhood V of 0, $f(q) = qF(q)$ with a holomorphic function F on V. Thus on the closure of V,

(8a) $|f(z)y^{k/2}|$ is bounded on $\mathcal{H}$ and $|f(z)| \le O(\exp(-2\pi y))$ as $y \to \infty$.

Writing the bound of $|f(z)\mathrm{Im}(z)^{k/2}|$ as c_0, we see that

$$|a(n,f)| = \left|\int_0^1 f(x+iy)e(-n(x+iy))dx\right| \le c_0 e^{2\pi ny}y^{-k/2}.$$

By taking the minimum of the function $c_0e^{2\pi ny}y^{-k/2}$, we conclude that

$$(8b) \qquad |a(n,f)| \le Cn^{k/2} \quad \text{for } f \in \mathcal{S}_k(\Gamma,\chi),$$

where C is a constant independent of n. Thus by (8a) $\alpha^* f\bar{g}y^{k-2}dx \wedge dy$ for $\alpha \in SL_2(\mathbf{Z})$ is exponentially decreasing as $\mathrm{Im}(z) \to \infty$, and hence the integral (7) converges. Thus $(\ ,\ )_N$ is a well defined positive definite hermitian product on $\mathcal{S}_k(\Gamma_0(N),\chi)$. More generally, for any subgroup Γ of finite index in $SL_2(\mathbf{Z})$, we can define $(f,g)_\Gamma$ for $f, g \in \mathcal{S}_k(\Gamma)$ by the same formula (7) replacing $\Gamma_0(N)$ by Γ. Note that if $\Gamma \supset \Gamma'$ and if $[\Gamma:\Gamma']$ is finite, then for $\omega = f\bar{g}y^{k-2}dx \wedge dy$ with $f,g \in \mathcal{S}_k(\Gamma)$, $\gamma^*\omega = \omega$ for all $\gamma \in \Gamma$. On the other hand, if $\Gamma = \coprod_j \Gamma'\gamma_j$, then $\Gamma = \coprod_j \gamma_j^{-1}\Gamma'$, and $\Psi = \coprod_j \gamma_j\Phi$ is a fundamental domain of Γ'. In fact for any $z \in \mathcal{H}$, we can find a unique $\gamma \in \Gamma$ such that $\gamma(z) \in \Phi$. Then we can write $\gamma = \gamma_j^{-1}\delta$ for a unique j and $\delta \in \Gamma'$. Thus $\delta(z) \in \gamma_j\Phi$ and Ψ is a fundamental domain of Γ'. This shows that

$$(9) \quad (f,g)_{\Gamma'} = \sum_i \int_\Phi (\gamma_i^{-1})^*\omega = \int_\Phi \omega = (\Gamma:\Gamma')(f,g)_\Gamma \quad \text{for } \Gamma \supset \Gamma' \ (f,g \in \mathcal{S}_k(\Gamma)).$$

For any $\alpha \in \Delta$, the group $\Gamma' = \Gamma \cap \alpha^{-1}\Gamma\alpha$ is of finite index in Γ. Thus for $f,g \in \mathcal{S}_k(\Gamma)$, we have $f|_k\alpha \in \mathcal{S}_k(\Gamma')$ and

$$\begin{aligned}\bar{g}(f|\alpha)y^{k-2}dx \wedge dy &= \overline{g(z)}\det(\alpha)^{k-1}f(\alpha(z))j(\alpha,z)^{-k}y^{k-2}dx \wedge dy \\ &= \alpha^*\overline{(g|\alpha^\iota)}f(z)y^{k-2}dx \wedge dy,\end{aligned}$$

where we have written $j(\begin{pmatrix} a & b \\ c & d\end{pmatrix},z) = (cz+d)$ and $\alpha^\iota = \det(\alpha)\alpha^{-1}$. Then we have, for the fundamental domain Ψ of Γ',

$$(f|\alpha,g)_{\Gamma'} = \int_\Psi \alpha^*\overline{(g|\alpha^\iota)}f(z)y^{k-2}dxdy = \int_{\alpha(\Psi)} \overline{(g|\alpha^\iota)}f(z)y^{k-2}dxdy = (f,g|\alpha^\iota)_{\alpha\Gamma'},$$

because $\alpha(\Psi)$ is a fundamental domain of ${}^\alpha\Gamma' = \alpha\Gamma'\alpha^{-1}$. Since

$$(\Gamma:\Gamma')\mathrm{vol}(\Phi) = \mathrm{vol}(\Psi) = \mathrm{vol}(\alpha(\Psi)) = (\Gamma:\alpha\Gamma'\alpha^{-1})\mathrm{vol}(\Phi)$$

under the invariant measure $y^{-2}dxdy$, $(\Gamma:\Gamma') = (\Gamma:\alpha\Gamma'\alpha^{-1})$. We now want to compute $(f|[\Gamma\alpha\Gamma],g)$ for $\Gamma = \Gamma_0(p^r)$. Decompose $\Gamma\alpha\Gamma = \coprod_j \Gamma\alpha_j$ and write Φ for the fundamental domain of Γ in $\mathcal{H}$. Then we have

$$(f|[\Gamma\alpha\Gamma],g) = \sum_j \chi(\alpha_j)(f|\alpha_j,g) = \sum_j \chi(\alpha_j)(f,g|\alpha_j^\iota) = (f,\sum_j \chi(\alpha_j)^{-1}g|\alpha_j^\iota).$$

Lemma 2. *We suppose that* $\#(\Gamma\backslash\Gamma\alpha\Gamma) = \#(\Gamma\backslash\Gamma\alpha^\iota\Gamma)$ *for* $\Gamma = \Gamma_0(p^r)$. *Then we may choose* α_j *so that* $\Gamma\alpha\Gamma = \coprod_j \Gamma\alpha_j$ and $\Gamma\alpha^\iota\Gamma = \coprod_j \Gamma\alpha_j^\iota$.

Proof. Since the involution ι brings a right coset onto a left coset, by assumption, the numbers of the right cosets and the left cosets in $\Gamma\alpha\Gamma$ are the same. If $\Gamma\alpha\Gamma$ contains $\Gamma\xi$ and $\eta\Gamma$, then $\xi = \delta\eta\gamma$ for δ and γ in Γ. Then for $\zeta = \delta^{-1}\xi = \eta\gamma$, $\Gamma\zeta = \Gamma\delta^{-1}\xi = \Gamma\xi$ and $\zeta\Gamma = \eta\gamma\Gamma = \eta\Gamma$. Thus we can choose α_i so that $\Gamma\alpha\Gamma = \bigcup_i\Gamma\alpha_i = \bigcup_i\alpha_i\Gamma$. Since ι is an involution, this means that $(\Gamma\alpha\Gamma)^\iota = \bigcup_i\Gamma\alpha_i^\iota$.

Note that

$$\Delta = \{\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \mid p\nmid a,\ p^r \mid c \text{ and } ad\text{-}bc > 0\}.$$

Then for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta$, $ad \equiv \det(\alpha) \mod p$. Thus if $\det(\alpha)$ is prime to p, then $\chi(\alpha^\iota) = \chi(d) = \chi^{-1}(a)\chi(\det(\alpha)) = \chi^{-1}(\alpha)\chi(\det(\alpha))$. Therefore by the above lemma, if $\Gamma\alpha\Gamma = \Gamma\alpha^\iota\Gamma$, we have

$$\textstyle\sum_i\chi(\alpha_i)^{-1}g \mid \alpha_i^\iota = \chi^{-1}(\det(\alpha))\sum_i\chi(\alpha_i^\iota)g \mid \alpha_i^\iota = \chi^{-1}(\det(\alpha))g \mid [\Gamma\alpha\Gamma].$$

Thus we have $T(q)^* = \chi^{-1}(q)T(q)$ if q is prime to N for $T(q)$ on $\mathcal{S}_k(\Gamma_0(N),\chi)$. More generally, we have

(10a) $$T(n)^* = \chi^{-1}(n)T(n) \text{ if } n \text{ is prime to } N.$$

Note that $\tau = \begin{pmatrix} 0 & -1 \\ p^r & 0 \end{pmatrix}$ normalizes $\Gamma_0(p^r)$ and for $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$, $\tau\alpha\tau^{-1} = \alpha^\iota$. Thus $\tau\{(\Gamma\alpha\Gamma\}\tau^{-1} = \Gamma\alpha^\iota\Gamma$ and $\#(\Gamma\backslash\Gamma\alpha^\iota\Gamma) = \#(\Gamma\backslash\Gamma\alpha\Gamma)$ for $\Gamma = \Gamma_0(p^r)$. Therefore we can choose the decomposition $\Gamma\alpha\Gamma = \coprod_j\Gamma\alpha_j$ so that $\Gamma\alpha^\iota\Gamma = \coprod_j\Gamma\alpha_j^\iota$ is a disjoint union. Since $\Gamma\alpha^\iota\Gamma = \coprod_j\Gamma\tau\alpha_j\tau^{-1}$ is also a disjoint union, by (1b) and $\chi(\alpha_j) = \chi((\tau\alpha_j\tau^{-1})^\iota)$, we have

$$f \mid T^*(q) = \textstyle\sum_j\chi(\alpha_j)^{-1}f \mid \alpha_j^\iota = \sum_j\chi((\tau\alpha_j\tau^{-1})^\iota)^{-1}f \mid \tau\alpha_j\tau^{-1} = \sum_j\chi(\alpha_j)^{-1}f \mid \tau\alpha_j\tau^{-1}.$$

We write $T_\chi(q)$ for $T(q)$ on $\mathcal{S}_k(\Gamma_0(p^r),\chi)$. Then for any $f \in \mathcal{S}_k(\Gamma_0(p^r),\chi)$

$$f \mid \tau T_{\bar\chi}(q)\tau^{-1} = \textstyle\sum_j\chi(\alpha_j)^{-1}f \mid \tau\alpha_j\tau^{-1} = f \mid T_\chi^*(q) = f \mid T^*(q).$$

Thus we have

(10b) $$\tau T_{\bar\chi}(q)\tau^{-1} = T^*(q) = T(q)^* \text{ for all primes } q.$$

Theorem 2 (Hecke). *If either* χ *is primitive modulo* p^r *or* $r = 0$, *then* $\mathbf{H}_k(\Gamma_0(p^r),\chi;\mathbf{C})$ *is semi-simple and* $\mathcal{M}_k(\Gamma_0(p^r),\chi)$ *is spanned by common eigenforms* f *of all Hecke operators* $T(n)$ *such that* $f \mid T(n) = a(n,f)f$.

Although this fact is true for all $k \geq 1$, all $\Gamma_0(N)$, and all χ primitive modulo arbitrary N, we prove the result only when $k \geq 2$ and $N = p^r$. (See [M, Th.4.7.2, Th.7.2.18] for the proof in the general case).

Proof. First we prove the theorem for $SL_2(\mathbf{Z})$. In this case, we see from (10) that $(f|T(n),g) = (f,g|T(n))$ and thus $T(n)$ is a hermitian operator. Since the $T(n)$'s are mutually commutative, we can diagonalize $T(n)$ simultaneously on $\mathcal{S}_k(\Gamma)$. This shows that $\mathbf{h}_k(SL_2(\mathbf{Z});\mathbf{C})$ can be embedded into a product of copies of $\mathbf{C}$ and hence $\mathbf{h}_k(SL_2(\mathbf{Z});\mathbf{C})$ is itself a product of copies of $\mathbf{C}$. Note that $\mathbf{h}_k(SL_2(\mathbf{Z});\mathbf{C}) \cong \mathbf{C}^r$ for $r = \dim_{\mathbf{C}}\mathcal{S}_k(SL_2(\mathbf{Z}))$ because $\mathrm{Hom}_{\mathbf{C}}(\mathbf{h}_k(\Gamma;\mathbf{C}),\mathbf{C}) = \mathcal{S}_k(\Gamma)$. Then each projection λ_i of $\mathbf{h}_k(SL_2(\mathbf{Z});\mathbf{C})$ into $\mathbf{C}$ is a $\mathbf{C}$-algebra homomorphism, and $\{\lambda_1, \ldots, \lambda_r\}$ form a basis of $\mathrm{Hom}_{\mathbf{C}}(\mathbf{h}_k(\Gamma;\mathbf{C}),\mathbf{C})$. Let λ be one of the λ_i's and f be the corresponding element in $\mathcal{S}_k(\Gamma)$. Then $a(n,f) = \langle T(n),f\rangle = \lambda(T(n))$ and hence $f = \sum_{n=1}^{\infty}\lambda(T(n))q^n$. Moreover

$$\begin{aligned} a(m,f|T(n)) &= \langle T(m),f|T(n)\rangle = a(1,f|T(n)T(m)) \\ &= \langle T(m)T(n),f\rangle = \lambda(T(m)T(n)) = \lambda(T(n))a(m,f). \end{aligned}$$

Thus $f|T(n) = \lambda(T(n))f$ and f is a common eigenform of all Hecke operators $T(n)$ belonging to the algebra homomorphism λ. We write $f_i = \sum_{n=1}^{\infty}\lambda_i(T(n))q^n$. Then $\{f_i\}_i$ gives a basis of $\mathcal{S}_k(\Gamma)$ over $\mathbf{C}$. Now we show that E_k is a common eigenform of all Hecke operators. We show more generally that

$$E_k(\chi)|T(q) = \sigma_{k-1,\chi}(q)E_k(\chi) \text{ for every prime } q.$$

We thus compute $a(n,E_k(\chi)|T(q)) = a(nq,E_k(\chi))+\chi(q)q^{k-1}a(n/q,E_k(\chi))$. If n is prime to q, then

$$\sigma_{k-1,\chi}(nq) = \sum_{d|nq}\chi(d)d^{k-1} = \sum_{d|n}\sum_{b|q}\chi(bd)(bd)^{k-1} = \sigma_{k-1,\chi}(n)\sigma_{k-1,\chi}(q).$$

Therefore $a(n,E_k(\chi)|T(q)) = \sigma_{k-1,\chi}(q)a(n,E_k(\chi))$. If n is divisible by q, then

$$\begin{aligned} a(n,E_k(\chi)|T(q)) &= a(nq,E_k(\chi))+\chi(q)q^{k-1}a(n/q,E_k(\chi)) \\ &= \sum_{d|nq}\chi(d)d^{k-1}+\chi(q)q^{k-1}\sum_{b|n/q}\chi(b)b^{k-1} \\ &= \sum_{d|nq}\chi(d)d^{k-1} + \sum_{qb|n}\chi(qb)(qb)^{k-1}. \end{aligned}$$

On the other hand, we have

$$\begin{aligned} \sigma_{k-1,\chi}(n)\sigma_{k-1,\chi}(q) &= \sum_{d|n}\sum_{b|q}\chi(bd)(bd)^{k-1} \\ &= \sum_{d|nq}\chi(d)d^{k-1}+\sum_{qb|n}\chi(qb)(qb)^{k-1}. \end{aligned}$$

In fact, obviously, $\{d \mid d \mid nq\} = \{d \mid d \mid n\} \cup \{qb \mid b \mid n\}$. The intersection $\{d \mid d \mid n\} \cap \{qb \mid b \mid n\}$ is given by

$$\{d \mid d \mid n,\ d = qb,\ b \mid n\} = \{qb \mid b \mid (n/q)\}.$$

Similarly we can show $G_k(\chi) \mid T(n) = \sigma'_{k-1,\chi}(n) G_k(\chi)$. Anyway this shows that $\mathcal{M}_k(SL_2(\mathbf{Z}))$ has a basis $\{f_1, \cdots, f_{r-1}, E_k\}$ which consists of common eigenforms of all Hecke operators $T(n)$, and hence the desired assertion for $\mathcal{M}_k(SL_2(\mathbf{Z}))$ follows from this.

Now we consider $\mathcal{S}_k(\Gamma_0(p^r),\chi)$. By (10), $\sqrt{\chi(n)}^{-1} T(n)$ is self-adjoint if n is prime to p. Thus, we can find a basis of $\mathcal{S}_k(\Gamma_0(p^r),\chi)$ consisting of common eigenforms of $T(n)$ for all n prime to p. We shall show that if $f \neq 0$ is a common eigenform of all operators $T(n)$ for n prime to p and if χ is primitive modulo p^r, then f is an eigenform even for $T(p)$. We consider the following set of positive integers:

$$X = \{n \mid p \nmid n,\ a(n,f) \neq 0\}.$$

We first show that X is not empty. If this set is empty, then $a(n,f) \neq 0$ only if n is divisible by p. Let $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ and put

$$g(z) = f(z/p) = pf \mid \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}(z).$$

Then g satisfies $g \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \chi(d) g$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Phi = \alpha^{-1}\Gamma_0(p^r)\alpha$ and is also invariant under $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Note that $\alpha^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\alpha = \begin{pmatrix} a & pb \\ c/p & d \end{pmatrix}$ and

$$\Phi = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid b \in p\mathbf{Z},\ c \in p^{r-1}\mathbf{Z},\ a,d \in \mathbf{Z},\quad ad\text{-}bc = 1\}.$$

To show that $g = 0$, we take integers m and n so that

$$(mp^{r-1}+1)(np^{r-1}+1) \equiv 1 \bmod p^r \text{ but } \chi(np^{r-1}+1) \neq 1.$$

Note that

$$\gamma = u^m({}^t u^{pr-1})u^n = \begin{pmatrix} 1+mp^{r-1} & mnp^{r-1}+m+n \\ p^{r-1} & 1+np^{r-1} \end{pmatrix} \in \Phi$$

and thus $g \mid \gamma = \chi(np^{r-1}+1)g$ but at the same time $g \mid u^m = g$, $g \mid {}^t u^{p^{r-1}} = g$ and $g \mid u^n = g$. Thus $\chi(np^{r-1}+1)g = g$ and hence $g = 0$. This shows that if $f \neq 0$, X is not empty. Take any n in X. Then writing $f \mid T(n) = a(n)f$, we have

$$0 \neq a(n,f) = \langle T(n),f\rangle = a(1,f \mid T(n)) = a(n)a(1,f).$$

Thus $a(1,f) \neq 0$ for any non-zero common eigenform f of Hecke operators $T(n)$ for n prime to p. Since $g = f \mid T(p)$ is also a common eigenform of all $T(n)$ for n prime to p, $a(1,g) \neq 0$. Put $h = a(1,g)f - a(1,f)g$. By definition,

$$a(1,h) = a(1,g)a(1,f)-a(1,f)a(1,g) = 0.$$

Since h is again a common eigenform of all $T(n)$ for n prime to p, and hence $a(1,h) \neq 0$ if $h \neq 0$. Thus h must be 0 and $f|T(p)$ is a constant multiple of f; namely, f is an eigenform of $T(p)$. Thus $\mathcal{S}_k(\Gamma_0(p^r),\chi)$ has a basis consisting of common eigenforms of all Hecke operators.

Next, we shall show that $\mathcal{M}_k(\Gamma_0(p^r),\chi)$ is spanned by $\mathcal{S}_k(\Gamma_0(p^r),\chi)$ and $E_k(z,\chi)$ and $G_k(z,\chi)$. Since $\mathcal{M}_2(SL_2(\mathbf{Z})) = \{0\}$ (Theorem 2.1), we may assume either $k > 2$ or $\chi \neq 1$ and $k \geq 2$. Consider the sequence

$$(*) \qquad 0 \to \mathcal{S}_k(\Gamma_0(p^r),\chi) \to \mathcal{M}_k(\Gamma_0(p^r),\chi) \xrightarrow{\varphi} \mathbf{C}^2 \to 0.$$

The last map φ is given by $\varphi(f) = (a(0,f),\ a(0,f|_k\delta))$ for $\delta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The surjectivity of φ follows from the fact that $\varphi(E_k(\chi)) = (2^{-1}L(1-k,\chi),0)$ and $\varphi(G_k(\chi)) = (0,w'L(1-k,\chi^{-1}))$ with $w' \neq 0$, which is a consequence of

$$E_k(z;\chi)|_k\delta = wG_k(\tfrac{z}{p^r};\chi^{-1}) \text{ with } w \neq 0 \text{ (see Proposition 1.1).}$$

Since by the functional equation (Theorem 2.3.2), $L(1-k,\chi)$ is a non-zero constant multiple of $L(k,\chi^{-1})$, which is non-zero because the Euler product converges if $k > 1$. Thus φ is surjective. Now let us show the exactness of the middle term. Pick a modular form f in $\mathcal{M}_k(\Gamma_0(p^r),\chi)$ and suppose that $\varphi(f) = 0$. By the strong approximation theorem (see Lemma 6.1.1), for each element α of $SL_2(\mathbf{Z})$, we can find $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^r)$ so that either

(i) $\alpha = \gamma\delta\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ for some integer j in the interval $[1,p^r]$,

or

(ii) $\gamma\begin{pmatrix} 1 & 0 \\ p^s i & 1 \end{pmatrix}$ for some integer i in the interval $[1,p^{r-s}]$ and s in $[1,r]$.

Then, in case (i), $a(0,f|\alpha) = \chi(d)a(0,f|\delta) = 0$. Now we deal with case (ii). Write simply $\Gamma' = \Gamma_1(p^r)$ and $\Gamma = \Gamma_0(p^r)$. Then we see that $\Gamma/\Gamma' \cong (\mathbf{Z}/p^r\mathbf{Z})^\times$ via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod p^r$, and Γ/Γ acts on equivalence classes of cusps of Γ': $C = \Gamma'\backslash SL_2(\mathbf{Z})/\Gamma'_\infty$, where $\Gamma'_\infty = \left\{\pm\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in \Gamma'\right\}$. Letting $SL_2(\mathbf{Z})$ act on the column vectors $(\mathbf{Z}/p^r\mathbf{Z})^2$, we see that Γ' is the stabilizer of the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Thus we can identify C with $\Gamma'\backslash(\mathbf{Z}/p^r\mathbf{Z})^2$. Then the cusp corresponding to $\begin{pmatrix} 1 & 0 \\ p^s i & 1 \end{pmatrix}$ for i prime to p is given by the vector $x_i = \begin{pmatrix} 1 \\ p^s i \end{pmatrix}$. Then the orbit $O(x_i)$ of x_i

under the action of $(\mathbf{Z}/p^r\mathbf{Z})^\times = \Gamma/\Gamma'$ is isomorphic to $(\mathbf{Z}/p^{r-s}\mathbf{Z})^\times$ via $(\mathbf{Z}/p^{r-s}\mathbf{Z})^\times \ni i \mapsto x_i$. Considering the function $\phi : i \mapsto a(0,f\left|\begin{pmatrix}1 & 0\\ p^s i & 1\end{pmatrix}\right.)$ as a function on $(\mathbf{Z}/p^{r-s}\mathbf{Z})^\times$, we see that $\phi(di) = \chi(d)\phi(i)$ for $d \in (\mathbf{Z}/p^r\mathbf{Z})^\times$. Since $s > 0$ and χ is primitive modulo p^r, we can find $d = 1+jp^{r-s}$ such that $\chi(d) \neq 1$. Since the action of $(\mathbf{Z}/p^r\mathbf{Z})^\times$ on $O(x_i)$ factors through $(\mathbf{Z}/p^{r-s}\mathbf{Z})^\times$, $\chi(d)\phi(i) = \phi(di) = \phi(i)$. This implies ϕ vanishes identically. That is, for the cusp in case (ii), the constant term of all modular forms in $\mathcal{M}_k(\Gamma_0(p^r),\chi)$ vanishes. This shows that $\mathrm{Ker}(\varphi) = \mathcal{S}_k(\Gamma_0(p^r),\chi)$. Thus $\mathcal{M}_k(\Gamma_0(p^r),\chi)$ is spanned by $\mathcal{S}_k(\Gamma_0(p^r),\chi)$ and $E_k(z,\chi)$ and $G_k(z,\chi)$. We have already verified that

$$E_k(\chi) \,|\, T(n) = \sigma_{k-1,\chi}(n)E_k(\chi) \text{ and } G_k(\chi) \,|\, T(n) = \sigma'_{k-1,\chi}(n)G_k(\chi) \text{ for all } n.$$

This finishes the proof of Theorem 2. We record the following fact shown in the proof of Theorem 2.

Corollary 1. *Suppose that* χ *is primitive modulo* p^r *and let* f *and* g *be elements in* $\mathcal{S}_k(\Gamma_0(p^r),\chi)$. *Then if* f *is a common eigenfunction of* $T(n)$ *for all* n *prime to* p, *then* f *is also an eigenfunction of* $T(p)$. *If* f *and* g *have the same eigenvalues for* $T(n)$ *for all* n *prime to* p *and* $g \neq 0$, *then* f *is a constant multiple of* g.

Corollary 2. *Let* f *be a common eigenform of all Hecke operators with* $a(1,f) = 1$ *in* $\mathcal{S}_k(SL_2(\mathbf{Z}))$. *Then the field* $\mathbf{Q}(f)$ *generated by all the Fourier coefficients of* f *is a finite extension of* $\mathbf{Q}$. *Moreover* $a(n,f)$ *are all algebraic integers and for all* $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, f^σ *is again a common eigenform in* $\mathcal{S}_k(SL_2(\mathbf{Z}))$.

Proof. Let $\Gamma = SL_2(\mathbf{Z})$. We know that $f = f_\lambda = \sum_{n=1}^\infty \lambda(T(n))q^n$ for an algebra homomorphism $\lambda : \mathbf{h}_k(\Gamma,\chi;\mathbf{C}) = \mathbf{h}_k(\Gamma,\chi;\mathbf{Q})\otimes_{\mathbf{Q}}\mathbf{C} \to \mathbf{C}$. Thus λ induces a $\mathbf{Q}$-algebra homomorphism of $\mathbf{h}_k(\Gamma;\mathbf{Q})$ into $\mathbf{C}$. Note that $\lambda(\mathbf{h}_k(\Gamma;\mathbf{Q}))$ is an algebra of finite dimension over $\mathbf{Q}$ which is generated by $\lambda(T(n))$. Thus $\mathbf{Q}(f) = \lambda(\mathbf{h}_k(\Gamma;\mathbf{Q}))$ and $\mathbf{Q}(f)$ is a finite extension over $\mathbf{Q}$. The image $\lambda(\mathbf{h}_k(\Gamma;\mathbf{Z}))$ is contained in the integer ring of $\lambda(\mathbf{h}_k(\Gamma;\mathbf{Q}))$. In fact, by representing $T(n)$ as a matrix using the basis h_i in Theorem 2.1, we see that $(h_0 \,|\, T(n),\cdots, h_{r-1} \,|\, T(n)) = (h_0,\cdots, h_{r-1})\Lambda(n)$ with $\Lambda(n) \in M_r(\mathbf{Z})$. Thus $\lambda(T(n))$ is a characteristic root of integral matrix $\Lambda(n)$ which is an algebraic integer. We know that

$$\mathrm{Hom}_{\mathbf{Z}\text{-alg}}(\mathbf{h}_k(\Gamma,\mathbf{Z}),\overline{\mathbf{Q}}) \cong \{f \,\big|\, f \,|\, T(n) = \lambda(T(n))f,\ \ a(1,f) = 1\}:\ \ \lambda \mapsto f_\lambda$$

Naturally $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on the left-hand side. The action is interpreted into $f \mapsto f^\sigma$ on the right-hand side, which shows the last assertion.

We will see the assertion of Corollary 2 also holds for $\mathcal{S}_k(\Gamma_0(p^r),\chi)$ for primitive χ in the following section.

§5.4. The Petersson inner product and the Rankin product

In this section, we study how we can explicitly construct a basis for the spaces of modular forms (as we have just done for $\Gamma = SL_2(\mathbf{Z})$).

Theorem 1. *Let* $a \geq 2$ *be an integer and let* ψ *be a character modulo* p^r *with* $\psi(-1) = (-1)^a$. *Suppose* $k > 2a+2$. *Then for any primitive character* χ *modulo* p^r $(r \geq 1)$ *with* $\chi(-1) = (-1)^k$, *there exist finitely many positive integers* $n_1, n_2, \cdots, n_r$ *such that* $G_a(\psi^{-1})E_{k-a}(\psi\chi) \mid T(n_i)$ *for* $i = 1, \cdots, r$ *together with* $G_k(\chi)$ *and* $E_k(\chi)$ *span* $\mathcal{M}_k(\Gamma_0(p^r),\chi)$ *over* $\mathbf{C}$. *The above assertion is true with* $E_a(\psi^{-1})$ *in place of* $G_a(\psi^{-1})$. *Similarly* $\mathcal{M}_k(SL_2(\mathbf{Z}))$ *is spanned by* E_k *and* $E_aE_{k-a} \mid T(n_i)$ *for some* n_i *and* $4 \leq a \in 2\mathbf{Z}$ *such that* $k > 2a+2$.

A more general result is obtained in [Wi1] (for example, the assertion of the theorem is true even if $a = 1$). The proof we will give later is basically the same as in [Wi1] although it is a little simpler because of our assumption that $a \geq 2$. For each Dirichlet character χ, we write $\mathbf{Z}[\chi]$ for the subring of $\mathbf{C}$ generated by all the values of χ. Before proving the theorem, we list several corollaries:

Corollary 1 (duality). *If* $k > 6$ *and* $\Gamma = \Gamma_0(p^r\mathbf{p})$ *and* χ *is a primitive character modulo* $p^r\mathbf{p}$ *for* $r \geq 0$, *then* $\mathcal{M}_k(\Gamma,\chi;A) = \mathcal{M}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}A$ *for any* $\mathbf{Z}[\chi]$*-subalgebra* A *of* $\mathbf{C}$, *where* $\mathbf{p} = 4$ *or* p *according as* $p = 2$ *or not. Moreover under the pairing in Theorem 3.1, we have the following isomorphisms:*

$$\mathrm{Hom}_A(\mathbf{H}_k(\Gamma,\chi;A),A) \cong \mathcal{M}_k(\Gamma,\chi;A),\ \mathrm{Hom}_A(\mathcal{M}_k(\Gamma,\chi;A),A) \cong \mathbf{H}_k(\Gamma,\chi;A),$$
$$\mathrm{Hom}_A(\mathbf{h}_k(\Gamma,\chi;A),A) \cong \mathcal{S}_k(\Gamma,\chi;A),\ \mathrm{Hom}_A(\mathcal{S}_k(\Gamma,\chi;A),A) \cong \mathbf{h}_k(\Gamma,\chi;A).$$

Proof. By the theorem, we can find a basis $\{f_i\}_{i=1,\ldots,r}$ of $\mathcal{M}_k(\Gamma,\chi)$ in $\mathcal{M}_k(\Gamma,\chi;\mathbf{Z}[\chi])$. In fact, we take any character ψ modulo $p\mathbf{p}^r$ with $\psi(-1) = -1$. Then taking a in the theorem to be 2, we find $\{f'_i\}_{i=1,\ldots,r}$ among $G_1(\psi^{-1})E_{k-1}(\psi\chi) \mid T(n_i)$, $G_k(\chi)$ and $E_k(\chi)$ which form a basis of $\mathcal{M}_k(\Gamma,\chi;K)$ over K, where K is the field $\mathbf{Q}(\chi,\psi)$ generated by the values of χ and ψ. Then choosing a suitable element $a_i \in K$ for each i, we can easily show that the $f_i = \mathrm{Tr}(a_if'_i) = \sum_\sigma a_i^\sigma f_i'^\sigma$ give a basis desired with coefficients in $\mathbf{Z}[\chi]$, where σ runs over $\mathrm{Gal}(K/\mathbf{Q}(\chi))$. Thus the natural linear map from $\mathcal{M}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}\mathbf{C}$ into $\mathcal{M}_k(\Gamma,\chi)$ is surjective. By our construction of f_i we can find $n_1, \ldots, n_r$ so that $\det(a(n_i,f_j))_{i,j=1,\ldots,r} \neq 0$. Then for any $\phi \in \mathcal{M}_k(\Gamma,\chi;\mathbf{Q}[\chi])$, we can solve simultaneously the linear equations $\sum_j x_j a(n_i,f_j) = a(n_i,\phi)$ $(i = 1,\ldots,r)$ within

$\mathbf{Q}(\chi)$. Then we see that ϕ is a linear combination of f_i with coefficients in $\mathbf{Q}(\chi)$. Thus $\dim_{\mathbf{Q}(\chi)}\mathcal{M}_k(\Gamma,\chi;\mathbf{Q}[\chi]) \le \dim_{\mathbf{C}}(\mathcal{M}_k(\Gamma,\chi))$. This shows $\mathcal{M}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes\mathbf{C} = \mathcal{M}_k(\Gamma,\chi)$ and $m_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes\mathbf{C} = \mathcal{M}_k(\Gamma,\chi)$. In the same manner as in the proof of Theorem 3.1, we know that

$$\mathrm{Hom}_{\mathbf{Z}[\chi]}(m_k(\Gamma,\chi;\mathbf{Z}[\chi]),\mathbf{Z}[\chi]) \cong \mathbf{H}_k(\Gamma,\chi;\mathbf{Z}[\chi]),$$
$$\mathrm{Hom}_{\mathbf{Z}[\chi]}(\mathbf{H}_k(\Gamma,\chi;\mathbf{Z}[\chi]),\mathbf{Z}[\chi]) \cong m_k(\Gamma,\chi;\mathbf{Z}[\chi]).$$

Obviously by definition, $\mathbf{H}_k(\Gamma,\chi;A)$ is a surjective image of $\mathbf{H}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes A$. If the image of an element T in $\mathbf{H}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes A$ vanishes in $\mathbf{H}_k(\Gamma,\chi;A)$, extending scalar to $\mathbf{C}$, it vanishes in $\mathbf{H}_k(\Gamma,\chi;\mathbf{C})$. Since $\mathcal{M}_k(\Gamma,\chi) = \mathcal{M}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes\mathbf{C}$, we know that $T = 0$. Thus $\mathbf{H}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes A = \mathbf{H}_k(\Gamma,\chi;A)$. Then we have

$$\begin{aligned} m_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}A &\cong \mathrm{Hom}_{\mathbf{Z}[\chi]}(\mathbf{H}_k(\Gamma,\chi;\mathbf{Z}[\chi]),\mathbf{Z}[\chi])\otimes A \\ &\cong \mathrm{Hom}_A(\mathbf{H}_k(\Gamma,\chi;A),A) \cong m_k(\Gamma,\chi;A). \end{aligned}$$

This shows the assertion for A.

Now we note a byproduct of the above argument. We have an exact sequence

$$0 \to \mathcal{M}_k(\Gamma,\chi;A) \to m_k(\Gamma,\chi;A) \to N(A) \to 0$$

for a torsion A-module N. Since A is flat over $\mathbf{Z}[\chi]$, by tensoring with A, we have another exact sequence

$$0 \to \mathcal{M}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes A \to m_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes A \to N(\mathbf{Z}[\chi])\otimes A \to 0.$$

Since the middle terms of the above two sequences coincide and the last maps of these sequences also coincide under this identification, we have

$$\mathcal{M}_k(\Gamma,\chi;A) \cong \mathcal{M}_k(\Gamma,\chi;\mathbf{Z}[\chi])\otimes A.$$

By Corollary 1 and Theorem 1, we know that

$$\mathbf{h}_k(\Gamma_0(pp^r),\chi;\mathbf{C}) = \mathbf{h}_k(\Gamma_0(pp^r),\chi;\mathbf{Q}(\chi))\otimes_{\mathbf{Q}(\chi)}\mathbf{C} \quad \text{if } k > 4.$$

Then, similarly to the proof of Corollary 3.1, we know the following result when $k > 6$. The result is actually true for all $k \ge 0$ [Sh3, p.789]. We will later show this result for $k \ge 2$ as Theorem 6.3.2.

Corollary 2. *Let* f *be a common eigenform of all Hecke operators in* $\mathcal{S}_k(\Gamma_0(pp^r),\chi)$ *such that* $a(1,f) = 1$. *Then the field* $\mathbf{Q}(f)$ *generated by all the Fourier coefficients of* f *is a finite extension of* $\mathbf{Q}$. *Moreover* $a(n,f)$ *are all algebraic integers and for all* $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, f^σ *is again a common eigenform in* $\mathcal{S}_k(\Gamma_0(pp^r),\chi^\sigma)$.

To prove the theorem, we shall prepare with some lemmas.

Lemma 1. *Let* g *be an element of* $\mathcal{S}_k(\Gamma,\chi)$ *and* $\{f\}$ *be the basis consisting of common eigenforms. We assume that* $\Gamma = \Gamma_0(\mathbf{p}p^r)$ *if* χ *is primitive modulo* $\mathbf{p}p^r$ *and* $\Gamma = SL_2(\mathbf{Z})$ *if* χ *is trivial. If we write* $g = \sum_f c(f,g)f$ *with* $c(f,g) \in \mathbf{C}$, *then* $c(f,g) = (g,f)/(f,f)$, *and if* $c(f,g) \neq 0$ *for all* f, *then* $g \mid T(n_i)$ *for some* n_i *spans* $\mathcal{S}_k(\Gamma,\chi)$.

Proof. Since the proof is exactly the same for $SL_2(\mathbf{Z})$ and $\Gamma_0(p^r)$, we only treat the case of $\Gamma = \Gamma_0(\mathbf{p}p^r)$. As already seen, $\mathbf{h}_k(\Gamma,\chi;\mathbf{C})$ is semi-simple and hence is isomorphic to $\mathbf{C}^d$ for some d as an algebra. Let λ_i be the i-th projection of $\mathbf{h}_k(\Gamma,\chi;\mathbf{C})$ onto $\mathbf{C}$, which is an algebra homomorphism. Then λ_i spans $\mathrm{Hom}_{\mathbf{C}}(\mathbf{h}_k(\Gamma,\chi;\mathbf{C}),\mathbf{C}) = \mathcal{S}_k(\Gamma,\chi)$. Let f_i be the cusp form corresponding to λ_i. Then $\{f_i\}$ forms a basis of $\mathcal{S}_k(\Gamma,\chi)$. We see that $a(n,f_i) = \langle T(n),f_i\rangle = \lambda_i(T(n))$ (in particular, $a(1,f_i) = 1$) and

$$\begin{aligned} a(m,f_i \mid T(n)) &= \langle T(m),f_i \mid T(n)\rangle = a(1,f_i \mid T(m)T(n)) \\ &= \lambda_i(T(m)T(n)) = \lambda_i(T(n))a(m,f_i). \end{aligned}$$

Therefore we have $f_i \mid T(n) = \lambda_i(T(n))f_i$. If $i \neq j$, then we can find $T(n)$ such that $\lambda_i(T(n)) \neq \lambda_j(T(n))$ since the $T(n)$'s generate the Hecke algebra $\mathbf{h}_k(\Gamma,\chi;\mathbf{C})$. Thus the chosen basis coincides with $\{f_i\}$. In the proof of the semi-simplicity of the Hecke algebras, we have shown that if f is a non-trivial common eigenform of Hecke operators $T(n)$ for all n prime to p, then f is also an eigenform for $T(p)$ and $a(1,f) \neq 0$. Moreover we have shown that $T(n)^* = \chi(n)^{-1}T(n)$ for n prime to p, where $T(n)^*$ is the adjoint of $T(n)$ under the Petersson inner product. Note that $T(n)^*$ commutes with $T(p)^*$. Therefore $T(n)$ commutes with $T(p)^*$ if n is prime to p. If f is a common eigenform for all $T(n)$, $f \mid T(p)^*$ is a common eigenform for $T(n)$ for all n prime to p having the same eigenvalues as f. Therefore if $f \mid T(p)^* \neq 0$, then $a(1,f \mid T(p)^*) \neq 0$ and $h = a(1,f \mid T(p)^*)f - a(1,f)f \mid T(p)^*$ is a common eigenform of $T(n)$ for all n prime to p with $a(1,h) = 0$; hence $h = 0$. Hence f is also an eigenform of $T(p)^*$. Thus what we have shown is that if f is a common eigenform for $T(n)$ with n prime to p, then f is also a common eigenform of $T(n)$ and $T(n)^*$ for all n including p. If there are two non-trivial eigenforms f and g belonging to the same eigenvalues of $T(n)$ for all n prime to p, then again by putting $h = a(1,f)g - a(1,g)f$, we know that h is a common eigenform of $T(n)$ for all n prime to p with $a(1,h) = 0$. Thus $h = 0$ and g is a constant multiple of f. This shows that λ_i is determined by the value at $T(n)$ for n prime to p. Thus, if $i \neq j$, then we can find n prime to p such that $\lambda_i(T(n)) \neq \lambda_j(T(n))$. Since $T(n)^* = \chi(n)^{-1}T(n)$, $T = (\sqrt{\chi(n)})^{-1}T(n)$ is self-adjoint and

$$(\sqrt{\chi(n)})^{-1}\lambda_i(T(n))(f_i,f_j) = (f_i \mid T,f_j) = (f_i,f_j \mid T) = (\sqrt{\chi(n)})^{-1}\lambda_j(T(n))(f_i,f_j).$$

This shows that $(f_i,f_j) = 0$ if $i \neq j$. Therefore, writing $g = \sum_i c(f_i,g)f_i$, then $(g,f_i) = c(f_i,g)(f_i,f_i)$ and the formula $c(f_i,g) = (g,f_i)/(f_i,f_i)$ follows.

Let us now prove the last assertion of the lemma. Let M be the vector subspace of $\mathbf{h}_k(\Gamma,\chi;\mathbf{C})$ generated by $T(n)$ for all n. Then the pairing $\langle h,f\rangle = a(1,f\,|\,h)$ is still non-degenerate on M (in fact, if $\langle h,f\rangle = 0$ for all $h \in M$, $a(n,f) = \langle T(n),f\rangle = 0$ and $f = 0$). Thus

$$\dim_{\mathbf{C}}(\mathbf{h}_k(\Gamma,\chi;\mathbf{C})) \geq \dim_{\mathbf{C}}M \geq \dim_{\mathbf{C}}(\mathcal{S}_k(\Gamma,\chi)) = \dim_{\mathbf{C}}(\mathbf{h}_k(\Gamma,\chi;\mathbf{C})).$$

Therefore $\mathbf{h}_k(\Gamma,\chi;\mathbf{C}) = M$. (This fact is even true for any subring A of $\mathbf{C}$ containing $\mathbf{Z}[\chi]$: $\mathbf{h}_k(\Gamma,\chi;A) = \sum_n AT(n)$.) Let 1_i be the idempotent corresponding to the i-th factor $\mathbf{C}$ of $\mathbf{h}_k(\Gamma,\chi;\mathbf{C})$; thus $\lambda_j(1_i) = \delta_{ij}$. Then one can express $1_i = \sum_j c(n_{ij})T(n_{ij})$ with $c(n_{ij}) \in \mathbf{C}$ and $n_{ij} > 0$. Then for g as in the lemma, we have

$$g\,|\,1_i = \sum_j \lambda_j(1_i)c(f_j,g)f_j = c(f_i,g)f_i.$$

On the other hand, $g\,|\,1_i = \sum_j c(n_{ij})g\,|\,T(n_{ij})$. Thus if $c(f_i,g) \neq 0$, then f_i can be expressed as a linear combination of $g\,|\,T(n_{ij})$. By picking a basis out of $\{g\,|\,T(n_{ij})\}_{ij}$, we get a desired basis $g\,|\,T(n_i)$.

To prove Theorem 1, we compute for each common eigenform f, $c(g,f) = (g,f)/(f,f)$ for $g = G_a(\psi^{-1})E_{k-a}(\psi\chi)$. Note that if $a \geq 2$, $G_a(\psi^{-1})$ has a non-trivial constant term only at the cusp 0 and $E_{k-a}(\psi\chi)$ has a non-trivial constant term only at infinity. Thus g is a cusp form (if $a \geq 2$). We write ξ for $\psi\chi$, l for k-a and h for $G_a(\psi^{-1})$. Then by definition

$$\begin{aligned} 2^{-1}E'_l(z;\xi) &= 2^{-1}\sum{}'_{(m,n)}\xi^{-1}(n)(mp^rz+n)^{-l} \\ &= \sum_{a=1}^{\infty} \xi^{-1}(a)a^{-l}\sum_{(cp^r,d)} \xi^{-1}(d)(cp^rz+d)^{-l} = L(l,\xi^{-1})\sum_{(cp^r,d)} \xi^{-1}(d)(cp^rz+d)^{-l}, \end{aligned}$$

where (cp^r,d) runs over all pairs of relatively prime integers with $d > 0$. Since (cp^r,d) is relatively prime, we can find integers a and b such that $ad-bcp^r = 1$ and $\gamma = \begin{pmatrix} a & b \\ cp^r & d \end{pmatrix} \in \Gamma_0(p^r)$. If we pick another $\delta = \begin{pmatrix} a' & b' \\ cp^r & d \end{pmatrix}$ in $\Gamma_0(p^r)$ with the same lower row, then $\gamma\delta^{-1} = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \in \Gamma_\infty$, where

$$\Gamma_\infty = \{\gamma \in \Gamma_0(p^r) \mid \gamma(\infty) = \infty\} = \{\pm\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \mid m \in \mathbf{Z}\}.$$

Therefore, we know that

$$E_l(z;\xi) = 2L(l,\xi^{-1})\sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(p)} \xi^{-1}(\gamma)j(\gamma,z)^{-l}.$$

Thus at least formally

$$c(g,f)(f,f) = 2L(l,\xi^{-1})\int_\Phi \bar{f}h(z)\sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(p)}\xi^{-1}(\gamma)j(\gamma,z)^{-l}y^{k-2}dxdy,$$

where Φ is the fundamental domain of $\Gamma_0(p^r)$. Note that

$$\gamma^*(y^{-2}dx\wedge dy) = y^{-2}dx\wedge dy \text{ for all } \gamma\in SL_2(\mathbf{R}),\ y(\gamma(z))^k = y(z)^k|j(\gamma,z)|^{-2k},$$
$$\text{and}\quad \overline{f(\gamma(z))}h(\gamma(z)) = \overline{f(z)}h(z)\xi^{-1}(\gamma)|j(\gamma,z)|^{2k}j(\gamma,z)^{-l}.$$

Therefore, we have

$$\overline{f(z)}h(z)\xi^{-1}(\gamma)j(\gamma,z)^{-l}\,y(z)^k = \overline{f(\gamma(z))}h(\gamma(z))y(\gamma(z))^k$$

and for a non-zero constant c_0 (see §1)

$$c(g,f)(f,f) = c_0L(l,\xi^{-1})\int_\Phi\sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(p)}\overline{f(\gamma(z))}h(\gamma(z))y(\gamma(z))^k\gamma^*(y^{-2}dxdy).$$

Since $\coprod_{\gamma\in\Gamma_\infty\backslash\Gamma_0(p)}\gamma\Phi$ is a fundamental domain of Γ_∞ and the domain $\{z = x+\sqrt{-1}y \mid y>0 \text{ and } 0<x<1\}$ also gives the fundamental domain of Γ_∞, we have, for $e(z) = \exp(2\pi\sqrt{-1}z)$,

$$c(g,f)(f,f) = c_0L(l,\xi^{-1})\int_0^\infty\int_0^1 \bar{f}h(z)y^{k-2}dxdy$$
$$= c_0L(l,\xi^{-1})\int_0^\infty\sum_{m,n}a(m,f)^ca(n,h)e((m+n)\sqrt{-1}y)\int_0^1 e((n-m)x)dxy^{k-2}dy,$$

where c denotes complex conjugation. As is well known,

$$\int_0^1 e((n-m)x)dx = \begin{cases}1 & \text{if } n=m,\\ 0 & \text{otherwise.}\end{cases}$$

Therefore,

$$c(g,f)(f,f) = c_0L(l,\xi^{-1})\int_0^\infty\sum_{n=1}^\infty a(n,f)^ca(n,h)\exp(-4\pi ny)y^{k-2}dy$$
$$= c_0(4\pi)^{-s}\Gamma(k-1)L(l,\xi^{-1})\sum_{n=1}^\infty a(n,f)^ca(n,h)n^{-s}\big|_{s=k-1}.$$

By the formula before Proposition 1.1, we know that

$$(1)\qquad c_0 = N^{k-l}\frac{(k-l-1)!}{(-2\pi i)^{k-l}G(\xi^{-1})}.$$

We need to justify that we may interchange the summation and the integral in the above computation. By (3.8b), we have $|a(n,f)| \le Cn^{k/2}$ and by Proposition 1.2 and (1.4a,b), $|a(n,h)| \le C'n^{a-1+\varepsilon}$ with any $\varepsilon>0$ for constants C and C' independent of n; therefore, the computation will be justified if $k-1 > \frac{k}{2}+a+\varepsilon$, that is, $k > 2a+2+2\varepsilon$. We now define the Rankin product zeta function of f and h by

$$(2)\qquad D(s,f,h) = \sum_{n=1}^\infty a(n,f)^ca(n,h)n^{-s}.$$

Here h is a general modular form, not necessarily $G_a(\psi^{-1})$. If f and h are cusp forms, then $|a(n,f)^c a(n,h)| \le Cn^{(k+a)/2}$ and thus D(s,f,h) converges absolutely if $\mathrm{Re}(s) > 1+\frac{k+a}{2}$ because D(s,f,h) is dominated by $\zeta(s-(k+a)/2)$. If h is not cuspidal, then $|a(n,f)^c a(n,h)| \le Cn^{(k/2)+a-1}$ and D(s,f,h) converges absolutely if $\mathrm{Re}(s) > a+\frac{k}{2}$ by the same reasoning. Thus Theorem 1 follows from

Lemma 2. *For two common eigenforms* $h \in \mathcal{M}_a(\Gamma_0(pp^r),\psi^{-1})$ *and* $f \in \mathcal{S}_k(\Gamma_0(pp^r),\chi)$, $D(k-1,f,h) \ne 0$ *if* $k > 2a+2$.

Proof. We compute the Euler product of D(s,f,h). We note the recurrence relation for each prime q:

$$T(q^r)T(q) = T(q^{r+1}) + \chi(q)q^{k-1}T(q^{r-1}).$$

Therefore for any common eigenforms f and h of all Hecke operators such that

$$a(1,f) = a(1,h) = 1,$$

we already know that $f|T(n) = a(n,f)f$ and $h|T(n) = a(n,h)h$. For simplicity, we write $a(n) = a(n,f)^c$ and $b(n) = a(n,h)$. From the relation, we know that

$$a(q^r)a(q) = a(q^{r+1}) + \chi(q)^{-1}q^{k-1}a(q^{r-1}) \text{ and}$$
$$b(q^r)b(q) = b(q^{r+1}) + \psi(q)^{-1}q^{k-1}b(q^{r-1})$$

if $r \ge 1$, where ψ (resp. χ) is the character of h (resp. f). We take two roots α, β of $X^2-a(q)X+\chi^{-1}(q)q^{k-1} = 0$ and α',β' of $X^2-b(q)X+\psi(q)^{-1}q^{k-1} = 0$. We write formally $P(X) = \sum_{n=0}^{\infty} a(q^n)X^n$. Then we have

$$P(X)(\alpha+\beta) = \sum_{n=0}^{\infty} a(q^{n+1})X^n+\alpha\beta\sum_{n=1}^{\infty} a(q^{n-1})X^n = (P(X)-1)X^{-1}+\alpha\beta XP(X).$$

This shows that

$$P(X) = (1-(\alpha+\beta)X+\alpha\beta X^2)^{-1} = (1-\alpha X)^{-1}(1-\beta X)^{-1} = \frac{\sum_{n=0}^{\infty}(\alpha^{n+1}-\beta^{n+1})X^n}{\alpha-\beta}$$

and

$$a(q^n) = (\alpha-\beta)^{-1}(\alpha^{n+1}-\beta^{n+1}), \quad b(q^n) = (\alpha'-\beta')^{-1}(\alpha'^{n+1}-\beta'^{n+1}).$$

Now computing

$$Q(X) = \sum_{n=0}^{\infty} a(q^n)b(q^n)X^n = \frac{\sum_{n=0}^{\infty}(\alpha^{n+1}-\beta^{n+1})(\alpha'^{n+1}-\beta'^{n+1})X^n}{(\alpha-\beta)(\alpha'-\beta')}$$
$$= \frac{1}{(\alpha-\beta)(\alpha'-\beta')X}\left\{\frac{1}{1-\alpha\alpha'X} - \frac{1}{1-\alpha\beta'X} - \frac{1}{1-\beta\alpha'X} + \frac{1}{1-\beta\beta'X}\right\}$$

$$= \frac{1-\alpha\alpha'\beta\beta'X^2}{(1-\alpha\alpha'X)(1-\alpha\beta'X)(1-\beta\alpha'X)(1-\beta\beta'X)}$$
$$= \frac{1-(\chi\psi)^{-1}(q)q^{k+a-2}X^2}{(1-\alpha\alpha'X)(1-\alpha\beta'X)(1-\beta\alpha'X)(1-\beta\beta'X)},$$

we find that

$$L(2\text{-}k\text{-}a+2s,\chi^{-1}\psi)D(s,f,h) = \prod_q \left\{ (1-\alpha\alpha'q^{-s})(1-\alpha\beta'q^{-s})(1-\beta\alpha'q^{-s})(1-\beta\beta'q^{-s}) \right\}^{-1}.$$

This infinite product converges absolutely at $s = k\text{-}1$ if $k > 2a+2$, because, writing $A = \alpha$ or β and $B = \alpha'$ or β', $|ABq^{-s}| < q^{-1}$ if $\mathrm{Re}(s) > 1+\frac{k}{2}+a\text{-}1$ for q sufficiently large, and the Euler product of $\zeta(s)$ converges if $\mathrm{Re}(s) > 1$. Since $f^c(z) = \overline{f(-\bar{z})}$, then $f^c \in \mathcal{S}_k(\Gamma,\chi^c)$ and $(f^c,f^c) = (f,f)$. Therefore we have, for $g = h^cE_{k\text{-}a}(\psi^{-1}\chi)$,

$$\begin{aligned} c(g,f)(f,f) &= c_0(4\pi)^{1\text{-}k}\Gamma(k\text{-}1)L(2\text{-}k\text{-}a+2s,\chi^{-1}\psi)D(s,f,h)\,|_{s=k\text{-}1} \\ &= c_0(4\pi)^{1\text{-}k}\Gamma(k\text{-}1)L(k\text{-}a,\chi^{-1}\psi)D(k\text{-}1,f,h). \end{aligned}$$

The convergence of the Euler product gives us the non-vanishing of $c(g,f)$ and we now have Theorem 1.

Corollary 3. *Suppose that* f *and* h *are normalized common eigenforms of all Hecke operators in* $\mathcal{S}_k(\Gamma_0(N),\chi)$ *and* $\mathcal{M}_a(\Gamma_0(N),\psi)$, *respectively. Put*

$$T(k\text{-}1,f,h) = \frac{N^{k\text{-}l}\Gamma(k\text{-}1)\Gamma(k\text{-}l)L_N(k\text{-}a,\chi^{-1}\psi)D(k\text{-}1,f,h)}{(2\pi\sqrt{-1})^{k\text{-}l}(4\pi)^{k\text{-}1}G(\chi^{-1}\psi)}.$$

Suppose that $\chi^{-1}\psi$ *is primitive modulo* $N = p^r$. *If* $k > 2a+2$, *then* $T(k\text{-}1,f,h) \in \mathbf{Q}(f,h)$, *where* $\mathbf{Q}(f,h)$ *is the finite extension of* $\mathbf{Q}$ *generated by the Fourier coefficients of* f *and* h. *Moreover for all* $\sigma \in \mathrm{Aut}(\mathbf{C})$,

$$T(k\text{-}1,f,h)^\sigma = T(k\text{-}1,f^\sigma,h^\sigma).$$

This is a special case of a general algebraicity theorem of Shimura (see Theorem 10.2.1 and also Theorem 7.4.1). As already seen

$$c(hE'_{k\text{-}a}(\psi^{-1}\chi^{-1}),f) = c_0(4\pi)^{1\text{-}k}\Gamma(k\text{-}1)\frac{L(k\text{-}a,\chi^{-1}\psi)D(k\text{-}1,f,h)}{(f,f)} = T(k\text{-}1,f,h).$$

Then the assertion follows easily from this formula and the fact that $E_k(\xi)^\sigma = E_k(\xi^\sigma)$.

We now want to show that $f^{\sigma c} = f^{c\sigma}$ for our later use. The n-th Fourier coefficient $a(n,f)$ of f is the eigenvalue of $T(n)$. On the other hand,

$(\sqrt{\chi(n)})^{-1}T(n)$ is self-adjoint if n is prime to p. Thus $(\sqrt{\chi(n)})^{-1}a(n,f)$ is real and

$$a(n,f)^c = \chi(n)^{-1}a(n,f).$$

In particular, $a(n,f)^{c\sigma} = \chi^\sigma(n)^{-1}a(n,f^\sigma) = a(n,f^{\sigma c})$. Since the p-th Fourier coefficient of f is determined by those for n prime to p as shown in the proof of Theorem 3.2, we also have $a(p,f)^{c\sigma} = a(p,f)^{\sigma c}$. In fact $f^{c\sigma}-f^{\sigma c}$ is a common eigenform of all $T(n)$ for n prime to p and $a(1,f^{c\sigma}-f^{\sigma c}) = 0$, and hence $f^{c\sigma}-f^{\sigma c} = 0$.

The above proof in particular shows that

(3) $a(n,f)^c = \chi^{-1}(n)a(n,f)$ *for* n *prime to* p *if* f *is a normalized eigenform in* $\mathcal{S}_k(\Gamma_0(p^r),\chi)$.

§5.5. Standard L-functions of holomorphic modular forms

Let $\lambda : \mathbf{H}_k(\Gamma_0(p^r),\chi;\mathbf{C}) \to \mathbf{C}$ be a $\mathbf{C}$-algebra homomorphism. We assume that χ is a primitive character modulo $N = p^r$. We define the standard L-function of λ by

(1) $$L(s,\lambda) = \sum_{n=1}^{\infty} \lambda(T(n))n^{-s}.$$

By Theorem 3.1, we have a common eigenform of all Hecke operators $f \in \mathcal{M}_k(\Gamma_0(p^r),\chi)$ such that $a(n,f) = \lambda(T(n))$ for all n. We then know from (3.8b) and (1.4a,b) that $|\lambda(T(n))n^{-s}| \le Cn^{-\mathrm{Re}(s)+(k/2)}$ if f is a cusp form, and $|\lambda(T(n))n^{-s}| \le Cn^{-\mathrm{Re}(s)+k-1+\varepsilon}$ (for all $\varepsilon > 0$) if f is just a modular form. When f is a cusp form, i.e. λ factors through $\mathbf{h}_k(\Gamma_0(p^r),\chi)$, then we see that

(2) $L(s,\lambda)$ converges absolutely if $\mathrm{Re}(s) > 1+\frac{k}{2}$.

If f is associated with λ, i.e., $f = \sum_{n=1}^{\infty}\lambda(T(n))q^n$, then by (3.10a,b)

(3) $$(f|\tau)|T(n) = \lambda(T(n))^c(f|\tau) \text{ for all } n,$$

where c denotes complex conjugation. Supposing that χ is primitive modulo p^r, we know from Corollary 3.2 that $f|\tau$ is a constant multiple of f^c:

Proposition 1. *Let* $f = \sum_{n=1}^{\infty}\lambda(T(n))q^n$ *for an algebra homomorphism* $\lambda : \mathbf{h}_k(\Gamma_0(p^r),\chi) \to \mathbf{C}$. *Define* $\lambda^c : \mathbf{h}_k(\Gamma_0(p^r),\chi^c) \to \mathbf{C}$ *by* $\lambda^c = c\circ\lambda\circ c$. *We suppose that* χ *is primitive modulo* p^r. *Then we have*

$$(4) \qquad f\,|\,\tau = p^{r(k-2)/2}W(\lambda)\sum_{n=1}^{\infty}\lambda(T(n))^c q^n,$$

for a constant $W(\lambda)$ *with* $W(\lambda)W(\lambda^c) = \chi(-1)$ *and* $|W(\lambda)| = 1$. *Here we agree to put* $\Gamma_0(p^0) = SL_2(\mathbf{Z})$ *and* $\chi = \mathrm{id}$ *in this case.*

Proof. We only need to prove the last assertion. By Corollary 3.2, $W(\lambda) \neq 0$. Since $\tau^2 = -p^r\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, we see that $(f\,|\,\tau)(z) = p^{(k-1)r}f(-1/p^r z))(p^r z)^{-k}$ and $(f\,|\,\tau)\,|\,\tau = \chi(-1)p^{(k-2)r}f$. Thus $W(\lambda)W(\lambda^c) = \chi(-1)$. Applying $f \mapsto \overline{f(-\bar{z})}$ to the formula (4), we see that $W(\lambda^c) = \chi(-1)W(\lambda)^c$. This shows that $|W(\lambda)| = 1$.

We now show the analytic continuation of $L(s,\lambda)$ and its functional equation. First assume that $f \in \mathcal{S}_k(\Gamma_0(p^r),\chi)$ for a Dirichlet character χ modulo p^r (here χ may be imprimitive). In this case, by (3.8a), the integral $\int_0^\infty f(iy)y^{s-1}dy$ is absolutely convergent for all s and gives an entire function of s. By the same type of computation as in §2.2, we have, if $\mathrm{Re}(s) > 1+\frac{k}{2}$,

$$\int_0^\infty f(iy)y^{s-1}dy = (2\pi)^{-s}\Gamma(s)L(s,\lambda).$$

Thus $L(s,\lambda)$ has an analytic continuation to an entire function on the whole s-plane. On the other hand, if either χ is primitive modulo p^r or $r = 0$, we see that

$$p^{r(k-2)/2}W(\lambda)(2\pi)^{-s}L(s,\lambda^c) = \int_0^\infty f\,|\,\tau(iy)y^{s-1}dy$$
$$= i^{-k}p^{-r}\int_0^\infty f\left(\frac{i}{p^r y}\right)y^{s-k-1}dy \overset{(p^r y)^{-1}\mapsto y}{=} i^{-k}p^{-r}\int_0^\infty f(iy)(p^r y)^{k-s}y^{-1}dy$$
$$= i^{-k}p^{-sr+(k-1)r}\Gamma(k-s)(2\pi)^{s-k}L(k-s,\lambda).$$

This shows

Theorem 1. *Suppose that* χ *is primitive modulo* p^r. *Then, for each algebra homomorphism* $\lambda : \mathbf{h}_k(\Gamma_0(p^r),\chi) \to \mathbf{C}$, *the L-function* $L(s,\lambda)$ *is continued to an entire function on the whole s-plane. If either* $r = 0$ *or* χ *is primitive modulo* p^r, *the L-function* $L(s,\lambda)$ *satisfies the following functional equation*

$$\Gamma_{\mathbf{C}}(s)L(s,\lambda) = p^{r((k/2)-s)}i^k W(\lambda)\Gamma_{\mathbf{C}}(k-s)L(k-s,\lambda^c) \quad \textit{for} \quad \Gamma_{\mathbf{C}}(s) = (2\pi)^{-s}\Gamma(s).$$

For any primitive character ψ modulo N, we can define

$$f_\psi = G(\psi^{-1})^{-1}\sum_{r=1}^{N-1}\psi^{-1}(r)f\,|\begin{pmatrix}1 & r/N\\ 0 & 1\end{pmatrix}.$$

Then we see from a similar computation as in (4.1.6c) that

(5) $$f_\psi = \sum_{n=1}^{\infty} \psi(n)a(n,f)q^n.$$

For any algebra homomorphism $\lambda : \mathbf{h}_k(\Gamma_0(p^r),\chi) \to \mathbf{C}$ and a primitive character $\psi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$, we define

$$L(s,\lambda\otimes\psi) = \sum_{n=1}^{\infty} \psi(n)\lambda(T(n))n^{-s}.$$

Thus we have, as a corollary to the proof of Theorem 1,

Corollary 1. *For each algebra homomorphism* $\lambda : \mathbf{h}_k(\Gamma_0(p^r),\chi) \to \mathbf{C}$ *and each primitive character* $\psi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$, *the L-function* $L(s,\lambda\otimes\psi)$ *is continued to an entire function on the whole s-plane.*

Proof. Although we proved Theorem 1 assuming that χ is primitive modulo p^r, it is clear from its proof that $\int_0^\infty f(iy)y^{s-1}dy$ is an entire function in s if f is a cusp form. Thus what we need to prove is that f_ψ is a cusp form for some character ξ of $\Gamma_0(M)$. It is easy to check that

(6) if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M)$ for the least common multiple $M = [N,p^r]$ of N and p^r, then $$f\left|\begin{pmatrix} 1 & r/N \\ 0 & 1 \end{pmatrix}\gamma = f\,|\,\gamma'\begin{pmatrix} 1 & rd^2/N \\ 0 & 1 \end{pmatrix}\right.$$
for $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_0(p^r)$ with $d' \equiv d \bmod p^r$.

This shows that

$$f_\psi\,|\,\gamma = G(\psi^{-1})^{-1}\sum_{r=1}^{N-1} \psi^{-1}(r)f\left|\begin{pmatrix} 1 & r/N \\ 0 & 1 \end{pmatrix}\gamma = G(\psi^{-1})^{-1}\sum_{r=1}^{N-1} \psi^{-1}(r)f\,|\,\gamma'\begin{pmatrix} 1 & rd^2/N \\ 0 & 1 \end{pmatrix}\right.$$
$$= G(\psi^{-1})^{-1}\chi(d)\textstyle\sum_{r=1}^{N-1}\psi^{-1}(d^{-2}r)f\left|\begin{pmatrix} 1 & r/N \\ 0 & 1 \end{pmatrix}\right. = \chi\psi^2(d)f.$$

Thus we have $f_\psi \in \mathcal{S}_k(\Gamma_0(M),\chi\psi^2)$.

Define an algebra homomorphism $\lambda\otimes\psi : \mathbf{h}_k(\Gamma_0([N,p^r]),\chi) \to \mathbf{C}$ by $f_\psi\,|\,T(n) = (\lambda\otimes\psi)(T(n))f_\psi$ (i.e. $(\lambda\otimes\psi)(T(n)) = \psi(n)\lambda(T(n))$). Then if N is prime to p, we can compute $W(\lambda\otimes\chi)$ explicitly by using $W(\lambda)$ (see for details [Sh, Prop.3.36], [M, §4.3] and [H5, (5.4-5)]).

Chapter 6. Modular forms and cohomology groups

In this chapter, we prove the Eichler-Shimura isomorphism between the space of modular forms and the cohomology group on each modular curve. This fact was first proven by Shimura in 1959 in [Sh1] (see also [Sh, VIII]). We shall give two proofs in §6.2 of this isomorphism. The first one is the original proof of Shimura based on the two dimension formulas. One is the formula for the space of cusp forms and the other is for the cohomology group. The other proof makes use of harmonic analysis on the modular curve. After studying the Hecke module structure of modular cohomology groups, in §6.5, we construct the p-adic standard L-function of $GL(2)_{/\mathbf{Q}}$ following the method (the so-called "p-adic Mellin transform") of Mazur and Manin in [Mz1], [MTT] and [Mn1,2]. Throughout this chapter, we use without warning the cohomological notation and definition described in Appendix at the end of the book. If the reader is not familiar with cohomology theory, it is recommended to have a look at the appendix first.

§6.1. Cohomology of modular groups

In this section, we shall prove the dimension formula of the cohomology group of congruence subgroups of $SL_2(\mathbf{Z})$ following [Sh, VIII]. Let Γ be a congruence subgroup of $SL_2(\mathbf{Z})$ and suppose for simplicity that Γ is torsion-free. (The general case without assuming the torsion-freeness of Γ is treated in [Sh, VIII].) If $N \geq 4$, $\Gamma_1(N)$ is torsion-free. In fact, if $\pm 1 \neq \zeta \in \Gamma$ satisfies $\zeta^m = 1$ for $m > 2$, then the absolute value of the sum of two eigenvalues of ζ is less than 2. Thus $|\mathrm{Tr}(\zeta)| = 0$ or 1. On the other hand, if $\zeta \in \Gamma_1(N)$, $\mathrm{Tr}(\zeta) \equiv 2 \bmod N$. It is easy to check that it is impossible to have $|\mathrm{Tr}(\zeta)| < 2$ and $\mathrm{Tr}(\zeta) \equiv 2 \bmod N$ if $N \geq 4$.

Exercise 1. If $N \geq 4$, why is $\mathrm{Tr}(\zeta) \equiv 2 \bmod N$ impossible?

Let R be a commutative ring, and for any left $R[\Gamma]$-module M, we consider the group cohomology group $H^i(\Gamma,M)$ (see Appendix for definition). Here we start from an open Riemann surface $Y = \Gamma\backslash\mathcal{H}$. For each $s \in \mathbf{P}^1(\mathbf{Q}) = \mathbf{Q}\cup\{\infty\}$, we consider the stabilizer Γ_s of s in Γ. If s is finite, writing $s = \frac{q}{p}$ as a reduced fraction, we can find integers x and y such that $qy-px = 1$. Putting $\sigma_s = \sigma = \begin{pmatrix} q & x \\ p & y \end{pmatrix} \in SL_2(\mathbf{Z})$, we have $\sigma(\infty) = s$. This shows that $\sigma^{-1}\Gamma_s\sigma$ is contained in $\{\pm 1\}\times U(\mathbf{Z})$ for $U(A) = \left\{\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \middle| \, m \in A\right\}$. Thus defining the distance from s by $d(z) = \mathrm{Im}(\sigma^{-1}(z))^{-1}$, we see that $d(z)$ is well defined on $\Gamma_s\backslash\mathcal{H}$, and we put $U_{s,\varepsilon} = \{z \in \Gamma_s\backslash\mathcal{H} \mid d(z) < \varepsilon\}$. For sufficiently small ε, $U_{s,\varepsilon}$ is naturally embedded into $\Gamma_s\backslash\mathcal{H}$. We identify two cusps if $U_{s,\varepsilon}\cap U_{t,\varepsilon} \neq \emptyset$ for

any $\varepsilon > 0$. We see easily that two cusps are the same if and only if $\gamma(t) = s$ for some $\gamma \in \Gamma$. Thus the set S of cusps is bijective to $\Gamma\backslash PSL_2(\mathbf{Z})/U$. Since Γ is a congruence subgroup, there is a positive integer N such that

$$\Gamma \supset \Gamma(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N\right\}.$$

Then it is obvious that $\#(S) \le (SL_2(\mathbf{Z}):\Gamma(N))$, which is finite. In the above proof of the finiteness of S, the following strong approximation theorem is proved implicitly:

Lemma 1. *Let* $\{N_i\}_{i\in\mathbf{N}}$ *be a sequence of integers such that* N_i *is a divisor of* N_{i+1} *for all* i. *Then* $SL_2(\mathbf{Z})$ *is dense in* $\varprojlim_i SL_2(\mathbf{Z}/N_i\mathbf{Z})$. *In particular, writing* $\hat{\mathbf{Z}} = \prod_p \mathbf{Z}_p = \varprojlim_N SL_2(\mathbf{Z}/N!\mathbf{Z})$, $SL_2(\mathbf{Z})$ *is dense in* $SL_2(\hat{\mathbf{Z}})$.

Proof. We need to show that the natural map $SL_2(\mathbf{Z}) \to SL_2(\mathbf{Z}/N\mathbf{Z})$ is surjective for any positive integer N. Let

$$V = \{v \in (\mathbf{Z}/N\mathbf{Z})^2 \mid \text{the order of } v \text{ is equal to } N\},$$

where the order means the order of the subgroup generated by v in the additive group $(\mathbf{Z}/N\mathbf{Z})^2$. Then the vector v is represented by $\begin{pmatrix} p \\ q \end{pmatrix}$ for relatively prime p and q. Thus we can find x and y in $\mathbf{Z}$ so that $py\text{-}qx = 1$ and for $\alpha = \begin{pmatrix} q & x \\ p & y \end{pmatrix} \in SL_2(\mathbf{Z})$, $\alpha v_0 \equiv v \bmod N$, where $v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Thus for any $\alpha_0 \in SL_2(\mathbf{Z}/N\mathbf{Z})$, we can find $\alpha \in SL_2(\mathbf{Z})$ so that $\alpha v_0 \equiv \alpha_0 v_0 \bmod N$. That is, $\alpha U(\mathbf{Z}/N\mathbf{Z}) = \alpha_0 U(\mathbf{Z}/N\mathbf{Z})$. The natural map $U(\mathbf{Z}) \to U(\mathbf{Z}/N\mathbf{Z})$ is obviously surjective, and hence by modifying α from the left by an element of $U(\mathbf{Z})$, we can find $\alpha' \in SL_2(\mathbf{Z})$ such that $\alpha' \equiv \alpha_0 \bmod N$. This shows the surjectivity.

Now we show that $Y\text{-}\bigcup_{s\in S} U_{s,\varepsilon} = Y_0$ is compact if $\{U_{s,\varepsilon}\}_{s\in S}$ do not overlap. We may assume that $\Gamma = SL_2(\mathbf{Z})$ because the above space is a finite covering of the space Y_0 for $SL_2(\mathbf{Z})$. Since $\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbf{Z})$, we can take its fundamental domain in the strip B in $\mathcal{H}$ with $|\mathrm{Re}(z)| \le \frac{1}{2}$. Since $y(\delta(z)) = y/(x^2+y^2)$ for $z = x+iy$ and $\delta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbf{Z})$, $x^2+y^2 > 1 \Leftrightarrow x(\delta(z))^2+y(\delta(z))^2 < 1$. Starting from a given $z = z_0 \in B$ with $x^2+y^2 < 1$, we apply δ to z and bring $\delta(z)$ back in B by tanslation by a power of α. We write this element in B as z_1. We can now define a sequence $z_0, z_1, \ldots, z_n, \ldots$, by repeating this process of first applying δ and then translating back into B by a power of α, that is, $z_n = \alpha^m(\delta(z_{n-1}))$ for a suitable integer m so that $z_n \in B$. As soon as we get $|z_n|^2 = \mathrm{Re}(z_n)^2+\mathrm{Im}(z_n)^2 > 1$, we stop the

process. If the sequence is of infinite length, there is a limit point because the unit disk centered at the origin is compact. Since $\mathrm{Im}(\delta(z)) = y/(x^2+y^2) > \mathrm{Im}(z)$, and the ratio $\mathrm{Im}(\delta(z))/\mathrm{Im}(z)$ is given by $1/(x^2+y^2)$. Thus the limit point has to be on the intersection of B and the boundary of the unit disk. This implies that there exist a positive number h such that a fundamental domain of $SL_2(\mathbf{Z})$ can be taken in $\{z \in B \mid \mathrm{Im}(z) \geq h\}$. In fact, a standard fundamental domain is given as the intersection of B and the domain outside the open unit disk centered at the origin; see [M, 4.1.2]. Thus $y(z) = \mathrm{Im}(z)$ is bounded below independent of z in this fundamental domain, and hence $y(z)$ is bounded below and above in the inverse image Φ_0 of Y_0 in this fundamental domain. That is, Φ_0 is relatively compact. This implies that Y_0 is compact.

To compactify $Y = \Gamma\backslash\mathcal{H}$, we need only compactify $U_{s,\varepsilon}$. Since $U_{s,\varepsilon}$ is isomorphic to $U_{\infty,\varepsilon}$, we compactify $U_{\infty,\varepsilon}$. Since Γ_∞ is a subgroup of U, there exists $N \in \mathbf{Z}$ such that $z \mapsto q = \mathbf{e}(\frac{z}{N})$ gives an isomorphism of $U_{\infty,\varepsilon}$ into $\mathbf{G}_m(\mathbf{C}) = \mathbf{C}^\times$ and $y(z) \to \infty \Leftrightarrow q \to 0$ on $U_{\infty,\varepsilon}$. We then add the cusp ∞ to $U_{\infty,\varepsilon}$ so that $\mathbf{e} : U_{\infty,\varepsilon} \cup \{\infty\} \to \mathbf{C}$ gives an isomorphism onto a neighborhood of 0 in $\mathbf{C}$. We write this compactification as $\overline{U}_{\infty,\varepsilon}$ and the corresponding compactification of $U_{s,\varepsilon}$ as $\overline{U}_{s,\varepsilon}$. Then $X = Y \cup S$ is a compact Riemann surface having $\overline{U}_{s,\varepsilon}$ as a neighborhood of $s \in S$. Thus we get X and $Y = X\text{-}S$ as in Appendix. We make the triangulation of $Y_0 = Y - \bigcup_{s\in S} U_{s,\varepsilon}$ for small ε and get a complex $\mathcal{K}$ satisfying the conditions (T1–3) in Appendix. We may assume that the fundamental domain Φ_0 of Y_0 in the inverse image of Y_0 in $\mathcal{H}$ consists of simplices of $\mathcal{K}$ (we may need to take out some simplices from $\mathcal{K}$ which overlap in Y_0). Let S_i be the set of all i-simplices of $\mathcal{K}$. We use the notation defined in Appendix for X and S, especially, H^q_P denotes the various parabolic cohomology group with respect to S (see Proposition A.1).

Proposition 1. *For any Γ-module* M, *let* $DM = \sum_{\gamma\in\Gamma} (\gamma-1)M$. *Then we have*
$$H^2_P(\Gamma,M) \cong M/DM \quad \textit{and} \quad H^2(\Gamma,M) = 0.$$

Proof. We choose $\mathcal{K}$ in a manner suitable to our proof. We triangulate X so that by cutting along the curves representing a basis of the homology group of X, we get a polygon of $4g$ sides, where g is the genus of X. We may assume that all the holes of Y_0 are inside this polygon. Fixing one vertex q_0 of this polygon and cutting the polygon from q_0 to each cusp of X, we have another simply connected polygon Φ_0 with $4g+c$ sides, where $c = \#(S)$ is the number of the cusps of X. We may identify this Φ_0 with a fundamental domain Φ of Γ. Thus Γ is generated by $2g+c$ elements $\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g$ and $\pi_1, \ldots, \pi_c$ with the sole relation

$$(\prod_{s\in S}\pi_s)\alpha_1\beta_1\alpha_1^{-1}\beta_1^{-1}\cdot\cdots\cdot\alpha_g\beta_g\alpha_g^{-1}\beta_g^{-1} = 1.$$

Here we have identified S naturally with $\{1,2,\ldots,c\}$. We use the same symbol Φ_0 for the sum of elements in the set S_2 of 2-simplices in Φ_0 which represents the domain Φ_0. Then, using the notation introduced in Appendix

$$\partial\Phi_0 = \sum_{s\in S} t_s + \sum_{j=1}^{g} \{(\alpha_j-1)s_j + (\beta_j-1)s'_j\}.$$

Here s_j (resp. s'_j, t_s) denotes the face of Φ_0 corresponding to α_j (resp. β_j, π_s). We extend $\mathcal{K}$ to a triangulation K of $\mathcal{H}_0 = \pi^{-1}(Y_0)$ for the projection $\pi : \mathcal{H} \to Y$ (as described in Appendix). Thus we have the chain complex: (A_i,∂) associated to K. Let u be a cocycle having values in M, i.e., $u \in A_2(M) = \mathrm{Hom}_{R[\Gamma]}(A_2,M)$ with $f\circ\partial = 0$. Since A_2 is generated over $R[\Gamma]$ by S_2, u is determined by the values of the simplices of S_2. Note that $\alpha\beta-1 = (\alpha-1)(\beta-1)+(\alpha-1)+(\beta-1)$. Since Γ is generated by α_j, β_j and π_c,

$$DM = \sum_{s\in S} (\pi_s-1)M + \sum_{j=1}^{g} \{(\alpha_j-1)M+(\beta_j-1)M\}.$$

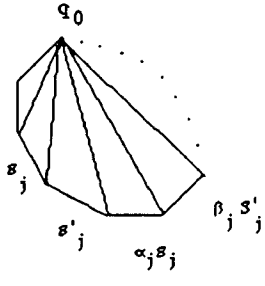
If $u = \partial w$ with $\partial w \in B_P^2(K,M)$ (see Proposition A.1 for B_P^2), then

$$u(\Phi_0) = \sum_{s\in S} w(t_s) + \sum_{j=1}^{g} \{(\alpha_j-1)w(s_j) + (\beta_j-1)w(s'_j)\} \in DM,$$

because $w(t_c) \in (\pi_c-1)M$ by the definition of $B_P^2(K,M)$. Thus $u \mapsto u(\Phi_0)$ gives a morphism of $H_P^2(K,M)$ into M/DM. This map is surjective because one can assign an arbitrary value to $u(\Phi_0)$ because there is no restriction to be a 2-cocycle. Conversely, if $u(\Phi_0) \in DM$, we can write

$$u(\Phi_0) = \sum_{s\in S} (\pi_s-1)y_s + \sum_{j=1}^{g} \{(\alpha_j-1)x_j+(\beta_j-1)x'_j\}.$$

Since Φ_0 is a polygon, we may assume that the triangulation is given by the triangles which is spanned by two vectors emanating from the vertex q_0 on the polygon and ending at the two vertices of the edges t_c, s_j, $\alpha_j(s_j)$, s'_j and $\beta_j(s'_j)$:



We define a chain $w \in A_1(M) = \mathrm{Hom}_{R[\Gamma]}(A_1,M)$ so that $w(t_s) = (\pi_s-1)y_s$, $w(s_i) = x_i$, $w(s'_i) = x'_i$ and $u = w\circ\partial$. In fact, it is sufficient to define w for the 1-simplices inside Φ_0. To do this, let us take a 1-simplex t connecting two vertices of Φ_0. Thus t divides Φ_0 into the union of two polygons a and b. Then we determine $w(t)$ so that $w(\partial a) = u(a)$ and $w(\partial b) = u(b)$. This is possible, because all the values of w at the edges of a or b except t are already given and the value of t is given by the formula $w(\partial a) = u(a)$: $w(t) = u(a) - \sum_{s\in A} w(s)$, where A is the set of edges of a different from t. Similarly if we denote by B the set of edges of b different from t, we have $-w(t) = u(b) - \sum_{s'\in B} w(s')$, because the orientation of t is reversed in b. Since

$$u(a)+u(b) = \sum_{s\in A} w(s) + \sum_{s'\in B} w(s'),$$

$w(t)$ is well defined. Thus we have a parabolic chain w on Φ_0 such that $w\circ\partial = u$. Then we extend w to A_1 by the $R[\Gamma]$-linearity to have $w\circ\partial = u$ on A_1. Thus the map $H^2_P(K,M) \to M/DM$ given by the evaluation at Φ_0 is injective. This finishes the proof of the first assertion. As for the second assertion, we consider the boundary exact sequence (Proposition A.2)

$$\begin{array}{ccccccc} \oplus_{s\in S}H^1(\Gamma_{\pi_s},M) & \to & H^2_P(\Gamma,M) & \to & H^2(\Gamma,M) & \to & 0 \quad \text{(exact)} \\ \wr\wr & & \wr\wr & & & & \\ \oplus_{s\in S}M/(\pi_s-1)M & \longrightarrow & M/DM. & & & & \end{array}$$

The above diagram is commutative by definition, and the second horizontal arrow is the natural projection $\oplus_{s\in S}m_s \bmod (\pi_s-1)M \mapsto \sum_s m_s \bmod DM$, which is obviously surjective. Then the exactness of the first row shows the vanishing of $H^2(\Gamma,M)$.

By the above proposition, we know that $H^2_c(Y,A) \cong A$ via the evaluation of 2-cocycles at Φ_0. As is well known, the Poincaré duality between $H^2_c(Y,A)$ and $H_2(Y,\partial Y;A)$ for $A = \mathbf{R}$ or $\mathbf{C}$ is given by the integration over 2-cycles of closed differential 2-forms, if one computes the cohomology groups using de Rham resolution. Thus we have

Corollary 1. *We have* $H^2_c(Y,A) \cong A$ *for all* A, *and if* $A = \mathbf{R}$ *or* $\mathbf{C}$, *this isomorphism is given by:* $H^2_c(Y,A) \ni [\omega] \mapsto \int_Y \omega \in A$, *where* ω *is a closed 2-form representing the de Rham cohomology class* $[\omega]$.

Proposition 2 (dimension formula). *Suppose that* R *is a field and* M *is of finite dimension over* R. *Let* g *be the genus of* X. *Then we have*

$$\dim(H^1_P(\Gamma,M)) = (2g-2)\dim(M)+\dim(H^0(\Gamma,M))+\dim(H^2_P(\Gamma,M))+\sum_{s\in S}\dim((\pi_s-1)M)).$$

Proof. Let Φ_0 be the fundamental domain of Y_0 as in the proof of Proposition 1. Then S_2, $S_1-\{t_s \mid s \in S\}$ and S_0 give a triangulation of Y_0. Thus by Euler's formula, we have $\#(S_2)-\#(S_1-\{t_s \mid s \in S\})+\#(S_0) = 2-2g$, where $\#(X)$ denotes the number of elements in a finite set X. On the other hand, $\#(S_i) = \mathrm{rank}_{R[\Gamma]}(A_i)$, and thus

$$\dim_R(A_i(M)) = \dim_R(\mathrm{Hom}_{R[\Gamma]}(A_i,M)) = \#(S_i)\dim_R(M).$$

Note that if we put $A^1_P(M) = \{u \in A_i(M) \mid u(t_s) \in (\pi_s-1)M\}$, then

$$\dim_R(A^1_P(M)) = \#(S_1)\dim_R(M) - \sum_{s\in S}(\dim_R(M)-\dim_R((\pi_s-1)M))$$

because of the exact sequence

$$0 \to A^1_P(M) \to A_1(M) \to \oplus_{s\in S} M/(\pi_s-1)M \to 0.$$

By definition, we have

$$H^1_P(K,M) = Z^1_P(K,M)/B^1(K,M), \quad H^2_P(K,M) = A_2(M)/B^2_P(K,M).$$

Thus, writing d(i) (resp. d, d') for the dimension of the i-th parabolic cohomology group (resp. dim(M), $\Sigma_{s\in S}\dim_R((\pi_c-1)M)$), we see that

$$d(0) = \dim(\mathrm{Ker}(\partial : A_0(M) \to A^1_P(M))) = \#(S_0)d-\dim(B^1(K,M)),$$
$$d(1) = \dim(Z^1_P(K,M))-\dim(B^1(K,M)),$$
$$d(2) = \dim(A_2(M))-\dim(B^2_P(K,M)) = \#(S_2)d-(\#(S_1)d+d'-\#(S)d-\dim(Z^1_P(K,M))).$$

Thus we have

$$d(0)-d(1)+d(2) = \#(S_0)d-(\#(S_1)d+d'-\#(S)d)+\#(S_2)d = (2-2g)d+d'.$$

That is, $d(1) = (2g-2)d+d(0)+d(2)-d'$, which is the desired formula.

We compute more explicitly the dimension of cohomology groups for some special Γ-modules. For a commutative ring R with identity, we consider the space L(n;R) of homogeneous polynomials of degree n with two indeterminates X and Y. By definition, $L(n;R) = L(n;\mathbf{Z})\otimes_{\mathbf{Z}}R$. We define the action of the semi-group $M_2(R)$ on L(n;R) by

$$\gamma P(X,Y) = P({}^t(\gamma^\iota\begin{pmatrix}X\\Y\end{pmatrix}))$$

where $\gamma^\iota = \mathrm{Tr}(\gamma)-\gamma = \det(\gamma)\gamma^{-1}$. Note that $\iota : M_2(R) \to M_2(R)$ is an involution, i.e., $(\alpha\beta)^\iota = \beta^\iota\alpha^\iota$ for all $\alpha, \beta \in M_2(R)$. Over $\mathbf{Q}$, this representation of $M_2(\mathbf{Q})$ on $L(n;\mathbf{Q})$ is equivalent to the symmetric n-th tensor representation of the natural identification of $M_2(\mathbf{Q})$ with itself. To make the dimension formula in Proposition 2 computable, we need to compute $\dim_R(M)$, $\dim_R(H^0(\Gamma,M))$, $\dim_R(H^2_P(\Gamma,M))$, $\dim_R((\pi_s-1)M)$ for $M = L(n;R)$. One can easily compute these dimensions when R is a field K of characteristic 0. We know from the definition that $\dim_R(M) = n+1$ (i.e. a standard basis is given by $X^n, X^{n-1}Y, \ldots, Y^n$). We claim that

$$(1) \qquad \dim_R(H^0(\Gamma,M)) = \dim_R(H^2_P(\Gamma,M)) = \begin{cases}1 & \text{if } n = 0,\\ 0 & \text{if } n > 0,\end{cases}$$

which follows from

Lemma 2 (irreducibility). *The Γ-module* L(n;K) *is absolutely irreducible if* K *is a field of characteristic* 0 *and* Γ *is a subgroup of finite index of* $SL_2(\mathbf{Z})$.

Proof. By the density of $SL_2(\mathbf{Z})$ in $SL_2(\mathbf{Z}_p)$, we may assume that $K = \overline{\mathbf{Q}}_p$, the algebraic closure of $\mathbf{Q}_p$. In fact, $V = L(n;\overline{\mathbf{Q}}_p) = L(n;\overline{\mathbf{Q}})\otimes\overline{\mathbf{Q}}_p$ is irreducible if and only if $L(n;\overline{\mathbf{Q}})$ is irreducible. Suppose that we have a $SL_2(\mathbf{Z}_p)$-stable vector subspace $W \neq \{0\}$ in V. We pick an element P(X,Y) in W whose degree j with respect to Y is maximal. Since $u(X^{n-j}Y^j)$

$= (X+Y)^{n-j}Y^j$ for $u = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, j has to be equal to n. Since $\alpha_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ acts on X^iY^{n-i} by the scalar a^{n-2i}, writing $P(X,Y) = \sum_i c_i X^i Y^{n-i}$ with $c_0 \neq 0$, we see that $\alpha_a P = \sum_i c_i a^{n-2i} X^i Y^{n-i} \in W$. Choosing distinct a_i for $i = 0, \ldots, n$, we can write Y^n as a linear combination of $\alpha_{a_i}P$; that is, $Y^n \in W$. Note that ${}^t u Y^n = (X+Y)^n \in W$ for the transpose ${}^t u$ of u. Since $(X+Y)^n$ involves X^iY^{n-i} non-trivially for all i, X^iY^{n-i} is a linear combination of $\{\alpha_{a_i}(X+Y)^n\}_i \subset W$. This shows that $W \supset V$, which finishes the proof.

To compute $\dim_K((\pi_s-1)M)$ when $n > 0$, we insert a definition. A cusp s is called a *regular* cusp if $\sigma_s^{-1}\Gamma_s\sigma_s$ is contained in $U(\mathbf{Z})$. A cusp which is not regular is called an *irregular* cusp. Then, we have, for some $0 \neq h \in \mathbf{Z}$

$$\sigma_s^{-1}\pi_s\sigma_s = \begin{cases} u^h & \text{if } s \text{ is regular,} \\ -u^h & \text{if } s \text{ is irregular.} \end{cases}$$

We see that $M/(\pi_s-1)M \cong M/(\pm u^h-1)M$ via $P \mapsto \sigma_s^{-1}P$. If either s is regular or n is even and positive, we see easily that $M/(u^h-1)M \cong K$ by $P \mapsto P(1,0)$, because -1 acts trivially on M. Then

(2a) If either $n > 0$ is even or s is regular, $\dim_K((\pi_s-1)L(n;K)) = n$.

Now we treat the remaining case where n is odd and s is irregular. In this case, $\sigma_s^{-1}\pi_s\sigma_s-1$ is invertible on $L(n;R)$ unless R is of characteristic 2. Thus

(2b) If n is odd and s is irregular, $\dim_K((\pi_s-1)M) = n+1$.

Summing up the above formulas, we have

Corollary 2. *If Γ is torsion-free and K is a field of characteristic 0, then*

$$(3) \qquad \dim_K(H^1_P(\Gamma,L_n(K))) = \begin{cases} (2g-2)(n+1)+n\#(S)+\delta_n\#(S_i), & \text{if } n > 0, \\ 2g, & \text{if } n = 0, \end{cases}$$

where S_i is the subset of S consisting of irregular cusps and δ_n is 0 or 1 according as n is even or odd.

Remark 1. If the reader is familiar with the dimension formula of the space of cusp forms $\mathcal{S}_k(\Gamma)$, he will notice the curious identity

$$(4) \qquad \dim_R(\mathcal{S}_k(\Gamma)) = \dim_K H^1_P(\Gamma,L(n;K)).$$

Since the dimension formula of $\mathcal{S}_{n+2}(\Gamma)$ is proven in various places (for example [Sh, Theorems 2.24 and 2.25] and [M, §2.5]) and since its direct proof without using cohomology groups requires either the Riemann-Roch theorem of curves or

the Eichler-Selberg trace formula, we shall not give the direct proof here. In the following section, we prove the Eichler-Shimura isomorphism $\mathcal{S}_k(\Gamma) \cong H^1_P(\Gamma, L(n;\mathbf{R}))$ which gives an indirect proof of this fact. In fact, we will give two proofs of this fact, and the first one actually uses the dimension formula (4).

§6.2. Eichler-Shimura isomorphisms

Now we establish a canonical $\mathbf{R}$-linear isomorphism between $\mathcal{S}_{n+2}(\Gamma)$ and the cohomology group $H^1_P(\Gamma, L(n;\mathbf{R}))$. We give two proofs. First we repeat the proof given in [Sh, VIII] which is based on the dimension formulas for $\mathcal{S}_{k+2}(\Gamma)$ and $H^1_P(\Gamma, L(n;\mathbf{R}))$, and the second one is based on the Hodge theory of manifolds with boundary.

For each point $z \in \mathcal{H}$, we consider the $L(n;\mathbf{C})$-valued differential form $\delta_n(z) = (X - zY)^n dz$. Let $\varepsilon = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{R})$, we can easily check (noting ${}^t\alpha\varepsilon\alpha = \det(\alpha)\varepsilon$ for $\alpha \in GL_2(\mathbf{C})$)

$$\gamma^*\delta_n(z) = \left((X \quad Y)\varepsilon \begin{pmatrix} \gamma(z) \\ 1 \end{pmatrix} \right)^n (cz+d)^{-2} dz$$

$$= \left((X \quad Y)^t\gamma^t\varepsilon \begin{pmatrix} z \\ 1 \end{pmatrix} \right)^n (cz+d)^{n-2} dz = (cz+d)^{-n-2}(\gamma\delta_n(z)).$$

Thus, putting $\omega(f) = 2\pi\sqrt{-1}\, f(z)\delta_n(z)$ for $f \in \mathcal{S}_{n+2}(\Gamma)$, we have $\gamma^*\omega(f) = \gamma\omega(f)$; thus $\omega(f)$ is a section of the sheaf of differential forms having values in the locally constant sheaf $\mathcal{L}(n;\mathbf{C})$ associated to the Γ-module $L(n;\mathbf{C})$. Referring the details of $\mathcal{L}(n;\mathbf{C})$ to Appendix, let us briefly state the definition of $\mathcal{L}(n;\mathbf{C}) = \underline{L(n;\mathbf{C})}$. For any Γ-module M, we can define $T = \Gamma\backslash\mathcal{H}\times M$ letting Γ act on $\mathcal{H}\times M$ by $\gamma(z,m) = (\gamma(z), \gamma m)$. Then $\underline{M}$ is the sheaf of locally constant sections of the projection $\pi : T \to Y = \Gamma\backslash\mathcal{H}$. Here we take $L(n;R)$ as M. We fix one point z in $\mathcal{H}^* = \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ (which is naturally embedded in $\mathbf{P}^1(\mathbf{C})$) and consider the integral, for each $\gamma \in \Gamma$,

$$\varphi_z(f)(\gamma) = \int_z^{\gamma(z)} \mathrm{Re}(\omega(f)) \in L(n;\mathbf{R}).$$

Since $\omega(f)$ is holomorphic, the integral is independent of the choice of the path between z and $\gamma(z)$. When $z \in \mathbf{P}^1(\mathbf{Q})$ (i.e. a cusp), we suppose that the projected image of the path in X is a well defined path near the cusp $z \in S$. Then the integral is convergent even if z is a cusp, because the cusp form is decreasing exponentially towards the cusp. For another point $z' \in \mathcal{H}^*$, we have

$$\varphi_z(f)(\gamma) - \varphi_{z'}(f)(\gamma) = \int_z^{z'} \mathrm{Re}(\omega(f)) - \int_{\gamma(z)}^{\gamma(z')} \mathrm{Re}(\omega(f)) = (1-\gamma)\int_z^{z'} \mathrm{Re}(\omega(f))$$

and for $\gamma,\delta \in \Gamma$

$$\varphi_z(f)(\gamma\delta) = \int_z^{\gamma\delta(z)} \mathrm{Re}(\omega(f)) = \int_{\gamma(z)}^{\gamma\delta(z)} \mathrm{Re}(\omega(f)) + \varphi_z(f)(\gamma) = \gamma\varphi_z(f)(\delta) + \varphi_z(f)(\gamma).$$

Thus $\varphi_z(f)$ is a 1-cocycle with values in $L(n;\mathbf{R})$ whose cohomology class is independent of the choice of the base point z. If $\pi(s) = s$ for $s \in \mathbf{P}^1(\mathbf{Q})$ with $\pi \in \Gamma$, then $\varphi_s(f)(\pi) = 0$. This shows that

$$\varphi_z(f)(\pi) = (1-\pi)\int_z^s \mathrm{Re}(\omega(f)) \in (\pi-1)L(n,\mathbf{R}) \text{ for all } \pi \in P.$$

Thus $\varphi_z(f)$ is a parabolic 1-cocycle and we obtain an $\mathbf{R}$-linear map $\varphi : \mathcal{S}_{n+2}(\Gamma) \to H^1_P(\Gamma,L(n;\mathbf{R}))$.

Theorem 1 (Eichler-Shimura). *Suppose that Γ is torsion-free. Then the map φ is a surjective isomorphism.*

Before going into the proof of this fact, we note an application. First of all, using the notation of Proposition A.1 applied to the curve $Y = \Gamma\backslash\mathcal{H}$ and its compactification X, for each commutative algebra R and for each $R[\Gamma]$-module M of finite type over R, we see that $A_i(M) = \mathrm{Hom}_{R[\Gamma]}(A_i,M)$ is of finite type over R because A_i is free of finite rank over $R[\Gamma]$. Therefore $H^i_*(\Gamma,M)$ is of finite type over R. Here "$*$" means either the usual cohomology, the compactly supported one or the parabolic one. Note that we have exact sequences

$$0 \to Z^1(K,M) \to \mathrm{Hom}_{R[\Gamma]}(A_1,M) \to \mathrm{Hom}_{R[\Gamma]}(A_2,M),$$
$$\mathrm{Hom}_{R[\Gamma]}(A_0,M) \to B^1(K,M) \to 0, \text{ and } 0 \to B^1(K,M) \to \mathrm{Hom}_{R[\Gamma]}(A_1,M).$$

If A is an R-flat algebra (or module), tensoring by A the above sequences over R, we have

$$Z^1(K,M)\otimes_R A = Z^1(K,M\otimes_R A), \quad B^1(K,M)\otimes_R A = B^1(K,M\otimes_R A)$$

and hence

(1a) $$H^1(\Gamma,M\otimes_R A) = H^1(\Gamma,M)\otimes_R A \text{ if } A \text{ is R-flat.}$$

Here the sentence "A is R-flat" is a terminology in commutative algebra meaning that $M\otimes_R A \to M'\otimes_R A \to M''\otimes_R A$ is exact whenever $M \to M' \to M''$ is exact as a sequence of R-modules ([Bour1, I]). By the exactness of

$$0 \to H^1_P(\Gamma,M) \to H^1(\Gamma,M) \to \oplus_{s\in S} H^1(\Gamma_s,M) \quad (S = X-Y),$$

we see that

(1b) $$H^1_P(\Gamma,M)\otimes_R A = H^1_P(\Gamma,M\otimes_R A) \textit{ if } A \textit{ is R-flat.}$$

We record here a corollary of the theorem which is an easy consequence of (1a,b).

Corollary 1. *Let* L_P *(resp.* L*) be the quotient of* $H^1_P(\Gamma,\mathcal{L}(n;\mathbf{Z}))$ *(resp.* $H^1(\Gamma,\mathcal{L}(n;\mathbf{Z}))$*) by the maximal torsion subgroup of* $H^1_P(\Gamma,\mathcal{L}(n;\mathbf{Z}))$ *(resp.* $H^1(\Gamma,\mathcal{L}(n;\mathbf{Z}))$*). Then the maximal torsion subgroup of* $H^1_P(\Gamma,\mathcal{L}(n;\mathbf{Z}))$ *(resp.* $H^1(\Gamma,\mathcal{L}(n;\mathbf{Z}))$*) is finite, and* L_P *(resp.* L*) is isomorphic to the image of* $H^1_P(\Gamma,\mathcal{L}(n;\mathbf{Z}))$ *(resp.* $H^1(\Gamma,\mathcal{L}(n;\mathbf{Z}))$*) in* $H^1_P(\Gamma,\mathcal{L}(n;\mathbf{R}))$ *(resp.* $H^1(\Gamma,\mathcal{L}(n;\mathbf{R}))$*). Moreover* $L_P\otimes_{\mathbf{Z}}\mathbf{R} = H^1_P(\Gamma,\mathcal{L}(n;\mathbf{R}))$ *and* $L\otimes_{\mathbf{Z}}\mathbf{R} = H^1(\Gamma,\mathcal{L}(n;\mathbf{R}))$*. Thus we can identify* L_P *with a* $\mathbf{Z}$*-lattice of the* $\mathbf{R}$*-vector -space* $\mathcal{S}_k(\Gamma)$ *for* $k = n+2$ *via* φ.

The injectivity of φ. Here we reproduce the proof given in [Sh, VIII]. We define a pairing on $L(n;\mathbf{Z})$. Consider the symmetric or skew symmetric matrix

$$\Theta = (\delta_{n-i,j}(-1)^i\binom{n}{j})_{0\le i,j\le n}.$$

Then we see easily that

$$^t\begin{pmatrix}u\\v\end{pmatrix}^n\Theta\begin{pmatrix}x\\y\end{pmatrix}^n = \det\begin{pmatrix}u & x\\ v & y\end{pmatrix}^n,$$

where $\begin{pmatrix}x\\y\end{pmatrix}^n = {}^t(x^n, x^{n-1}y, \ldots, y^n)$. Regarding each entry $u^{n-i}v^i$ $(x^{n-i}y^i)$ of $\begin{pmatrix}u\\v\end{pmatrix}^n$ (resp. $\begin{pmatrix}x\\y\end{pmatrix}^n$) as a monomial of degree n of indeterminate u and v (resp. x and y) and letting $\gamma\in GL_2(\mathbf{C})$ act on them as an element of $L(n;\mathbf{C})$, we see that

$$(*)\qquad \gamma(u^n,u^{n-1}v,\ldots,v^n)\Theta^t\{\gamma(x^n,x^{n-1}y,\ldots,y^n)\} = \det(\gamma)^n\,{}^t\begin{pmatrix}u\\v\end{pmatrix}^n\Theta\begin{pmatrix}x\\y\end{pmatrix}^n.$$

We regard $L(1;A)$ as the space of A-linear forms on the column vector space A^2, i.e. the A-dual of A^2. Now we have the pairing $A^2\times A^2$ given by $[\begin{pmatrix}x\\y\end{pmatrix},\begin{pmatrix}u\\v\end{pmatrix}] = \det\begin{pmatrix}x & u\\ y & v\end{pmatrix}$. We identify A^{n+1} with the symmetric n-fold tensor product $(A^2)^{\otimes n}$ and consider $L(n;A) = L(1;A)^{\otimes n}$ to be the dual of $(A^2)^{\otimes n}$. Identifying $u^{n-i}v^i$ with $e_1^{\otimes(n-i)}\otimes e_2^{\otimes i}$ for the standard basis $e_1 = {}^t(1,0)$ and $e_2 = {}^t(0,1)$, we have a pairing on $(A^2)^{\otimes n}$ whose matrix is given by Θ. Since $L(n;A)$ is the dual of $(A^2)^{\otimes n}$ whose basis dual to $\{X^{n-i}Y^i\}_i$ is given by $\{e_1^{\otimes(n-i)}\otimes e_2^{\otimes i}\}$, we can define a pairing $\langle\,,\rangle : L(n;A)\times L(n;A)\to A$ by

$$(2a)\qquad \langle\sum_{i=0}^n a_iX^{n-i}Y^i,\sum_{j=0}^n b_jX^{n-j}Y^j\rangle = \sum_{k=0}^n (-1)^{n-k}\binom{n}{k}^{-1}a_{n-k}b_k,$$

as long as $\binom{n}{k}^{-1}\in A$. In particular,

$$(2b)\qquad \langle(X-zY)^n,(X-\bar{z}Y)^n\rangle = \sum_{k=0}^n (-1)^{n-k}\binom{n}{k}z^{n-k}\bar{z}^k = (\bar{z}-z)^n.$$

We see from $(*)$ that for any $\gamma\in GL_2(A)$

$$[\gamma x,y] = [x,\gamma^{\iota}y] \quad \text{for} \quad x, y \in (A^2)^{\otimes n}$$

and hence

(2c) $$\langle \gamma P,Q\rangle = \langle P,\gamma^{\iota}Q\rangle \quad \text{for} \quad P, Q \in L(n;A).$$

This induces a pairing via the cup product (see [Bd,II.7])

(3a) $$\langle\ ,\ \rangle : H^1_c(Y,\mathcal{L}(m;A))\otimes H^1(Y,\mathcal{L}(m;A)) \to H^2_c(Y,A) \cong A.$$

The last isomorphism is the one in Corollary 1.1. The differential form realizing the class $\langle \mathrm{Re}(\omega(f)),\mathrm{Re}(\omega(g))\rangle$ can be made explicit as follows. Writing any polynomial $P = \sum_{i=0}^{n} a_i X^{n-i}Y^i$ as a column vector ${}^t(a_0,\ldots,a_n)$ which we denote by $\underline{P}$, we know that $\langle \mathrm{Re}(\omega(f)),\mathrm{Re}(\omega(g))\rangle$ is represented by the closed form

$$\Omega(f,g) = \underline{{}^t\mathrm{Re}(\omega(f))}\wedge\Theta^{-1}\underline{\mathrm{Re}(\omega(g))}.$$

Thus by Corollary 1.1, we have $\langle \mathrm{Re}(\omega(f)), \mathrm{Re}(\omega(g))\rangle = \int_Y \Omega(f,g)$. Thus we get a pairing for $f,g \in \mathcal{S}_{n+2}(\Gamma)$ given by $A(f,g) = \int_Y \Omega(f,g)$. We can compute $A(f,g)$ in terms of the Petersson inner product: Note that $\omega(f) = f(z)(X-zY)^n dz$. Thus, by (2b), we have, for the complex conjugation c,

$$\underline{{}^t\omega(f)}\wedge\Theta^{-1}\underline{(\omega(g))^c} = -2\sqrt{-1}\,(f\bar{g})(\bar{z}-z)^n dx\wedge dy = (-2\sqrt{-1})^{n+1} f\bar{g}y^{k-2}dx\wedge dy$$

$(k = n+2)$. This shows that

(3b) $$A(f,g) = -(-2\sqrt{-1})^{n-1}\{(f,g)+(-1)^{n+1}(g,f)\},\quad A(f,\sqrt{-1}^{\,n-1}g) = 2^n\mathrm{Re}((f,g))$$
$$\text{and } A(f,\sqrt{-1}^{\,n}g) = -2^n\sqrt{-1}\,\mathrm{Im}((f,g)).$$

In particular, the pairing $A(f,g)$ on $\mathcal{S}_{n+2}(\Gamma)$ is non-degenerate. We are going to show that if $\varphi(f) = 0$ in the cohomology group, then $A(f,g) = 0$ for all $g \in \mathcal{S}_{n+2}(\Gamma)$. The injectivity of φ follows from this fact. We consider the following function for a constant vector $a \in L(n;\mathbf{R})$ (later we will specify the vector a suitably for our computation) and for a fixed point $z \in \mathcal{H}$

$$F(w) = \int_z^w \mathrm{Re}(\omega(f)) + a.$$

Then we see that

$$F(\gamma(w)) = \int_z^{\gamma(w)} \mathrm{Re}(\omega(f))+a = \int_{\gamma(z)}^{\gamma(w)} \mathrm{Re}(\omega(f))+\varphi_z(f)(\gamma)+a$$
$$= \int_z^w \gamma^*\mathrm{Re}(\omega(f))+\varphi_z(f)(\gamma)+a = \rho_n(\gamma)F(w)+\varphi_z(f)(\gamma)+(1-\gamma)a.$$

Since $\varphi(f) = 0$, we can find $b \in L(n;\mathbf{R})$ so that $\varphi_z(f)(\gamma) = (\gamma-1)b$. Thus by taking $-b$ as a, we have $F(\gamma(w)) = \gamma F(w)$ for all w. On the other hand, we see

that $dF = \omega(f)$, where d is the exterior differential operator. Similarly, we define $G(w) = \int_z^w \mathrm{Re}(\omega(g))$. Then we have $dG = \mathrm{Re}(\omega(g))$ and

$$\Omega(f,g) = {}^tdF\wedge\Theta^{-1}dG = d({}^tF\cdot\Theta^{-1}dG) = d({}^tF\cdot\Theta^{-1}\mathrm{Re}(\omega(g))).$$

Let Φ_0 be the fundamental domain of Y_0 as in the proof of Proposition 1.1 (see (T1-3) in Appendix). Then using the notation introduced there, we know that the boundary of Φ_0 is of the form:

$$\partial\Phi_0 = \sum_{s\in S} t_s + \sum_{j=1}^{g} \{(\alpha_j-1)s_j + (\beta_j-1)s'_j\}.$$

Thus we have, shrinking the holes of Y_0 (i.e. $Y_0 \to Y$)

$$A(f,g) = \lim_{Y_0\to X}\int_Y d({}^tF\cdot\mathrm{Re}(\omega(g))) = \lim_{Y_0\to X}\int_{\partial\Phi_0} {}^tF\cdot\Theta^{-1}\mathrm{Re}(\omega(g)).$$

Since $F(\alpha(w)) = \alpha F(w)$ for all $\alpha \in \Gamma$, we see for any 1-simplex Δ that

$$\int_{\alpha(\Delta)} {}^tF\cdot\Theta^{-1}\mathrm{Re}(\omega(g)) = \int_\Delta {}^t\alpha^*F\cdot\Theta^{-1}\alpha^*\mathrm{Re}(\omega(g))$$
$$= \int_\Delta {}^tF\cdot{}^t\alpha\Theta^{-1}\alpha\mathrm{Re}(\omega(g)) = \int_\Delta {}^tF\cdot\Theta^{-1}\mathrm{Re}(\omega(g)).$$

Thus we have

$$A(f,g) = \sum_{s\in S} \lim_{Y_0\to X}\int_{t_s} {}^tF\cdot\Theta\mathrm{Re}(\omega(g)) = 0,$$

because $F(w)$ is bounded near cusps and $\mathrm{Re}(\omega(g))$ is rapidly decreasing at each cusp. This shows the vanishing of f and the injectivity of φ.

By the dimension identity (6.1.4), we conclude that φ is also surjective. However this proof of surjectivity requires the Riemann-Roch theorem (the dimension formula (6.1.4)) which comes from algebraic geometry. We now give a sketch of a purely cohomological proof of the surjectivity, which is a version of the treatment given in [MM], [MSh] and [Ha] in our special case:

The surjectivity of φ. We show the surjectivity of the scalar extension of φ to $\mathbf{C}$:

(4) $\mathcal{S}_k(\Gamma)\oplus\mathcal{S}_k(\Gamma)^c = \mathcal{S}_k(\Gamma)\otimes_{\mathbf{R}}\mathbf{C} \cong H^1_P(Y,\mathcal{L}(n;\mathbf{R}))\otimes_{\mathbf{R}}\mathbf{C} = H^1_P(Y,\mathcal{L}(n;\mathbf{C}))$.

Here $\mathcal{S}_k(\Gamma)^c = \{\overline{f(z)} \mid f \in \mathcal{S}_k(\Gamma)\}$ with "$\overline{}$" denoting complex conjugation, and $H^1_P(Y,\mathcal{L}(n;\mathbf{C}))$ is the natural image of the sheaf cohomology group $H^1_c(Y,\mathcal{L}(n;\mathbf{C}))$ of compact support in the usual sheaf cohomology group $H^1(Y,\mathcal{L}(n;\mathbf{C}))$. We resort to the Hodge theory of Riemannian manifolds with boundary to prove the theorem. We refer for technical details to standard texts in differential geometry. The boundary exact sequence of Corollary A.2 combined with the isomorphism between the sheaf cohomology group $H^1(Y,\mathcal{L}(n;\mathbf{C}))$ and the group cohomology group $H^1(\Gamma,L(n;\mathbf{C}))$ (see Cor. A.1 and Prop.A.4) tells us that $H^1_P(Y,\mathcal{L}(n;\mathbf{C}))$ is naturally isomorphic to $H^1_P(\Gamma,L(n;\mathbf{C}))$. We can compute

$H^1(Y,\mathcal{L}(n;\mathbf{C}))$ using the de Rham cohomology theory (i.e. $H^1(Y,\mathcal{L}(n;\mathbf{C})) \cong H^1_{DR}(Y,\mathcal{L}(n;\mathbf{C}))$; see Theorem A.2 and Proposition A.4). We have already defined the differential form $\omega(f)$ attached to $f \in \mathcal{S}_k(\Gamma)$. For $f \in \mathcal{S}_k(\Gamma)^c$, we define $\omega(f) = f(z)(X-\bar{z}Y)^n d\bar{z}$. Then $\omega(f)$ for $f \in \mathcal{S}_k(\Gamma)$ is holomorphic and for $f \in \mathcal{S}_k(\Gamma)^c$ is antiholomorphic. Anyway they are closed forms, which define cohomology classes in $H^1_{DR}(Y,\mathcal{L}(n;\mathbf{C}))$. Thus we have a map

$$\Phi : \mathcal{S}_k(\Gamma)\oplus\mathcal{S}_k(\Gamma)^c \to H^1_{DR}(Y,\mathcal{L}(n;\mathbf{C})) = H^1(Y,\mathcal{L}(n;\mathbf{C})).$$

Identifying $H^1(Y,\mathcal{L}(n;\mathbf{C}))$ with $H^1(\Gamma,L(n;\mathbf{C}))$ by the canonical isomorphism, it is not so difficult to show that $\mathrm{Re}(\Phi(f)) = \varphi(f)$ for $f \in \mathcal{S}_k(\Gamma)$ tracking down all the isomorphisms between various cohomology groups presented in Appendix. Thus by the first proof, Φ is injective. The point here is to prove the surjectivity of Φ onto $H^1_P(Y,\mathcal{L}(n;\mathbf{C}))$. First we shall show that Φ takes values in $H^1_P(Y,\mathcal{L}(n;\mathbf{C}))$. If $f \in \mathcal{S}_k(\Gamma)\oplus\mathcal{S}_k(\Gamma)^c$, we define for each cusp $s \in \mathbf{P}^1(\mathbf{Q})$,

$$F_s(z) = \int_s^z \omega(f).$$

This integral is well defined because f is decreasing exponentially towards the cusp s. As already seen, $dF_s = \omega(f)$. Note here that $F_s(z)$ is not invariant under Γ; thus $\gamma^{-1}F_s(\gamma(z))$ may be different from $F_s(z)$. However F_s does behave nicely under $\Gamma_s = \{\gamma \in \Gamma \mid \gamma(s) = s\}$, i.e. $\gamma^{-1}F_s(\gamma(z)) = F_s(z)$ for $\gamma \in \Gamma_s$. Thus F_s is a section of $\mathcal{L}(n;\mathbf{C})$ on $U_s-\{s\}$ for a small neighborhood U_s of s on X. Taking a C^∞ function ϕ_s such that its support is contained in U_s and $\phi_s = 1$ on a still smaller neighborhood of s, we define $F = \sum_{s\in S}\phi_s F_s$. Then F is a smooth global section of $\mathcal{L}(n;\mathbf{C})$ and $\omega(f)-dF$ is compactly supported. Thus the cohomology class of $\omega(f)$ falls in $H^1_P(Y,\mathcal{L}(n;\mathbf{C}))$.

Now we construct a Laplacian acting on the sheaf of smooth differential p-forms $\mathcal{A}^p$ on Y with values in $\mathcal{L}(n;A)$ (for $A = \mathbf{R}$ and $\mathbf{C}$). Since $\pi : SL_2(\mathbf{R}) \to \mathcal{H}$ given by $x \mapsto x(\sqrt{-1})$ induces an isomorphism $\pi : SL_2(\mathbf{R})/SO_2(\mathbf{R}) \cong \mathcal{H}$, we can consider a new covering space $\mathcal{L}'(n;\mathbf{C}) = \Gamma\backslash(SL_2(\mathbf{R})\times L(n;A))/SO_2(\mathbf{R})$, where the action is given by $\gamma(x,P)u = (\gamma xu, P\,|\,u)$ for $(\gamma,u) \in \Gamma\times SO_2(\mathbf{R})$ with the right action of $SL_2(\mathbf{R})$ given by $P\,|\,x(X,Y) = P((X,Y)^t x)$. We claim:

(5) We have an isomorphism of covering spaces of Y: $\mathcal{L}(n;A)_{/Y} \cong \mathcal{L}'(n;A)_{/Y}$ induced by the map: $(x,P) \mapsto (x,P\,|\,x)$ on $SL_2(\mathbf{R})\times L(n;A)$ for $A = \mathbf{R}$ and $\mathbf{C}$.

Let us prove (5). The map is well defined because $\gamma(x,P)$ corresponds to $(\gamma x,\gamma P\,|\,\gamma x) = (\gamma x,P) = (\gamma,1)(x,P)$. It is obvious that the map induces an isomorphism at each fiber and hence, it is an isomorphism globally because both covering spaces are locally trivial.

Hereafter we identify $\mathcal{L}'(n;A)$ with $\mathcal{L}(n;A)$ by the map (5). The merit of the new realization is that it is easy to give a canonical hermitian pairing to each fiber. Since $SO_2(\mathbf{R})$ is a connected compact group, the image of $SO_2(\mathbf{R})$ in $GL(L(n;\mathbf{R}))$ is compact, which is thus contained in a compact orthogonal group of a positive definite symmetric form S on $L(n;\mathbf{R})$. In fact, we can take as S the symmetric n-th tensor of the standard hermitian inner product: $(P,Q) = P(e_1)\overline{Q(e_1)}+P(e_2)\overline{Q(e_2)}$ on $L(1;\mathbf{R})$, where $e_1 = {}^t(1,0)$ and $e_2 = {}^t(0,1)$ make up the standard basis. Since $S(P|u,Q|u) = S(P,Q)$ for $u \in SO_2(\mathbf{R})$, this product induces a positive definite hermitian product on each fiber of $\mathcal{L}'(n;\mathbf{C})$ $(= L(n;\mathbf{C}))$. On $\mathcal{H}$, we have as $SL_2(\mathbf{R})$-invariant Riemannian metric $y^{-2}(dx^2+dy^2) = y^{-2}dz\otimes d\bar{z}$. Take any pair of $\mathbf{C}$-valued differential forms $\{\omega_i\}_{i=1,2}$ on a simply connected open set U in Y which gives an orthonormal basis at each fiber on U under the Riemannian metric. For example, $\omega_1 = y^{-1}dx$ and $\omega_2 = y^{-1}dy$ are a good choice. Then we define $*\omega_i = \omega_j$ $(i \neq j)$, $*(\omega_1\wedge\omega_2) = 1$ and $*1 = \omega_1\wedge\omega_2$. Extend this operator $\mathbf{C}$-linearly to the space of differential forms defined on U. Then we know from de Rham that the operator "$*$" is independent of the choice of the basis (ω_1,ω_2) and hence extends to a global operator on the sheaf $\mathcal{A}_{\mathbf{C}}^1$. Let us write F for $\mathcal{L}(n;\mathbf{C})$ and consider the sheaf $\mathcal{A}_F^1$ of smooth differential forms with values in F. Since the sheaf $\mathcal{L}(n;\mathbf{C})$ is locally constant, the same procedure of defining the "$*$" operator works well for $\mathcal{A}_F^1$. For $\omega,\eta \in \mathcal{A}_F^1(Y)$, writing

$$*\omega|_U = \phi_1(z)\omega_1+\phi_2(z)\omega_2 \text{ and } \eta = \varphi_1(z)\omega_1+\varphi_2(z)\omega_2,$$

we define $S(\eta,\omega) = \sum_{i,j}S(\phi_i,\overline{\varphi}_j)\omega_i\wedge*\omega_j$. Then $S(\eta,\omega)$ patches up together well to give a global 2-form. We define $(\eta,\omega) = \int_Y S(\eta,\omega)$. Then $(\ ,\ )$ is a positive hermitian form defined on the subspace of square integrable forms in $\mathcal{A}_F^1(Y)$. Similarly we can define a positive pairing $(\ ,\ )$ between $\mathcal{A}_F^0(Y)$ and $\mathcal{A}_F^2(Y)$. Let d' (resp. d'') be the holomorphic (resp. antiholomorphic) exterior differential operator. We then define the formal adjoint δ' and δ'' of d' and d'' respectively. That is, $(d'\omega,\eta) = (\omega,\delta'\eta)$ (resp. $(d''\omega,\eta) = (\omega,\delta''\eta)$) for all square integrable ω with square integrable $d'\omega$ (resp. $d''\omega$) and all square integrable η. We put $\delta = \delta'+\delta''$. Then δ is the adjoint of the exterior differential operator d. We define the Laplacians $\Delta = d\delta+\delta d$, $\Delta' = d'\delta'+\delta'd'$ and $\Delta'' = d''\delta''+\delta''d''$. It is easy to see that $\Delta = \Delta'+\Delta''$. We call ω harmonic if $\Delta\omega = 0$. Write $\omega = \sum_j f_j(X-zY)^{n-j}(X-\bar{z}Y)^j dz+\sum_j f'_j(X-zY)^{n-j}(X-\bar{z}Y)^j d\bar{z}$. Then we have, for $\gamma \in \Gamma$,

$$f_j(\gamma(z)) = f_j(z)j(\gamma,z)^{n-j+2}j(\gamma,\bar{z})^j \text{ and } f'_j(\gamma(z)) = f'_j(z)j(\gamma,z)^{n-j}j(\gamma,\bar{z})^{j+2},$$

where $j(\gamma,z) = cz+d$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If ω is square integrable and harmonic, by the spectral theory of the unitary representation of $SL_2(\mathbf{R})$ on the L_2-space $L_2(\Gamma\backslash SL_2(\mathbf{R}))$, it is known that each $f_j(z)$ and $f'_j(z)$ and all their derivatives are exponentially decreasing as $\mathrm{Im}(\alpha(z)) \to \infty$ for all $\alpha \in SL_2(\mathbf{Z})$ [Ha]. The

description of the spectral theory would take us beyond the scope of this book. Thus we just admit this fact and conclude the proof. By the exponential decay towards the cusps, if ω is square integrable and harmonic, it is easy to show $\Delta'\omega = \Delta''\omega = 0$. In particular, $d'\omega = d''\omega = 0$ and $\delta'\omega = \delta''\omega = 0$ if ω is harmonic and square integrable. Thus if ω is harmonic and square integrable, ω is a sum of holomorphic form and anti-holomorphic form. Thus we may assume that ω is holomorphic ($f'_j = 0$). We now show that $\omega = \omega(f_0)$ for a holomorphic cusp form f_0 on Γ of weight n+2 if ω is holomorphic. To do this, we compute δ' for $\omega = \sum_j f_j(X-zY)^{n-j}(X-\bar{z}Y)^j dz$. Here we have written down ω as a section of $\mathcal{L}(n;\mathbf{C})$. The section of $\mathcal{L}'(n;\mathbf{C})$ corresponding to ω is

$$\sum_j f_j(g(i))j(g,i)^{-n+j}j(g,-i)^{-j}(X-iY)^{n-j}(X+iY)^j dg(i) \quad (i = \sqrt{-1},\ g \in SL_2(\mathbf{R})).$$

Writing $\phi = \sum_k \phi_k(X-zY)^{n-k}(X-\bar{z}Y)^k$ for a C^∞-global section of $\mathcal{L}(n;\mathbf{C})$, we have $f_k(\gamma(z)) = f_k(z)j(\gamma,z)^{n-k}j(\gamma,\bar{z})^k$ and

$$d'\phi = \sum_{k=0}^{n}\left(\frac{\partial}{\partial z} + \frac{n-k}{2iy}\right)\phi_k(X-zY)^{n-k}(X-\bar{z}Y)^k - \frac{n-k}{2iy}\sum_{k=0}^{n-1}\phi_k(X-zY)^{n-k-1}(X-\bar{z}Y)^{k+1}.$$

Then the C^∞-section of $\mathcal{L}'(n;\mathbf{C})$ corresponding to $d'\phi$ is given by

$$\sum_{k=0}^{n}\left(\frac{\partial}{\partial z} + \frac{n-k}{2iy}\right)\phi_k(X-iY)^{n-k}(X+iY)^k j(g,i)^{-n+k}j(g,-i)^{-k}$$
$$-\frac{n-k}{2iy}\sum_{k=0}^{n-1}\phi_k(X-zY)^{n-k-1}(X-\bar{z}Y)^{k+1}j(g,i)^{-n+k+1}j(g,-i)^{-k-1}.$$

We write δ_{n-k} for the differential operator $\frac{\partial}{\partial z} + \frac{n-k}{2iy}$. Noting the fact:

$$S((X-iY)^{n-j}(X+iY)^j, \overline{(X-iY)^{n-k}(X+iY)^k}) = 2^n\delta_{j,k} \text{ and}$$
$$y(g(i)) = \mathrm{Im}(g(i)) = |j(g,i)|^{-2},$$

we have

$$(d'\phi,\omega) = 2^n\left\{\sum_{k=0}^{n-1}\int_Y \bar{f}_k\,\delta_{n-k}\phi_k y^n dxdy - \sum_{k=0}^{n-1}\int_Y \bar{f}_{k+1}\phi_k\,\frac{n-k}{2iy}y^n dxdy\right\}.$$

It is easy to see that (see the proof of Theorem 10.1.2), for $\varepsilon = y^2\frac{\partial}{\partial\bar{z}}$,

$$\int_Y \bar{f}_k\,\delta_{n-k}\phi_k y^n dxdy = \int_Y \overline{\varepsilon f_k}\,y^{n-2}dxdy.$$

Thus we have

$$\delta'\omega = \sum_{k=0}^{n}\left(\varepsilon f_k + \frac{n-k}{2iy}f_{k+1}\right)(X-zY)^{n-k}(X-\bar{z}Y)^k.$$

By a direct computation, we have for $\bar{\delta}_k = \frac{\partial}{\partial\bar{z}} - \frac{k}{2iy}$

$$d''\omega = \sum_{k=0}^{n}\left(\bar{\delta}_k f_k + \frac{k+1}{2iy}f_{k+1}\right)(X-zY)^{n-k}(X-\bar{z}Y)^k,$$

where we agree to assume that $f_{n+1} = 0$. By the fact: $d''\omega = \delta'\omega = 0$, we know that

$$\frac{\partial f_0}{\partial \bar{z}} = -\frac{1}{2iy} f_1 \text{ and } \frac{\partial f_0}{\partial \bar{z}} = -\frac{n}{2iy^3} f_1.$$

This implies $f_1 = 0$ and f_0 is holomorphic. Again using $d''\omega = 0$, we conclude $f_j = 0$ for $j > 0$. Thus $\omega = \omega(f_0)$ for $f_0 \in \mathcal{S}_k(\Gamma)$. If ω is antiholomorphic, $\omega = \omega(f_0)$ for $f_0 \in \mathcal{S}_k(\Gamma)^c$.

Now we want to define Hodge operators. Let ϕ be a square integrable smooth 1-form. Consider the L_2-space L of 1-forms with values in L(n;**C**). Let Ψ be the L_2-closure of $\{\Delta\phi \mid \mathrm{Supp}(\phi) \text{ is compact}\}$ in L. Writing $\Gamma_c(\mathcal{A}_F{}^1)$ for the space of compactly supported global sections for the sheaf $\mathcal{A}_F{}^1$, we take, for any compactly supported $\omega \in \mathcal{A}_F{}^1$, a unique form $\psi \in \Psi$ such that $|\omega-\psi| = \sqrt{(\omega-\psi,\omega-\psi)}$ is minimal, i.e. ψ is the orthogonal projection of ω in Ψ. Then we put $H\omega = \omega-\psi$. Then by definition $(H\omega,\Delta\gamma) = 0$ for all compactly supported γ. This implies $H\omega$ is a harmonic current. Since Δ is an elliptic operator, any harmonic current is in fact an analytic function (cf. [DuS, §3] or [Ko, Appendix]). Then it is well known that we can find a smooth solution of the equation $\Delta\mu = \omega-H\omega$ because on Ψ the spectrum of Δ does not vanish. Hence Δ has a formal inverse defined on Ψ, which we write G [Ko, Appendix, §7]. Thus $\mu = G\omega$ and $HG = 0$. That is, $\Delta G\omega = (1-H)\omega$. Since d commutes with Δ, G commutes with d, and hence $H\omega$ is cohomologous to ω if ω is closed. As already shown, $H\omega$ is in the image of Φ. Thus Φ is surjective.

§6.3. Hecke operators on cohomology groups

Let $\Delta = \{\alpha \in M_2(\mathbf{Z}) \mid \det(\alpha) \neq 0\}$. We can let the semi-group Δ act on $\mathcal{H}$ as follows. If $\det(\alpha) > 0$, α acts on $\mathcal{H}$ by the usual linear fractional transformation. If $\alpha = j = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, we put $j(z) = -\bar{z}$. If $\det(\alpha) < 0$, we can decompose $\alpha = \alpha j j$ with $\det(\alpha j) > 0$ and define $\alpha(z) = (\alpha j)(j(z))$. One can easily check that this action is well defined (i.e. associative). Actually, identifying $\mathcal{H}$ with $SL_2(\mathbf{R})/SO_2(\mathbf{R}) = GL_2(\mathbf{R})/O_2(\mathbf{R})$, this action is the left multiplication by elements of $GL_2(\mathbf{R})$. Let $\alpha \in \Delta$ and $\langle\Gamma,\Gamma',\alpha^\iota\rangle$ be the semi-group in Δ generated by $\alpha^\iota = \det(\alpha)\alpha^{-1}$ and two congruence subgroups Γ and Γ'.

For any $\langle\Gamma,\Gamma',\alpha^\iota\rangle$-module M, we define the Hecke operator $[\Gamma\alpha\Gamma']$ with $\det(\alpha) > 0$ acting on $H^1(\Gamma,M)$ as follows. First decompose $\Gamma\alpha\Gamma' = \coprod_i \Gamma\alpha_i$. For each $\gamma \in \Gamma'$, we can write $\alpha_i\gamma = \gamma_i\alpha_j$ $(\gamma_i^{-1}\alpha_i = \alpha_j\gamma^{-1})$ for a unique j

with $\gamma_i \in \Gamma$. Then for each inhomogeneous cocycle $u : \Gamma \to L_n(A)$ (see Appendix about cocycles), we define $v = u \mid [\Gamma\alpha\Gamma']$ by $v(\gamma) = \sum_i \alpha_i^\iota u(\gamma_i)$, where $\alpha^\iota = \det(\alpha)\alpha^{-1}$. For $\gamma,\delta \in \Gamma$, we define γ_i and δ_i as above. Now let us check that v is a cocycle. Note that $\alpha_i\gamma\delta = \gamma_i\delta_j\alpha_k$ for some k. Thus

$$\begin{aligned} v(\gamma\delta) &= \textstyle\sum_i \alpha_i^\iota u(\gamma_i\delta_j) = \sum_i \{\alpha_i^\iota\gamma_i u(\delta_j)+\alpha_i^\iota u(\gamma_i)\} \\ &= \textstyle\sum_i (\gamma_i^{-1}\alpha_i)^\iota u(\delta_j)+v(\gamma) = \sum_i (\alpha_j\gamma^{-1})^\iota u(\delta_j)+v(\gamma) = \gamma v(\delta)+v(\gamma). \end{aligned}$$

This shows that v is a 1-cocycle of Γ'. If u is a 1-coboundary, i.e. $u(\gamma) = (\gamma-1)x$, then

$$v(\gamma) = \textstyle\sum_i \alpha_i^\iota(\gamma_i-1)x = \sum_j (\alpha_j\gamma^{-1})^\iota x - \sum_i \alpha_i^\iota x = (\gamma-1)\sum_i \alpha_i^\iota x$$

and v is a 1-coboundary. This shows that the operator $[\Gamma\alpha\Gamma']$ is a well defined linear operator on $H^1(\Gamma,M)$ into $H^1(\Gamma',M)$. Now if u is parabolic, by replacing γ as above by any parabolic element $\pi \in P$, we know from the above computation that if $u(\pi) = (\pi-1)x$, then $v(\pi) = (\pi-1)\sum_i \alpha_i^\iota x$. Thus v is again parabolic and $[\Gamma\alpha\Gamma']$ sends $H^1_P(\Gamma,M)$ into $H^1_P(\Gamma',M)$. We define the multiplication in the abstract Hecke ring $R(\Gamma,\Delta)$ as in [Sh, 3.2] and [M, §2.7]. We see easily that $[\Gamma\alpha\Gamma]\circ[\Gamma\beta\Gamma] = [(\Gamma\alpha\Gamma)\cdot(\Gamma\beta\Gamma)]$ and hence $R(\Gamma,\Delta)$ acts on the cohomology group if M is a Δ-module. When $\Gamma = \Gamma' = \Gamma_0(N)$ for a positive integer N and M is a Δ'^ι-module for

$$\Delta' = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta \mid \det(\alpha) \neq 0,\ c \in N\mathbf{Z} \text{ and } d\mathbf{Z}+N\mathbf{Z} = \mathbf{Z}\},$$

we define the Hecke operator $T(n)$ for each integer $n > 0$ by the action of $\sum[\Gamma\alpha\Gamma]$, where $\Gamma\alpha\Gamma$ runs over all double cosets in $\{\alpha \in \Delta'^\iota \mid \det(\alpha) = n\}$.

For a fixed point $z \in \mathcal{H}$, let us compute $\varphi_z(g)(\gamma) = \int_z^{\gamma(z)} \mathrm{Re}(\omega(g))$ for $g = f \mid [\Gamma\alpha\Gamma] = \sum_i f \mid \alpha_i$ $(\Gamma\alpha\Gamma = \coprod_i \Gamma\alpha_i)$ in terms of $f \in \mathcal{S}_k(\Gamma)$. Note that

$$\delta_n(\alpha(z)) = \det(\alpha)(cz+d)^{-n-2}\alpha\delta_n(z).$$

Since scalar t of Δ acts on $L(n;\mathbf{C})$ via the scalar multiplication by t^n, we obtain $\alpha^\iota \mathrm{Re}(\omega(f))\circ\alpha = \mathrm{Re}(\omega(f \mid \alpha))$, where $f \mid \alpha = \det(\alpha)^{k-1}f(\alpha(z))j(\alpha,z)^{-k}$ $(k = n+2)$. From this fact, we know that

$$\varphi_z(g)(\gamma) = \textstyle\sum_i \alpha_i^\iota \int_z^{\gamma(z)} \alpha_i{}^*\mathrm{Re}(\omega(f)) = \sum_i \alpha_i^\iota \int_{\alpha_i(z)}^{\alpha_i\gamma(z)} \mathrm{Re}(\omega(f)).$$

As in the proof of Theorem 2.1, we put $F(w) = \int_z^w \mathrm{Re}(\omega(f))+a$. Then the 1-cocycle $u(\gamma) = F(\gamma(w))-\gamma F(w)$ represents the cohomology class of $\varphi(f)$. Then we see that

$$\varphi_z(g)(\gamma) = \sum_i \alpha_i^t\{F(\gamma_i\alpha_j(z))-F(\alpha_i(z))\}$$
$$= \sum_i \alpha_i^t\{u(\gamma_i)+\gamma_i F(\alpha_j(z))\} - \sum_i \alpha_i^t F(\alpha_i(z)) = u \mid [\Gamma\alpha\Gamma](\gamma) + (\gamma-1)x$$

for $x = \sum_i \alpha_i^t F(\alpha_i(z))$, since $\alpha_i^t\gamma_i = \gamma\alpha_j^t$. This shows that the isomorphism φ as in Theorem 2.1 is in fact an isomorphism of Hecke modules (i.e. compatible with Hecke operators). Similarly the isomorphism

$$\Phi : \mathcal{S}_k(\Gamma)\oplus\mathcal{S}_k(\Gamma)^c \cong H^1_P(\Gamma,L(n;\mathbf{C}))$$

is an isomorphism of Hecke modules.

Let N be a positive integer and $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to A^\times$ be a character with values in a ring A. We define a new Δ'^t-module $L(n,\chi;A)$ as follows. We take $L(n;A)$ as the underlying A-module of $L(n,\chi;A)$ and define a new action of Δ'^t by, writing the original action of $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta'$ on $L(n;A)$ as $\gamma\bullet P$,

$$\gamma^t P = \chi(d)\gamma^t\bullet P.$$

When we regard $L(n,\chi;A)$ as a left $\Gamma_0(N)$-module, the action is given by

$$\gamma P = \chi(d)\gamma\bullet P \quad \text{for} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Theorem 1. *For any positive integer* N, *we have natural isomorphisms of Hecke modules* $\Phi : \mathcal{S}_k(\Gamma_0(N),\chi)\oplus\mathcal{S}_k(\Gamma_0(N),\overline{\chi})^c \cong H^1_P(\Gamma_0(N),L(n,\chi;\mathbf{C}))$, *where* $\overline{\chi}$ *denotes the complex conjugate of* χ *and*

$$\mathcal{S}_k(\Gamma_0(N),\overline{\chi})^c = \{\overline{f(z)} \mid f \in \mathcal{S}_k(\Gamma_0(N),\overline{\chi})\}.$$

Proof. We can define the cocycle $\varphi_z(f)$ for $f \in \mathcal{S}_k(\Gamma_0(N),\chi)\oplus\mathcal{S}_k(\Gamma_0(N),\overline{\chi})^c$ by

$$\varphi_z(f)(\gamma) = \int_z^{\gamma(z)} \omega(f).$$

Then it is easy to check that $\varphi_z(f)$ in fact has values in $\mathcal{L}(n,\chi;\mathbf{C})$ (not just in $\mathcal{L}(n;\mathbf{C})$). Thus we have a natural map associating the cohomology class of $\varphi_z(f)$ to f:

$$\Phi : \mathcal{S}_k(\Gamma_0(N),\chi)\oplus\mathcal{S}_k(\Gamma_0(N),\overline{\chi})^c \to H^1_P(\Gamma_0(N),L(n,\chi;\mathbf{C})).$$

Now we take a small normal subgroup Γ of $\Gamma_0(N)$ of finite index in $\Gamma_1(N)$. We may assume that Γ is torsion-free. Then χ as a character of $\Gamma_0(N)$ factors through the finite quotient $G = \Gamma_0(N)/\Gamma$. The double coset $\Gamma 1_2 \Gamma_0(N) = \Gamma_0(N)$ defines two trace operators:

$$\mathrm{Tr} : H^1_P(\Gamma,L(n;\mathbf{C})) \to H^1_P(\Gamma_0(N),L(n,\chi;\mathbf{C})),$$
$$\mathrm{Tr} : \mathcal{S}_k(\Gamma)\oplus\mathcal{S}_k(\Gamma)^c \to \mathcal{S}_k(\Gamma_0(N),\chi)\oplus\mathcal{S}_k(\Gamma_0(N),\overline{\chi})^c.$$

We have dropped the symbol χ from the left-hand side of Tr, not only because $L(n,\chi;\mathbf{C}) = L(n;\mathbf{C})$ as Γ-module but also because the action of G given by the operator $[\Gamma\alpha\Gamma] = [\Gamma\alpha]$ for $\alpha \in \Gamma_0(N)$ is defined relative to the action of α on $L(n;\mathbf{C})$. Write "res" for the map given by restricting cocycles of $\Gamma_0(N)$ to the smaller subgroup Γ. Then it is obvious that Tr∘res is multiplication by the index $[\Gamma_0(N):\Gamma_1(N)]$. This shows that res induces an isomorphism from $H^1_P(\Gamma_0(N),L(n,\chi;\mathbf{C}))$ (resp. $\mathcal{S}_k(\Gamma_0(N),\chi)\oplus\mathcal{S}_k(\Gamma_0(N),\overline{\chi})^c$) onto

$$H^1_P(\Gamma,L(n;\mathbf{C}))[\chi] = \{x \in H^1_P(\Gamma,L(n;\mathbf{C})) \mid x|g = \chi(g)x \text{ for } g \in G\} \text{ (resp.}$$
$$\{\mathcal{S}_k(\Gamma)\oplus\mathcal{S}_k(\Gamma)^c\}[\chi] = \{x \in \mathcal{S}_k(\Gamma)\oplus\mathcal{S}_k(\Gamma)^c \mid x|g = \chi(g)x \text{ for } g \in G\}).$$

Thus we have a commutative diagram:

$$\begin{array}{ccc} \Phi : \mathcal{S}_k(\Gamma_0(N),\chi)\oplus\mathcal{S}_k(\Gamma_0(N),\overline{\chi})^c & \to & H^1_P(\Gamma_0(N),L(n,\chi;\mathbf{C})) \\ \downarrow \text{inclusion} & & \downarrow \text{res} \\ \Phi : \{\mathcal{S}_k(\Gamma)\oplus\mathcal{S}_k(\Gamma)^c\}[\chi] & \longrightarrow & H^1_P(\Gamma,L(n;\mathbf{C}))[\chi]. \end{array}$$

Since the lower horizontal arrow is a surjective isomorphism of Hecke modules by Theorem 2.1, so is the upper top line.

Theorem 2. *For every positive integer* N *and every character* $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$, *we have, if* $k \geq 2$

$$\mathcal{S}_k(\Gamma_0(N),\chi;A) = \mathcal{S}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}A \text{ and}$$
$$\mathrm{Hom}_{\mathbf{Z}[\chi]}(\mathbf{h}_k(\Gamma_0(N),\chi;A),A) \cong \mathcal{S}_k(\Gamma_0(N),\chi;A) \text{ by } \phi \mapsto \textstyle\sum_{n=1}^\infty \phi(T(n))q^n$$

for any $\mathbf{Z}[\chi]$*-algebra* A *inside* $\mathbf{C}$ *or* $\overline{\mathbf{Q}}_p$.

Proof. By Theorem 5.3.1, we have

$$\mathrm{Hom}_{\mathbf{C}}(\mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{C}),\mathbf{C}) \cong \mathcal{S}_k(\Gamma_0(N),\chi) \text{ via } \phi \mapsto \textstyle\sum_{n=1}^\infty \phi(T(n))q^n.$$

On the other hand, by Theorem 1, $\mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi])$ leaves stable the image L of $H^1_P(\Gamma_0(N),L(n,\chi;A))$ in $\mathcal{S}_k(\Gamma_0(N),\chi)\oplus\mathcal{S}_k(\Gamma_0(N),\overline{\chi})^c$. This implies

$$\mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{C}) = \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}\mathbf{C},$$

and therefore

$$\mathrm{Hom}_{\mathbf{C}}(\mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{C}),\mathbf{C}) = \mathrm{Hom}_{\mathbf{Z}[\chi]}(\mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]),\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}\mathbf{C}.$$

The image of $\mathrm{Hom}_{\mathbf{Z}[\chi]}(\mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]),\mathbf{Z}[\chi])$ in $\mathcal{S}_k(\Gamma_0(N),\chi)$ is exactly the space $\mathcal{S}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi])$, and hence the assertion follows for $A = \mathbf{C}$. We can deduce the assertion for general A from that for $\mathbf{C}$ in the same manner as in the proof of Corollary 5.4.1.

Now assume that $N = pp^\alpha$ for a prime p. We now want to describe the similar result for $\mathcal{M}(\chi) = \mathcal{M}_k(\Gamma_0(N),\chi)$. The map Φ is well defined even on $\mathcal{M}_k(\Gamma_0(N),\chi)$ and gives a commutative diagram for $\Gamma = \Gamma_0(N)$ whose rows are exact:

$$\begin{array}{ccccccc} 0 \to & \mathcal{S}(\Gamma,\chi)\oplus\mathcal{S}(\Gamma,\overline{\chi})^c & \xrightarrow{\iota} & \mathcal{M}(\chi)\oplus\mathcal{S}(\Gamma,\overline{\chi})^c & \to & \mathrm{Coker}(\iota) \\ & \wr\Phi & & \downarrow\Phi & & \downarrow\Phi' \\ 0 \to & H^1_P(\Gamma,L(n,\chi;\mathbf{C})) & \to & H^1(\Gamma,L(n,\chi;\mathbf{C})) & \to & \oplus_{s\in S}H_s{}^1(\Gamma_s,L(n,\chi;\mathbf{C})). \end{array}$$

We now claim, for any field K containing $\mathbf{Q}(\chi)$, that if $\alpha \geq 0$

$$(1)\ H^1(\Gamma_0(pp^\alpha)_s,L(n,\chi;K)) = \begin{cases} K, & \text{if } s \text{ is equivalent to either } \infty \text{ or } 0, \\ 0, & \text{otherwise.} \end{cases}$$

When $s = 0$ or ∞, the assertion follows from the argument which proves (1.2a,b), since Γ_s is generated by either $\pi_\infty = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\pi_0 = \begin{pmatrix} 1 & 0 \\ pp^\alpha & 1 \end{pmatrix}$ modulo the center $\{\pm 1_2\}$. As seen in §1, $S \cong \Gamma_0(p^\alpha q)\backslash SL_2(\mathbf{Z})/\Gamma_\infty \cong \{\text{ideals of } \mathbf{Z}/p^\alpha\mathbf{p}\mathbf{Z}\}$ given by

$$s = \frac{r}{t} \mapsto \begin{pmatrix} r & * \\ t & * \end{pmatrix} \mapsto (t).$$

The last isomorphism follows from the strong approximation theorem (Lemma 1.1) and the fact that the image of $\Gamma_0(pp^\alpha)$ in $SL_2(\mathbf{Z}/p^\alpha\mathbf{p}\mathbf{Z})$ is the subgroup of upper triangular matrices which fixes one line in $(\mathbf{Z}/p^\alpha\mathbf{p}\mathbf{Z})^2$. This implies that each cusp s which is equivalent to neither ∞ nor 0 is represented by $\alpha_u = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$ for $u \in p\mathbf{Z}\text{-}pp^\alpha\mathbf{Z}$. Then $\pi_s = \alpha_u\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\alpha_u{}^{-1} = \begin{pmatrix} 1-uh & h \\ -u^2h & 1+uh \end{pmatrix} \in \Gamma_0(p^\alpha\mathbf{p})$ for some $h \in \mathbf{Z}$. Since π_s is a generator of $\Gamma_0(p^\alpha\mathbf{p})_s$, h is determined by the condition that $u^2h \in p^\alpha\mathbf{p}\mathbf{Z}$ and $|h|_p$ is as large as possible. Thus we know that $|h|_p = \max(|p^\alpha\mathbf{p}|_p|u|_p{}^{-2},1) > |p^\alpha\mathbf{p}|_p$. Then by the primitivity of χ, $\chi(1+uh) \neq 1$ and $\pi_s\text{-}1$ is invertible on $L(n,\chi;K)$. This shows the vanishing of the cohomology because of $H^1(\Gamma_0(p^\alpha\mathbf{p})_s,L(n,\chi;K)) = L(n,\chi;K)/(\pi_s\text{-}1)L(n,\chi;K)$. If $k > 2$, we already know from Proposition 5.1.2 that the Fourier expansion of $E_k(\chi)$ (resp. $G(\chi)^{-1}G_k(\chi)$) has non-trivial constant term at ∞ (resp. 0) and has no-constant term at 0 (resp. ∞). We will see in Chapter 9 the same assertion for $k = 2$ provided that $\chi \neq \mathrm{id}$. This shows that the map Φ' of $\mathrm{Coker}(\iota)$ to $\oplus_{s\in S}H^1(\Gamma_0(p^\alpha)_s,L(n,\chi;\mathbf{R}))$ induced from Φ is in fact surjective. Comparing the dimension, Φ' is an isomorphism. Thus we have

Theorem 3. *Let* $N = pp^{\alpha}$ *with* $\alpha \geq 0$, $k = n+2$ *and* χ *be a primitive character modulo* N. *Then we have the following commutative diagram whose rows are exact:*

$$\begin{array}{ccccccc} 0 \to & \mathcal{S}_k(\chi)\oplus\mathcal{S}_k(\overline{\chi})^c & \xrightarrow{\iota} & \mathcal{M}_k(\chi)\oplus\mathcal{S}_k(\overline{\chi})^c & \to & \mathrm{Coker}(\iota) \\ & \wr\Phi & & \wr\Phi & & \wr \\ 0 \to & H^1_P(L(n,\chi;\mathbf{C})) & \to & H^1(L(n,\chi;\mathbf{C})) & \to & \oplus_{s\in S}H_s{}^1(L(n,\chi;\mathbf{C})). \end{array}$$

Now we deal with the case of $SL_2(\mathbf{Z})$. When $k > 2$, the argument is completely the same as in the case of Theorem 3. When $k = 2$ (i.e. $n = 0$), the small circle around ∞ in X is bounded by Y_0. Thus the natural restriction map:

$$H^1(SL_2(\mathbf{Z}),\mathbf{C}) \to H^1(\{\pm 1\}U(\mathbf{Z}),\mathbf{C})$$

for $U(\mathbf{Z}) = \left\{\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \middle| \, m \in \mathbf{Z}\right\}$ is a zero map. This in particular means that the constant term of any modular form of weight 2 for $SL_2(\mathbf{Z})$ vanishes. Thus $\mathcal{M}_2(SL_2(\mathbf{Z})) = \mathcal{S}_2(SL_2(\mathbf{Z})) = \{0\}$, and we have

Theorem 4. *We have the following commutative diagram if* $k = n+2 > 2$:

$$\begin{array}{ccccccc} \mathcal{S}_k(SL_2(\mathbf{Z}))\oplus\mathcal{S}_k(SL_2(\mathbf{Z}))^c & \xrightarrow{\iota} & \mathcal{M}_k(SL_2(\mathbf{Z}))\oplus\mathcal{S}_k(SL_2(\mathbf{Z}))^c & \to & \mathrm{Coker}(\iota) \\ \wr\Phi & & \wr\Phi & & \wr \\ 0 \to H^1_P(SL_2(\mathbf{Z}),L(n;\mathbf{C})) & \longrightarrow & H^1(SL_2(\mathbf{Z}),L(n;\mathbf{C})) & \to & H^1_\infty(L(n;\mathbf{C})) \to 0, \end{array}$$

where $H^1_\infty(L(n;\mathbf{C})) = H^1(\{\pm 1\}U(\mathbf{Z}),L(n;\mathbf{C}))$. *When* $k = 2$, *we have the following commutative diagram:*

$$\begin{array}{ccc} \mathcal{S}_2(SL_2(\mathbf{Z}))\oplus\mathcal{S}_2(SL_2(\mathbf{Z}))^c & \cong & \mathcal{M}_k(SL_2(\mathbf{Z}))\oplus\mathcal{S}_k(SL_2(\mathbf{Z}))^c \\ \wr\Phi & & \wr\Phi \\ H^1_P(SL_2(\mathbf{Z}),\mathbf{C}) & \cong & H^1(SL_2(\mathbf{Z}),\mathbf{C}). \end{array}$$

Then in the same manner as in the proof of Theorem 2, we have

Corollary 1. *For every prime power* $N = p^{\alpha}$ *and every primitive character* $\chi : (\mathbf{Z}/N\mathbf{Z})^{\times} \to \mathbf{C}^{\times}$, *we have, if* $k \geq 2$,

$$\mathcal{M}_k(\Gamma_0(N),\chi;A) = \mathcal{M}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}A.$$

Let $N \geq 4$ be an integer. Then $\Gamma = \Gamma_1(N)$ is torsion-free. We can consider for primes q the double coset action $T(q) = [\Gamma\alpha\Gamma]$ for $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$ on modular forms f on $\Gamma_1(N)$, which is given by $f|T(q) = \sum_i f|_k\alpha_i$ for the decomposition $\Gamma\alpha\Gamma = \coprod_i\Gamma\alpha_i$. In fact, we can choose α_i so that $\Gamma_0(N)\alpha\Gamma_0(N) = \coprod_i\Gamma_0(N)\alpha_i$. Therefore we have two commutative diagrams:

$$\begin{array}{ccc} \mathcal{M}_k(\Gamma_0(N),\chi) & \subset & \mathcal{M}_k(\Gamma_1(N)) \\ \downarrow T(q) & & \downarrow T(q) \\ \mathcal{M}_k(\Gamma_0(N),\chi) & \subset & \mathcal{M}_k(\Gamma_1(N)) \end{array}$$

and

$$\begin{array}{ccc} H^1(\Gamma_0(N),L(n,\chi;A)) & \subset & H^1(\Gamma_1(N),L(n;A)) \\ \downarrow T(q) & & \downarrow T(q) \\ H^1(\Gamma_0(N),L(n,\chi;A)) & \subset & H^1(\Gamma_1(N),L(n;A)). \end{array}$$

The finite group $(\mathbf{Z}/N\mathbf{Z})^\times \cong \Gamma_1(N)\backslash\Gamma_0(N)$ acts on $\mathcal{M}_k(\Gamma_1(N))$ by

$$f\,|\,\langle d\rangle = f\,|_k\begin{pmatrix} a & b \\ c & d\end{pmatrix} \quad \text{for } \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma_0(N).$$

Similarly the operator $\langle d\rangle$ acts on the cohomology via the action of $[\Gamma\begin{pmatrix} a & b \\ c & d\end{pmatrix}\Gamma]$. Now we define $T(n)$ for general positive integers n by

$$a(m,f\,|\,T(n)) = \textstyle\sum_{b\,|\,(m,n)} b^{k-1}a(mn/b^2,f\,|\,\langle b\rangle),$$

where b runs over all common positive divisors of m and n prime to N. This action again coincides with the action of $\sum_{\Gamma\alpha\Gamma}[\Gamma\alpha\Gamma]$ where $\Gamma\alpha\Gamma$ runs over all distinct double cosets in

$$\{\alpha \in \Delta\,|\,\det(\alpha) = n \text{ and } \alpha \equiv \begin{pmatrix} 1 & * \\ 0 & *\end{pmatrix} \bmod NM_2(\mathbf{Z})\}$$

(see [Sh, III] or [M, §4.5]). Anyway we can define the Hecke algebra $\mathbf{H}_k(\Gamma_1(N);A)$ (resp. $\mathbf{h}_k(\Gamma_1(N);A)$) for any subring A of $\mathbf{C}$ as an A-subalgebra of the A-torsion-free part of $H^1(\Gamma_1(N),L(n;A))$ (resp. $H^1_P(\Gamma_1(N),L(n;A))$ for $n = k-2$. Then, by the Eichler-Shimura isomorphism, these algebras act faithfully on $\mathcal{M}_k(\Gamma_1(N))$ and $\mathcal{S}_k(\Gamma_1(N))$. Note that we have not proven that $\mathcal{M}_k(\Gamma_1(N);A)$ is stable under $\mathbf{H}_k(\Gamma_1(N);A)$ although it can be proven using a geometric interpretation of modular forms due to Katz [K5] (see also [H1, §1]). Anyway we have

(2a) $\mathbf{H}_k(\Gamma_1(N);A) = \mathbf{H}_k(\Gamma_1(N);\mathbf{Z})\otimes_{\mathbf{Z}}A$ and $\mathbf{h}_k(\Gamma_1(N);A) = \mathbf{h}_k(\Gamma_1(N);\mathbf{Z})\otimes_{\mathbf{Z}}A$ for $k \geq 2$.

There are natural A-algebra homomorphisms

(2b) $\mathbf{H}_k(\Gamma_1(N);A) \to \mathbf{H}_k(\Gamma_0(N),\chi;A)$ and $\mathbf{h}_k(\Gamma_1(N);A) \to \mathbf{h}_k(\Gamma_0(N),\chi;A)$,

which take $T(n)$ to $T(n)$ and hence are surjective. These homomorphisms are obtained by restricting $T(n)$ for $\Gamma_1(N)$ to the space of modular forms for $\Gamma_0(N)$.

Now we want to describe the action of Hecke operators in terms of sheaf cohomology groups $H^1_c(Y,\mathcal{L}(n,\chi;A))$, $H^1_P(Y,\mathcal{L}(n,\chi;A))$ and $H^1(Y,\mathcal{L}(n,\chi;A))$. To include the most general case, we take a $\langle\Gamma,\Gamma',\alpha\rangle^1$-module M for congruence sub-

groups Γ and Γ' and $\alpha \in \Delta$. We consider the locally constant sheaf $\underline{M}$ associated with M. We can in fact split the operator $[\Gamma\alpha\Gamma']$ on $H^1_*(\Gamma,M)$ into three parts: $[\Gamma\alpha\Gamma'] = \mathrm{Tr}_{\Gamma'/\Phi^\alpha}\circ[\Phi\alpha\Phi^\alpha]\circ\mathrm{res}_{\Gamma/\Phi}$, where $\Phi = \alpha\Gamma'\alpha^{-1}\cap\Gamma$, $\Phi^\alpha = \alpha^{-1}\Phi\alpha$ and $\mathrm{Tr}_{\Gamma'/\Phi^\alpha} = [\Gamma' 1_2 \Phi^\alpha]$ for $1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This can be checked as follows. Note that

$$\Gamma' = \bigcup_i \Phi^\alpha\delta_i \quad\Rightarrow\quad \alpha^{-1}\Gamma\alpha\Gamma' = \bigcup_i \alpha^{-1}\Gamma\alpha\delta_i \quad\Rightarrow\quad \Gamma\alpha\Gamma' = \bigcup_i \Gamma\alpha\delta_i.$$

Moreover if the first decomposition is disjoint, then the other two are also disjoint. Then by definition, it is clear that $[\Gamma\alpha\Gamma'] = \mathrm{Tr}_{\Gamma'/\Phi^\alpha}\circ[\Phi\alpha\Phi^\alpha]\circ\mathrm{res}_{\Gamma/\Phi}$.

Exercise 1. Give a detailed proof of $[\Gamma\alpha\Gamma'] = \mathrm{Tr}_{\Gamma'/\Phi^\alpha}\circ[\Phi\alpha\Phi^\alpha]\circ\mathrm{res}_{\Gamma/\Phi}$.

We now construct the corresponding morphism of sheaves. The operator $[\Phi\alpha\Phi^\alpha]$ is easy to take care. We write $Y(\Phi)$ for $\Phi\backslash\mathcal{H}$. Then the map

$$\alpha_* : \mathcal{H}\times M \ni (z,m) \mapsto (\alpha^{-1}(z),\alpha^1 m) \in \mathcal{H}\times M$$

induces a morphism $\alpha_* : \underline{M}_{/Y(\Phi)} \to \underline{M}_{/Y(\Phi^\alpha)}$ because

$$\alpha_*(\gamma(z,m)) = \alpha^{-1}\gamma\alpha\alpha_*(z,m).$$

Thus we have $[\Phi\alpha\Phi^\alpha] : H^1_*(Y(\Phi),\underline{M}) \to H^1_*(Y(\Phi^\alpha),\underline{M})$. The restriction map is induced from the projection $\underline{M}_{/Y(\Phi)} \to \underline{M}_{/Y(\Gamma)}$. Now we define the trace operator. Since the projection $\pi : Y(\Phi^\alpha) \to Y(\Gamma')$ is étale (i.e. it is a local homeomorphism), for each small open set U in a simply connected open set in $Y(\Gamma')$, $\pi^{-1}(U)$ is a disjoint union of open sets each isomorphic to U. Thus taking an open subset U_0 in $\mathcal{H}$ isomorphically projected down to U, we know that $\pi_*\underline{M}(U) \cong M(U_0)^{[\Gamma':\Phi^\alpha]}$. This isomorphism is given as follows. We may identify $\pi^{-1}(U)$ with the image of the disjoint union $\bigcup_i\delta_i(U_0)$ for a disjoint decomposition $\Gamma' = \bigcup_i\Phi^\alpha\delta_i$. Then we identify $\underline{M}(\delta_i(U_0)) = M$ with $\underline{M}(U_0) = M$ by $\underline{M}(\delta_i(U_0)) \ni x \mapsto \delta_i^1 x \in \underline{M}(U_0) = \underline{M}(U)$. Now it is clear that

$$\pi_*\underline{M}_{/Y(\Gamma')} = \Gamma'\backslash(\mathcal{H}\times \mathrm{Ind}_{\Gamma'/\Phi^\alpha}(M)),$$

where $\mathrm{Ind}_{\Gamma'/\Phi^\alpha}(M)$ is the induced module $M\otimes_{Z[\Phi^\alpha]}Z[\Gamma']$ with the Γ'-action given by $\gamma(m\otimes a) = m\otimes a\gamma^1$. Since the direct image of a flabby sheaf is flabby by definition and π_* is an exact functor because π is a local homeomorphism, any flabby resolution of $\underline{M}_{/Y(\Phi^\alpha)}$ gives rise to a flabby resolution of $(\pi_*\underline{M})_{/Y(\Gamma')}$ just by applying π_*. Thus we know that $H^i_*(Y(\Gamma'),\pi_*\underline{M}) = H^i_*(Y(\Phi^\alpha),\underline{M})$. This gives in particular a proof of Shapiro's lemma in group cohomology asserting that for any pair of groups $G \supset H$ and H-module M

$$H^i(G,\mathrm{Ind}_{G/H}(M)) = H^i(H,M). \tag{3}$$

Now we define $\mathrm{Tr} : \pi_*\underline{M}_{/Y(\Gamma')}(U) \to \underline{M}(U)_{/Y(\Gamma')}$ by $\mathrm{Tr}(x) = \sum_i \delta_i{}^t x$, which induces a morphism of sheaves. Obviously this is induced from the map $\mathrm{tr} : \mathbf{Z}[\Gamma'] \to \mathbf{Z}[\Phi^\alpha]$:

$$\mathrm{Tr} = \mathrm{id}\otimes\mathrm{tr} : \mathrm{Ind}_{\Gamma'/\Phi^\alpha}(M) = M\otimes_{\mathbf{Z}[\Phi^\alpha]}\mathbf{Z}[\Gamma'] \to M.$$

Then Tr induces a map of cohomology groups:

$$\mathrm{Tr} : H^i_*(Y(\Phi^\alpha),\underline{M}) = H^i_*(Y(\Gamma'),\pi_*\underline{M}) \to H^i_*(Y(\Gamma'),\underline{M}).$$

We define $[\Gamma\alpha\Gamma'] : H^i(Y(\Gamma),M) \to H^i(Y(\Gamma'),\underline{M})$ by $\mathrm{Tr}_{\Gamma'/\Phi^\alpha}\circ[\Phi\alpha\Phi^\alpha]\circ\mathrm{res}_{\Gamma/\Phi}$. It is tautological to check that this action of the Hecke ring is compatible with the canonical isomorphisms between sheaf cohomology and group cohomology.

Let us now assume that M is also an A-module for a commutative ring A. Then, writing M^* for the A-dual of M, we have a pairing by the cup product

$$\langle\ ,\ \rangle_\Gamma\ :\ H^1_c(Y,M)\otimes H^1(Y,M^*) \to H^2_c(Y,A) = A \quad (Y = Y(\Gamma) = \Gamma\backslash\mathcal{H}).$$

First we suppose that A is a $\mathbf{Q}$-algebra. Then this pairing is non-degenerate (for example, extending scalars to $\mathbf{C}$ and then it is clear for $M = L(n,v;\mathbf{C}) = M^*$ (see (2.3a)); see [Bd,II.7] for a proof in general). We have a commutative diagram for a subgroup Φ of Γ,

$$\begin{array}{ccc}
\mathrm{Ind}_{\Gamma/\Phi}(M\otimes_A M^*) & & \\
\| & \searrow \langle\ ,\ \rangle & \\
\langle\ ,\ \rangle : \mathrm{Ind}_{\Gamma/\Phi}(M)\otimes_A M^* & \to & A[\Phi\backslash\Gamma] \\
\downarrow \mathrm{Tr}\otimes\mathrm{id} & & \downarrow \mathrm{Tr} \\
\langle\ ,\ \rangle : M\otimes_A M^* & \longrightarrow & A.
\end{array}$$

Note that $\mathrm{Tr} : A[\Phi\backslash\Gamma] \to A$ induces an identity on

$$A = H^1_c(Y(\Phi),A) = H^1_c(Y(\Gamma),A[\Phi\backslash\Gamma]) \to H^1_c(Y(\Gamma),A) = A.$$

This is an easy consequence of Proposition 1.1 and its proof. Then the above diagram induces another commutative diagram:

$$\begin{array}{ccc}
\langle\ ,\ \rangle\ :\ H^i_c(Y(\Phi),\underline{M})\otimes H^{2-i}(Y(\Phi),\underline{M^*}) & \to & A \\
\uparrow \mathrm{id}\otimes\mathrm{res} & & \| \\
\langle\ ,\ \rangle\ :\ H^i_c(Y(\Phi),\underline{M})\otimes H^{2-i}(Y(\Gamma),\underline{M^*}) & \to & A \\
\downarrow \mathrm{Tr}\otimes\mathrm{id} & & \| \\
\langle\ ,\ \rangle\ :\ H^i_c(Y(\Gamma),\underline{M})\otimes H^{2-i}(Y(\Gamma),\underline{M^*}) & \to & A.
\end{array}$$

We thus have

(4a) $$\langle \mathrm{Tr}_{\Gamma/\Phi}(x),y\rangle_\Gamma = \langle x,\mathrm{res}_{\Gamma/\Phi}(y)\rangle_\Phi \quad \text{if } \Gamma \supset \Phi.$$

We see easily that

(4b) $$\langle x \mid [\Phi\alpha\Phi^{\alpha}], y\rangle_{\Phi\alpha} = \langle x, y \mid [\Phi^{\alpha}\alpha^{*}\Phi]\rangle_{\Phi} \text{ for } \Phi^{\alpha} = \alpha^{-1}\Phi\alpha.$$

In particular, when $M = L(n,\chi;A)$, we identify M^* with the dual lattice under $\langle\ ,\ \rangle$ in $L(n,\chi^{-1};A\otimes\mathbf{Q})$. From (2.2c), $\langle\alpha x,y\rangle = \langle x,\alpha^{\iota}y\rangle$, we see that

(4c) $$\langle x \mid [\Phi\alpha\Phi^{\alpha}], y\rangle_{\Phi\alpha} = \langle x, y \mid [\Phi^{\alpha}\alpha^{\iota}\Phi]\rangle_{\Phi} \text{ for } \Phi^{\alpha} = \alpha^{-1}\Phi\alpha.$$

This implies, for $x \in H^{i}_{c}(Y(\Gamma),\underline{M})$ and $y \in H^{2-i}(Y(\Gamma'),\underline{M^*})$,

(4d) $$\langle x \mid [\Gamma\alpha\Gamma'], y\rangle_{\Gamma'} = \langle x, y \mid [\Gamma'\alpha^{\iota}\Gamma]\rangle_{\Gamma}.$$

Now we specialize our argument to the case where $M = L(n,\chi;A)$. We write $L^*(n,\chi^{-1};A)$ for the dual module in $L(n,\chi^{-1};A\otimes\mathbf{Q})$ under $\langle\ ,\ \rangle$. It is easy to see from (2.2a) that

(5) $$L^*(n,\chi^{-1};A) = \textstyle\sum_{i=0}^{n} A\binom{n}{i}X^{n-i}Y^{i} \text{ in } L(n,\chi^{-1};A).$$

Since $\Gamma_0(N)\alpha^{\iota}\Gamma_0(N) = \tau\Gamma_0(N)\alpha\Gamma_0(N)\tau^{-1}$ for $\tau = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$, if we modify the pairing $\langle\ ,\ \rangle$ and define a new one $(\ ,\ )$ by

(6a) $$(x,y) = \langle x \mid \tau, y\rangle,$$

we have

(6b) $$(x \mid T(n), y) = (x, y \mid T(n)).$$

Since $(\ ,\ )$ is non-degenerate for any field of characteristic 0, we see from Theorem 5.3.2 and the Eichler-Shimura isomorphism

Theorem 5. *Suppose that either* χ *is primitive modulo* p^{α} *or* $\alpha = 0$. *Then* $H^1_c(Y_0(p^{\alpha}),\mathcal{L}(n,\chi;K))$, $H^1_P(Y_0(p^{\alpha}),\mathcal{L}(n,\chi;K))$ *and* $H^1(Y_0(p^{\alpha}),\mathcal{L}(n,\chi;K))$ *are all semi-simple Hecke modules provided that* K *is a field of characteristic* 0.

Proof. Let K/F be a field extension of characteristic 0. Then the assertion for K is equivalent to that for F. If the result is known for $K = \mathbf{Q}$, then the assertion is true for all fields of characteristic 0 by extending scalars to K. To prove the assertion for $K = \mathbf{Q}$, extending scalars to $\mathbf{C}$, we may assume that $K = \mathbf{C}$. By Theorem 5.3.2 and the Eichler-Shimura isomorphism (Theorems 1-4), we know that the assertion for H^1_P and H^1. Then the assertion for the compact supported cohomology group follows from the duality (6b) compatible with the Hecke module structure on H^1.

We continue to study the Hecke module structure of cohomology groups. We know that the following isomorphisms of Hecke modules:

$$\mathcal{M}_k(\Gamma_0(p^\alpha),\chi;K) \cong \mathrm{Hom}_K(\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;K),K),$$
$$\mathcal{S}_k(\Gamma_0(p^\alpha),\chi;K) \cong \mathrm{Hom}_K(\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K),K).$$

Since $\mathcal{S}_k(\Gamma_0(p^\alpha),\bar{\chi};K^c)^c \cong \mathcal{S}_k(\Gamma_0(p^\alpha),\chi;K)$ as Hecke modules via $\bar{f} \leftrightarrow f$,

$$H^1_P(\Gamma_0(p^\alpha),L(n,\chi;K)) \cong \mathrm{Hom}_K(\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K),K)^2.$$

Since $\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)$ is semi-simple, we know that

(7) $\mathrm{Hom}_K(\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K),K) \cong \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)$ as Hecke modules,

because any semi-simple algebra S over K is self-dual under the pairing $(x,y) = \mathrm{Tr}_{K/Q}(xy)$. Thus $H^1_P(\Gamma_0(p^\alpha),L(n,\chi;K))$ is free of rank two over $\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)$. Thus we have

Corollary 2. *Suppose that* K *is a field of characteristic* 0 *and* χ *is a primitive character modulo* p^α. *Then* $H^1_P(\Gamma_0(p^\alpha),L(n,\chi;K))$ *is free of rank two over the Hecke algebra* $\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)$. *Moreover, we have the following isomorphisms as Hecke modules: if either* $\chi \neq \mathrm{id}$ *or* $k > 2$

$$H^1(\Gamma_0(p^\alpha),L(n,\chi;K)) \cong H^1_c(\Gamma_0(p^\alpha),L(n,\chi;K))$$
$$\cong \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)\oplus\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;K)$$

and if $\chi = \mathrm{id}$ *and* $k = 2$

$$H^1(SL_2(\mathbf{Z}),K) \cong H^1_c(SL_2(\mathbf{Z}),K) \cong \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)^2 = \{0\}.$$

Since $\mathcal{M}_k(\Gamma_0(p^\alpha),\chi;K) \cong \mathrm{Hom}_K(\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;K),K) \cong \mathbf{H}_k(\Gamma_0(p^\alpha),\chi;K)$ and $\mathcal{S}_k(\Gamma_0(p^\alpha),\chi) \cong \mathrm{Hom}_K(\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K),K) \cong \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)$ as Hecke module and since these Hecke algebras are all semi-simple, we see that

(8) $$\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;K) \cong \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)\oplus\mathbf{E}_k(\Gamma_0(p^\alpha),\chi;K)$$

for an algebra direct summand $\mathbf{E}_k(\Gamma_0(p^\alpha),\chi;K)$. Let E be the idempotent of $\mathbf{E}_k(\Gamma_0(p^\alpha),\chi;K)$ in $\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;K)$. To get each of the following exact sequences in one line, we drop $\Gamma_0(p^\alpha)$ from the notation of the following cohomology groups in (9b,c) and (10) and also denote by H_s^i for the i-th cohomology group for $\Gamma_0(p^\alpha)_s$ $(s \in S)$. Then the exact sequences of Hecke modules

(9a) $0 \to \mathcal{S}_k(\Gamma_0(p^\alpha),\chi;K) \xrightarrow{\iota} \mathcal{M}_k(\Gamma_0(p^\alpha),\chi;K) \to \mathrm{Coker}(\iota) \to 0,$

(9b) $0 \to H^1_P(L(n,\chi;K)) \to H^1(L(n,\chi;K)) \to \oplus_{s\in S}H_s{}^1(L(n,\chi;K)) \to 0,$

(9c) $0 \to \oplus_{s\in S}H_s{}^0(L(n,\chi;K)) \to H^1_c(L(n,\chi;K)) \to H^1_P(L(n,\chi;K)) \to 0,$

are all split as Hecke modules by the idempotent E unless $\chi = \mathrm{id}$ and $k = 2$ for the last two sequences. In the special case of $\chi = \mathrm{id}$ and $k = 2$, we have

$$\text{(9d)} \qquad H^1(SL_2(\mathbf{Z}),K) \cong H^1_c(SL_2(\mathbf{Z}),K) \cong H^1_P(SL_2(\mathbf{Z}),K).$$

Now we consider the action of $j = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ on $H^1_P(\Gamma_0(p^\alpha),L(n,\chi,K))$. Since j normalizes $\Gamma_0(p^\alpha)$, j acts on $H^1_P(\Gamma_0(p^\alpha),L(n,\chi,K))$ via $[\Gamma_0(p^\alpha)j\Gamma_0(p^\alpha)]$. Then $j^2 = 1$. Since $j\{\alpha \in \Delta'' \mid \det(\alpha) = n\}j^{-1} = \{\alpha \in \Delta'' \mid \det(\alpha) = n\}$, j commutes with $T(n)$. Thus the eigenspaces of j

$$\text{(10)} \qquad H^1_P(L(n,\chi,K))^{\pm} = \{x \in H^1_P(L(n,\chi,K)) \mid x \mid j = \pm(-1)^{n+1}x\}$$

is naturally a Hecke module. When $K = \mathbf{C}$, we see that the action of j is given by $\omega \mapsto j^t(j^*\omega)$ at the level of differential forms. This is just interpreted in terms of modular forms as $f(z) \mapsto f(-\bar{z})$. Thus j brings holomorphic modular forms onto anti-holomorphic ones. Then the Krull-Schmidt theorem tells us that $H^1_P(\Gamma_0(p^\alpha),L(n,\chi,\mathbf{C}))^{\pm}$ is free of rank one over $\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;\mathbf{C})$. By the semi-simplicity of $\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K)$, the same assertion is true for all fields K of characteristic 0. Thus we have, for all fields K of characteristic 0, that

$$\text{(11)} \qquad H^1_P(\Gamma_0(p^\alpha),L(n,\chi,K))^{\pm} \text{ is free of rank one over } \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;K).$$

§6.4. Algebraicity theorem for standard *L*-functions of GL(2)

In this section, we prove the algebraicity result for the Mellin transform of holomorphic modular forms which are called the standard L-functions of GL(2). In the following section, we construct the p-adic standard L-function of GL(2) attached to modular forms of weight $k \geq 2$. Thus, in the rest of this chapter, we fix a prime p and embeddings $\overline{\mathbf{Q}} \to \mathbf{C}$ and $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$. For simplicity, we only deal with modular forms in $\mathcal{S}_k(\Gamma_0(p^\alpha),\chi)$ for a primitive character χ modulo p^α. This restriction is caused by our neglecting to cover the theory of primitive (or new) forms of arbitrary level N. Since such theory is fully expounded in [M], it is strongly recommended to the reader to carry out our construction for primitive forms of arbitrary level (using the theory in [M]).

Here we understand that $\chi = \mathrm{id}$ and $\Gamma_0(p^0) = SL_2(\mathbf{Z})$ when $\alpha = 0$. As seen in Theorem 5.3.2, $\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;\mathbf{C})$ is semi-simple, and $\mathcal{S}_k(\Gamma_0(p^\alpha),\chi)$ is spanned by common eigenforms of all Hecke operators $T(n)$. Let f be one of these common eigenforms. We also know that, if we take the $\mathbf{Q}(\chi)$-algebra homomorphism $\lambda : \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;\mathbf{Q}(\chi)) \to \mathbf{C}$ given by $f \mid T(n) = \lambda(T(n))f$, then f

is a constant multiple of $\sum_{n=1}^{\infty}\lambda(T(n))q^n$. The form f with $a(n,f) = \lambda(T(n))$ is called a normalized eigenform. We fix such a λ and its normalized eigenform f. We write $\mathbf{Q}(\lambda)$ (resp. $\mathbf{Q}_p(\lambda)$) for the subfield of $\overline{\mathbf{Q}}$ (resp. $\overline{\mathbf{Q}}_p$) generated by $\lambda(T(n))$ for all n over $\mathbf{Q}$ (resp. $\mathbf{Q}_p$). Let $\mathcal{O}$ be the p-adic integer ring of $\mathbf{Q}_p(\lambda)$ and put $\mathcal{V} = \mathcal{O}\cap\mathbf{Q}(\lambda)$. By Theorem 3.2, the field $\mathbf{Q}(\lambda)$ (resp. $\mathbf{Q}_p(\lambda)$) is a finite extension of $\mathbf{Q}$ (resp. $\mathbf{Q}_p$). We now consider a new compactification X^* of $Y = \Gamma_0(p^\alpha)\backslash\mathcal{H}$. Since $\Gamma_s\backslash\mathcal{H}$ is a cylinder isomorphic to the space T in §4.1, we add to Y a circle S^1 at each cusp $s \in S$ as we did in §4.1 for T at $i\infty$ and write this compactification X^*. This type of compactification is called the Borel-Serre compactification of Y. Then for each $r \in \mathbf{Q}$, the vertical line c^r connecting r and the cusp ∞ is a relative cycle in $H^1(X^*,\partial X^*;\mathbf{Z})$, where $\partial X^* = \bigcup_{s\in S}S^1$. Identifying c^r with $\mathbf{R}_+ = \{x \in \mathbf{R} \mid x > 0\}$, we then have a natural morphism induced from $\mathbf{R}_+ = c^r \to X$,

$$(1) \qquad \mathrm{Int}_r : H^1_c(Y,\mathcal{L}(n,\chi;A)) \to H^1_c(\mathbf{R}_+,\mathcal{L}(n,\chi;A)) = L(n;A).$$

This morphism is realized by the integration $\omega \mapsto \int_{c^r}\omega$ for closed forms ω. When $\Gamma_0(p^\alpha)$ has non-trivial torsion, we just take a normal subgroup Γ of finite index of $\Gamma_1(p^\alpha)$ and we define $H^1_c(Y,\mathcal{L}(n,\chi;A))$ to be the image of the restriction map in $H^1_c(\Gamma\backslash\mathcal{H},\mathcal{L}(n;A))[\chi]$.

We have a natural surjection $\pi : H^1_c(Y,\mathcal{L}(n,\chi;A)) \to H^1_P(Y,\mathcal{L}(n,\chi;A))$. We want to show that there exists a section (defined over $K = A\otimes_{\mathbf{Z}}\mathbf{Q}$) $\iota : H^1_P(Y,\mathcal{L}(n,\chi;A)) \to H^1_c(Y,\mathcal{L}(n,\chi;K))$ which is compatible with Hecke operators. We already know from (3.8) that π has a unique section of Hecke modules if A is a $\mathbf{Q}$-algebra. Now we let A be a subalgebra of $\overline{\mathbf{Q}}$ or $\overline{\mathbf{Q}}_p$ containing the integer ring of $\mathbf{Q}(\lambda)$ and write K for the quotient field of A. Thus writing E for the idempotent of the Eisenstein part $\mathbf{E}_k(\Gamma_0(p^\alpha),\chi;A)$ in $\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;A)$, we can find $0 \neq \eta \in A$ such that $\eta E \in \mathbf{H}_k(\Gamma_0(p^\alpha),\chi;A)$. Since the splitting of π over K is given by this E (3.8c), we know that $\iota = 1\text{-}E$: $H^1_P(Y,\mathcal{L}(n,\chi;A)) \to H^1_c(Y,\mathcal{L}(n,\chi;K))$ satisfies $\pi\circ\iota = \mathrm{id}$, and $\eta\circ\iota$ has values in $H^1_c(Y,\mathcal{L}(n,\chi;A))$. Now suppose that A is a principal ideal domain. We put

$$H^1_P(Y,\mathcal{L}(n,\chi;A))^{\pm}[\lambda] = \{x \in H^1_P(Y,\mathcal{L}(n,\chi;A))^{\pm} \mid x \mid T(n) = \lambda(T(n))x\}.$$

Then this module is free of rank one over A because its scalar extension to K is free of rank one over K (3.10). Now we choose a generator $\delta_{\pm}(\lambda)$ of the above A-module. Now we define a complex quantity (called a canonical period)

$\Omega^{\pm}(\lambda) = \Omega^{\pm}_{A}(\lambda) \in \mathbf{C}^{\times}$ as follows. For $f = \sum_{n=1}^{\infty} \lambda(T(n))q^n \in \mathcal{S}_k(\Gamma_0(p^{\alpha}),\chi)$, define

$$\omega_{\pm}(\lambda) = \frac{\omega(f)\pm(-1)^{n+1}\omega(f)\,|\,j}{2}.$$

Then $0 \neq \omega_{\pm}(\lambda) \in H^1_P(Y,\mathcal{L}(n,\chi;\mathbf{C}))^{\pm}[\lambda]$, and we define $\Omega^{\pm}(\lambda) = \Omega^{\pm}_{A}(\lambda)$ by

$$\omega_{\pm}(\lambda) = \Omega^{\pm}(\lambda)\delta_{\pm}(\lambda). \tag{2}$$

For each field automorphism σ of $\mathbf{C}$, we always agree to choose $\delta_{\pm}(\lambda^{\sigma})$ to be $\delta_{\pm}(\lambda)^{\sigma}$, where $\lambda^{\sigma} : \mathbf{h}_k(\Gamma_0(p^{\alpha}),\chi^{\sigma};\mathbf{Q}(\chi)) \to \mathbf{C}$ is the $\mathbf{Q}(\chi^{\sigma})$-algebra homomorphism given by $\lambda^{\sigma}(T(n)) = \lambda(T(n))^{\sigma}$ for all n. Anyway the period $\Omega^{\pm}(\lambda)$ is determined up to units in A. We just fix one so that the above compatibility condition holds for the Galois action. Since $\omega_{\pm}(\lambda)$ is exponentially decreasing at each cusp, we know that

$$\mathrm{Int}_r(\iota(\omega_{\pm}(\lambda))) = \int_{c_r}\omega_{\pm}(\lambda) = \Omega^{\pm}(\lambda)\mathrm{Int}_r(\iota(\delta(\lambda))) \in \Omega^{\pm}(\lambda)L(n;K). \tag{3a}$$

Note that

$$\frac{\eta\mathrm{Int}_r(\iota(\omega_{\pm}(\lambda)))}{\Omega^{\pm}(\lambda)} \in L(n;A). \tag{3b}$$

Exercise 1. Give a detailed proof of (3a).

Now we compute the value (3b). Note that

$$\omega_{\pm}(\lambda) = 2^{-1}(2\pi\sqrt{-1})(f(z)(X-zY)^n dz \pm f(-\bar{z})(X-\bar{z}Y)^n d\bar{z}).$$

This shows that

$$\begin{aligned}\mathrm{Int}_0(\omega_{\pm}(\lambda)) &= 2^{-1}i^{j+1}(2\pi i)\sum_{j=0}^{n}\binom{n}{j}\{(-1)^{j+1}\pm 1\}\int_0^{\infty}\sum_n \lambda(T(n))\exp(-2\pi y)y^j dy \\ &= -2^{-1}\sum_{j=0}^{n}\binom{n}{j}\{1\pm(-1)^j\}j!(-2\pi i)^{-j}L(j+1,\lambda).\end{aligned}$$

This shows in particular that $\binom{n}{j}\dfrac{j!L(1+j,\lambda)}{(-2\pi i)^j\Omega^{\pm}(\lambda)} \in \eta^{-1}A$ for $j = 0,1,\ldots,n$, where the sign of $\Omega^{\pm}(\lambda)$ is given by the sign of $(-1)^j$. Let ψ be any primitive Dirichlet character modulo N. Then a computation similar to (4.1.6c) (see also Corollary 5.5.1) shows

$$\begin{aligned}&\sum_{j=1}^{N}\psi^{-1}(j)\begin{pmatrix}1 & -j/N\\ 0 & 1\end{pmatrix}\mathrm{Int}_{(j/N)}(\omega_{\pm}(\lambda)) \\ &\quad = -2^{-1}G(\psi^{-1})\sum_{j=0}^{n}\binom{n}{j}\{1\pm\psi(-1)(-1)^j\}j!(-2\pi\sqrt{-1})^{-j}L(j+1,\lambda\otimes\psi).\end{aligned}$$

This shows

Theorem 1. *Let* $\lambda : \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;\mathbf{Z}[\chi]) \to \mathbf{C}$ *be a* $\mathbf{Z}[\chi]$*-algebra homomorphism. Suppose that either* $\alpha = 0$ *or* χ *is primitive. Then for each Dirichlet character* ψ *and each integer* j *with* $0 \le j \le n$ $(n = k-2)$*, we have*

$$S(j,\lambda\otimes\psi) = \frac{G(\psi^{-1})j!L(j+1,\lambda\otimes\psi)}{(2\pi\sqrt{-1})^j\Omega^{\pm}_{\mathbf{Q}(\lambda)}(\lambda)} \in \overline{\mathbf{Q}},$$

and for every $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$,

$$S(j,\lambda\otimes\psi)^\sigma = S(j,\lambda^\sigma\otimes\psi^\sigma),$$

where the sign of $\Omega^{\pm}(\lambda)$ *is given by the sign of* $(-1)^j\psi(-1)$*. Moreover, the p-adic absolute value* $|S(j,\lambda\otimes\psi)|_p$ *is bounded independently of* ψ *and* j.

§6.5. Mazur's p-adic Mellin transforms

We are now ready to construct p-adic standard L-functions. Such L-functions were first constructed by Mazur for weight 2 forms in [Mz1] and [MzS]. It was then generalized to higher weight modular forms by Manin [Mn1,2]. For further study and conjectures concerning the materials here, we refer to the paper of Mazur, Tate and Teitelbaum [MTT]. We give an exposition of the construction using the method of modular symbols following the formulation in [Ki], which is quite similar to the one we have already given for abelian L-functions in §4.4.

We shall use the same notation introduced in the previous section. In particular, $\lambda : \mathbf{h}_k(\Gamma_0(p^\alpha),\chi;\mathbf{Z}[\chi]) \to \overline{\mathbf{Q}}$ is a $\mathbf{Z}[\chi]$-algebra homomorphism for a primitive character χ modulo p^α (we assume that $\chi = \mathrm{id}$ if $\alpha = 0$). Let $\mathcal{O}$ be the p-adic integer ring of $\mathbf{Q}_p(\lambda)$. We put $K = \mathbf{Q}(\lambda)$ and $A = \mathcal{O}\cap K$. Then A is a discrete valuation ring and $\Omega^{\pm}_A(\lambda)$ is well defined. We assume the following ordinarity condition necessary to have a good p-adic L-function of λ:

$$(\mathrm{Ord}_p) \qquad |\lambda(T(p))|_p = 1.$$

The algebra homomorphism satisfying this condition is called *"ordinary"* or *"p-ordinary"*. We can construct a standard "p-adic L-function" without assuming (Ord_p) (see [MTT]). However, the function obtained is not an Iwasawa function (i.e. is not of the form $\Phi(u^s-1)$ for a power series $\Phi \in \mathcal{O}[[T]]$).

For the moment, we assume that $\alpha > 0$. Recalling that c^r is the relative cycle represented by the vertical line from $r \in \mathbf{Q}$ to $i\infty$ on the Borel-Serre compactification X^* of $Y = \Gamma_0(p^\alpha)\backslash\mathcal{H}$, we consider the map

$$(1) \qquad c : p^{-\infty}\mathbf{Z} = \bigcup_{i=1}^{\infty} p^{-i}\mathbf{Z} \to \mathrm{Hom}_K(H^1_c(Y,\mathcal{L}(n,\chi;K)),L(n;K))$$

given by $c(r)(\omega) = \mathrm{Int}_r(\omega)$.

We define for each $\omega \in H^1_c(Y,\mathcal{L}(n,\chi;K))$, $c_\omega : p^{-\infty}\mathbf{Z} \to L(n;K)$ by

$$c_\omega(r) = \begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix} c(r)(\omega).$$

Then $c_\omega(r+1) = c_\omega(r)$ by definition, and c_ω factors through $\mathbf{Q}_p/\mathbf{Z}_p = p^{-\infty}\mathbf{Z}/\mathbf{Z}$. Supposing $\omega \mid T(p) = a_p\omega$ with $|a_p|_p = 1$, we define a distribution Φ_ω on $\mathbf{Z}_p^\times$ by

$$(2) \qquad \Phi_\omega(z+p^m\mathbf{Z}_p) = a_p^{-m}\begin{pmatrix} p^m & 0 \\ 0 & 1 \end{pmatrix} c_\omega\left(\frac{z}{p^m}\right) \text{ for } z = 1,2,\ldots \text{ prime to } p.$$

This is well defined because $c(r+1) = c(r)$. If we write $G = \mathbf{Z}_p^\times$ and fix an isomorphism $G \cong \mu\times\mathbf{Z}_p$ with a finite group μ, we see that

$$\mu = \{\zeta \in \mathbf{Z}_p^\times \mid \zeta^{\varphi(p)} = 1\}$$

where φ is the Euler function and $\mathbf{p} = 4$ or p according as $p = 2$ or not. Then the subgroup $G_\alpha = 1+p^\alpha\mathbf{p}\mathbf{Z}_p$ corresponds to $p^\alpha\mathbf{Z}_p$. Thus (2) is tantamount to giving the value of the distribution Φ_ω on the standard fundamental system of open sets. To show that Φ_ξ actually gives a distribution, we can check the distribution relation (4.3.3) in exactly the same manner as in §4.4:

$$\begin{aligned}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\sum_{j=1}^{p-1} c_\omega\left(\frac{x+j}{p}\right) &= \sum_j \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & (j-x)/p \\ 0 & 1 \end{pmatrix} c((j+x)/p)(\omega) \\ &= \sum_j \begin{pmatrix} p & -x+j \\ 0 & 1 \end{pmatrix} c((j+x)/p)(\omega) = \sum_j \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} p & j \\ 0 & 1 \end{pmatrix}^\iota c((j+x)/p)(\omega) \\ &= \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} c(x/p)(\omega \mid T(p)) = a_p c_\omega(x)\end{aligned}$$

and

$$\sum_{j=1}^{p-1} \Phi_\omega(x+jp^m+p^{m+1}\mathbf{Z}_p) = \Phi_\omega(x+p^m\mathbf{Z}).$$

This shows the necessity of assuming $|a_p|_p = 1$ to have a measure, not just a distribution. By a similar argument, we see that

$$(3) \quad |\Phi_\omega(z+p^m\mathbf{Z}_p)|_p = \left|a_p^{-m}\begin{pmatrix} p^m & 0 \\ 0 & 1 \end{pmatrix} c_\omega\left(\frac{z}{p^m}\right)\right|_p = \left|\begin{pmatrix} p^m & -z \\ 0 & 1 \end{pmatrix} \mathrm{Int}_{z/p^m}(\omega)\right|_p \text{ is}$$

bounded independent of z and m.

Thus Φ_ω is bounded, and by Proposition 4.3.2, we have a unique measure Φ_ω extending the distribution Φ_ω. Projecting down to the coefficient in $\binom{m}{j}X^{m-j}Y^j$

of Φ_ω, we get a measure $\varphi_{\omega,j}$. Now we want to show $d\Phi_{\omega,j}(x) = x^j d\varphi_{\omega,0}$. To show this, we may assume that ω is integral (i.e. ω has coefficients in $L(n,\chi;A)$) by multiplying ω by a constant if necessary). We follow the argument given in [Ki] which originates from Manin [Mn1,2]. For each $\phi \in \mathcal{C}(\mathbf{Z}_p^\times;A)$, take a locally constant function $\phi_k : (\mathbf{Z}/p^{n(k)}\mathbf{Z})^\times \to A$ such that $|\phi_k - \phi|_p < p^{-k}$ and $n(k) \geq k$. Then we know that

$$|\Phi_\omega(\phi_k) - \Phi_\omega(\phi)|_p < |\Phi_\omega|_p p^{-k} < p^{-k}$$

and
$$\begin{aligned}
\Phi_\omega(\phi_k) &= \sum_{z=1,\,(p,z)=1}^{p^{n(k)}-1} \phi_k(z) a_p^{-n(k)} \begin{pmatrix} p^{n(k)} & 0 \\ 0 & 1 \end{pmatrix} c_\omega\left(\frac{z}{p^{n(k)}}\right) \\
&= \sum_{z=1,\,(p,z)=1}^{p^{n(k)}-1} \phi_k(z) a_p^{-n(k)} \begin{pmatrix} p^{n(k)} & -z \\ 0 & 1 \end{pmatrix} c\left(\frac{z}{p^{n(k)}}\right)(\omega) \\
&= a_p^{-n(k)} \sum_{j=0}^{m} \sum_{z=1,\,(p,z)=1}^{p^{n(k)}-1} \phi_k(z)(X+zY)^{m-j}(p^{n(k)}Y)^j c_j\left(\frac{z}{p^{n(k)}}\right)(\omega) \\
&\equiv a_p^{-n(k)} \sum_{z=1,\,(p,z)=1}^{p^{n(k)}-1} \phi_k(z)(X+zY)^m c_0\left(\frac{z}{p^{n(k)}}\right)(\omega) \bmod p^k \\
&\equiv \sum_{j=0}^{m} \int \phi(z) z^j d\varphi_{\omega,0}(z) \binom{m}{j} X^{m-j}Y^j \bmod p^k,
\end{aligned}$$

where c_j is the coefficient of c in $X^{n-j}Y^j$. Thus taking the limit making $k \to \infty$, we see that

$$\int \phi\, d\varphi_{\omega,j} = \int \phi(z) z^j d\varphi_{\omega,0}(z) \quad \text{for all } \phi \in \mathcal{C}(\mathbf{Z}_p^\times;K). \tag{4}$$

Now we take $\omega = \iota(\delta_\pm(\lambda))$. Then we write Φ_ω as $\Phi^\pm = \Phi^\pm_\lambda$ and compute the integral $\int \phi\, d\Phi^\pm$ for each primitive character ϕ of $(\mathbf{Z}/p^r\mathbf{Z})^\times$. We see that

$$\begin{aligned}
(5) \quad \int \phi\, d\Phi^\pm &= \sum_{x \in (\mathbf{Z}/p^r\mathbf{Z})^\times} \phi(x) \lambda(T(p))^{-r} \begin{pmatrix} p^r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x/p^r \\ 0 & 1 \end{pmatrix} \int_{c(x/p^r)} \delta_\pm(\lambda) \\
&= \lambda(T(p))^{-r} \begin{pmatrix} p^r & 0 \\ 0 & 1 \end{pmatrix} \int_{c0} \sum_{x \in (\mathbf{Z}/p^r\mathbf{Z})^\times} \phi(x) \begin{pmatrix} 1 & -x/p^r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x/p^r \\ 0 & 1 \end{pmatrix}^* \delta_\pm(\lambda) \\
&= \lambda(T(p))^{-r} \begin{pmatrix} p^r & 0 \\ 0 & 1 \end{pmatrix} \Omega^\pm(\lambda)^{-1} G(\phi) \int_{c0} \omega_\pm(\lambda) \\
&= -2^{-1}\lambda(T(p))^{-r} G(\phi) \Omega^\pm(\lambda)^{-1} \sum_{j=0}^{n} \binom{n}{j} \{1 \pm \phi(-1)(-1)^j\} j!(-2\pi i)^{-j} p^{jr} L(j+1, \lambda\otimes\phi^{-1}).
\end{aligned}$$

Thus projecting down to the coefficient in $\binom{m}{j}X^m$ of $-\Phi^{\pm}$, we get by (4) a measure $\varphi^{\pm} = \varphi_{\lambda}^{\pm}$ satisfying, for all characters $\phi : (\mathbf{Z}/p^r\mathbf{Z})^{\times} \to K^{\times}$,

(6) $$\int \phi(z)z^j d\varphi^{\pm}(z) = \lambda(T(p))^{-r}p^{rj}\frac{G(\phi)L(1+j,\lambda\otimes\phi^{-1})}{(-2\pi i)^j\Omega^{\pm}(\lambda)} \quad \text{if } 0 < j < k-1$$

and $\phi(-1)(-1)^j$ has the same sign as that of $\varphi^{\pm}$, and $\int \phi(z)z^j d\varphi^{\pm}(z) = 0$ if the sign of $\phi(-1)(-1)^j$ does not match.

Now we suppose that $\alpha = 0$. By the ordinarity assumption, we know that one of the roots of $X^2-\lambda(T(p))X+p^{k-1} = 0$, say a, is a p-adic unit and the other one is non-unit, because $k \geq 2$. We write b for the other root. Then we define $f'(z) = f(z)-bf(pz)$ for $f = \sum_{n=1}^{\infty}\lambda(T(n))q^n$. Then $f' \in \mathcal{S}_k(\Gamma_0(p))$. It is easy to verify that $f' \mid T(p) = af'$ and $f' \mid T(n) = \lambda(T(n))f'$ for all n prime to p.

Exercise 1. Give a detailed proof of the above fact. (Note the $T(p)$ of level 1 and $T(p)$ of level p are different.)

We now use $\omega = \delta'_{\pm}(\lambda) = \Omega^{\pm}(\lambda)^{-1}\omega(f')$ to construct a measure. By the same computation, we get for each integer j with $0 < j < k-1$

(7) $$\int \phi(z)z^j d\varphi^{\pm}(z) = a^{-r}p^{rj}\frac{G(\phi)(1-b\phi^{-1}(p)p^{-1-j})L(1+j,\lambda\otimes\phi^{-1})}{(-2\pi i)^j\Omega^{\pm}(\lambda)}$$ if the sign of $\phi(-1)(-1)^j$ is equal to the sign of $\varphi^{\pm}$, and $\int \phi(z)z^j d\varphi^{\pm}(z) = 0$ if the sign of $\phi(-1)(-1)^j$ does not match the sign of $\varphi^{\pm}$.

Summing up all these discussions, we get

Theorem 1. *Let* p *be a prime, and* $\lambda : \mathbf{h}_k(\Gamma_0(p^{\alpha}),\chi;\mathbf{Z}[\chi]) \to \overline{\mathbf{Q}}$ *be a* $\mathbf{Z}[\chi]$*-algebra homomorphism for a primitive character* χ *modulo* p^{α} *(we allow that* $\chi = \mathrm{id}$ *if* $\alpha = 0$*). Then we have two p-adic measures* $\varphi_{\lambda}^{\pm}$ *on* $\mathbf{Z}_p^{\times}$ *satisfying the evaluation formulas in (6) and (7).*

We now define the p-adic L-function for λ and a primitive character ψ modulo p^{β} as follows. We take the transcendental factor either $\Omega_A^{+}(\lambda)$ or $\Omega_A^{-}(\lambda)$ according to the sign of $\psi(-1)$. We also take the measure either φ_{λ}^{+} or φ_{λ}^{-} again according to $\psi(-1)$. We write our choice of $\Omega^{\pm}$ (resp. $\varphi^{\pm}$) as Ω^{ψ} (resp. φ_{ψ}). Then we define

$$L_p(s,\lambda\otimes\psi) = \int_{\mathbf{Z}_p^{\times}}\psi^{-1}(z)\langle z\rangle^{s-1}d\varphi_{\psi}.$$

Corollary 1. *Let the notation be as above. In particular, let* ψ *be a primitive character modulo* p^{β}. *Let* $\lambda : \mathbf{h}_k(\Gamma_0(p^{\alpha}),\chi;\mathbf{Z}[\chi]) \to \overline{\mathbf{Q}}$ *for* $k \geq 2$ *be a* $\mathbf{Z}[\chi]$-*algebra homomorphism for a primitive character* χ *modulo* p^{α}. *Then we have an evaluation formula: if either* $\alpha > 0$ *or* $\beta > 0$, *then*

$$L_p(1+j,\lambda\otimes\psi) = \lambda(T(p))^{-r}p^{rj}\frac{G(\psi^{-1}\omega^{-j})L(1+j,\lambda\otimes\psi\omega^{j})}{(-2\pi i)^{j}\Omega^{\psi}(\lambda)};$$

if $\alpha = \beta = 0$, *then*

$$L_p(1+j,\lambda\otimes\psi) = a^{-r}p^{rj}\frac{G(\omega^{-j})(1-\omega^{-j}(p)ap^{-1-j})L(1+j,\lambda\otimes\omega^{j})}{(-2\pi i)^{j}\Omega^{+}(\lambda)},$$

where a *is the unique p-adic unit root of the equation* $X^2-\lambda(T(p))X+p^{k-1}$.

For further study of this type of p-adic L-functions, see [Ki] and [GS].

Chapter 7. Ordinary Λ-adic forms, two variable p-adic Rankin products and Galois representations

A typical problem of p-adic number theory is the problem of p-adic interpolation, which can be stated as follows:

For a given complex analytic function f(s) *whose values at infinitely many integer points* k *are algebraic numbers, is there some* p*-adically convergent power series* F(s) *(with coefficients in a* p*-adic field) of* p*-adic variable* s *such that* F(k) = f(k) *for all integers* k *such that* f(k) *is algebraic?*

Many successful answers to this problem have already been discussed in Chapters 3, 4 and 6. Instead of taking complex analytic functions, we take complex analytic modular forms here and consider the problem of p-adic interpolation. We present, in this chapter and Chapter 10, some recent developments in the theory of p-adic modular forms, in particular, (i) p-adic analytic parametrization of classical modular forms, (ii) p-adic L-functions attached to each p-adically parametrized family of modular forms and (iii) Galois representations of these families of modular forms. Let us briefly explain what the p-adic family of modular forms is. As already studied in Chapter 2, a typical example of modular forms is given by the absolutely convergent Eisenstein series (see Chapter 5):

$$E_k(z) = 2^{-1}\zeta(1-k) + \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n \quad (k > 2),$$

where $\sigma_m(n) = \sum_{0<d\,|\,n} d^m$ is the sum of m-th powers of divisors of n. We modify $\sigma_{k-1}(n)$ by removing the (k-1)-th powers of the divisors d divisible by p. Then the modified coefficient $\sigma^{(p)}{}_{k-1}(n) = \sum_{0<d\,|\,n,(d,p)=1} d^{k-1}$ depends p-adic continuously on the weight k; in fact,

$$\text{if } k \equiv k' \equiv 0 \bmod p^{\alpha-1}(p-1), \quad \text{then } \sigma^{(p)}{}_{k-1}(n) \equiv \sigma^{(p)}{}_{k'-1}(n) \mod p^{\alpha}.$$

Thus for a fixed integer n, we can consider the function $k \mapsto \sigma^{(p)}{}_{k-1}(n)$ as the restriction of a continuous function $\sigma^{(p)}{}_{s-1}(n)$ of the variable s which varies in the p-adic integer ring $\mathbf{Z}_p$. Actually, this dependence on the weight k is p-adic analytic; that is, the continuous function which induces $s \mapsto \sigma^{(p)}{}_{s-1}(n)$ can be expanded at each $s \in \mathbf{Z}_p$ into a power series p-adically convergent on a neighborhood of s. Then the formal Fourier expansion

$$E(s) = 2^{-1}\zeta_p(1-s) + \sum_{n=1}^{\infty}\sigma^{(p)}{}_{s-1}(n)q^n$$

may be considered as a solution to the problem of p-adic interpolation for the Eisenstein series E_k, where $\zeta_p(s)$ is the p-adic Riemann zeta function given in Theorem 3.5.2. Note that $E(k) = E_k(z) - p^{k-1}E_k(pz)$ because of the modification to $\sigma^{(p)}{}_{k-1}(n)$ from $\sigma_{k-1}(n)$.

For the moment, let us define naively a p-adic family of modular forms $\{f_k\}$ to be an infinite set of modular forms parametrized by the weight k whose Fourier coefficients depend p-adic analytically on the weight k. Later, we shall give a more precise definition. In fact, in the case of $\{E_k\}$, the coefficients are integers and thus can be considered as complex numbers as well as p-adic numbers automatically. In the general case, the coefficients of f_k may not be just integers, and in fact there are many examples of such families with algebraic Fourier coefficients. With this general case in mind, we fix, once and for all, an algebraic closure $\overline{\mathbf{Q}}_p$ of the p-adic field $\mathbf{Q}_p$ and an embedding of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_p$. Thus we can discuss the p-adic analyticity of Fourier coefficients of f_k relative to k.

To each modular form $f = \sum_{n=0}^{\infty} a_n q^n$, we have associated in Chapter 5 an L-function $L(s,f) = \sum_{n=1}^{\infty} a_n n^{-s}$, and for each pair of modular forms f and $g = \sum_{n=0}^{\infty} b_n q^n$, we have another L-function $D(s,f,g) = \sum_{n=1}^{\infty} \bar{a}_n b_n n^{-s}$. Once such a p-adic family of modular forms $\{f_k\}$ is given, it is natural to ask the problem of p-adic interpolation of the values (or more precisely their algebraic part) of $\{L(m,f_k)\}$ and $\{D(m,f_k,f_l)\}$ by varying the weight k. We shall treat this problem for $D(s,f,g)$ later in this chapter and in Chapter 10 (as for the treatment for $L(m,f_k)$, see [Ki] and [GS]). As for the p-adic interpolation of Galois representations, often one can canonically attach a Galois representation π_k (of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$) into $GL_2(\overline{\mathbf{Q}}_p)$ to each element f_k in the family. Then we may also consider the problem of p-adic interpolation of the function $k \mapsto \pi_k(\sigma) \in M_2(\overline{\mathbf{Q}}_p)$ for any fixed $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. If one succeeds in interpolating the function $k \mapsto \pi_k(\sigma)$ for every σ, one may eventually obtain a big Galois representation into the matrix ring over the ring of analytic functions on $\mathbf{Z}_p$. We shall formulate this problem more clearly later, in §7.5.

§7.1. p-Adic families of Eisenstein series

Here, we study the p-adic family of modular forms given by Eisenstein series. We write Γ for $\Gamma_0(N)$ or $\Gamma_1(N)$. Since we have already fixed embeddings of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_p$ and $\mathbf{C}$, any algebraic number in $\overline{\mathbf{Q}}$ can be regarded as a complex number as well as a p-adic number. We fix a base ring $\mathcal{O}$, which is the p-adic integer ring of a finite extension of $\mathbf{Q}_p$. Sometimes we need to consider the completion Ω of $\overline{\mathbf{Q}}_p$ under $|\ |_p$ (which is known to be algebraically closed). We fix a character $\psi = \omega^a$ of $(\mathbf{Z}/\mathbf{p}\mathbf{Z})^\times$ ($\mathbf{p} = 4$ when $p = 2$ and $\mathbf{p} = p$ otherwise) for the Teichmüller character ω. We mean by a p-adic analytic family (of character ψ) an infinite set of modular forms $\{f_k\}_{k=M}^{\infty}$ for some positive integer M satisfying the following three conditions:

(Λ1) $f_k \in \mathcal{M}_k(\Gamma_0(\mathbf{p}),\psi\omega^{-k})$,

(Λ2) $a(n,f_k) \in \overline{\mathbf{Q}}$ *for all* n,

(Λ3) *there exists a power series* $A(n;X) \in \mathcal{O}[[X]]$ *for each* $n \geq 0$ *such that* $a(n,f_k) = A(n;u^k-1)$ *for all* $k \geq M$,

where $u = 1+\mathbf{p}$ (which is a topological generator of the multiplicative group $W = 1+\mathbf{p}\mathbf{Z}_p$). The family $\{f_k\}$ is called cuspidal if f_k is a cusp form for almost all k (i.e. except finitely many positive k). Note that $u^k-1 = (1+\mathbf{p})^k-1$ is always divisible by p, and hence $|u^k-1|_p < 1$. The convergence of $A(n;u^k-1)$ follows from this fact.

We now introduce the space of p-adic modular forms. First, we already know (see Theorem 5.2.1, Corollary 5.4.1, Theorem 6.3.2, Corollary 6.3.1) that if $k \geq 2$

(1) $$\mathcal{M}_k(\Gamma_0(\mathbf{p}p^\alpha),\chi) = \mathcal{M}_k(\Gamma_0(\mathbf{p}p^\alpha),\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}\mathbf{C} \text{ and}$$
$$\mathcal{M}_k(\Gamma_0(\mathbf{p}p^\alpha),\chi;A) = \mathcal{M}_k(\Gamma_0(\mathbf{p}p^\alpha),\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}A.$$

The assertion (1) holds for any subring A of $\mathbf{C}$ containing $\mathbf{Z}[\chi]$. Thus we can define the space $\mathcal{M}_k(\Gamma_0(\mathbf{p}p^\alpha),\chi;A)$ for any ring A (inside Ω or $\overline{\mathbf{Q}}_p$) by the right-hand side of (1). Since $\mathcal{M}_k(\Gamma_0(\mathbf{p}p^\alpha),\chi;\mathbf{Z}[\chi])$ is naturally embedded into the power series ring $\mathbf{Z}[\chi][[q]]$ via q-expansion, we can regard $\mathcal{M}_k(\Gamma_0(\mathbf{p}p^\alpha),\chi;A)$ as a subspace of the power series ring $A[[q]]$. For each $f \in \mathcal{M}_k(\Gamma_0(\mathbf{p}p^\alpha),\chi;A)$, its q-expansion will be written as $f(q) = \sum_{n=0}^{\infty} a(n,f)q^n$.

Let Λ be the one variable power series ring $\mathcal{O}[[X]]$ with coefficients in $\mathcal{O}$. We call a formal q-expansion $F(q) = \sum_{n=0}^{\infty}A(n,F;X)q^n \in \Lambda[[q]]$ a Λ-adic form of character ψ if the following condition is satisfied:

(Λ) *the formal q-expansion* $F(u^k-1)$ *gives the q-expansion of a modular form in* $\mathcal{M}_k(\Gamma_0(q),\psi\omega^{-k};\mathcal{O})$ *for all but finitely many positive integers* k.

This is the definition of Λ-adic forms given in [Wil]. A Λ-adic form F is called a Λ-adic cusp form if $F(u^k-1)$ is a cusp form for almost all k. We will see later that there exists a Λ-adic cusp form which specializes to a non-cuspidal form at $k = 1$. By our definition, *to give a* p-*adic family of modular forms* $\{f_k\}$ *is to give a simultaneous* p-*adic interpolation of their Fourier coefficients by the power series* $A(n;X)$. That is, by evaluating the p-adic analytic functions $A(n;u^s-1)$ at integers $k \geq a$, we get the n-th Fourier coefficient of the modular form f_k. When we defined a p-adic analytic family $\{f_k\}$, we required an extra condition that $f_k = F(u^k-1)$ is a classical (complex analytic) modular form for almost all k.

Thus a Λ-adic form F gives rise to a p-adic family $\{F(u^k-1)\}$ if $F(u^k-1)$ is a classical form for all but finitely many k.

Now we want to construct an example of a p-adic family out of the set of Eisenstein series $\{E_k\}$. Since the n-th coefficient of E_k for positive n is a sum of (k-1)-th powers of divisors of n, we first show, for a positive integer a prime to p, the existence of a power series $\Phi(X)$ such that $\Phi(u^k-1) = a^k$ $(u = 1+\mathbf{p})$ for integers k. We consider the binomial power series:

$$(1+X)^s = \sum_{m=0}^{\infty} \binom{s}{m} X^m.$$

As seen in Chapter 3, $(1+X)^s$ is a power series with coefficients in $\mathbf{Z}_p$. This power series converges in the interior of the unit disk. Thus we can define the p-adic power $\gamma^s = (1+(\gamma-1))^s$ (for $\gamma \in 1+\mathbf{p}\mathbf{Z}_p = W$) with exponent $s \in \mathbf{Z}_p$ and a morphism from the additive group $\mathbf{Z}_p$ into the group of one-units $W = 1+\mathbf{p}\mathbf{Z}_p$ by

$$s \mapsto u^s = (1+\mathbf{p})^s = \sum_{m=0}^{\infty} \binom{s}{m} \mathbf{p}^m.$$

As seen in §1.3, the p-adic logarithm function log induces an isomorphism $W \cong \mathbf{p}\mathbf{Z}_p$. As a power series, we have an identity $\log((1+X)^s) = s\log(1+X)$; thus, also as a map, $log(u^s) = s\,log(u)$. Note that $|log(z)|_p \le |\mathbf{p}|_p$ for any $z \in W$ and $|log(u)|_p = |\mathbf{p}|_p \ne 0$. Therefore, for any given $z \in W$, by putting $s(z) = log(z)/log(u)$, we have $s(z) \in \mathbf{Z}_p$. Thus $s : W \cong \mathbf{Z}_p$. Therefore we can write $z = u^{s(z)} = (1+(u-1))^{s(z)}$. Thus if an integer d satisfies the congruence $d \equiv 1 \bmod \mathbf{p}$, then we can write $d = u^{s(d)}$, and for the power series

$$A_d(X) = d^{-1}(1+X)^{s(d)} = d^{-1}\sum_{m=1}^{\infty} \binom{s(d)}{m} X^m,$$

we have $A_d(u^k-1) = d^{-1}u^{s(d)k} = d^{k-1}$. Therefore $A_d(X)$ has the desired property for d when $d \equiv 1 \bmod \mathbf{p}$. To treat the case of d not congruent to 1 mod $\mathbf{p}$, we use the decomposition $\mathbf{Z}_p^\times = W \times \mu$ introduced in §3.5 and the associated projection $x \mapsto \langle x\rangle = \omega(x)^{-1}x$ of $\mathbf{Z}_p^\times$ to W. For each integer d prime to p, we put

$$A_d(X) = d^{-1}(1+X)^{s(\langle d\rangle)}.$$

Then we know that $A_d(u^k-1) = d^{-1}u^{s(\langle d\rangle)k} = d^{-1}\langle d\rangle^k = \omega(d)^{-k}d^{k-1}$. In particular, if $k \equiv 0 \bmod \varphi(\mathbf{p})$, then $A_d(u^k-1) = d^{k-1}$. We now define for $0 < n \in \mathbf{Z}$ and for each even Dirichlet character $\psi = \omega^a$ of μ

$$A_\psi(n;X) = \sum_{0<d\,|\,n,\ (p,d)=1} \psi(d)A_d(X).$$

This power series $A_\psi(n;X)$ is quite near to the power series we wanted to find, since $A_\psi(n;u^k-1) = \sigma^{(p)}_{k-1}(n)$ if $k \equiv a \bmod \varphi(\mathbf{p})$ for the Euler function φ. More generally, we have

$$A_\psi(n;u^k-1) = \sum_{0<d\,|\,n,\ (p,d)=1} \psi\omega^{-k}(d)d^{k-1} = \sigma_{k-1,\psi\omega^{-k}}(n) \quad \text{for all } k > 0.$$

Now we consider the p-adic interpolation of a constant term. We consider the Dirichlet L-function

$$L(s,\xi) = \sum_{n=1}^{\infty} \xi(n)n^{-s} = \prod_q (1-\xi(q)q^{-s})^{-1}.$$

As seen in §3.6, we have that

(2a) There exists a power series $\Phi_\psi(X)$ in $\mathbf{Z}_p[[X]]$ for each character ψ of $(\mathbf{Z}/p\mathbf{Z})^\times$ with $\psi(-1) = 1$ such that for all integer $k > 1$

$$\Phi_\psi(u^k-1) = \begin{cases} (1-\psi\omega^{-k}(p)p^{k-1})L(1-k,\psi\omega^{-k}) & \text{if } \psi \neq \mathrm{id}, \\ \Phi_{\mathrm{id}}(u^k-1) = (u^k-1)(1-\omega^{-k}(p)p^{k-1})L(1-k,\omega^{-k}) & \text{if } \psi = \mathrm{id}. \end{cases}$$

Let $\Lambda = \mathcal{O}[[X]]$ and define the Λ-adic Eisenstein series $E(\psi)(X) \in \Lambda[[q]]$ for each even character $\psi = \omega^a$ with $0 \le a < p-1$ by

$$E(\psi)(X) = \sum_{n=0}^{\infty} A_\psi(n;X)q^n,$$

where $A_\psi(0;X) = \Phi_\psi(X)/2$ if $\psi = \omega^a \neq \mathrm{id}$ and $A_{\mathrm{id}}(0;X) = \Phi_{\mathrm{id}}(X)/2X$.

Proposition 1. *For each positive even integer* $k \ge 2$ *with* $k \equiv a \bmod \varphi(\mathbf{p})$, *we have*

$$E(\psi)(u^k-1) = E_k(z) - p^{k-1}E_k(pz) = E_k(\iota_p) \in \mathcal{M}_k(\Gamma_0(p)) \ \textit{in}\ \mathbf{Q}[[q]],$$

where ι_p *is the trivial character modulo* p. *More generally, for each non-trivial Dirichlet character* $\chi : (\mathbf{Z}/p^\alpha\mathbf{p}\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times$ *with* $\chi|_\mu = \psi$ *and for* $k \ge 1$, *we have* $E(\psi)(\chi(u)u^k-1) = E_k(\chi\omega^{-k}) \in \mathcal{M}_k(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k})$.

This proposition shows that we get the classical Eisenstein series even from the specialization at $\chi(u)u^k-1$ with $\chi(u) \neq 1$, which is not included in the definition of p-adic analytic families and Λ-adic forms. When $\psi = \mathrm{id}$, $E(\psi)$ is not a Λ-adic form because it has a singularity at $X = 0$. However $XE(\psi)$ is a Λ-adic form.

Proof. Assume that $k \equiv a \bmod \varphi(\mathbf{p})$ for the Euler function φ. Write

$$E_k(z) - p^{k-1}E_k(pz) = \sum_{n=0}^{\infty} a_n q^n.$$

Then we have

$$a_0 = (1-p^{k-1})\zeta(1-k)/2 = (1-p^{k-1})L(1-k,\psi\omega^{-k})/2 = A_\psi(0;u^k-1).$$

As already seen, $a_n = \sigma_{k-1}(n) = A_\psi(n;u^k-1)$ if n is prime to p. When n is divisible by p, then

$$\sigma_{k-1}(n) - p^{k-1}\sigma_{k-1}(n/p) = \sum_{d|n} d^{k-1} - p^{k-1}\sum_{dp|n} d^{k-1}$$
$$= \sum_{d|n,\ (d,p)=1} d^{k-1} = \sigma^{(p)}_{k-1}(n) = A_\psi(n;u^k-1).$$

This shows the identity of the power series as in the lemma. Note that $p^{k-1}E_k(pz) = E_k|_k\begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}$. Thus $E_k(z) - p^{k-1}E_k(pz)$ is a modular form for

$$\Gamma = SL_2(\mathbf{Z}) \cap \begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}^{-1} SL_2(\mathbf{Z}) \begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}.$$

One sees easily that Γ contains $\Gamma_0(p)$. The general case of non-trivial character $\chi\omega^{-k}$ is much easier. In fact, writing $s(d) = s(\langle d\rangle)$, we see from $\chi(u)^{s(d)} = \chi(\langle u\rangle)^{s(d)} = \chi(\langle d\rangle)$ that

$$A_\psi(n;\chi(u)u^k-1) = \sum_{0<d|n} d^{-1}\psi(d)(1+\chi(u)u^k-1)^{s(d)} = \sum_{0<d|n} \chi\omega^{-k}(d)d^{k-1} = \sigma_{k-1,\chi\omega^{-k}}(n).$$

As seen in Theorem 3.5.2, if $\chi\omega^{-k}$ is non-trivial and $\chi|_\mu = \psi$, we have

(2b) $$A_\psi(0;\chi(u)u^k-1) = 2^{-1}L(1-k,\chi\omega^{-k}).$$

This shows the assertion in the general case. Strictly speaking, we have only proven the proposition when $k > 2$ because the Fourier expansion of the Eisenstein series was not yet computed for $k = 1$ and 2 in §5.1. This will be done in Chapter 9.

Now we can produce many p-adic families of cusp forms by using $E(\psi)$. In fact, we take a modular form $f \in \mathcal{M}_m(\Gamma_0(p^\alpha\mathbf{p}),\chi;\mathcal{O})$ for a character χ having values in $\mathcal{O}$ and make the product $fE(\psi)(X)$ inside $\Lambda[[q]]$. Then we have

$$fE(\psi)(u^k-1) \in \mathcal{M}_{k+m}(\Gamma_0(p^\alpha\mathbf{p}),\chi\psi\omega^{-k};\mathcal{O}).$$

Lemma 1. *For* $u \in \mathcal{O}^\times$ *and* $v \in \mathcal{O}$ *with* $|v|_p < 1$, *the substitution* $A(X) \mapsto A(uX+v)$ *gives a ring automorphism of* $\Lambda = \mathcal{O}[[X]]$.

Proof. For $A(X) = \sum_{n=0}^\infty a_nX^n$, we see that

$$A(uX+v) = \sum_{m=0}^\infty X^m\{\sum_{n=m}^\infty a_nu^mv^{n-m}\binom{n}{m}\}.$$

The inner infinite sum is absolutely convergent p-adically, since v is divisible by p. Thus $A(uX+v)$ is a well defined power series. The substitution of $u^{-1}X-u^{-1}v$ for X gives an inverse map, and hence $A(X) \mapsto A(uX+v)$ is a ring automorphism.

Let $f \in \mathcal{M}_m(\Gamma_0(\mathbf{p}p^\alpha),\chi;\mathcal{O})$. Expanding $fE(\psi)(X)$ as $\sum_{n=0}^\infty a_n(X)q^n$ and defining a new series (called the convolution product of f and $E(\psi)$) by

$$F(X) = f*E(\psi)(X) = \sum_{n=0}^{\infty} a_n(\chi^{-1}(u)u^{-m}X+(u^{-m}\chi(u)^{-1}-1))q^n,$$

we know that

$$F(u^k-1) = fE(\psi)(\chi^{-1}(u)u^{k-m}-1) \in \mathcal{M}_k(\Gamma_0(p^\alpha\mathbf{p}),\chi_0\psi\omega^{-k}) \text{ for all } k > m,$$

where χ_0 is defined by writing χ as the product $\varepsilon\chi_0$ for characters ε of W and χ_0 of μ. In particular, if f is a cusp form of level $\mathbf{p}$, we obtain Λ-adic cusp forms in this way.

So far, we have constructed Λ-adic Eisenstein series using $E_k(\psi)$. We now want to do the same thing using $G_k(\psi)$. This is easier in fact, because $G_k(\chi)$ does not have a constant term usually (see Proposition 5.1.2). We then define

(3a) $$B_\psi(n;X) = \sum_{0<d\,|\,n,\ (d,p)=1} \psi(n/d)A_d(X) \text{ for } n \text{ prime to } p$$
$$\text{and } G(\psi)(X) = \sum_{n=1}^{\infty} B_\psi(n;X)q^n.$$

Then, when $\chi|_\mu = \psi$, we have $B_\psi(n;\chi(u)u^k-1) = \sigma'_{k,\chi\omega^{-k}}(n)$, and we have another p-adic analytic family of modular forms $G(\psi)$ such that, for each character χ modulo $p^\alpha\mathbf{p}$,

(3b) $$G(\psi)(\chi(u)u^k-1)$$
$$= G_k(z;\chi\omega^{-k})-p^{k-1}G_k(pz;\chi\omega^{-k}) \in \mathcal{M}_k(\Gamma_0(p^{\alpha+1}\mathbf{p}),\omega^{a-k}) \text{ if } k > 1.$$

§7.2. The projection to the ordinary part

In this section, we first define the idempotent attached to T(p) which gives the projection to the "ordinary" part. We have defined for each character $\chi : (\mathbf{Z}/p^\alpha\mathbf{Z})^\times \to \mathcal{O}^\times$

$$\mathcal{M}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O}) = \mathcal{M}_k(\Gamma_0(p^\alpha),\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}\mathcal{O},$$
$$\mathcal{S}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O}) = \mathcal{S}_k(\Gamma_0(p^\alpha),\chi;\mathbf{Z}[\chi])\otimes_{\mathbf{Z}[\chi]}\mathcal{O}.$$

We may regard these spaces as the $\mathcal{O}$-linear span of $\mathcal{M}_k(\Gamma_0(p^\alpha),\chi;\mathbf{Z}[\chi])$ or $\mathcal{S}_k(\Gamma_0(p^\alpha),\chi;\mathbf{Z}[\chi])$ in $\mathcal{O}[[q]]$. Then the Hecke operators T(n) act on these spaces and satisfy the formula (5.3.5) describing their effect on coefficients of q^n. In particular, we have the $\mathcal{O}$-duality between the Hecke algebras and the spaces of cusp forms. When χ is primitive modulo p^α or $\Gamma = SL_2(\mathbf{Z})$, the Hecke algebra $\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;\mathbf{Q}(\chi))$ is semi-simple and hence

$$\mathbf{H}_k(\Gamma,\chi;\mathbf{Q}_p(\chi)) = \mathbf{H}_k(\Gamma,\chi;\mathbf{Q}(\chi))\otimes_{\mathbf{Q}(\chi)}\mathbf{Q}_p(\chi)$$

is again semi-simple. Thus $\mathbf{H}_k(\Gamma,\chi;\mathbf{Q}_p(\chi)) \cong \prod_\lambda \mathbf{Q}_p(\lambda)$, where λ runs over conjugacy classes in $\mathrm{Hom}_{\mathbf{Q}_p(\chi)\text{-alg}}(\mathbf{H}_k(\Gamma,\chi;\mathbf{Q}_p(\chi)),\overline{\mathbf{Q}}_p)$ under $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p(\chi))$.

Proposition 1. *Let* K *be a finite extension of* $\mathbf{Q}_p(\chi)$. *If* f *is a common eigenform of all Hecke operators in* $\mathcal{M}_k(\Gamma_0(p^\alpha),\chi;K)$ *normalized so that* $a(1,f) = 1$, *then* f *is actually a complex common eigenform in* $\mathcal{M}_k(\Gamma_0(p^\alpha),\chi;\mathbf{C})$.

Proof. We define a K-algebra homomorphism $\lambda : \mathbf{H}_k(\Gamma_0(p^\alpha),\chi;K) \to K$ by $f|h = \lambda(h)f$. Then $a(n,f) = \lambda(T(n))$. Since we have

$$\mathbf{H}_k(\Gamma_0(p^\alpha),\chi:K) = \mathbf{H}_k(\Gamma_0(p^\alpha),\chi:\mathbf{Q}(\chi))\otimes K,$$

we can restrict λ to $\mathbf{H}_k(\Gamma_0(p^\alpha),\chi:\mathbf{Q}(\chi))$. Since $\mathbf{H}_k(\Gamma_0(p^\alpha),\chi:\mathbf{Q}(\chi))$ is of finite dimension over $\mathbf{Q}$, λ in fact has values in $\overline{\mathbf{Q}}$. Since

$$\mathbf{H}_k(\Gamma_0(p^\alpha),\chi:\mathbf{C}) = \mathbf{H}_k(\Gamma_0(p^\alpha),\chi:\mathbf{Q}(\chi))\otimes \mathbf{C},$$

we can extend λ to a $\mathbf{C}$-algebra homomorphism of $\mathbf{H}_k(\Gamma_0(p^\alpha),\chi:\mathbf{C})$ into $\mathbf{C}$. Then by the duality, we can find f' in $\mathcal{M}_k(\Gamma_0(p^\alpha),\chi;\mathbf{C})$ such that $a(n,f') = \lambda(T(n)) = a(n,f)$. Thus $f = f' \in \mathcal{M}_k(\Gamma_0(p^\alpha),\chi;\mathbf{C})$.

Lemma 1. *Let* K *be a finite extension of* $\mathbf{Q}_p$ *and* $\mathcal{O}$ *be its* p*-adic integer ring. For any commutative* $\mathcal{O}$*-algebra* A *of finite rank over* $\mathcal{O}$ *and for any* $x \in A$, *the limit* $\lim_{n\to\infty} x^{n!}$ *exists in* A *and gives an idempotent of* A.

Proof. First assume that A is the p-adic integer ring of a finite extension of K. Let p be the maximal ideal of A and write p^f for $\#(A/p)$. Then we have $\#((A/p^r)^\times) = p^{r-1}(p^f-1)$. Therefore for any $x \in A^\times$, $x^{p^{fr}(p^f-1)} \equiv 1 \bmod p^r$. This shows that the limit of $\{x^{p^{fn}(p^f-1)}\}$ as $n \to \infty$ exists in A and is equal to 1 for $x \in A^\times$. Therefore $\lim_{n\to\infty} x^{n!} = \lim_{n\to\infty} x^{p^{fn}(p^f-1)} = 1$ for $x \in A^\times$. When x is in p, then obviously, the above limit vanishes. Now we proceed to the general case. If the scalar extension $A\otimes_{\mathcal{O}}K$ is semi-simple, then it is a product of finite extensions of K and the image of x in each simple factor is contained in the p-adic integer ring of the factor. Then applying the above argument, we know the existence of the limit, which is an idempotent. If the nilpotent radical of A is non-trivial, write $x = s + n$ in $A\otimes_{\mathcal{O}}K$ with s semi-simple and n nilpotent. (By a theorem of Wedderburn, this is always possible.) For sufficiently large f, $\lim_{n\to\infty} s^{p^{fn}(p^f-1)}$ exists in the subalgebra $\mathcal{O}[s]$ of A generated over $\mathcal{O}$ by s, since $\mathcal{O}[s]$ has no non-trivial nilpotent radical and is of finite rank as $\mathcal{O}$-module because it is the surjective image of A. On the other hand, if $n^j = 0$, then

$$(s+n)^{p^{fr}} = s^{p^{fr}} + \sum_{i=1}^{j-1} \binom{p^{fr}}{i} s^{p^{fr}-i} n^i.$$

Note that $\binom{p^{fr}}{i} = p^{fr}!/(p^{fr}-i)!i!$. Since $p^{fn}!$ is divisible by $(p^{fr}-i)!p^{fr}$ and $0 < i < j$, $\left|\binom{p^{fr}}{i}\right|_p < Cp^{-fr}$ for a constant C independent of r. This shows that the term $\sum_{i=1}^{j-1}\binom{p^{fr}}{i}s^{p^{fr}-i}n^i$ vanishes after taking the limit, and we know the existence of the limit $e = \lim_{n\to\infty} x^{n!} = \lim_{n\to\infty} s^{n!}$, which is an idempotent.

Let K be a finite extension of $\mathbf{Q}_p(\chi)$. We now define the ordinary projector e of the Hecke algebra $\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O})$ by $e = \lim_{n\to\infty} T(p)^{n!}$. We see easily that if f is an eigenform of $T(p)$ with eigenvalue a, then

$$f\,|\,e = \begin{cases} f & \text{if } |a|_p = 1, \\ 0 & \text{if } |a|_p < 1. \end{cases} \tag{1}$$

We say a p-adic modular form f is ordinary if $f\,|\,e = f$. There are examples of ordinary forms and non-ordinary forms. For any character χ modulo p^α $(\alpha > 0)$, we have $\sigma_{m,\chi}(p) = 1+\chi(p)p^m = 1$ and $\sigma'_{m,\chi}(p) = p^m+\chi(p) = p^m$. Thus $G_k(\chi)\,|\,e = 0$ and $E_k(\chi)\,|\,e = E_k(\chi)$ if $k > 1$. Now we define the ordinary part of the Hecke algebras and the spaces of modular forms by

$$\mathbf{H}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O}) = e\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O}),\ \mathbf{h}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O}) = e\mathbf{h}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O}),$$
$$\mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O}) = \mathcal{M}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O})\,|\,e,\ \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O}) = \mathcal{S}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O})\,|\,e.$$

By definition, $\mathbf{H}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O})$ is the largest algebra direct summand of $\mathbf{H}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O})$ on which the image of $T(p)$ is a unit. Again by definition, $\langle hh',f\rangle = a(1,f\,|\,hh') = \langle h',f\,|\,h\rangle$ for $h,h' \in \mathbf{H}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O})$ and $f \in \mathcal{M}_k(\Gamma_0(p^\alpha),\chi;\mathcal{O})$. Thus this pairing induces isomorphisms:

$$\mathrm{Hom}_{\mathcal{O}}(\mathbf{H}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O}),\mathcal{O}) \cong m_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O}) \text{ and}$$
$$\mathrm{Hom}_{\mathcal{O}}(\mathbf{h}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O}),\mathcal{O}) \cong \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi;\mathcal{O}).$$

One of the fundamental theorems in the theory of ordinary forms is

Theorem 1. *Suppose* $k \geq 2$. *Then we have*

$$\begin{aligned}\mathrm{rank}_{\mathcal{O}}\mathbf{H}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi\omega^{-k};\mathcal{O}) &= \mathrm{rank}_{\mathcal{O}}\,\mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi\omega^{-k};\mathcal{O}) \\ &= \mathrm{rank}_{\mathcal{O}}\,\mathcal{M}_2^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi\omega^{-2};\mathcal{O}), \\ \mathrm{rank}_{\mathcal{O}}\mathbf{h}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi\omega^{-k};\mathcal{O}) &= \mathrm{rank}_{\mathcal{O}}\,\mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi\omega^{-k};\mathcal{O}) \\ &= \mathrm{rank}_{\mathcal{O}}\,\mathcal{S}_2^{\mathrm{ord}}(\Gamma_0(p^\alpha),\chi\omega^{-2};\mathcal{O}).\end{aligned}$$

Here χ is any character modulo p^α primitive or imprimitive. The proof of this fact will be divided into two steps: (i) the first step is to show that the rank as above is bounded independently of k, and (ii) the second step is to show that the rank is equal for all k. Putting off the second step to the next section, we first prove the boundedness of the rank by cohomological means. Since $\mathbf{H}_k(\Gamma_0(N),\chi;A)$ is a residue ring of $\mathbf{H}_k(\Gamma_1(N);A)$ by (6.3.2b), the boundedness of the rank follows from that of $\mathbf{H}_k(\Gamma_1(N);\mathbf{Z}_p)$. Since $\mathbf{H}_k(\Gamma_1(N);\mathbf{C}) \cong \oplus_\chi \mathbf{H}_k(\Gamma_0(N),\chi;\mathbf{C})$ is the $\mathbf{C}$-dual of $\mathcal{M}_k(\Gamma_1(N)) = \oplus_\chi \mathcal{M}_k(\Gamma_0(N),\chi)$, by (6.3.2b), it is sufficient to prove the assertion for sufficiently large N. Thus the boundedness follows from

Theorem 2. *Let* N *be a positive integer prime to* p. *Then the integer* $\mathrm{rank}_{\mathbf{Z}_p}(\mathbf{h}_k^{\mathrm{ord}}(\Gamma_1(Np^\alpha);\mathbf{Z}_p))$ *is bounded independently of* k *if* $k \geq 2$ *and* $\alpha \geq 1$.

Proof. Write Γ for $\Gamma_1(Np^\alpha)$. Let L be the intersection of the image L' of $H^1(\Gamma,L(n;\mathbf{Z}))$ in $H^1(\Gamma,L(n;\mathbf{R}))$ with $H^1_P(\Gamma,L(n;\mathbf{R}))$. Then L is a lattice of $H^1_P(\Gamma,L(n;\mathbf{R}))$, and $\mathbf{h}_k(\Gamma;\mathbf{Z})$ for $k = n+2$ is by definition a subalgebra of $\mathrm{End}_{\mathbf{Z}}(L)$ which is free of finite rank over $\mathbf{Z}$. Let $L_p = L\otimes_{\mathbf{Z}}\mathbf{Z}_p$. Then $\mathbf{h}_k(\Gamma;\mathbf{Z}_p) = \mathbf{h}_k(\Gamma;\mathbf{Z})\otimes_{\mathbf{Z}}\mathbf{Z}_p$ is a subalgebra of $\mathrm{End}_{\mathbf{Z}_p}(L_p)$. Thus $\mathbf{h}_k^{\mathrm{ord}}(\Gamma;\mathbf{Z}_p)$ is a subalgebra of $\mathrm{End}_{\mathbf{Z}_p}(eL_p)$ for the idempotent e attached to T(p). Thus what we have to prove is the boundedness of the rank of eL_p independent of n. The exact sequence of Γ-modules

$$0 \to L(n;\mathbf{Z}) \xrightarrow{p} L(n;\mathbf{Z}) \to L(n;\mathbf{Z}/p\mathbf{Z}) \to 0$$

yields the cohomology exact sequence

$$H^1(\Gamma,L(n;\mathbf{Z})) \xrightarrow{p} H^1(\Gamma,L(n;\mathbf{Z})) \to H^1(\Gamma,L(n;\mathbf{Z}/p\mathbf{Z})).$$

Therefore $H^1(\Gamma,L(n;\mathbf{Z}))\otimes\mathbf{Z}/p\mathbf{Z}$ can be embedded into $H^1(\Gamma,L(n;\mathbf{Z}/p\mathbf{Z}))$. Note that $L/pL = L_p/pL_p$, L/pL injects into L'/pL', and L'/pL' is a surjective image of

$$H^1(\Gamma,L(n;\mathbf{Z}))/pH^1(\Gamma,L(n;\mathbf{Z})) = H^1(\Gamma,L(n;\mathbf{Z}))\otimes_{\mathbf{Z}}\mathbf{Z}/p\mathbf{Z}.$$

Thus it is sufficient to show that the dimension of $eH^1(\Gamma,L(n;\mathbf{Z}/p\mathbf{Z}))$ is bounded independently of n. We shall show this fact by constructing an embedding of

$$eH^1(\Gamma,L(n;\mathbf{Z}/p\mathbf{Z})) \text{ into } eH^1(\Gamma,\mathbf{Z}/p\mathbf{Z}).$$

Note that, for $P(X,Y) = \sum_{i=0}^n a_i X^{n-i}Y^i \in L(n;A)$,

$$\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}P(X,Y) = \sum_{i=0}^{n} a_i(X-mY)^{n-i}Y^i \text{ and hence } \left(\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}P\right)(1,0) = P(1,0).$$

Let us define maps $i : L(n;\mathbf{Z}/p\mathbf{Z}) \to \mathbf{Z}/p\mathbf{Z}$ and $j : \mathbf{Z}/p\mathbf{Z} \to L(n;\mathbf{Z}/p\mathbf{Z})$ by $i(P(X,Y)) = P(1,0)$ and $j(x) = xY^n$. Since $\gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod p$ for any $\gamma \in \Gamma = \Gamma_1(Np^\alpha)$, i and j are homomorphisms of Γ-module. Thus combining i or j with a 1-cocycle u, we obtain the following two morphisms of cohomology groups:

$$I = i_* : H^1(\Gamma, L(n;\mathbf{Z}/p\mathbf{Z})) \to H^1(\Gamma, \mathbf{Z}/p\mathbf{Z}) \text{ and}$$
$$j_* : H^1(\Gamma, \mathbf{Z}/p\mathbf{Z}) \to H^1(\Gamma, L(n;\mathbf{Z}/p\mathbf{Z})).$$

We want to show that I is an isomorphism of $eH^1(\Gamma, L(n;\mathbf{Z}/p\mathbf{Z}))$ onto $eH^1(\Gamma, \mathbf{Z}/p\mathbf{Z})$. We consider the exact sequence of Γ-modules

$$0 \to \mathrm{Ker}(i) \to L(n;\mathbf{Z}/p\mathbf{Z}) \to \mathbf{Z}/p\mathbf{Z} \to 0.$$

This yields another exact sequence:

$$H^1(\Gamma, \mathrm{Ker}(i)) \to H^1(\Gamma, L(n;A)) \to H^1(\Gamma, \mathbf{Z}/p\mathbf{Z}) \to H^2(\Gamma, \mathrm{Ker}(i)).$$

Note that for $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, α^ι leaves Ker(i) stable and hence T(p) acts naturally on $H^q(\Gamma, \mathrm{Ker}(i))$. On the other hand, the $\mathbf{Z}/p\mathbf{Z}$-module Ker(i) is generated by monomials $X^{n-i}Y^i$ for $i > 0$. Thus for $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, the action of α^ι is nilpotent on Ker(i). Since $\Gamma\alpha\Gamma = \coprod_{i=1}^{p-1} \Gamma\alpha\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$, the action of T(p) is nilpotent on $H^q(\Gamma, \mathrm{Ker}(i))$ for $q > 0$. This shows the desired assertion.

We shall give another proof of the theorem when $\alpha = 1$. When $\alpha = 1$, we modify j_* and construct a map $J : H^1(\Gamma, \mathbf{Z}/p\mathbf{Z}) \to H^1(\Gamma, L(n;\mathbf{Z}/p\mathbf{Z}))$ so that $J \circ I = (-1)^n T(p)$ on $H^1(\Gamma_1(Np), L(n;\mathbf{Z}/p\mathbf{Z}))$. Thus $(-1)^n T(p)^{-1} J$ actually gives the inverse of I on $eH^1(\Gamma_1(Np), \mathbf{Z}/p\mathbf{Z})$. We consider the double coset $\Gamma\delta\Gamma$ for $\delta \in SL_2(\mathbf{Z})$ such that

$$\delta \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \bmod p \text{ and } \delta \equiv 1 \bmod N.$$

One can always find such an element (see Lemma 6.1.1). Then we have a disjoint decomposition

$$\Gamma\delta\Gamma = \coprod_{i=1}^{p} \Gamma\delta\delta_i \text{ for } \delta_i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}.$$

Similarly we take $\tau \in M_2(\mathbf{Z})$ with $\det(\tau) = p$ such that

$$\tau \equiv \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \bmod p^2 \text{ and } \tau \equiv \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \bmod N.$$

We can find such τ as follows. By Lemma 6.1.1, we can find $\sigma \in SL_2(\mathbf{Z})$ such that $\sigma \equiv 1 \bmod p^2$ and

$$\sigma \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \bmod N^2.$$

Then $\tau = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}\sigma$ does the job. Then one can easily verify that τ normalizes Γ and induces an automorphism of $H^1(\Gamma,\mathbf{Z}/p\mathbf{Z}) = \mathrm{Hom}(\Gamma,\mathbf{Z}/p\mathbf{Z})$ which takes $u : \Gamma \to \mathbf{Z}/p\mathbf{Z}$ to $u\,|\,[\tau](\gamma) = u(\tau\gamma\tau^{-1})$. Note that

$$T(p) = \Gamma\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma = \coprod_{i=1}^{p} \Gamma\tau\delta\delta_i$$

because $\Gamma\tau\delta\delta_i \equiv \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \bmod Np^2$ and $\det(\tau\delta\delta_i) = p$. Define J to be $[\Gamma\delta\Gamma]\circ j_*\circ[\tau]$. We compute $J\circ I$. Let $u : \Gamma \to L(n;\mathbf{Z}/p\mathbf{Z})$ be a 1-cocycle. Then if $\delta\delta_i\gamma = \gamma_i\delta\delta_j$ for $\gamma,\gamma_i \in \Gamma$, then $\tau\delta\delta_i\gamma = \tau\gamma_i\tau^{-1}\tau\delta\delta_j$ with $\tau\gamma_i\tau^{-1} \in \Gamma$. Thus

$$J(I(u))(\gamma) = \sum_{i=1}^{p} (\delta\delta_i)^{\iota} j\circ i\circ u(\tau\gamma_i\tau^{-1}).$$

Note that $j(i(P(X,Y))) = a_0Y^n = (-1)^n\tau^{\iota}P(X,Y)$. Thus

$$J(I(u))(\gamma) = (-1)^n\sum_{i=1}^{p}(\delta\delta_i)^{\iota}\tau^{\iota}u(\tau\gamma_i\tau^{-1}) = (-1)^n\sum_{i=1}^{p}(\tau\delta\delta_i)^{\iota}u(\tau\gamma_i\tau^{-1}) = (-1)^n u\,|\,T(p).$$

Thus, we have $J\circ I = (-1)^nT(p)$, giving another proof of the theorem.

Here we add one more result for our later use in §10.4, which is a special case of [H1, Th.3.2]:

Proposition 2. *If* $k > 2$ *and* $p \geq 5$, *then* e *induces*
$e : \mathcal{S}_k^{\mathrm{ord}}(SL_2(\mathbf{Z});\mathbf{Q}_p) \cong \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p);\mathbf{Q}_p)$, $e : \mathcal{M}_k^{\mathrm{ord}}(SL_2(\mathbf{Z});\mathbf{Q}_p) \cong \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p);\mathbf{Q}_p)$, *where the ordinary part for* $SL_2(\mathbf{Z})$ *is defined with respect to the Hecke operator* $T(p)$ *of level* 1.

Proof. We start a general argument. We consider any

$$\Gamma = \Gamma(N) = \{\gamma \in SL_2(\mathbf{Z})\,|\,\gamma \equiv 1 \bmod N\} \quad \text{for} \quad N > 3.$$

Then Γ is torsion-free. Now we put $\Gamma_0 = \Gamma\cap\Gamma_0(p)$. Then we have

$$I' = I\circ\mathrm{res}: H^1(\Gamma,L(n;\mathbf{Z}/p\mathbf{Z})) \to H^1(\Gamma_0,L(n;\mathbf{Z}/p\mathbf{Z})) \to H^1(\Gamma_0,L(0,\omega^n;\mathbf{Z}/p\mathbf{Z})).$$

Since we can show by the strong approximation theorem (Lemma 6.1.1) that

$$\Gamma\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma = \coprod_{0\leq u<p}\Gamma\begin{pmatrix} 1 & Nu \\ 0 & p \end{pmatrix}\coprod\Gamma\sigma\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \text{(see [Sh, Prop.3.33])}$$

for $\sigma \in SL_2(\mathbf{Z})$ with $\sigma \equiv \begin{pmatrix} p^{-1} & 0 \\ 0 & p \end{pmatrix}$ mod N, we know that

$$i_*(\left\{\sigma\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right\}^{\iota} P) = (\sigma^{\iota}P)((1,0)\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}) = (\sigma^{\iota}P)(0,0) = 0 \quad (\text{if} \quad n > 0)$$

for any homogeneous polynomial P with coefficients in $\mathbf{Z}/p\mathbf{Z}$. Since T(p) of level N and T(p) of level Np are different, we add the subscript "N" to indicate the level. Then $f \mid T_N(p) = f \mid T_{Np}(p) + f \mid \sigma\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. By the above argument, the term corresponding to $\sigma\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ does not affect to the value of i_*. Similarly we consider the trace map as in §6.3:

$$\mathrm{Tr} = [\Gamma_0 1_2 \Gamma] : H^1(\Gamma_0, L(n;\mathbf{Z}/p\mathbf{Z})) \to H^1(\Gamma, L(n;\mathbf{Z}/p\mathbf{Z})).$$

Then we consider

$$J' = \mathrm{Tr}\circ j_*\circ\tau : H^1(\Gamma_0, L(0,\omega^{-n};\mathbf{Z}/p\mathbf{Z})) \to H^1(\Gamma_0, L(n;\mathbf{Z}/p\mathbf{Z})) \to H^1(\Gamma, L(n;\mathbf{Z})).$$

Then basically by the same computation as in the case of $\alpha = 1$, we have

$$J'\circ I' = (-1)^n T_N(p).$$

Let us now compute $I'\circ J'$. We pick a cocycle $v \in Z(\Gamma_0, L(0,\omega^{-n};\mathbf{Z}/p\mathbf{Z}))$. Then, noting that $\Gamma = \coprod_{0\le u<p}\Gamma_0\delta\delta_u\coprod\Gamma_0$, we see that

$$I'(J'(v))(\gamma) = \sum_{u=0}^{p-1} i(\delta_u{}^{\iota}j(v(\gamma_u))) + i(j(v(\gamma))) = \sum_{u=0}^{p-1} i(\delta_u{}^{\iota}j(v(\gamma_u))) = v \mid T_N(p)(\gamma),$$

where $\delta\delta_u\gamma = \gamma_u\alpha$ for an α in $\{\delta\delta_v \mid v = 0,\dots,p-1\}\cup\{1_2\}$ for the identity matrix 1_2. Here we have used the fact that $i\circ j = 0$. By this, we have

$$(2) \qquad H^1_{\mathrm{ord}}(\Gamma, L(n;\mathbf{Z}/p\mathbf{Z})) \cong H^1_{\mathrm{ord}}(\Gamma_0, L(0,\omega^{-n};\mathbf{Z}/p\mathbf{Z})) \cong H^1_{\mathrm{ord}}(\Gamma_0, L(n;\mathbf{Z}/p\mathbf{Z})).$$

Now we consider the cohomology sequence attached to

$$0 \to L(n;\mathbf{Z}_p) \xrightarrow{p} L(n;\mathbf{Z}_p) \to L(n;\mathbf{Z}/p\mathbf{Z}) \to 0,$$

which gives rise to, for $\Phi = \Gamma$ and Γ_0,

$$(3)\ 0 \to H^i(\Phi, L(n;\mathbf{Z}_p))\otimes_{\mathbf{Z}}\mathbf{Z}/p\mathbf{Z} \to H^i(\Phi, L(n;\mathbf{Z}/p\mathbf{Z})) \to H^{i+1}(\Phi, L(n;\mathbf{Z}_p))[p] \to 0,$$

where $H^2(\Phi, L(n;\mathbf{Z}))[p]$ is the kernel of the multiplication by p on $H^2(\Phi, L(n;\mathbf{Z}))$. By Proposition 6.1.1, we know that $H^2(\Phi, L(n;\mathbf{Z}))[p] = 0$. Thus we see that

$$(4) \qquad H^1(\Phi, L(n;\mathbf{Z}))\otimes_{\mathbf{Z}}\mathbf{Z}/p\mathbf{Z} \cong H^1(\Phi, L(n;\mathbf{Z}/p\mathbf{Z})).$$

Note that $H^0(\Phi,L(n;\mathbf{Z}/p\mathbf{Z})) = L(n;\mathbf{Z}/p\mathbf{Z})^\Phi$ may be non-trivial. We have the map induced by the projector e attached to $T(p)$ of level p:

$$e : H^1(\Gamma,L(n;\mathbf{Z}_p)) \to H^1(\Gamma_0,L(n;\mathbf{Z}_p)).$$

Then (2) shows that e is an isomorphism after reducing modulo p. Then by Nakayama's lemma, we know that the map e is surjective. If x is an element in $L(n;\mathbf{Z}/p\mathbf{Z})$, then $x \mid T(p) = \sum_{0\le u<p}\begin{pmatrix}1 & Nu\\ 0 & p\end{pmatrix}^\iota x$. We know that for each monomial $X^{n-j}Y^j$, we have

$$\sum_{0\le u<p}\begin{pmatrix}1 & Nu\\ 0 & p\end{pmatrix}^\iota X^{n-j}Y^j = \sum_{0\le u<p}(X+NuY)^{n-j}(pY)^j,$$

which is obviously 0 if $j>0$ because $p=0$ in $\mathbf{Z}/p\mathbf{Z}$. Thus, we know

$$\sum_{0\le u<p}\begin{pmatrix}1 & Nu\\ 0 & p\end{pmatrix}^\iota X^n \text{ consists only of terms involving } Y.$$

This shows $x \mid T(p)^2 = 0$ and hence $H^0_{\mathrm{ord}}(\Phi,L(n;\mathbf{Z}/p\mathbf{Z})) = 0$ because $e = \lim_{n\to\infty} T(p)^{n!}$. Applying the operator e to the exact sequence (3) for $i=0$, we have

$$H^1_{\mathrm{ord}}(\Phi,L(n;\mathbf{Z}_p))[p] = 0.$$

Thus $H^1_{\mathrm{ord}}(\Phi,L(n;\mathbf{Z}_p))$ is torsion-free. Therefore we conclude from (2) and (3) that e induces an isomorphism:

$$H^1_{\mathrm{ord}}(\Gamma,L(n;\mathbf{Z}_p)) \cong H^1_{\mathrm{ord}}(\Gamma_0,L(n;\mathbf{Z}_p)). \tag{5}$$

Note that $G = SL_2(\mathbf{Z})/\Gamma \cong \Gamma_0(p)/\Gamma_0 \cong SL_2(\mathbf{Z}/N\mathbf{Z})$. If N is a prime, then $\#(SL_2(\mathbf{Z}/N\mathbf{Z})) = N(N+1)(N-1)$. Since $p \ge 5$, we can always choose N so that $\#(SL_2(\mathbf{Z}/N\mathbf{Z}))$ is prime to p. Then it is well known that

$$\begin{aligned}\text{res: } H^1(SL_2(\mathbf{Z}),L(n;\mathbf{Z}_p)) &\cong H^0(G,H^1(\Gamma,L(n;\mathbf{Z}_p))),\\ \text{res: } H^1(\Gamma_0(p),L(n;\mathbf{Z}_p)) &\cong H^0(G,H^1(\Gamma_0,L(n;\mathbf{Z}_p))).\end{aligned}$$

This combined with (5) shows that e induces

$$H^1_{\mathrm{ord}}(SL_2(\mathbf{Z}),L(n;\mathbf{Z}_p)) \cong H^1_{\mathrm{ord}}(\Gamma_0(p),L(n;\mathbf{Z}_p)).$$

By this, we know that $\dim \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p);\mathbf{Q}_p) = \dim \mathcal{M}_k^{\mathrm{ord}}(SL_2(\mathbf{Z});\mathbf{Q}_p)$, which shows the assertion for $\mathcal{M}_k$. Then the assertion for $\mathcal{S}_k$ follows from that for $\mathcal{M}_k$.

Corollary 1. *For all fields* A *of characteristic* 0, *the algebra* $\mathbf{h}_k^{ord}(\Gamma_0(p);A)$ *is semi-simple if* $k > 2$ *and* $p \geq 5$.

In fact, the assertion is true even for $k = 2$. This fact follows from the fact that $\mathcal{S}_2(SL_2(\mathbf{Z})) = 0$ and [M, Th.4.6.13]. In this case, if $f \in \mathcal{S}_2(\Gamma_0(p))$ is a normalized eigenform, then f is primitive in the sense of [M, §4.6] and $f \mid \tau = \pm p^{(k-2)/2} f^c$ for $\tau = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$.

Proof. We know that $\mathbf{h}_k(SL_2(\mathbf{Z});\mathbf{C})$ is semi-simple. Thus $\mathbf{h}_k^{ord}(SL_2(\mathbf{Z});\mathbf{Q}_p)$ is semi-simple. Thus we can find a basis $\{f_1, \ldots, f_r\}$ of $\mathcal{S}_k^{ord}(SL_2(\mathbf{Z});\overline{\mathbf{Q}}_p)$ consisting of common eigenforms of all Hecke operators. Let f be one of them. We write $f \mid T(p) = af$. Then $|a|_p = 1$. We take roots α and β of $X^2 - aX + p^{k-1} = 0$. Then one of α and β, say α, is a p-adic unit, i.e. $|\alpha|_p = 1$. Then $|\beta|_p = p^{1-k} < 1$. We define $f' = f(z) - \beta f(pz)$. Then it is easy to check by the formula (5.3.5) that

$$f' \mid T(n) = a(n,f)f' \text{ if } n \text{ is prime to } p \text{ and } f' \mid T(p) = \alpha f'.$$

Thus f' is an ordinary form. As shown in the proof of Theorem 5.3.2, if $a(q,f_i) = a(q,f_j)$ for all primes outside p, then $i = j$. This implies $f_1', \ldots, f_r'$ are linearly independent. Then by Proposition 2, they form a basis of $\mathcal{S}_k^{ord}(\Gamma_0(p),\overline{\mathbf{Q}}_p)$. Therefore $\mathbf{h}_k^{ord}(SL_2(\mathbf{Z});\overline{\mathbf{Q}}_p)$ is semi-simple, which shows the assertion.

§7.3. Ordinary Λ-adic forms

In this section, we study the structure of the space of ordinary Λ-adic forms following the method of Wiles [Wil]. Actually the space of Λ-adic forms is the Λ-dual of the p-ordinary Hecke algebra of level p^∞ defined in [H3] and [H4]. Then all the results concerning the structure of the space of ordinary Λ-adic forms follow from the structure theorem of the ordinary Hecke algebra proved in [H3] and [H4]. However, we have adopted the method of Wiles, which is more compact. We ease (in appearance) a little bit the requirement (Λ) to be a Λ-adic form given in §7.1: for each character χ modulo $p^\alpha\mathbf{p}$ (which may not be primitive), a formal q-expansion $F(X;q) = \sum_{n=0}^{\infty} a(n;F)(X)q^n$ with coefficients in $\Lambda = \mathcal{O}[[X]]$ is called a Λ-adic modular form F(X) of character χ (with values in $\mathcal{O}^\times$) if the following condition is satisfied: for the generator $u = 1+\mathbf{p}$

(Λ') $F(u^k-1;q) \in \mathcal{M}_k(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};\mathcal{O})$ for almost all positive k (i.e. all but finitely many positive k).

When $F(u^k-1;q)$ is a cusp (resp. a p-ordinary) form for all sufficiently large k, we say that F is a cusp (resp. an ordinary) form. Let $\mathbf{M} = \mathbf{M}(\chi;\Lambda)$ (resp. $\mathbf{S} = \mathbf{S}(\chi;\Lambda)$, $\mathbf{M}^{ord} = \mathbf{M}^{ord}(\chi;\Lambda)$, $\mathbf{S}^{ord} = \mathbf{S}^{ord}(\chi;\Lambda)$) be the Λ-module of all Λ-adic modular (resp. cusp, ordinary modular, ordinary cusp) forms. To introduce a Hecke operator on $\mathbf{M}$ and $\mathbf{S}$, we consider the character $\kappa : W = 1+\mathbf{p}\mathbf{Z}_p \to \Lambda^\times$ given by $\kappa(u^s) = \kappa(u^s)(X) = (1+X)^s$. It is obviously a continuous character with respect to the m-adic topology on Λ, where m is the maximal ideal of Λ. Note that for integers n prime to p, $\kappa(\langle n\rangle)(u^k-1) = \kappa(u^{s(n)})(u^k-1) = u^{ks(n)} = \omega^{-k}(n)n^k$, where we write $\langle n\rangle = \omega(n)^{-1}n = u^{s(n)}$ ($s(n) = log(\langle n\rangle)/log(u)$). Then we define for each Λ-adic form $F \in \mathbf{M}(\chi;\Lambda)$ a formal q-expansion $F|T(n)$ by

$$(1) \qquad a(m,F|T(n))(X) = \sum_{b|(m,n)} \kappa(\langle b\rangle)(X)\chi(b)b^{-1}a(mn/b^2,F)(X),$$

where b runs over all common divisors prime to p of m and n. We evaluate this formal power series $F|T(n)$ at u^k-1 where $F(u^k-1;q)$ is meaningful as a modular form. Then we see that

$$\begin{aligned} a(m,F|T(n))(u^k-1) &= \sum_{b|(m,n)} \kappa(\langle b\rangle)(u^k-1)\chi(b)b^{-1}a(mn/b^2,F)(u^k-1) \\ &= \sum_{b|(m,n)} \chi\omega^{-k}(b)b^{k-1}a(mn/b^2,F(u^k-1)) = a(m,F(u^k-1)|T(n)). \end{aligned}$$

This shows that $F|T(n)(u^k-1) = F(u^k-1)|T(n) \in \mathcal{M}_k(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};\mathcal{O})$. Therefore, F is again a Λ-adic form. Thus, the operator T(n) is well defined and so we now have Hecke operators T(n) acting on $\mathbf{M}$ and $\mathbf{S}$ and their ordinary parts.

Lemma 1 (Weierstrass preparation theorem). *Any power series* F(X) *in* Λ *can be decomposed into a product of a unit power series* U(X), *some power of a prime element in* $\mathcal{O}$, *and a distinguished polynomial* $P(X) \in \mathcal{O}[X]$. (A polynomial $P(X) = a_0+a_1X+\cdots+X^n$ is called "distinguished" if $|a_i|_p < 1$ for all i.)

Since this fact can be found in any book in commutative ring theory or p-adic number theory (for example [Bour1, III], [L, V.2], [Wa, Th.7.3]), we omit the proof. By this lemma, each non-zero power series with coefficients in $\mathcal{O}$ has only finitely many zeros in the disk $\{x \in \mathcal{O} \mid |x|_p < 1\}$.

Theorem 1 (A. Wiles). *The space of ordinary* Λ*-adic modular forms (resp. ordinary* Λ*-adic cusp forms) of character* χ *is free of finite rank over* Λ.

Proof. The proof is the same for $\mathbf{M}^{\mathrm{ord}}$ and $\mathbf{S}^{\mathrm{ord}}$. We shall give a proof only for $\mathbf{M}^{\mathrm{ord}}$. We prove first that $\mathbf{M}^{\mathrm{ord}}$ is finitely generated and is Λ-torsion-free. By definition, $\mathbf{M}^{\mathrm{ord}}$ is a Λ-submodule of the power series ring $\Lambda[[q]]$. Therefore it is Λ-torsion-free. We now prove that the rank of any finitely generated free Λ-submodule M of $\mathbf{M}^{\mathrm{ord}}$ is bounded. Let $\{F_1, F_2, \cdots, F_r\}$ be a basis of M over Λ. Since $F_1, \cdots, F_r$ are linearly independent over Λ, we can find positive integers $n_1, \ldots, n_r$ such that $D(X) = \det(a(n_i,F_j)) \neq 0$ in Λ. By the above lemma, we can take the weight k so that $D(u^k\text{-}1) \neq 0$ and $F_i(u^k\text{-}1)$ has meaning, that is, is an element of $\mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha \mathbf{p}),\chi\omega^{-k};\mathcal{O})$ for all i. Write f_i for $F_i(u^k\text{-}1)$. Then $D(u^k\text{-}1) = \det(a(n_i,f_j)) \neq 0$. Thus the modular forms $f_1, \ldots, f_r$ span a free module of rank r in $\mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha \mathbf{p}),\chi\omega^{-k};\mathcal{O})$ whose rank is bounded independently of the weight k. Thus r is bounded by a positive number independent of M. This shows that if $F_1, \cdots, F_r$ is a maximal set of linearly independent elements in $\mathbf{M}^{\mathrm{ord}}$, any element in $\mathbf{M}^{\mathrm{ord}}$ can be expressed as a linear combination of the F_i's if one allows coefficients in the quotient field $\mathbf{L}$ of Λ. We thus consider $V = \mathbf{M}^{\mathrm{ord}} \otimes_\Lambda \mathbf{L}$, which is a finite dimensional space over $\mathbf{L}$ embedded in $\mathbf{L}[[q]]$. For each $F \in \mathbf{M}^{\mathrm{ord}}$, write $F = \sum_i x_i F_i$ with $x_i \in \mathbf{L}$. Then x_i is the solution of the linear equations $(a(n_i,F_j))x = (a(n_i,F)) \in \Lambda^r$. Therefore $Dx_i \in \Lambda$, and thus $D\mathbf{M}^{\mathrm{ord}}$ is contained in $\Lambda F_1 + \cdots + \Lambda F_r$. Therefore $\mathbf{M}^{\mathrm{ord}}$ is finitely generated since Λ is noetherian. To prove the freeness over Λ, we note the following facts:

(i) Λ is a unique factorization domain;

(ii) Λ is a compact ring.

The first fact follows easily from Lemma 1 (see [Bour1, VII.3.9]). The second fact follows from the fact that for the maximal ideal m of Λ, Λ/m^n is always a finite ring and we have topologically $\Lambda = \varprojlim_\alpha (\Lambda/m^\alpha) = \varprojlim_\alpha (\Lambda/P^\alpha)$ for any non-trivial element P in m. Since $\mathbf{M}^{\mathrm{ord}}$ is finitely generated, we can find k so that $F(u^k\text{-}1)$ is meaningful for all F in $\mathbf{M}^{\mathrm{ord}}$. If $F(u^k\text{-}1) = 0$, then $a(n,F)(u^k\text{-}1)$ is divisible by $P = P_k = X\text{-}(u^k\text{-}1)$ for all n. Thus by dividing F by P, we still have an element of $\mathbf{M}^{\mathrm{ord}}$, because $(F/P_k) = F(u^j\text{-}1)/(u^j\text{-}u^k)$ for all $j \neq k$, which is a modular form. Thus

$$P\mathbf{M}^{\mathrm{ord}} = \{F \in \mathbf{M}^{\mathrm{ord}} \mid F(u^k\text{-}1) = 0\}.$$

So $\mathbf{M}^{\mathrm{ord}}/P\mathbf{M}^{\mathrm{ord}}$ can be embedded into $\mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha \mathbf{p}),\chi\omega^{-k};\mathcal{O})$. Thus $\mathbf{M}^{\mathrm{ord}}/P\mathbf{M}^{\mathrm{ord}}$ is $\mathcal{O}$-free of finite rank. Let us take F_i $(i=1, \cdots, r)$ so that $F_i \bmod P\mathbf{M}^{\mathrm{ord}}$ gives an $\mathcal{O}$-basis of $\mathbf{M}^{\mathrm{ord}}/P\mathbf{M}^{\mathrm{ord}}$. Note that the F_i's are linearly independent over Λ. In fact, if not, we may suppose that $\lambda_1 F_1 + \cdots + \lambda_r F_r = 0$

with at least one of the λ_i's not divisible by P. Then reducing modulo P, we have a non-trivial linear relation between the F_i mod P, which is a contradiction, and hence the F_i's are linearly independent. Consider $M = \Lambda F_1 + \cdots + \Lambda F_r$. Then M is a Λ-free module of rank r and M/PM coincides with $\mathbf{M}^{ord}/P\mathbf{M}^{ord}$ because if F is an element of $\mathbf{M}^{ord}$, then we can find a finite linear combination G_0 of the F_j's such that $F-G_0$ is divisible by P. We now apply this argument to $(F-G_0)/P$ and get another linear combination G_1 of the F_j's such that $(F-G_0)/P-G_1$ is divisible by P. Continuing this process, we can find the G_j's which are linear combinations of the F_j's such that $F \equiv G_0+G_1P+\cdots+G_{j-1}P^{j-1} \bmod P^j$. Thus $M/P^jM = \mathbf{M}^{ord}/P^j\mathbf{M}^{ord}$. Note that the series $G_0+G_1P+\cdots+G_{j-1}P^{j-1}$ converges in M by identifying M with Λ^r by the basis F_j's. Thus $M = \mathbf{M}^{ord}$ and hence $\mathbf{M}^{ord}$ is Λ-free.

From the above proof, we know for sufficiently large k that $\mathbf{M}^{ord}/P\mathbf{M}^{ord}$ for $P = X-(u^k-1)$ is naturally embedded into $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};\mathcal{O})$; in particular, we have, for sufficiently large k,

$$\mathrm{rank}_\Lambda(\mathbf{M}^{ord}(\chi,\Lambda)) \le \mathrm{rank}_{\mathcal{O}}(\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};\mathcal{O})).$$

Now we want to define the idempotent e on $\mathbf{M} = \mathbf{M}(\chi,\Lambda)$. Take F in $\mathbf{M}$. We may assume that $F(u^k-1)$ is meaningful for every $k \ge a$. We consider the sum $\mathcal{M}_{a,k}(A) = \sum_{j=a}^k \mathcal{M}_j(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-j};A)$ inside $A[[q]]$ for a subalgebra A of $\mathbf{C}$ or $\overline{\mathbf{Q}}_p$. The space $\mathcal{M}_{a,k}(A)$ is in fact isomorphic to the direct sum. In fact, over A which is a subalgebra of $\mathbf{C}$, we see that if $\sum_{j=a}^k f_j = 0$ for $f_j \in \mathcal{M}_j(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-j};A)$, then for any $\gamma \in \Gamma_1(p^\alpha\mathbf{p})$,

$$\sum_{j=a}^k f_j(\gamma(z)) = \sum_{j=a}^k f_j(z)j(\gamma,z)^j = 0.$$

We can of course choose $\gamma_i \in \Gamma_1(p^\alpha\mathbf{p})$ so that $\det(j(\gamma_i,z)^j) \ne 0$ $(0 \le i \le k-a$ and $a \le j \le k)$. This shows that $f_j = 0$. For A inside $\overline{\mathbf{Q}}_p$, the space over A is defined by the scalar extension of the space over $\overline{\mathbf{Q}} \cap A$; hence, we know the assertion. Thus we have a natural action of $T(n)$ on $\mathcal{M}_{a,k}(A)$. Since $\mathcal{M}_{a,k}(\mathcal{O})$ is $\mathcal{O}$-free of finite rank, the subalgebra R of $\mathrm{End}_{\mathcal{O}}(\mathcal{M}_{a,k}(\mathcal{O}))$ generated by $T(p)$ over $\mathcal{O}$ is $\mathcal{O}$-free of finite rank. Thus we can take the limit $e_k = \lim_{n\to\infty} T(p)^{n!}$ in R. This idempotent preserves $\mathcal{M}_{a,j}(\mathcal{O})$ for $j \le k$ and induces the projector e on each subspace stable under e. Now we consider the Λ-submodules

$$\mathbf{M}_{a,k} = \{G \in \mathbf{M} \mid G(u^j-1) \in \mathcal{M}_j(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-j};\mathcal{O}) \text{ for all } j \text{ in } [a,k]\},$$
$$\mathbf{M}'_{a,k} = \{G \in \mathbf{M}_{a,k} \mid G(u^j-1) = 0 \text{ for all } j \text{ in } [a,k]\}.$$

We note that $\mathbf{M}'_{a,k}$ may not equal $\Omega_k\mathbf{M}_{a,k}$, where $\Omega_k = \prod_{j=a}^{k}(X-(u^j-1))$. By definition, the map $G \mapsto \sum_{j=a}^{k} G(u^j-1)$ induces an injection of $\mathbf{M}_{a,k}/\mathbf{M}'_{a,k}$ into $\mathcal{M}_{a,k}(\mathcal{O})$. Since $T(p)$ preserves $\mathbf{M}'_{a,k}$ and $\mathbf{M}_{a,k}$, the idempotent e_k acts on $\mathbf{M}_{a,k}/\mathbf{M}'_{a,k}$. If $a \le j \le k$, we have the natural projection $\pi_{k,j}$ of $\mathbf{M}_{a,k}/\mathbf{M}'_{a,k}$ to $\mathbf{M}_{a,j}/\mathbf{M}'_{a,j}$ satisfying $e_j\circ\pi_{k,j} = \pi_{k,j}\circ e_k$. Note that $\Omega_k\Lambda$ is the kernel of the map $G \mapsto \sum_{j=a}^{k} G(u^j-1)$ on Λ, and hence $\mathbf{M}_{a,k}/\mathbf{M}'_{a,k}$ can be embedded into $(\Lambda/\Omega_k)[[q]]$. The sequence of ideals $\{\Omega_k\Lambda\}$ is a decreasing sequence of ideals of Λ and $\bigcap_k \Omega_k\Lambda = \{0\}$, since any power series has only finitely many zeros inside the unit disk in $\overline{\mathbf{Q}}_p$. Thus $\Lambda = \varprojlim_k (\Lambda/\Omega_k)$. Therefore $a(n,F\,|\,e)(X) = \varprojlim_k a(n,F\,|\,e_k)$ exists in Λ and $a(n,F\,|\,e)(u^k-1) = a(n,F(u^k-1)\,|\,e)$. This shows that $F\,|\,e \in \mathbf{M}^{ord}$. Since the projective limit topology of the p-adic topology of Λ/Ω_k coincides with the m-adic topology of Λ for the maximal ideal m of Λ, the above proof shows

$$F\,|\,e = \lim_{n\to\infty}(F\,|\,T(p)^{n!}) \text{ under the } m\text{-adic topology.} \tag{2}$$

Summing up, we have

Proposition 1. *There exists a unique projector* e *on* $\mathbf{M}(\chi,\Lambda)$ *to* $\mathbf{M}^{ord}(\chi,\Lambda)$ *which satisfies* $F\,|\,e(u^k-1) = F(u^k-1)\,|\,e$ *for all* $F \in \mathbf{M}(\chi,\Lambda)$.

In §1, we constructed a Λ-adic modular form $E(\chi)$ out of Eisenstein series for characters χ of μ ($\mu = \{\zeta \in \mathbf{Z}_p \,|\, \zeta^{p-1} = 1\}$). We can extend the construction to characters χ modulo $p^\alpha\mathbf{p}$ as follows. Let $\chi : (\mathbf{Z}/p^\alpha\mathbf{p}\mathbf{Z})^\times \to \mathcal{O}^\times$ be a primitive character, and put $\chi_0 = \chi|_\mu$. We define $E(\chi)(X) = E(\chi_0)(\zeta X+(\zeta-1))$ for $\zeta = \chi(u)$. Then we see from Proposition 1.1 that $E(\chi)(u^k-1) = E(\chi_0)(\zeta u^k-1) = E_k(\chi\omega^{-k})$. Thus $E(\chi)$ is a Λ-adic form of character χ in the sense of (Λ'). Moreover take a modular form $g \in \mathcal{M}_a(\Gamma_0(p^\beta\mathbf{p}),\psi;\mathcal{O})$ for a finite order character $\psi : \mathbf{Z}_p^\times \to \mathcal{O}^\times$, and put $\psi_0 = \psi|_\mu$. Then multiplying $E(\chi\psi_0^{-1})$ to g and making the variable change $X \mapsto \psi(u)^{-1}u^{-a}X+(\psi(u)^{-1}u^{-a}-1)$ in $gE(\chi)(X)$, we obtain $g*E(\chi\psi_0^{-1})(X) \in \mathbf{M}(\chi\psi_0,\Lambda)$ such that $g*E(\chi\psi_0^{-1})(u^k-1) = gE_{k-a}(\chi\psi^{-1}\omega^{-k})$ for all $k \ge a$, which is an element in $\mathcal{M}_k(\Gamma_0(p^\gamma\mathbf{p}),\chi\omega^{-k};\mathcal{O})$ for $\gamma = \max(\alpha,\beta)$. For any Λ-algebra A, we define $\mathbf{M}^{ord}(\chi;A) = \mathbf{M}^{ord}(\chi;\Lambda)\otimes_\Lambda A$. Now we prove

Proposition 2. *Let* χ *be either a primitive character modulo* $p^\alpha\mathbf{p}$ *having values in* $\mathcal{O}^\times$ *or* $\chi = \mathrm{id}$ *and* $\alpha = 0$. *Let* $g = G_a(\psi)$ *for a character* $\psi : (\mathbf{Z}/p^\alpha\mathbf{p}\mathbf{Z})^\times \to \mathcal{O}^\times$ *with* $\psi(-1) = (-1)^a$. *Then the elements of the form*

$(g*E(\chi\psi_0^{-1})\,|\,e)\,|\,T(n)$ $(\psi_0 = \psi\,|\,\mu)$ *together with* $E(\chi)$ *span* $\mathbf{M}^{ord}(\chi,\mathbf{L})$ *over the quotient field* $\mathbf{L}$ *of* Λ. *Moreover if* $k > 2a+2$ *and* $\chi\omega^{-k}$ *is primitive modulo* $p^\alpha\mathbf{p}$, *then the K-subspace of* $K[[q]]$ *spanned by the specialized image of* $\mathbf{M}^{ord}(\chi,\Lambda)$ *at weight* k *contains the whole space* $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$ *and coincides with* $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$ *if* k *is sufficiently large.*

Taking a to be 2, we know by Corollary 5.4.1 that any ordinary modular form can be lifted to a Λ-adic ordinary form (up to constant multiple) if $k > 6$ and that $\mathbf{M}^{ord}(\chi,\Lambda)/P_k\mathbf{M}^{ord}(\chi,\Lambda)\otimes K \cong \mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$ if k is large and $\chi\omega^{-k}$ is primitive. Moreover we know the independence of the dimension of $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$ from the weight if k is large, as long as $\chi\omega^{-k}$ is primitive. This fact is actually true for all $k \geq 2$ as we will see later.

Proof. By Theorem 5.4.1, as long as $\chi\omega^{-k}$ is primitive, the modular forms of the type $g*E(\chi\psi_0^{-1})\,|\,T(n)(u^k-1) = gE_{k-a}(\psi^{-1}\chi\omega^{-k})\,|\,T(n)$ $(n = 1, 2, \cdots)$ together with $E_k(\chi\omega^{-k}) = E(\chi)(u^k-1)$ and $G_k(\chi\omega^{-k})$ span $\mathcal{M}_k(\Gamma,\chi\omega^{-k};K)$ for $\Gamma = \Gamma_0(p^\alpha\mathbf{p})$. Hence ordinary forms of the form

$$(g*E(\chi\psi_0^{-1})\,|\,e)\,|\,T(n)(u^k-1) = (gE_{k-a}(\chi\psi^{-1}\omega^{-k})\,|\,e)\,|\,T(n)$$

together with $E(\chi)(u^k-1)$ span $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$, because we know that e annihilates $G_k(\chi\omega^{-k})$ because $G_k(\chi\omega^{-k})\,|\,T(p) = p^{k-1}G_k(\chi\omega^{-k})$. Thus the subspace of $K[[q]]$ spanned by the specialization of Λ-adic forms at weight k contains $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$ if $k > 2a+2$. By the proof of Theorem 1, it is clear that for sufficiently large k, the specialization map from $\mathbf{M}/P_k\mathbf{M}$ $(P_k = X+1-u^k \in \Lambda)$ for $\mathbf{M} = \mathbf{M}^{ord}(\chi;\Lambda)$ into $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$ is injective. Choosing large k so that $\chi\omega^{-k}$ is primitive, we then know that $\{F_i\}_{i\in I}$ (in the proof of Theorem 1) span $\mathbf{M}^{ord}(\chi;\mathbf{L})$ if $\{F_i(u^k-1)\}_i$ span $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$ over K. This shows the proposition.

By definition, we also know that, for any character $\varepsilon : W/W^{p\beta} \to \mathcal{O}^\times$,

$$\begin{aligned}(g*E(\chi\psi_0^{-1}\,|\,e)\,|\,T(n)(\varepsilon(u)u^k-1) &= (g*E(\chi\psi_0^{-1})(\varepsilon(u)u^k-1)\,|\,e)\,|\,T(n)\\ &= (gE_{k-a}(\varepsilon\chi\psi^{-1}\omega^{-k})\,|\,e)\,|\,T(n).\end{aligned}$$

Defining formally $\varepsilon_*F(X;q) = F(\varepsilon(u)X+(\varepsilon(u)-1))$ as an element of $\Lambda[[q]]$, we see from the above formula that $\varepsilon_*(g*E(\chi\psi_0^{-1})\,|\,e)\,|\,T(n)$ is a Λ-adic form of character $\varepsilon\chi$ as long as $\varepsilon\chi$ is primitive modulo $\mathbf{p}p^{\max(\alpha,\beta)}$. We now show that this is always the case without assuming the condition on primitivity. The point of the argument is that for integer $\beta \geq \alpha$, defining $\Gamma_{\alpha,\beta} = \Gamma_1(p^\alpha)\cap\Gamma_0(p^\beta)$, we have

$$\Gamma_{\alpha,\beta}\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_{\alpha,\beta-1} = \Gamma_{\alpha,\beta}\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_{\alpha,\beta} \text{ as sets.}$$

This fact can be shown as follows. Writing η for $\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}$, we know $\Gamma\eta\Gamma' = \bigcup_i \Gamma\eta\delta_i$ is disjoint if $\Gamma' = \bigcup_i(\eta^{-1}\Gamma\eta\cap\Gamma')\delta_i$ is a disjoint union. In our case, we see easily that

$$\Gamma_{\alpha,\beta-1} = \bigcup_{i=1}^{p}(\eta^{-1}\Gamma_{\alpha,\beta}\eta\cap\Gamma_{\alpha,\beta-1})\delta_i \text{ and } \Gamma_{\alpha,\beta} = \bigcup_{i=1}^{p}(\eta^{-1}\Gamma_{\alpha,\beta}\eta\cap\Gamma_{\alpha,\beta})\delta_i$$

for the same $\delta_i = \begin{pmatrix}1 & i\\ 0 & 1\end{pmatrix}$. This implies that $T(p)^{\beta-\alpha}$ not only acts on $\mathcal{S}_k(\Gamma_0(p^\beta\mathbf{p}),\chi)$ but also decreases the level up to $p^\alpha\mathbf{p}$ if χ is primitive modulo $p^\alpha\mathbf{p}$. In other words, $T(p)^{\beta-\alpha}$ brings $\mathcal{S}_k(\Gamma_0(p^\beta\mathbf{p}),\chi)$ into $\mathcal{S}_k(\Gamma_0(p^\alpha\mathbf{p}),\chi)$. Thus actually $\varepsilon_*(g*E(\chi\psi_0^{-1})\,|\,T(n)\,|\,e) = \varepsilon_*(g*E(\chi\psi_0^{-1})\,|\,T(n))\,|\,e$ has level $p^\alpha\mathbf{p}$, which is the conductor of $\varepsilon\chi$ (i.e. $\varepsilon\chi$ is primitive modulo $p^\alpha\mathbf{p}$). This shows our claim. Thus $F \mapsto \varepsilon_* F$ takes ordinary Λ-adic forms of character χ to those of character $\varepsilon\chi$, because the forms $g*E(\chi\psi_0^{-1})\,|\,T(n)\,|\,e$ $(n = 1, 2, \ldots)$ span the total space $\mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{L})$. Since ε_* is induced from the ring automorphism of the ring Λ, ε_* is injective. Since $(\varepsilon\varepsilon')_* = \varepsilon_*\varepsilon'_*$ and hence $\varepsilon_*\varepsilon^{-1}{}_* = \varepsilon^{-1}{}_*\varepsilon'_* = \mathrm{id}_* = \mathrm{id}$, ε_* has to be a surjective isomorphism. We have $\varepsilon_* : \mathbf{M}^{\mathrm{ord}}(\chi;\Lambda) \cong \mathbf{M}^{\mathrm{ord}}(\varepsilon\chi;\Lambda)$ for any finite order character $\varepsilon : W \to \mathcal{O}^\times$. Summing up we have

Theorem 2. *For each finite order character* $\varepsilon : W \to \mathcal{O}^\times$, *we have an isomorphism* $\varepsilon_* : \mathbf{M}^{\mathrm{ord}}(\chi;\Lambda) \cong \mathbf{M}^{\mathrm{ord}}(\varepsilon\chi;\Lambda)$ *functorial in* ε *(i.e.* $(\varepsilon\varepsilon')_* = \varepsilon_*\varepsilon'_*$*). Moreover, for almost all positive integers* k, $F(\varepsilon(u)u^k-1)$ *is an element of* $\mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\beta\mathbf{p}),\varepsilon\chi\omega^{-k};\mathcal{O})$ *if* $F \in \mathbf{M}^{\mathrm{ord}}(\chi;\Lambda)$, *where* β *is the minimum exponent such that* $\varepsilon\chi$ *factors through* W/W^{p^β}. *The same assertion also holds for cusp forms.*

By this theorem, without losing much generality, we may assume that χ is a character modulo $\mathbf{p}$ as we did in the definition (Λ). Hereafter we assume that χ is a character of $(\mathbf{Z}/\mathbf{p}\mathbf{Z})^\times$. For each character ε of W with values in $\overline{\mathbf{Q}}_p$, we write $\mathcal{O}[\varepsilon]$ for the subring of $\overline{\mathbf{Q}}_p$ generated over $\mathcal{O}$ by the values of ε. To prove the following theorem, we need a careful analysis of group cohomology attached to the space of modular forms. Although the following theorem itself is true for all primes p, the cuspidal theory is empty for $p \le 7$ because *a posteriori* we find that $\mathbf{S}^{\mathrm{ord}}(\chi;\Lambda) = 0$ for all $p \le 7$. (We should mention that if we consider $\Gamma_0(Np^\alpha)$ in place of $\Gamma_0(p^\alpha)$ for N prime to p, the theory is not empty even for $p = 2$ and 3.) Assuming $p \ge 5$, the analysis of group cohomology becomes a

lot easier because $\Gamma_1(p)$ is torsion-free. For this reason, we throw away the primes $p = 2$ and 3 and give the exposition only when $p \geq 5$.

Theorem 3. *For all integers* $k \geq 1$ *and a primitive finite order character* ε *of* W/W^{p^α} *and for any modular form* $f \in \mathcal{M}_k(\Gamma_0(p^\alpha \mathbf{p}),\varepsilon\chi\omega^{-k};\mathcal{O}[\varepsilon])$, *there exists a* Λ*-adic form* F *of character* χ *such that* $F(\varepsilon(u)u^k-1) = f$. *Moreover if* $k \geq 2$, *we have the isomorphisms:*

$$\mathbf{M}^{ord}(\chi;\Lambda)/P_{k,\varepsilon}\mathbf{M}^{ord}(\chi;\Lambda) \cong \mathcal{M}_k^{ord}(\Gamma_0(p^\alpha \mathbf{p}),\varepsilon\chi\omega^{-k};\mathcal{O}[\varepsilon]),$$
$$\mathbf{S}^{ord}(\chi;\Lambda)/P_{k,\varepsilon}\mathbf{S}^{ord}(\chi;\Lambda) \cong \mathcal{S}_k^{ord}(\Gamma_0(p^\alpha \mathbf{p}),\varepsilon\chi\omega^{-k};\mathcal{O}[\varepsilon]),$$

where the map is induced by $F \mapsto F(\varepsilon(u)u^k-1)$ *and* $P_{k,\varepsilon}$ *is the prime ideal generated by* $X-(\varepsilon(u)u^k-1)$.

Proof. We consider the Λ-adic Eisenstein series $E' = XE(id)(X;q)$. We know from Theorem 3.6.2 that

$$2^{-1}(u^s-1)\zeta_p(1-s)\,|_{s=0} = 2^{-1}log(u)(p^{-1}-1)$$

which is a p-adic unit. Thus we have $E'(0;q) = 2^{-1}log(u)(p^{-1}-1)$. We put

$$E(X;q) = \{2^{-1}log(u)(p^{-1}-1)\}^{-1}E'(X;q) \in \mathbf{M}^{ord}(id,\Lambda).$$

Then $E(0;q) = 1$ and for any $g \in \mathcal{M}_k^{ord}(\Gamma_0(p^\alpha \mathbf{p}),\varepsilon\chi\omega^{-k};\mathcal{O}[\varepsilon])$, defining

$$g*E(X;q) = gE(\varepsilon^{-1}(u)u^{-k}X+(\varepsilon^{-1}(u)u^{-k}-1)) \in \mathbf{M}(\chi;\Lambda),$$

we have $(g*E)\,|\,e(0) = (g*E(0))\,|\,e = g$. This shows the first assertion. By Proposition 2, we get, if k is sufficiently large

$$(*)\quad \{\mathbf{M}^{ord}(\chi;\Lambda)/P_{k,\varepsilon}\mathbf{M}^{ord}(\chi;\Lambda)\}\otimes_{\mathcal{O}}K \cong \mathcal{M}_{k,\varepsilon}^{ord} = \mathcal{M}_k^{ord}(\Gamma_0(p^\alpha \mathbf{p}),\varepsilon\chi\omega^{-k};K[\varepsilon]).$$

Since the unique Eisenstein series in $\mathcal{M}_k^{ord}(\Gamma_0(p^\alpha \mathbf{p}),\varepsilon\chi\omega^{-k};K[\varepsilon])$ is given by $E(\chi)(\varepsilon(u)u^k-1)$, we conclude, if k is sufficiently large, that

$$(**)\quad \{\mathbf{S}^{ord}(\chi;\Lambda)/P_{k,\varepsilon}\mathbf{S}^{ord}(\chi;\Lambda)\}\otimes_{\mathcal{O}}K \cong \mathcal{S}_{k,\varepsilon}^{ord} = \mathcal{S}_k^{ord}(\Gamma_0(p^\alpha \mathbf{p}),\varepsilon\chi\omega^{-k};K[\varepsilon]).$$

This combined with the first assertion shows the second assertion for large k. Thus we need to show that $(*)$ and $(**)$ hold for $k \geq 2$. First we show that $(*)$ for $k \geq 2$. Then $(**)$ follows from $(*)$ by the same argument as above. Since every classical (ordinary) form lifts to a Λ-adic ordinary form, the image M of specialization in $\mathcal{O}[\varepsilon][[q]]$ contains $\mathcal{M}_{k,\varepsilon}^{ord}$ and $M/\mathcal{M}_k^{ord}$ is $\mathcal{O}$-free. Thus we only need to prove the following equality of the ranks:

$$\mathrm{rank}_{\mathcal{O}[\varepsilon]}\mathcal{M}_{k,\varepsilon}^{ord} = \mathrm{rank}_\Lambda \mathbf{M}^{ord}(\chi;\Lambda).$$

For this we may extend scalars and may therefore assume that $\varepsilon\chi\omega^{-k}$ has values in $\mathcal{O}$. Let $\psi : (\mathbf{Z}/p^{\beta}\mathbf{p}\mathbf{Z})^{\times} \to \mathcal{O}^{\times}$ be a character. We pick a prime element ϖ of $\mathcal{O}$ and put $\mathbf{F} = \mathcal{O}/\varpi\mathcal{O}$. We take a normal subgroup Δ of $\Gamma_0(\mathbf{p})$ so that $\Gamma_0(\mathbf{p})/\Delta$ has order prime to p and Δ is torsion-free. If $p > 2$, $\Delta = \Gamma(4)$ does the job. Then for any $\mathcal{O}[\Gamma_0(\mathbf{p})]$-module M,

$$H^0(\Gamma_0(\mathbf{p}p^{\alpha}),H^q(\Delta\cap\Gamma_0(\mathbf{p}p^{\beta}),M)) \cong H^q(\Gamma_0(\mathbf{p}p^{\beta}),M)$$

because $\mathrm{Tr}\circ\mathrm{res} = (\Gamma_0(\mathbf{p}):\Lambda)$. For the moment, we suppose that $p > 2$. Then by Proposition 6.1.1, $H^2(\Delta\cap\Gamma_0(\mathbf{p}p^{\alpha}),M) = 0 = H^2(\Gamma_0(\mathbf{p}p^{\alpha}),M)$. From the cohomology exact sequence attached to

$$(***) \qquad 0 \to L(n,\psi;\mathcal{O}) \xrightarrow{\varpi} L(n,\psi;\mathcal{O}) \to L(n,\psi;\mathbf{F}) \to 0,$$

we get an exact sequence for $\Gamma = \Gamma_0(p^{\beta}\mathbf{p})$:

$$0 \to H^1(\Gamma,L(n,\psi;\mathcal{O}))\otimes_{\mathcal{O}}\mathbf{F} \to H^1(\Gamma,L(n,\psi;\mathbf{F})) \to H^2(\Gamma,L(n,\psi;\mathcal{O})) = 0.$$

This shows that $\dim_K eH^1(\Gamma_0(p^{\beta}\mathbf{p}),L(n,\psi;K)) = \dim_{\mathbf{F}} eH^1(\Gamma_0(p^{\beta}\mathbf{p}),L(n,\psi;\mathbf{F}))$. Now we again consider the map $i : L(n,\psi;\mathbf{F}) \to L(0,\psi\omega^n;\mathbf{F})$ given by $i(P(X,Y)) = P(1,0)$, which is a homomorphism of $\Gamma_0(p^{\beta}\mathbf{p})$-modules. Here we have $\psi\omega^n$ in place of ψ because on X^n,

$$\Gamma_0(\mathbf{p}p^{\beta}) \ni \gamma \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \bmod p \quad \text{for } a \in \mathbf{Z}_p^{\times}$$

acts by $a^n\psi(a) \equiv \psi\omega^n(a) \bmod p$. Exactly in the same manner as in the proof of Theorem 2.2, we know that i induces an isomorphism

$$i_* : eH^1(\Gamma_0(p^{\beta}\mathbf{p}),L(n,\psi;\mathbf{F})) \cong eH^1(\Gamma_0(p^{\beta}\mathbf{p}),L(0,\psi\omega^n;\mathbf{F})).$$

Note that $\psi(u) \equiv 1 \bmod p$ for the maximal ideal p of $\mathcal{O}$ because $\psi(u)$ is a p-power root of unity and there are no p-power roots of unity except 1 in a characteristic p situation. Thus if $\psi = \varepsilon\chi\omega^{-k}$, we have for $\Gamma = \Gamma_0(p^{\alpha}\mathbf{p})$, writing χ_μ for the restriction of χ to μ and noting the fact that $\chi \equiv \chi_\mu \bmod p$,

$$i_* : eH^1(\Gamma,L(n,\psi;\mathbf{F})) \cong eH^1(\Gamma,L(0,\chi\omega^{-2};\mathbf{F})) \cong eH^1(\Gamma_0(\mathbf{p}),L(0,\chi_\mu\omega^{-2};\mathbf{F})).$$

Here the last isomorphism follows from the fact that e decreases the level to the conductor of the character. Now, for any $\mathcal{O}$-module M, writing $M[\varpi]$ for the submodule killed by ϖ, from the exact sequence $(***)$, we have the following exact sequence for $\Gamma = \Gamma_0(p^{\beta}\mathbf{p})$:

$$0 \to H^0(\Gamma,L(n,\psi;\mathcal{O}))\otimes_{\mathcal{O}}F \xrightarrow{\iota} H^0(\Gamma,L(n,\psi;\mathbf{F})) \to H^1(\Gamma,L(n,\psi;\mathcal{O}))[\varpi] \to 0.$$

We see easily by definition, for all j, that

$$X^{n-j}Y^j \mid T(p) = \sum_{i=1}^{p} \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}^{\iota} X^{n-j}Y^j = \sum_i p^j(X+iY)^{n-j}Y^j.$$

If $j > 0$, then $X^{n-j}Y^j \mid T(p) \equiv 0 \bmod p$. If $j = 0$, $X^n \mid T(p) \bmod p$ does not have a term involving X^n. Thus $X^n \mid T(p)^2 \equiv 0 \bmod p$. Anyway, we have $eH^0(\Gamma,L(n,\psi;\mathbf{F})) = 0$ for all ψ and n. Thus $eH^1(\Gamma,L(n,\psi;\mathcal{O}))$ is $\mathcal{O}$-free. Thus we have from Theorem 6.3.3 that

$$\begin{aligned}
&2\dim_K \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\varepsilon\chi\omega^{-k};K)-1 \\
&\quad = \dim_K \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\varepsilon\chi\omega^{-k};K)+\dim_K \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\varepsilon\chi\omega^{-k};K) \\
&\quad = \dim_K H^1_{\mathrm{ord}}(\Gamma_0(\mathbf{p}p^\alpha),L(n,\varepsilon\chi\omega^{-k};K)) \\
&\quad = \dim_{\mathbf{F}} H^1_{\mathrm{ord}}(\Gamma_0(\mathbf{p}p^\alpha),L(n,\varepsilon\chi\omega^{-k};\mathbf{F})) \\
&\quad = \dim_{\mathbf{F}} H^1_{\mathrm{ord}}(\Gamma_0(\mathbf{p}),L(n,\chi_\mu\omega^{-2};\mathbf{F})) \\
&\quad = \mathrm{rank}_{\mathcal{O}} H^1_{\mathrm{ord}}(\Gamma_0(\mathbf{p}),L(0,\chi_\mu\omega^{-2};\mathcal{O})) \\
&\quad = \dim_K H^1_{\mathrm{ord}}(\Gamma_0(\mathbf{p}),L(0,\chi_\mu\omega^{-2};K)) \\
&\quad = \dim_K \mathcal{S}_2^{\mathrm{ord}}(\Gamma_0(\mathbf{p}),\chi_\mu\omega^{-2};K) + \dim_K \mathcal{M}_2^{\mathrm{ord}}(\Gamma_0(\mathbf{p}),\chi_\mu\omega^{-2};K) \\
&\quad = 2\dim_K \mathcal{M}_2^{\mathrm{ord}}(\Gamma_0(\mathbf{p}),\chi_\mu\omega^{-2};K)-1.
\end{aligned}$$

This shows that $\dim_K \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(q),\varepsilon\chi\omega^{-k};K)$ is independent of $k \geq 2$ and ε. This number coincides with the rank of $\mathbf{M}^{\mathrm{ord}}(\chi;\Lambda)$ because of $(*)$ for large k. Therefore for any $k \geq 2$, we have

$$\dim_K \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(q),\varepsilon\chi\omega^{-k};K) = \mathrm{rank}_\Lambda \mathbf{M}^{\mathrm{ord}}(\chi;\Lambda),$$

which is what we wanted. This also finishes the proof of Theorem 2.1 when $p > 2$.

We now give a sketch of the argument in the case when $p = 2$. We replace $\Gamma_0(\mathbf{p}p^\alpha)$ in the above argument by $\Gamma'_0(\mathbf{p}p^\alpha) = \Gamma_0(\mathbf{p}p^\alpha)\cap\Gamma_1(5)$. Then $\Gamma'_0(\mathbf{p}p^\alpha)$ is torsion-free, and we know by the same argument that

$$H^1_{\mathrm{ord}}(\Gamma'_0(p^\alpha\mathbf{p}),L(n,\varepsilon\chi\omega^{-k};\mathbf{F})) \cong H^1_{\mathrm{ord}}(\Gamma'_0(\mathbf{p}),L(0,\chi_\mu\omega^{-2};\mathbf{F})).$$

This shows first that

$$\dim_K \mathcal{M}_k^{\mathrm{ord}}(\Gamma'_0(p^\alpha\mathbf{p}),\varepsilon\chi\omega^{-k};K) = \dim_K \mathcal{M}_2^{\mathrm{ord}}(\Gamma'_0(\mathbf{p}),\chi_\mu\omega^{-2};K)$$

and then taking the subspace invariant under $\Gamma_0(p^\alpha\mathbf{p})$, we can conclude with the desired identity:

$$\dim_K \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(2^{\alpha+2}),\varepsilon\chi\omega^{-k};K) = \dim_K \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(4),\varepsilon_\mu\omega^{-2};K) = 1.$$

Anyway the ordinary part $\mathbf{S}^{\mathrm{ord}}(\chi;\Lambda) = 0$ if $p \le 7$ as is clear from the fact that $\dim \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p)) = \dim \mathcal{S}_k^{\mathrm{ord}}(\mathrm{SL}_2(\mathbf{Z})) = 0$ if $k \le 10$ (see Proposition 2.2 and the dimension formula for $\mathcal{S}_k^{\mathrm{ord}}(\mathrm{SL}_2(\mathbf{Z}))$ in §5.2).

We now define the universal ordinary Hecke algebra $\mathbf{H}^{\mathrm{ord}}(\chi;\Lambda)$ (resp. $\mathbf{h}^{\mathrm{ord}}(\chi;\Lambda)$) by the subalgebra of $\mathrm{End}_\Lambda(\mathbf{M}^{\mathrm{ord}}(\chi,\Lambda))$ (resp. $\mathrm{End}_\Lambda(\mathbf{S}^{\mathrm{ord}}(\chi,\Lambda))$) generated by all the $T(n)$'s over Λ. For any Λ-algebra A, we define $\mathbf{H}^{\mathrm{ord}}(\chi;A)$ (resp. $\mathbf{h}^{\mathrm{ord}}(\chi;A)$) by $\mathbf{H}^{\mathrm{ord}}(\chi;\Lambda)\otimes_\Lambda A$ (resp. $\mathbf{h}^{\mathrm{ord}}(\chi;\Lambda)\otimes_\Lambda A$). Similarly we define

$$\mathbf{M}^{\mathrm{ord}}(\chi;A) = \mathbf{M}^{\mathrm{ord}}(\chi;\Lambda)\otimes_\Lambda A,\quad \mathbf{S}^{\mathrm{ord}}(\chi;A) = \mathbf{S}^{\mathrm{ord}}(\chi;\Lambda)\otimes_\Lambda A,$$
$$\mathbf{M}(\chi;A) = \mathbf{M}(\chi;\Lambda)\otimes_\Lambda A \text{ and } \mathbf{S}(\chi;A) = \mathbf{S}(\chi;\Lambda)\otimes_\Lambda A.$$

Then we have the well defined projection map $e : \mathbf{M}(\chi;A) \to \mathbf{M}^{\mathrm{ord}}(\chi;A)$.

Theorem 4 (semi-simplicity). $\mathbf{H}^{\mathrm{ord}}(\chi;\Lambda)$ *(resp.* $\mathbf{h}^{\mathrm{ord}}(\chi;\Lambda)$*) is reduced; i.e.,* $\mathbf{H}^{\mathrm{ord}}(\chi;\mathbf{L})$ *(resp.* $\mathbf{h}^{\mathrm{ord}}(\chi;\mathbf{L})$*) for the quotient field* $\mathbf{L}$ *of* Λ *is semi-simple.*

Proof. We choose a basis $\{F_i\}_{i=1,\cdots,r}$ of $\mathbf{M}^{\mathrm{ord}} = \mathbf{M}^{\mathrm{ord}}(\chi,\Lambda)$. Then we can identify $\mathrm{End}_\Lambda(\mathbf{M}^{\mathrm{ord}})$ with the matrix ring $M_r(\Lambda)$. Suppose $h \in \mathbf{H}^{\mathrm{ord}}(\chi;\Lambda)$ is nilpotent. For $k \ge 2$, $\mathrm{End}_\Lambda(\mathbf{M}^{\mathrm{ord}})\otimes_\Lambda \Lambda/P_k\Lambda \cong \mathrm{End}_{\mathcal{O}}(\mathbf{M}^{\mathrm{ord}}/P_k\mathbf{M}^{\mathrm{ord}})$ for $P_k = X-(u^k-1)$. Note that the image of h in $\mathrm{End}_{\mathcal{O}}(\mathbf{M}^{\mathrm{ord}}/P_k\mathbf{M}^{\mathrm{ord}})$ gives an element of $\mathbf{H}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};\mathcal{O})$ because $\mathbf{M}^{\mathrm{ord}}/P_k\mathbf{M}^{\mathrm{ord}}\otimes_{\mathcal{O}}K \cong \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};K)$. By Corollary 2.1 and Theorem 5.3.2, $\mathbf{H}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};\mathcal{O})$ has no non-trivial nilpotent elements. Thus the image of h in $\mathbf{H}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\chi\omega^{-k};\mathcal{O})$ is trivial. Thus h is divisible by P_k. Since we have $h \in \bigcap_k P_k M_r(\Lambda) = \{0\}$, where the intersection is taken over all $k \ge 2$, this finishes the proof.

We now define the pairing

$$\langle\ ,\ \rangle : \mathbf{H}^{\mathrm{ord}}(\chi;A) \times \mathbf{M}^{\mathrm{ord}}(\chi;A) \to A \text{ by } \langle H,F\rangle = a(1,F\,|\,H) \in A.$$

We also define $\mathbf{m}^{\mathrm{ord}}(\chi;A)$ by $\{F \in \mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{K}) \mid a(n,F) \in A \text{ if } n > 0\}$, where $\mathbf{K}$ is the quotient field of A.

Theorem 5 (duality). *For any extension* A *of* Λ*, the above pairing induces*
(i) $\mathrm{Hom}_A(\mathbf{H}^{\mathrm{ord}}(\chi;A),A) \cong \mathbf{m}^{\mathrm{ord}}(\chi;A)$ *and* $\mathrm{Hom}_A(\mathbf{m}^{\mathrm{ord}}(\chi;A), A) \cong \mathbf{H}^{\mathrm{ord}}(\chi;A)$,
(ii) $\mathrm{Hom}_A(\mathbf{h}^{\mathrm{ord}}(\chi;A),A) \cong \mathbf{S}^{\mathrm{ord}}(\chi;A)$ *and* $\mathrm{Hom}_A(\mathbf{S}^{\mathrm{ord}}(\chi;A), A) \cong \mathbf{h}^{\mathrm{ord}}(\chi;A)$.
In particular, $\mathbf{H}^{\mathrm{ord}}(\chi;A)$ *and* $\mathbf{h}^{\mathrm{ord}}(\chi;A)$ *are free of finite rank over* A.

The freeness of $\mathbf{h}^{\mathrm{ord}}(\chi;\Lambda)$ over Λ was first proven in [H1] directly without using Λ-adic forms for $p \ge 5$.

Proof. We can prove the first part of (i) and (ii) in exactly the same manner as Theorem 5.3.1. Since the arguments are the same for (i) and (ii) for the second part, we only prove the second part of (ii). Since $\mathbf{S}^{\mathrm{ord}}(\chi;\Lambda)$ is Λ-free, we may assume that $A = \Lambda$. We note that over the integral closure A of Λ in a finite extension of $\mathbf{L}$, for each A-torsion-free module M, the double dual $M^{**} = (M^*)^*$ may not be isomorphic to M, where $M^* = \mathrm{Hom}_A(M,A)$. For example, for the maximal ideal m of Λ, $m^{**} \cong \Lambda$. Writing $\mathbf{h}$ (resp. $\mathbf{S}$) for $\mathbf{h}^{\mathrm{ord}}(\chi;\Lambda)$ (resp. $\mathbf{S}^{\mathrm{ord}}(\chi;\Lambda)$), we have a natural map $\mathbf{h} \to \mathbf{h}^{**} = \mathrm{Hom}_\Lambda(\mathbf{S},\Lambda)$ which is Λ-free. This map is injective because of the non-degeneracy of the pairing. Thus $\mathbf{N} = \mathbf{h}^{**}/\mathbf{h}$ is a torsion Λ-module. Since after localizing at any height one prime P of Λ, we get the identity

$$\mathbf{h}^{**}{}_P = \mathrm{Hom}_{\Lambda_P}(\mathrm{Hom}_{\Lambda_P}(\mathbf{h}_P,\Lambda_P),\Lambda_P) = \mathbf{h}_P$$

because Λ_P is a discrete valuation ring. Since the Krull dimension of Λ is 2, $\mathbf{N}$ is killed by a power of m. Thus $\mathbf{N}$ is a finite module. Since $\mathbf{h}^{**}$ is Λ-free, $\mathbf{S} = \mathbf{h}^{***}$. Thus we have

$$\begin{aligned}(*)\ \mathrm{Hom}_{\mathcal{O}}(\mathbf{h}^{**}/P_k\mathbf{h}^{**},\mathcal{O}) &\cong \mathbf{S}/P_k\mathbf{S}\\ &\cong \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(\mathbf{p}),\chi\omega^{-k};\mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}(\mathbf{h}_k^{\mathrm{ord}}(\Gamma_0(\mathbf{p}),\chi\omega^{-k};\mathcal{O}),\mathcal{O}).\end{aligned}$$

On the other hand, from the exact sequence $0 \to \mathbf{h} \to \mathbf{h}^{**} \to \mathbf{N} \to 0$, we get another exact sequence (see Theorem 1.1.2):

$$\mathrm{Tor}_\Lambda^1(\mathbf{N},\Lambda/P_k\Lambda) \to \mathbf{h}/P_k\mathbf{h} \to \mathbf{h}^{**}/P_k\mathbf{h}^{**} \to \mathbf{N}/P_k\mathbf{N} \to 0.$$

Since $\mathbf{N}$ is finite, the module $\mathrm{Tor}_\Lambda^1(\mathbf{N},\Lambda/P_k\Lambda)$ is finite, and thus we have another exact sequence

$$0 \to \mathbf{h}_k(\Gamma_0(\mathbf{p}),\chi\omega^{-k};\mathcal{O}) \to \mathbf{h}^{**}/P_k\mathbf{h}^{**} \to \mathbf{N}/P_k\mathbf{N} \to 0,$$

because the image of $\mathbf{h}/P_k\mathbf{h}$ is the subalgebra of the $\mathcal{O}$-free algebra $\mathbf{h}^{**}/P_k\mathbf{h}^{**}$ generated by the $T(n)$'s, which is $\mathbf{h}_k(\Gamma_0(\mathbf{p}),\chi\omega^{-k};\mathcal{O})$. The above exact sequence yields, by $\mathcal{O}$-duality (see Theorem 1.1.1)

$$0 \to \mathrm{Hom}_{\mathcal{O}}(\mathbf{h}^{**}/P_k\mathbf{h}^{**},\mathcal{O}) \to \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(\mathbf{p}),\chi\omega^{-k};\mathcal{O}) \to \mathrm{Ext}_{\mathcal{O}}^1(\mathbf{N}/P_k\mathbf{N},\mathcal{O}) \to 0.$$

Then by $(*)$, we know that $\mathrm{Ext}_{\mathcal{O}}^1(\mathbf{N}/P_k\mathbf{N},\mathcal{O}) = 0$. Since $\mathcal{O}$ is a valuation ring, $\mathrm{Ext}_{\mathcal{O}}^1(\mathbf{N}/P_k\mathbf{N},\mathcal{O}) \cong \mathbf{N}/P_k\mathbf{N} = 0$ (Corollary 1.1.1). Then Nakayama's lemma shows that $\mathbf{N} = 0$ showing $\mathbf{h} = \mathbf{h}^{**} = \mathrm{Hom}_\Lambda(\mathbf{S},\Lambda)$.

By Theorem 5, we know that $\mathbf{H}^{\mathrm{ord}}(\chi;\mathbf{L}) = \prod_{\mathbf{K}}\mathbf{K}$ for finite extensions $\mathbf{K}/\mathbf{L}$. We fix an algebraic closure $\bar{\mathbf{L}}$ of $\mathbf{L}$ and take a finite extension $\mathbf{K}/\mathbf{L}$ inside $\bar{\mathbf{L}}$ which contains all the isomorphic images of the simple components of the Hecke algebra. The elements F_i corresponding to the i-th projection λ_i to $\mathbf{K}$ in $\mathrm{Hom}_A(\mathbf{H}^{\mathrm{ord}}(\chi;\mathbf{K}),\mathbf{K}) \cong \mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{K})$ give a basis of $\mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{K})$ consisting of com-

mon eigenforms of all Hecke operators $T(n)$ whose coefficients at n are given by $\lambda_i(T(n)) \in \mathbf{K}$. Thus we have

Theorem 6. *For a finite extension* $\mathbf{K}$ *in* $\overline{\mathbf{L}}$, $\mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{K})$ *and* $\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{K})$ *have basis consisting of common eigenforms of all Hecke operators. If one normalizes such a basis of* $\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{K})$ *so that coefficients of* q *are equal to* 1, *then the basis elements are contained in* $\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I})$, *where* $\mathbf{I}$ *is the integral closure of* Λ *in* $\mathbf{K}$.

The last assertion follows from the fact that $\mathbf{H}^{\mathrm{ord}}(\chi;\mathbf{I})$ is finite over Λ and hence $\lambda_i(T(n)) \in \mathbf{I}$.

Let us explain a little about the meaning of a common eigenform $F \in \mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I})$. The evaluation of power series at $\varepsilon(u)u^k-1$ gives an algebra homomorphism $\Lambda \to \mathcal{O}$, whose kernel is generated by $P_{k,\varepsilon} = X-(\varepsilon(u)u^k-1)$ for a finite order character $\varepsilon : W/W^{p^\alpha} \to \overline{\mathbf{Q}}_p$. Since $\mathbf{I}$ is a Λ-module of finite type and is integrally closed, we can find a prime ideal $\mathbf{P}$ of $\mathbf{I}$ such that $\mathbf{P}\cap\Lambda = P_{k,\varepsilon}\Lambda$. We identify $\Lambda/P_{k,\varepsilon}\Lambda$ with $\mathcal{O}[\varepsilon]$, which is a subring of $\overline{\mathbf{Q}}_p$ generated by the values of ε over $\mathcal{O}$. Then $\mathbf{I}/\mathbf{P}$ can be identified with a finite extension of $\mathcal{O}$. Thus there exists an algebra homomorphism φ from $\mathbf{I}$ into $\overline{\mathbf{Q}}_p$ extending the evaluation morphism $F(X) \mapsto F(\varepsilon(u)u^k-1)$. We identify $\mathbf{I}/\mathbf{P}$ with a finite extension of $\mathcal{O}$ by taking such a homomorphism φ (φ may not be uniquely determined if $\mathbf{I}/\mathbf{P}$ is a non-trivial extension of $\mathcal{O}$). Anyway, we see that for an element $F = \sum_{n=1}^{\infty} a(n,F)q^n \in \mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I})$, taking the reduction $F \bmod \mathbf{P}$ is equivalent to considering the formal power series $\varphi(F) = \sum_{n=1}^{\infty} \varphi(a(n,F))q^n \in \overline{\mathbf{Q}}_p[[q]]$. We now show that $\varphi(F) \in \mathcal{S}_k(\Gamma_0(p^\alpha\mathbf{p}),\varepsilon\chi\omega^{-k};\overline{\mathbf{Q}}_p)$. In fact,

$$\begin{aligned}\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I})\otimes_{\mathbf{I}}(\mathbf{I}/\mathbf{P}) &= (\mathbf{S}^{\mathrm{ord}}(\chi;\Lambda)\otimes_\Lambda \mathbf{I})\otimes_{\mathbf{I}}(\mathbf{I}/\mathbf{P})\\ &= \mathbf{S}^{\mathrm{ord}}(\chi;\Lambda)\otimes_\Lambda(\mathbf{I}\otimes_{\mathbf{I}}(\mathbf{I}/\mathbf{P})) = (\mathbf{S}^{\mathrm{ord}}(\chi;\Lambda)\otimes_\Lambda \Lambda/P_k\Lambda)\otimes_{\mathcal{O}}\varphi(\mathbf{I})\end{aligned}$$

which is isomorphic to $\mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\varepsilon\chi\omega^{-k};\varphi(\mathbf{I}))$. In other words, by expressing $F = \sum_i \lambda_i F_i$ with $F_i \in \mathbf{S}^{\mathrm{ord}}(\chi;\Lambda)$ and $\lambda_i \in \mathbf{I}$, we see that $\varphi(F) = \sum_i \varphi(\lambda_i)F_i(\varepsilon(u)u^k-1) \in \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\varepsilon\chi\omega^{-k};\varphi(\mathbf{I}))$. If F is a common eigenform of all Hecke operators, then $\varphi(F)$ is a common eigenform of all Hecke operators in $\mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha\mathbf{p}),\varepsilon\chi\omega^{-k};\varphi(\mathbf{I}))$. Hence by Proposition 2.1, $\varphi(F)$ is even a classical complex common eigenform. We write $F(\mathbf{P})$ for $\varphi(F)$. Let $\mathcal{A}(\mathbf{I})$ be the set of all algebra homomorphisms from $\mathbf{I}$ into $\overline{\mathbf{Q}}_p$ which induce on Λ the evaluation $F(X) \mapsto F(\varepsilon(u)u^k-1)$ for some $k > 1$ and some finite order character $\varepsilon : W \to \overline{\mathbf{Q}}_p^\times$. Each point in $\mathcal{A}(\mathbf{I})$ is called an arithmetic point of

$\mathrm{Spec}(\mathbf{I})(\overline{\mathbf{Q}}_p)$. Then $\{F(\mathbf{P})\}$ for $\mathbf{P} \in \mathcal{A}(\mathbf{I})$ gives a p-adic family of common eigenforms parametrized by $\mathrm{Spec}(\mathbf{I})(\overline{\mathbf{Q}}_p) = \mathrm{Hom}_{\mathcal{O}\text{-alg}}(\mathbf{I}, \overline{\mathbf{Q}}_p)$. If $\mathbf{I} = \Lambda$, then we may identify the set of integers ≥ 2 with a subset of $\mathcal{A}(\mathbf{I})$ by $k \mapsto P_k = P_{k,\mathrm{id}}$, and we get the p-adic eigen-family of modular forms in the sense of §1. Usually we do not need to extend scalars to a non-trivial extension $\mathbf{I}$; in particular, if there is no congruence modulo p between eigenforms in $\mathcal{S}_k(\Gamma_0(p^\alpha \mathbf{p}), \varepsilon\chi\omega^{-k}; \overline{\mathbf{Q}}_p)$ for at least one pair (k,χ), it is known that $\mathbf{h}^{\mathrm{ord}}(\chi;\Lambda)$ is isomorphic to a product of copies of Λ. We will return to this question later.

Theorem 7. *Each normalized common eigenform of all Hecke operators in* $\mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha \mathbf{p}), \varepsilon\chi\omega^{-k}; \overline{\mathbf{Q}})$ *for* $k \geq 1$ *is of the form* $\varphi(F)$ *for a normalized common eigenform* F *in* $\mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{I})$ *for a suitable extension* $\mathbf{I}$ *of* Λ. *The same assertion also holds for cusp forms.*

Proof. Let f be a normalized common eigenform in $\mathcal{M}_k(\Gamma_0(p^\alpha \mathbf{p}), \varepsilon\chi\omega^{-k}; \overline{\mathbf{Q}}_p)$ for $k \geq 1$. By extending scalars to a finite extension of $\mathcal{O}$, we may assume that f has coefficients in $\mathcal{O}$. We already know from Theorem 3 that f lifts to a Λ-adic ordinary form F. Then there exists an algebra homomorphism λ_0 of the Hecke algebra $\mathbf{H}$ of $\mathbf{M}^{\mathrm{ord}}(\chi;\Lambda)/P_{k,\varepsilon}\mathbf{M}^{\mathrm{ord}}(\chi;\Lambda)$ $(= \mathcal{M}_k^{\mathrm{ord}}(\Gamma_0(p^\alpha \mathbf{p}), \varepsilon\chi\omega^{-k}; \mathcal{O})$ if $k \geq 2)$ into $\mathcal{O}$ such that $\lambda_0(T(n)) = a(n,f)$. By definition, we have a natural surjective algebra homomorphism $\mathbf{H}^{\mathrm{ord}}(\chi,\Lambda) \to \mathbf{H}$ taking $T(n)$ to $T(n)$. Pulling back λ_0 to $\mathbf{H}^{\mathrm{ord}}(\chi,\Lambda)$ via the above homomorphism, we have an algebra homomorphism $\lambda_0 : \mathbf{H}^{\mathrm{ord}}(\chi,\Lambda) \to \mathcal{O}$. Let p be a minimal prime ideal of $\mathbf{h}^{\mathrm{ord}}(\chi,\Lambda)$ contained in $\mathrm{Ker}(\lambda_0)$. Then $\mathbf{I}' = \mathbf{H}^{\mathrm{ord}}(\chi,\Lambda)/p$ is a finite extension of Λ. Let $\mathbf{I}$ be the integral closure of Λ in the quotient field $\mathbf{K}$ of $\mathbf{I}'$. Then $\mathbf{I}'$ is contained in $\mathbf{I}$ and λ_0 factors through the natural projection $\lambda: \mathbf{H}^{\mathrm{ord}}(\chi,\Lambda) \to \mathbf{I}$. That is, there exists an algebra homomorphism φ of $\mathbf{I}$ into $\overline{\mathbf{Q}}_p$ such that $\lambda_0 = \varphi \circ \lambda$. This shows that $f = \varphi(F)$ for the common $\mathbf{I}$-adic eigenform F corresponding to λ.

§7.4. Two variable p-adic Rankin product

In this section, we construct the two variable p-adic Rankin product which interpolates the values $D(k-1,f,g)$ where f and g vary on the families $\{f = F(u^k-1)\}_k$ and $\{g = G(u^l-1)\}_l$ for two Λ-adic forms F and G. Here k is the weight of f and F is assumed to be ordinary. Thus this two variable interpolation is purely non-abelian and does not include the abelian (cyclotomic) variable. We extend this two variable p-adic L-function to a three variable one in §10.4 including a cyclotomic variable. For interpolation with respect to the cyclotomic variable, there is another method due to Panchishkin [Pa, IV].

We start with an abstract argument. Let S be a space of modular forms with the action of Hecke operators $T(n)$. We assume that S is an A-module of finite type for a noetherian integral domain A. Let $h(S)$ be the Hecke algebra of S over A, i.e. $h(S)$ is the subalgebra of $\mathrm{End}_A(S)$ generated over A by Hecke operators $T(n)$ for all positive n. We assume

(S1) S *is embedded into* $A[[q]]$ *via the q-expansion* $f \mapsto \sum_{n=0}^{\infty} a(n,f)q^n$;

(S2) $S \cong \mathrm{Hom}_A(h(S),A)$ *via the pairing* $\langle f,h\rangle = a(1,f|h)$;

(S3) $h(S)\otimes_A K$ *is semi-simple for the quotient field* K *of* A.

By semi-simplicity, we have a non-degenerate pairing $(\ ,\ )$ on $D = h(S)\otimes_A K$ given by $(h,g) = \mathrm{Tr}_{D/K}(hg)$. By this, we have a natural isomorphism $i : D \to D^*$ given by $i(h)(g) = (h,g)$. Thus we have $i^{-1} : S(K) = D^* \to D = S(K)^*$. Hence we have the dual pairing $(\ ,\ )_A : S(K)\times S(K) \to K$ given by $(f,g)_A = i^{-1}(f)(g)$. By definition, $(f,g)_A$ satisfies

$$(f|h,g)_A = (f,g|h)_A. \tag{1a}$$

We call this pairing $(\ ,\ )_A$ the algebraic Petersson inner product. In particular, if $f|h = \lambda(h)f$ for an algebra homomorphism $\lambda : h(S) \to A$ with $a(1,f) = 1$ (i.e. f is the normalized eigenform), the number

$$c(f,g) = \frac{(f,g)_A}{(f,f)_A} \in K \tag{1b}$$

is well defined. In fact, by (S3), after extending the scalar field K by a finite extension if necessary, $S(K)$ has a basis consisting of normalized eigenforms. Then $c(f,g)$ is the coefficient of f when we express g as a linear combination of normalized eigenforms.

Now we return to concrete examples. First we consider $\mathcal{S}_k(\Gamma_0(p^\alpha),\chi_0)$. On this space, we have a Petersson inner product $(\ ,\ )$. As seen in (5.3.10b), if we modify $(\ ,\ )$ to define a new product $(\ ,\ )_\infty$ by

$$(f,g)_\infty = (g,f^c|\tau) \qquad \text{for } \tau = \begin{pmatrix} 0 & -1 \\ p^\alpha & 0 \end{pmatrix},$$

then we see that $(f|h,g)_\infty = (f,g|h)_\infty$ and hence we again have, by (5.5.3)

$$c(f,g) = \frac{(f,g)_C}{(f,f)_C} = \frac{(f,g)_\infty}{(f,f)_\infty}, \tag{1c}$$

where $(\ ,\ )_C$ is as in (1a) for $A = \mathbf{C}$. Now we suppose that

(P1) $f = \sum_{n=1}^{\infty} \lambda_0(T(n))q^n$ and $h = \sum_{n=1}^{\infty} \varphi_0(T(n))q^n$ for two algebra homomorphisms with $k > l$,

$\lambda_0 : \mathbf{h}_k^{ord}(\Gamma_0(p^\alpha),\chi_0;\mathbf{Q}(\chi_0)) \to \overline{\mathbf{Q}}$ and $\varphi_0 : \mathbf{h}_l(\Gamma_0(p^\beta),\psi_0;\mathbf{Q}(\psi_0)) \to \overline{\mathbf{Q}}$;

(P2) χ_0 is either a primitive character modulo p^α or the identity character modulo p (i.e. $\alpha = 1$).

By the ordinarity assumption on λ, the condition (P2) actually follows from (P1). Then we define

(2) $L(s,\lambda_0{}^c\otimes\varphi_0)$

$$= (1-\chi_0{}^{-1}\psi_0(p)p^{-2s-2+k+l})L(2s+2-k-l,\chi_0{}^{-1}\psi_0)\sum_{n=1}^{\infty}\lambda_0(T(n))^c\varphi_0(T(n))n^{-s}$$

$$= \prod_q\{(1-\alpha_q{}^c\alpha'_q q^{-s})(1-\alpha_q{}^c\beta'_q q^{-s})(1-\beta_q{}^c\alpha'_q q^{-s})(1-\beta_q{}^c\beta'_q q^{-s})\}^{-1},$$

where we have written

$$L(s,\lambda_0) = \prod_q\{(1-\alpha_q q^{-s})(1-\beta_q q^{-s})\}^{-1} \text{ and}$$

$$L(s,\varphi_0) = \prod_q\{(1-\alpha'_q q^{-s})(1-\beta'_q q^{-s})\}^{-1}.$$

To make computation easy, we make the following assumption:

(P3) $\chi_0\psi_0{}^{-1}$ is primitive modulo p^γ with $\gamma = \max(\alpha,\beta)$.

The condition (P3) ensures that

$E_{k-l}(\psi_0{}^{-1}\chi_0)$

$$= \{p^{-\gamma(k-l)}G(\psi_0\chi_0{}^{-1})\frac{(-2\pi\sqrt{-1})^{k-l}}{(k-1)!}\}^{-1}\sum_{(m,n)\in\{Z^2-(0,0)\}/\{\pm1\}}\psi_0\chi_0{}^{-1}(n)(mp^\gamma z+n)^{-k},$$

which is the key in the computation in §5.4. Then we replace g in (1b,c) by $hE_{k-l}(\psi_0{}^{-1}\chi_0)$ for $h \in \mathcal{M}_l(\Gamma_0(p^\beta),\psi_0)$. Note that $f^c \mid \tau = (p^\alpha)^{(k-2)/2}W(\lambda_0{}^c)f$ for an algebraic constant $W(\lambda_0)$ with $|W(\lambda_0)| = 1$. Then if $\alpha \geq \beta$, we have by the same computation as in §5.4, for $A = \mathbf{Q}(\lambda_0,\varphi_0)$ and $E = E_{k-l}(\psi_0{}^{-1}\chi_0)$,

(3) $$c(f,hE) = \frac{(f,hE)_A}{(f,f)_A} = \frac{p^{\alpha(k-l)}\Gamma(k-l)\Gamma(k-1)L(k-1,\lambda_0{}^c\otimes\varphi_0)}{G(\chi_0{}^{-1}\psi_0)(-2\pi\sqrt{-1})^{k-l}(4\pi)^{k-1}(f,f)} \in \mathbf{Q}(\lambda_0,\varphi_0),$$

where $\mathbf{Q}(\lambda_0,\varphi_0)$ is the field generated by the values of λ_0 and φ_0. Now let $\mathbf{K}$ be a finite extension of the quotient field $\mathbf{L}$ of Λ and $\mathbf{I}$ be the integral closure of Λ in $\mathbf{K}$. We consider an $\mathbf{I}$-adic normalized eigenform $F \in \mathbf{S}^{ord}(\chi_0;\mathbf{I})$. We consider the $\mathbf{I}$-algebra homomorphism $\lambda : \mathbf{h}^{ord}(\lambda;\mathbf{I}) \to \mathbf{I}$ given by $F \mid T(n) = \lambda(T(n))F$. Then for

$$h*E(X;q) = hE(u^{-l}X+(u^{-l}-1);q) \text{ with } E(X;q) = E(\psi_0{}^{-1}\chi_0)(X;q),$$

we have an element $L_p(\lambda^c\otimes\varphi_0) \in \mathbf{K}$ (for the quotient field $\mathbf{K}$ of $\mathbf{I}$) given by

$$L_p(\lambda^c\otimes\varphi_0) = \frac{(F,e(h*E))_{\mathbf{I}}}{(F,F)_{\mathbf{I}}} \in \mathbf{K}. \tag{4}$$

Now any element L in $\mathbf{I}$ can be considered as a function on

$$\mathcal{X}(\mathbf{I}) = \mathrm{Hom}_{\mathcal{O}\text{-alg}}(\mathbf{I},\overline{\mathbf{Q}}_p) = \mathrm{Spec}(\mathbf{I})(\overline{\mathbf{Q}}_p)$$

by $L(P) = P(L)$. When $\mathbf{I} = \Lambda$, we have $\mathcal{X}(\Lambda) \cong \{x \in \overline{\mathbf{Q}}_p \mid |x-1|_p < 1\}$ via $x \mapsto P_x$ with $P_x(\Phi) = \Phi(x-1)$, and $L \in \Lambda$ gives a p-adic analytic function on this unit disk. Thus our domain $\mathcal{X}(\mathbf{I})$ is a covering space of $\mathcal{X}(\Lambda)$ via $P \mapsto P|_\Lambda$. Note that $\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{K}) = \mathbf{K}F\oplus(\mathbf{K}F)^\perp$ for the orthogonal complement $(\mathbf{K}F)^\perp$ of $\mathbf{K}F$ under $(\ ,\ )_{\mathbf{I}}$. If $P \in \mathcal{A}(\mathbf{I})$ with $P|_\Lambda = P_{k,\varepsilon}$ and if $\varepsilon\chi\omega^{-k}$ is primitive modulo $p^\alpha\mathfrak{p}$, then $\mathcal{S}_k(\Gamma_0(\mathfrak{p}p^\alpha),\varepsilon\chi\omega^{-k};K[\varepsilon]) = K[\varepsilon]f+(K[\varepsilon]f)^\perp$ for $f = F(\varepsilon(u)u^k-1)$ and the orthogonal complement $(K[\varepsilon]f)^\perp$ of $K[\varepsilon]f$ under $(\ ,\ )_{K[\varepsilon]}$. Localizing at P, we see that

$$\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I}_P)/P\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I}_P) = \mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(\mathfrak{p}p^\alpha),\varepsilon\chi\omega^{-k};K[\varepsilon]) \text{ by Theorem 3.3.}$$

In particular, we have $(\ ,\ )_{K[\varepsilon]} = (\ ,\ )_{\mathbf{I}} \bmod P$. This shows that if we write $g = e(hE_{k-l}(\psi_0^{-1}\chi_P))$ and $G = e(h*E_{\psi_0^{-1}\chi_0})$ and define $\lambda_P = \lambda \bmod P$ by $P\circ\lambda$ which factors through $\mathcal{S}_k(\Gamma_0(p^\alpha),\varepsilon\chi\omega^{-k};\mathcal{O}[\varepsilon])$ by Theorem 3.3, we have

$$L_p(\lambda^c\otimes\varphi_0)(P) = \frac{(F,G)_{\mathbf{I}}}{(F,F)_{\mathbf{I}}} \bmod P = \frac{(f,g)_{K[\varepsilon]}}{(f,f)_{K[\varepsilon]}} = \frac{p^{\alpha(k-l)}\Gamma(k-l)\Gamma(k-1)L(k-1,\lambda_P{}^c\otimes\varphi_0)}{G(\chi_P{}^{-1}\psi_0)(-2\pi i)^{k-l}(4\pi)^{k-1}(f,f)}$$

as long as $\chi_0 = \chi_P = \varepsilon\chi\omega^{-k}$ is primitive modulo p^α with $\alpha \geq \beta > 0$, and χ_0, ψ_0, $\lambda_0 = \lambda_P$ and φ_0 satisfy the conditions (P1-3). We compute the value $L_p(\lambda^c\otimes\varphi_0)$ when $\beta > \alpha$. We have

$$\begin{aligned} L_p(\lambda^c\otimes\varphi_0)(P) &= \frac{(f,e(hE_{k-l}(\psi_0^{-1}\chi_P)))_\infty}{(f,f)_\infty} \\ &= \lambda_P(T(p))^{-\delta}\frac{(f,e(hE_{k-l}(\psi_0^{-1}\chi_P)\,|\,T(p)^\delta))_\infty}{(f,f)_\infty} \\ &= \lambda_P(T(p))^{-\delta}\frac{(f,hE_{k-l}(\psi_0^{-1}\chi_P)\,|\,T(p)^\delta)_\infty}{(f,f)_\infty} \quad \text{if } \delta = \max(\beta-\alpha,0). \end{aligned}$$

Since T(p) decreases the exponent of p in the level by one as long as the character of the modular form is imprimitive, taking δ to be the difference of the expo-

nent of p in the level of $hE_{k-l}(\psi_0^{-1}\chi_P)$ and α, we get the last equality in the above formula. Note that, supposing $\beta > \alpha$,

$$T(p)^\delta = [\Gamma_0(p^\beta)\begin{pmatrix}1 & 0\\ 0 & p^\delta\end{pmatrix}\Gamma_0(p^\alpha)].$$

Thus we see that

$$(f,hE_{k-l}(\psi_0^{-1}\chi_P)\,|\,T(p)^\delta)_\infty = (hE_{k-l}(\psi_0^{-1}\chi_P)\,|\,[\Gamma_0(p^\beta)\begin{pmatrix}1 & 0\\ 0 & p^\delta\end{pmatrix}\Gamma_0(p^\alpha)],f^c\,|\,\tau)_{\Gamma_0(p^\alpha)}$$

$$= (hE_{k-l}(\psi_0^{-1}\chi_P),f^c\,|\,\tau\,|\,[\Gamma_0(p^\alpha)\begin{pmatrix}p^\delta & 0\\ 0 & 1\end{pmatrix}\Gamma_0(p^\beta)])_{\Gamma_0(p^\beta)}.$$

Since $\begin{pmatrix}p^{-\delta} & 0\\ 0 & 1\end{pmatrix}\Gamma_0(p^\alpha)\begin{pmatrix}p^\delta & 0\\ 0 & 1\end{pmatrix}\cap\Gamma_0(p^\beta) = \Gamma_0(p^\beta)$, we see that

$$\Gamma_0(p^\alpha)\begin{pmatrix}p^\delta & 0\\ 0 & 1\end{pmatrix}\Gamma_0(p^\beta) = \Gamma_0(p^\alpha)\begin{pmatrix}p^\delta & 0\\ 0 & 1\end{pmatrix}.$$

This implies, if χ_P is primitive modulo p^α with $\alpha > 0$,

$$(f,hE_{k-l}(\psi_0^{-1}\chi_P)\,|\,T(p)^\delta)_\infty = p^{\delta(k-l)}(hE_{k-l}(\psi_0^{-1}\chi_P),(f^c\,|\,\tau)(p^\delta z))_{\Gamma_0(p^\beta)}$$

$$= p^{\delta(k-l)}\lambda_P(T(p))^{-\delta}\varphi_0(T(p))^\delta\frac{p^{\alpha(k-l)}\Gamma(k-l)\Gamma(k-1)L(k-1,\lambda_P{}^c\otimes\varphi_0)}{G(\chi_P{}^{-1}\psi_0)(-2\pi\sqrt{-1})^{k-l}(4\pi)^{k-1}}.$$

Thus we have, in general, if χ_P is primitive modulo p^α $(\alpha > 0)$, under (P1-3), for $\delta = \max(\beta-\alpha,0)$,

$$L_p(\lambda^c\otimes\varphi_0)(P) = p^{\max(\alpha,\beta)(k-l)}\lambda_P(T(p))^{-\delta}\varphi_0(T(p))^\delta\frac{\Gamma(k-l)\Gamma(k-1)L(k-1,\lambda_P{}^c\otimes\varphi_0)}{G(\chi_P{}^{-1}\psi_0)(-2\pi i)^{k-l}(4\pi)^{k-1}(f,f)}.$$

Thus we get

Theorem 1 (one variable interpolation). *Let* $\lambda : \mathbf{h}^{ord}(\chi;\mathbf{I}) \to \mathbf{I}$ *be an* $\mathbf{I}$*-algebra homomorphism and* $\varphi_0 : \mathbf{h}_k(\Gamma_0(p^\beta),\psi_0;\mathcal{O}) \to \overline{\mathbf{Q}}_p$ *be an* $\mathcal{O}$*-algebra homomorphism. Then we have a unique* p*-adic L-function* $L_p(\lambda^c\otimes\varphi_0) \in \mathbf{K}$ *with the following evaluation property: for* $P \in \mathcal{A}(\mathbf{I})$ *with primitive* χ_P *modulo* p^α $(\alpha > 0)$ *and* $P\,|_\Lambda = P_{k,\varepsilon}$ *for integers* $k > l > 0$, *assuming (P1-3) for* $\lambda_0 = \lambda_P$ *and* $\chi_0 = \chi_P$, *we have*

$$L_p(\lambda^c\otimes\varphi_0)(P) = p^{\max(\alpha,\beta)(k-l)}\{\lambda_P(T(p))^{-1}\varphi_0(T(p))\}^{\max(\beta-\alpha,0)}$$
$$\times\frac{\Gamma(k-l)\Gamma(k-1)L(k-1,\lambda_P{}^c\otimes\varphi_0)}{G(\chi_P{}^{-1}\psi_0)(-2\pi\sqrt{-1})^{k-l}(4\pi)^{k-1}(F(P),F(P))_{\Gamma_0(p^\alpha)}},$$

where $F \in \mathbf{S}^{ord}(\chi;\mathbf{I})$ *is the normalized eigenform attached to* λ.

We remove the condition (P3) in §10.5. We now want to vary φ_0 along another p-adic family. Let $\mathbf{M}$ be another finite extension of $\mathbf{L}$ and $\mathbf{J}$ be the integral closure of Λ in $\mathbf{M}$. Let G be another $\mathbf{J}$-adic cusp form, i.e.

$G = \sum_{n=0}^{\infty} a(n;G)q^n \in \mathbf{S}(\psi,\mathbf{J})$. We suppose that G is a normalized eigenform of all Hecke operators. Henceforth, for each arithmetic point $P \in \mathcal{A}(\mathbf{J})$, we write $k(P) = k$ and $\varepsilon_P = \varepsilon$ if $P|_\Lambda = P_{k,\varepsilon}$. We also write the conductor of ε as $p^{\alpha(P)}\mathbf{p}$. An arithmetic point $P \in \mathcal{A}(\mathbf{J})$ is called admissible (relative to G) if

$$G(P) = \sum_{n=1}^{\infty} P(a(n;G))q^n \in \mathcal{S}_k(\Gamma_0(p^\beta\mathbf{p}),\psi_P;\overline{\mathbf{Q}})$$

for some β and $\psi_P = \varepsilon\psi\omega^{-k}$. If G is ordinary, all arithmetic points are admissible relative to G by Theorem 3.3. Then we define the two variable convolution product $G*E(\chi\psi^{-1})$ as follows. We consider another copy of Λ identified with $\mathcal{O}[[Y]]$. We regard $\mathbf{J}$ as an $\mathcal{O}[[Y]]$-algebra and take the completed tensor product $\Lambda\hat{\otimes}_{\mathcal{O}}\mathbf{J} = \mathcal{O}[[X]]\hat{\otimes}_{\mathcal{O}}\mathbf{J} = \mathbf{J}[[X]]$. We define

$$G*E(X) = GE((1+X)(1+Y)^{-1}-1) \in \mathbf{J}[[X]] \quad \text{for} \quad E = E(\chi\psi^{-1}).$$

Then, for the Λ-algebra homomorphism $\mathrm{id}\otimes Q : \Lambda\hat{\otimes}_{\mathcal{O}}\mathbf{J} \to \Lambda = \mathcal{O}[[X]]$ ($Q \in \mathcal{A}(\mathbf{J})$), we have

$$\mathrm{id}\otimes Q(G*E) = G(Q)E(\varepsilon_Q(u)^{-1}u^{-k(Q)}X+(\varepsilon_Q(u)^{-1}u^{-k(Q)}-1)) = G(Q)*E.$$

If one has a formal q-expansion $H = \sum_{n=1}^{\infty} a(n;H)q^n \in \Lambda\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[q]]$ and if

$$\mathrm{id}\otimes Q(H) = \sum_{n=1}^{\infty} \mathrm{id}\otimes Q(a(n;H))q^n \in \mathbf{M}(\chi;\Lambda)$$

for all arithmetic points $Q \in \mathcal{A}(\mathbf{J})$ with $k(Q) \geq a$ (for a given integer $a > 0$), then we claim that

$$H \in \mathbf{M}(\chi;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}. \tag{5}$$

To see this, write $H = \sum_\Phi \Phi H_\Phi$ with $H_\Phi \in \mathcal{O}[[X,Y]]$ for a basis $\{\Phi\}$ of $\mathbf{M}$ over $\mathbf{L}$. Choosing a dual basis $\{\Phi^*\}$ of $\{\Phi\}$ under the pairing $(x,y) = \mathrm{Tr}_{\mathbf{M}/\mathbf{L}}(xy)$, we can solve $H_\Phi = \mathrm{Tr}_{\mathbf{M}[[X]]/\mathbf{L}[[X]]}(\Phi^*H)$. This shows that $\mathrm{id}\otimes Q(H_\Phi) \in \mathbf{M}(\chi;\Lambda)$ for almost all admissible Q because the denominator of Φ^* has only finitely many roots in $\mathcal{X}(\mathbf{J})$. Thus to prove (5), we may assume that $\mathbf{J} = \Lambda$. Then we write $H = H(X,Y;q) \in \mathcal{O}[[X,Y]][[q]]$. Since P_k is admissible for all sufficiently large k relative to G by definition, we write a for the integer such that P_k is admissible if $k \geq a$. We put $H_0(X) = H(X,u^a-1)$. Then $H(X,Y)-H_0(X)$ vanishes at u^a-1, and thus $H_1 = (H(X,Y)-H(X,u^a-1))/Y_1$ ($\in \mathcal{O}[[X,Y]]$) for $Y_1 = Y-(u^a-1)$ satisfies $H_1(X,u^k-1) \in \mathbf{M}(\chi;\Lambda)$ for all $k \geq a+1$. Now we define $Y_2 = Y-(u^{a+1}-1)$ and repeat the above process to get $H_2 = (H_1(X,Y)-H_1(X,u^{a+1}-1))/Y_2$, satisfying $H_2(X,u^k-1) \in \mathbf{M}(\chi;\Lambda)$ for all $k \geq a+2$. We then define inductively

$$H_j = \frac{H_{j-1}(X,Y)-H_{j-1}(X,u^{a+j-1}-1)}{Y_j} \quad \text{for} \quad Y_j = Y-(u^{a+j-1}-1).$$

Then $H_j(X,u^{a+j}-1) \in \mathbf{M}(\chi;\Lambda)$ and $H = \sum_{n=0}^{\infty} H_n(X,u^{a+n}-1)\prod_{j=1}^{n} Y_j$, which is convergent under the adic topology of the maximal ideal of $\mathcal{O}[[X,Y]]$. This shows $H \in \mathbf{M}(\chi;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}$. Since the projection $e : \mathbf{M}(\chi;\Lambda) \to \mathbf{M}^{\mathrm{ord}}(\chi;\Lambda)$ extends to

$$(6) \qquad e : \mathbf{M}(\chi;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J} \to \mathbf{M}^{\mathrm{ord}}(\chi;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J},$$

we can think of $e(G*E(\chi\psi^{-1}))$, which satisfies

$$\mathrm{id}\otimes Q(e(G*E(\chi\psi^{-1}))) = e(G(Q)*E(\chi\psi^{-1})).$$

Let $\mathbf{h}(\psi;\mathbf{J})$ be the $\mathbf{J}$-subalgebra of $\mathrm{End}_{\mathbf{J}}(\mathbf{S}(\psi;\mathbf{J}))$ generated by Hecke operators $T(n)$ for all n and $\varphi : \mathbf{h}(\psi;\mathbf{J}) \to \mathbf{J}$ be the $\mathbf{J}$-algebra homomorphism given by $G\,|\,T(n) = \varphi(T(n))G$. For each admissible point $Q \in \mathcal{A}(\mathbf{J})$, φ specializes to

$$\varphi_Q : \mathbf{h}_{k(Q)}(\Gamma_0(p^\beta),\psi_Q;\mathcal{O}[\varepsilon_Q]) \to \overline{\mathbf{Q}}_p \quad \text{for } \psi_Q = \varepsilon_Q\psi\omega^{-k(Q)}$$

attached to $G(Q)$. Now considering $e(G*E_{\chi\psi^{-1}}) \in \mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{I})\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ and extending the scalar product $(\ ,\ )_{\mathbf{I}}$ on $\mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{I})$ to

$$(\ ,\ )_{\mathbf{I}\otimes\mathbf{J}} : \mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{I})\hat{\otimes}_{\mathcal{O}}\mathbf{J} \times \mathbf{M}^{\mathrm{ord}}(\chi;\mathbf{I})\hat{\otimes}_{\mathcal{O}}\mathbf{J} \to H^{-1}\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}$$

(for the denominator H of $(\ ,\ )_{\mathbf{I}}$) by $\mathbf{J}$-linearity, we define

$$L_p(\lambda^c\otimes\varphi) = \frac{(F,e(G*E(\chi\psi^{-1})))_{\mathbf{I}\otimes\mathbf{J}}}{(F,F)_{\mathbf{I}}} \in H^{-1}\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}.$$

Then, after specializing $L_p(\lambda^c\otimes\varphi)$ along $\mathrm{id}\otimes Q$, we get the function $L_p(\lambda^c\otimes\varphi_Q)$ in Theorem 1. Thus we have, regarding $L_p(\lambda^c\otimes\phi)$ as a function on $\mathcal{X}(\mathbf{I})\times\mathcal{X}(\mathbf{J})$ by $L_p(\lambda^c\otimes\varphi)(P,Q) = P\otimes Q(L_p(\lambda^c\otimes\varphi))$,

Theorem 2 (Two variable interpolation). *Let* $\lambda : \mathbf{h}^{\mathrm{ord}}(\chi;\mathbf{I}) \to \mathbf{I}$ *be an* $\mathbf{I}$*-algebra homomorphism and* G *be a normalized eigenform in* $\mathbf{S}(\psi;\mathbf{J})$. *For each admissible point* Q *of* $\mathcal{A}(\mathbf{J})$, *we write* $\varphi_Q : \mathbf{h}_{k(Q)}(\Gamma_0(p^\beta),\varepsilon_Q\psi\omega^{-k(Q)};\mathcal{O}[\varepsilon]) \to \overline{\mathbf{Q}}_p$ *for the* $\mathcal{O}[\varepsilon]$*-algebra homomorphism associated with* $G(Q)$. *Then we have a unique* p*-adic L-function* $L_p(\lambda^c\otimes\varphi)$ *in the quotient field of* $\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ *with the following evaluation property: for* $P \in \mathcal{A}(\mathbf{I})$ *with primitive* χ_P *modulo* p^α $(\alpha > 0)$, *and admissible* $Q \in \mathcal{A}(\mathbf{J})$ *with* ψ_Q *modulo* p^β, *assuming (P1-3) for* $\lambda_0 = \lambda_P$, $\varphi_0 = \varphi_Q$ *and* $\chi_0 = \chi_P$, $\psi_0 = \psi_Q$, *we have*

$$L_p(\lambda^c\otimes\varphi)(P,Q) = p^{\max(\alpha,\beta)(k(P)-k(Q))}\{\lambda_p(T(p))^{-1}\varphi_Q(T(p))\}^{\max(\beta-\alpha,0)}$$
$$\times\frac{\Gamma(k(P)-1)\Gamma(k(P)-k(Q))L(k(P)-1,\lambda_P{}^c\otimes\varphi_Q)}{G(\chi_P{}^{-1}\psi_Q)(-2\pi\sqrt{-1})^{k(P)-k(Q)}(4\pi)^{k(P)-1}(F(P),F(P))_{\Gamma_0(p^\alpha)}} \quad \textit{if } k(P) > k(Q),$$

where $F \in \mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I})$ *is the normalized eigenform attached to* λ.

Note that $XE(id)(X)\,|_{X=0} = \frac{1}{2}(1-\frac{1}{p})log(u)$. Therefore, if $\psi = \chi$, we have

$$e(G*XE(id))(X,X) = \frac{1}{2}(1-\frac{1}{p})log(u)e(G).$$

Noting that, by definition, $(F,F)_{\mathbf{I}} = 1$, we have

Theorem 3 (residue formula). *Under the notation of Theorem 2, suppose that* $\chi = \psi$. *Then we have*

$$\{((1+X)(1+Y)^{-1}-1)L_p(\lambda^c\otimes\varphi)\}\,\Big|_{X=Y} = \frac{1}{2}(1-\frac{1}{p})\log(u)(F,e(G))_{\mathbf{I}}.$$

§7.5. Ordinary Galois representations into $GL_2(\mathbf{Z}_p[[X]])$

Now we shall explain Wiles' method [Wi1] of constructing Galois representations attached to each $\mathbf{I}$-adic common eigenform F. Let $\mathbf{K}$ be the quotient field of $\mathbf{I}$. A Galois representation $\pi : Gal(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{K})$ is said to be continuous if there exists an $\mathbf{I}$-submodule L of $\mathbf{K}^2$ such that L is of finite type over $\mathbf{I}$, $L\otimes_{\mathbf{I}}\mathbf{K} = \mathbf{K}^2$, L is stable under π, and as a map $\pi : Gal(\overline{\mathbf{Q}}/\mathbf{Q}) \to End_{\mathbf{I}}(L)$ is continuous under the $\mathbf{m}$-adic topology on $End_{\mathbf{I}}(L)$ for the maximal ideal $\mathbf{m}$ of $\mathbf{I}$. Since L is of finite type over $\mathbf{I}$, there is a surjective homomorphism of $\mathbf{I}$-modules $\varphi : \mathbf{I}^n \to L$. Thus if we write $\mathbf{m}$ for the maximal ideal of $\mathbf{I}$, then $L/\mathbf{m}^iL$ is the surjective image of $(\mathbf{I}/\mathbf{m}^i)^n$ which is a finite module. This shows that $End_{\mathbf{I}}(L)$ is a profinite ring and hence compact. Thus it is natural to consider continuous representations into $End_{\mathbf{I}}(L)$ from the absolute Galois group which is compact under the Krull topology. On the other hand, $\mathbf{I}$ is a huge ring of Krull dimension 2, and thus $\mathbf{K}$ cannot be a locally compact field [Bour1, VI.9.3]. This implies that the image of a continuous representation of $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ into $GL_2(\mathbf{K})$ under any topology which makes $\mathbf{K}$ a topological field is very small. This is the reason why we take the $\mathbf{m}$-adic topology on $End_{\mathbf{I}}(L)$ to define the continuity of π. This definition of continuity does not depend on the choice of L by the Artin-Rees lemma [Bour1, III.3.1]. We also say that π is *unramified* at a rational prime q if the kernel of π contains the inertia group of q (§1.3). We first state the result:

Theorem 1. *Let* F *be an* $\mathbf{I}$*-adic normalized eigenform in* $\mathbf{S}^{ord}(\chi;\mathbf{I})$ *corresponding to the* Λ*-algebra homomorphism* $\lambda : \mathbf{h}^{ord}(\chi,\Lambda) \to \mathbf{I}$. *Let* $\mathbf{K}$ *be the quotient field of* $\mathbf{I}$. *Then there exists a unique Galois representation* $\pi : Gal(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{K})$ *such that*

(i) π *is continuous and is absolutely irreducible,*

(ii) π *is unramified outside* p,

(iii) *for each rational prime* q *prime to* p,

$$\det(1-\pi(Frob_q)T) = 1 - \lambda(T(q))T + \chi(q)\kappa(\langle q\rangle)q^{-1}T^2,$$

where Frob_q *is the Frobenius element at* q *and* $\kappa : W = 1+p\mathbf{Z}_p \to \Lambda^\times$ *is the character given by* $\kappa(u^s) = (1+X)^s$ *and* $\langle x\rangle = \omega(x)^{-1}x \in W$.

This theorem was first proven in [H4], but here we give a different construction found by Wiles [Wil]. Before giving a proof of this fact, let us explain a little about the reduction of the representation modulo a prime ideal of $\mathbf{I}$ (or modulo each point of $\mathcal{A}(\mathbf{I})$). Let P be a prime ideal of $\mathbf{I}$. We sometimes identify P with the algebra homomorphism $P : \mathbf{I} \to \mathbf{I}/P$ given by reduction modulo P. For each element $\lambda \in \mathbf{I}$, we regard λ as a function on $\mathrm{Spec}(\mathbf{I})$ via $\lambda(P) = P(\lambda) = \lambda \bmod P \in \mathbf{I}/P$. We want to reduce π modulo P; thus, we consider the representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on L/PL. It should look like a representation π' into $GL_2(K_P)$ (K_P is the quotient field of $\mathbf{I}/P$) such that:

(1a) π' is unramified outside p;
(1b) $\det(1-\pi'(\mathrm{Frob}_q)T) = 1-\lambda(T(q))(P)T+\chi(q)\kappa(\langle q\rangle)q^{-1}(P)T^2$ for all prime q outside p.

If $P|_\Lambda = P_{k,\varepsilon}\Lambda$, then $\lambda(T(q))(P)$ is equal to $a(q,F(P))$ and

$$\chi(q)\kappa(\langle q\rangle)q^{-1}(P) = \varepsilon\chi\omega^{-k}(q)q^{k-1} = \chi_P(q)q^{k-1}.$$

A Galois representation $\pi(P)$ into $GL_2(\overline{K}_P)$ for an algebraic closure $\overline{K}_P$ of K_P is called a residual representation of π if $\pi(P)$ is continuous under the $\mathbf{m}$-adic topology on $\overline{K}_P$, semi-simple and satisfies the conditions (1a,b). Since $\mathbf{I}$ is of Krull dimension 2, K_P is always locally compact under $\mathbf{m}$-adic topology for $P \neq \{0\}$, and thus the continuity of $\pi \bmod P$ is clear. Since L may not be free of rank 2 over $\mathbf{I}$, it is not *a priori* clear that the residual representation exists for all prime ideal P. In fact it exists:

Corollary 1. *For every prime ideal* P, *the residual representation* $\pi(P)$ *of* π *exists and is unique up to isomorphisms over* $\overline{K}_P$.

Proof. We proceed by induction on the height of P. Suppose that P is of height 1. Since Λ is a unique factorization domain [Bour1, VII], the localization Λ_P of Λ at any $P\cap\Lambda$ is a valuation ring. Then, the localization A at P is a finite normal extension of Λ_P. Therefore A is also a valuation ring. We take an $\mathbf{I}$-submodule L of $\mathbf{K}^2$ of finite type which is stable under π and $L\otimes\mathbf{K} = \mathbf{K}^2$. Consider $V = L\otimes_{\mathbf{I}}A$, which is stable under π and $V\otimes\mathbf{K} = \mathbf{K}^2$. Therefore V is a free A-module of rank 2. Identifying V with A^2, we have a Galois representation π into $GL_2(A)$ satisfying the conditions of Theorem 1. Then by reducing π modulo P and taking its semi-simplification, we obtain a residual Galois representation $\pi(P)$. Uniqueness of π follows from the fact that $\mathrm{Tr}(\pi(P)(\mathrm{Frob}_q))$ is given by $\lambda(T(q))(P)$ and that Frob_q is dense in the Galois

group of the maximal unramified extension outside p of $\mathbf{Q}$. Now we replace Λ by the normalization of $\Lambda/P\cap\Lambda$ and $\mathbf{I}$ by the integral closure $\mathbf{I}'$ of $\Lambda/P\cap\Lambda$ in the quotient field of $\mathbf{I}/P$. For any prime ideal P' of height 1 in $\mathbf{I}'$, we apply the same argument to $\pi \bmod P$ and get the residual representation $(\pi \bmod P) \bmod P'$. This representation is just the residual representation attached to a prime ideal in $\mathbf{I}$ of height 2, which is the pullback of P' in $\mathbf{I}$. Continuing this process, we get the claimed result for all prime ideals of $\mathbf{I}$.

Even if the actual representation π is not known to exist, we can consider the residual representations separately. Thus if an $\mathbf{I}$-adic common eigenform F is given, then for each point $P \in \mathcal{X}(\mathbf{I})$, we call a semi-simple Galois representation π' into $GL_2(A_P)$ a residual representation modulo P if π' satisfies the conditions (1a,b) for P, where A_P is the integral closure of $\mathcal{O}_P$ in its quotient field. Our method of proving the theorem is to show that the desired π exists if there exist infinitely many distinct primes $\{P\}$ in $\mathcal{X}(\mathbf{I})$ which have the residual representation modulo P. Such a family of infinitely many residual representations is supplied by the following theorem of Deligne:

Theorem 2 (P. Deligne [D]). *Let* M *be a finite extension of* $\mathbf{Q}_p$. *Let* $\lambda : \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]) \to M$ *be an algebra homomorphism. Then there exists a unique Galois representation* $\pi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(M)$ *such that*

(i) π *is continuous and absolutely irreducible over* M,

(ii) π *is unramified outside* Np,

(iii) *for each prime* q *outside* Np,

$$\det(1-\pi(\mathrm{Frob}_q)X) = 1 - \lambda(T(q))X + \chi(q)q^{k-1}X^2.$$

This result in the case where $k = 2$ (except the determination of ramified places) is a classical result due to Eichler and Shimura and its proof can be found in [Sh, Th.7.24]. The unramifiedness outside Np was later proven by Igusa in the case of weight 2. The case $k \geq 2$ is treated in Deligne's work [D]. The remaining case $k = 1$ is dealt with by Deligne and Serre in [DS]. Note that $\chi(-1) = (-1)^k$ and thus $\det(\pi(c)) = \chi(-1)(-1)^{k-1} = -1$ for complex conjugation c. For further study of ramification, see [La] and [Cl]. Then Theorem 1 follows from the above theorem of Deligne and the following result of Wiles:

Theorem 3 (Wiles [Wi1]). *Let* F *be an* $\mathbf{I}$*-adic normalized common eigenform and suppose that there exists an infinite set* S *of distinct points in* $\mathcal{X}(\mathbf{I})$ *such that for every* $P \in S$, *the residual representation* $\pi(P)$ *into* $GL_2(\mathcal{O}_P)$ *exists, where* $\mathcal{O}_P$ *is the* p*-adic integer ring of the quotient field of* $\mathbf{I}/\mathbf{P}$. *Then there exists a Galois representation* $\pi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{K})$ *satisfying the conditions of Theorem 1.*

In fact, if F is ordinary, we can take $\mathcal{A}(\mathbf{I})$ as the set S by the theorem of Deligne. Even if F is not ordinary, we can take as S the set of admissible points in $\mathcal{A}(\mathbf{I})$. For ordinary F, we can avoid the use of infinitely many modular forms of different weight, taking as S the set $\{P \in \mathcal{A}(\mathbf{I}) \mid k(P) = k\}$. Thus for a fixed weight $k > 1$, if we have Deligne's Galois representation for every common eigenform of weight k, Theorem 1 follows from Theorem 3. In particular, if we take $k = 2$, Theorem 1 follows from the result in [Sh, §7.6], which shows the existence of Galois representations attached to modular forms of weight 2.

Now we start the proof of Theorem 3. Although Theorem 3 holds even for $p = 2$, we prove the theorem assuming $p > 2$ for simplicity. We refer to [Wil] for the proof in the general case. Let us fix $P \in S$ and write π for $\pi(P)$ and M for K_P. Let A be the p-adic integer ring of M. Thus π has values in $GL_2(A)$. Let G be the Galois group of the maximal extension unramified outside p. Since π is unramified outside p, we may consider π as a representation of G. We write L for A^2 and consider L as a G-module via π. We write c for complex conjugation. Since $c^2 = 1$ and $\det(\pi(c)) = -1$, the eigenvalues of $\pi(c)$ are ± 1. We decompose $L = L_+ \oplus L_-$ into the sum of the ± 1 eigenspaces of $\pi(c)$. Thus by identifying L with A^2 via the basis of $L_\pm$, we may assume that

$$\pi(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

For each $\sigma \in G$, we write $\pi(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$ and define a function $x: G \times G \to A$ by $x(\sigma,\tau) = b(\sigma)c(\tau)$. Then these functions satisfy the following properties:

(2a) as functions on G or G^2, a, d and x are continuous,

(2b) $a(\sigma\tau) = a(\sigma)a(\tau)+x(\sigma,\tau)$, $d(\sigma\tau) = d(\sigma)d(\tau)+x(\tau,\sigma)$ and

$$x(\sigma\tau,\rho\gamma) = a(\sigma)a(\gamma)x(\tau,\rho)+a(\gamma)d(\tau)x(\sigma,\rho)+a(\sigma)d(\rho)x(\tau,\gamma)+d(\tau)d(\rho)x(\sigma,\gamma),$$

(2c) $a(1) = d(1) = d(c) = 1$, $a(c) = -1$, and

$$x(\sigma,\rho) = x(\rho,\tau) = 0 \text{ if } \rho = 1 \text{ or } c,$$

(2d) $x(\sigma,\tau)x(\rho,\eta) = x(\sigma,\eta)x(\rho,\tau)$.

The properties (2c) and (2d) follow directly from the definition, and the first half of (2b) can be proven by computing directly the multiplicative formula

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}\begin{pmatrix} a(\tau) & b(\tau) \\ c(\tau) & d(\tau) \end{pmatrix} = \begin{pmatrix} a(\sigma\tau) & b(\sigma\tau) \\ c(\sigma\tau) & d(\sigma\tau) \end{pmatrix}.$$

Then, in addition to the two first formulas of (2b), we also have

$$b(\sigma\tau) = a(\sigma)b(\tau)+b(\sigma)d(\tau) \text{ and } c(\sigma\tau) = c(\sigma)a(\tau)+d(\sigma)c(\tau).$$

Thus we know that

$$x(\sigma\tau,\rho\gamma) = b(\sigma\tau)c(\rho\gamma) = (a(\sigma)b(\tau)+b(\sigma)d(\tau))(c(\rho)a(\gamma)+d(\rho)c(\gamma))$$
$$= a(\sigma)a(\gamma)x(\tau,\rho)+a(\gamma)d(\tau)x(\sigma,\rho)+a(\sigma)d(\rho)x(\tau,\gamma)+d(\tau)d(\rho)x(\sigma,\gamma).$$

For any topological algebra R, we now define a *pseudo-representation* of G into R to be a triple $\pi' = (a, d, x)$ consisting of continuous functions on G or G^2 satisfying the conditions (2a-d). We define the trace $\mathrm{Tr}(\pi')$ (resp. the determinant $\det(\pi')$) of the pseudo-representation π' to be a function on G given by

$$\mathrm{Tr}(\pi')(\sigma) = a(\sigma)+d(\sigma) \text{ (resp. } \det(\pi')(\sigma) = a(\sigma)d(\sigma)-x(\sigma,\sigma)).$$

Our proof of Theorem 3 is divided into two parts: the steps are represented by the following two propositions:

Proposition 1. *Let* $\pi' = (a, d, x)$ *be a pseudo-representation of* G *into an integral domain* R *with quotient field* Q. *Then there exists a continuous representation* $\pi : G \to GL_2(Q)$ *with the same trace and determinant as* π'.

Proposition 2. *Let* a *and* b *be two ideals of* $\mathbf{I}$. *Let* $\pi(a)$ *and* $\pi(b)$ *be pseudo-representations into* $\mathbf{I}/a$ *and* $\mathbf{I}/b$, *respectively. Suppose that* $\pi(a)$ *and* $\pi(b)$ *are compatible; that is, there exist functions* Tr *and* det *on a dense subset* Σ *of* G *with values in* $\mathbf{I}/a\cap b$ *such that for all* $\sigma \in \Sigma$,

$$\mathrm{Tr}(\pi(a)(\sigma)) \equiv \mathrm{Tr}(\sigma) \bmod a \text{ and } \mathrm{Tr}(\pi(b)(\sigma)) \equiv \mathrm{Tr}(\sigma) \bmod b,$$
$$\det(\pi(a)(\sigma)) \equiv \det(\sigma) \bmod a \text{ and } \det(\pi(b)(\sigma)) \equiv \det(\sigma) \bmod b.$$

Then there exists a pseudo-representation $\pi(a\cap b)$ *of* G *into* $\mathbf{I}/a\cap b$ *such that*

$$\mathrm{Tr}(\pi(a\cap b)(\sigma)) = \mathrm{Tr}(\sigma) \text{ and } \det(\pi(a\cap b)(\sigma)) = \det(\sigma) \text{ on } \Sigma.$$

First admitting these two propositions, let us prove Theorem 3. Since G is unramified outside p, the set Σ of Frobenius elements for primes outside p is dense in G (Chebotarev density theorem: Theorem 1.3.1). We put $\mathrm{Tr}(\mathrm{Frob}_q) = \lambda(T(q))$ and $\det(\mathrm{Frob}_q) = \chi(q)\kappa(\langle q\rangle)q^{-1}$. We number each element of S and write $S = \{P_i\}_{i=1}^{\infty}$ and π_i for $\pi(P_i)$. We construct out of each residual representation π_i for $P \in S$, a pseudo-representation π'_i. Then all the π'_i's are compatible. Then by the above proposition, we can construct a pseudo-representation π'^i into $\mathbf{I}/\bigcap_{j=1}^{i}P_j$ so that $\mathrm{Tr}(\pi'^i(\sigma)) \equiv \mathrm{Tr}(\pi'^{i-1}(\sigma)) \bmod \bigcap_{j=1}^{i-1}P_j$ on Σ. Both sides of this congruence are continuous functions and hence

$$\mathrm{Tr}(\pi'^i(\sigma)) \equiv \mathrm{Tr}(\pi'^{i-1}(\sigma)) \bmod P_1\cap \cdots \cap P_{i-1} \text{ on } G.$$

Note that by definition, if $\pi^i = (a_i, d_i, x_i)$, $a_i(\sigma) = 2^{-1}(\mathrm{Tr}(\pi'^i(\sigma))-\mathrm{Tr}(\pi'^i(\sigma c)))$ and $d_i(\sigma) = 2^{-1}(\mathrm{Tr}(\pi'^i(\sigma))+\mathrm{Tr}(\pi'^i(\sigma c)))$ and $x_i(\sigma,\tau) = a_i(\sigma\tau)-a_i(\sigma)a_i(\tau)$. Therefore we have

$$a_i(\sigma) \equiv a_{i-1}(\sigma) \bmod P_1\cap \cdots \cap P_{i-1},\ d_i(\sigma) \equiv d_{i-1}(\sigma) \bmod P_1\cap \cdots \cap P_{i-1}$$

$$\text{and} \quad x_i(\sigma,\tau) \equiv x_{i-1}(\sigma,\tau) \bmod P_1 \cap \cdots \cap P_{i-1}.$$

Thus we can define a pseudo-representation π' into $\mathbf{I} = \varprojlim_i \mathbf{I}/P_1 \cap \cdots \cap P_i$ by

$$\pi'(\sigma) = \varprojlim_i \pi'^i(\sigma).$$

Then we can construct the representation π out of π' by Proposition 1.

Wenow prove Proposition 1. We divide our argument into two cases:

Case 1: there exist ρ and $\gamma \in G$ such that $x(\rho,\gamma) \neq 0$, and

Case 2: $x(\sigma,\tau) = 0$ for all σ,τ in G.

Case 1. We define $\pi(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$ by putting

$$c(\sigma) = x(\rho,\sigma) \quad \text{and} \quad b(\sigma) = x(\sigma,\gamma)/x(\rho,\gamma).$$

Then $b(\sigma)c(\tau) = x(\rho,\tau)x(\sigma,\gamma)/x(\rho,\gamma) = x(\sigma,\tau)$ by (2d). Thus we know that the entry of $\pi(\sigma)\pi(\tau)$ at the upper left corner is equal to, by (2b),

$$a(\sigma)a(\tau)+b(\sigma)c(\tau) = a(\sigma)a(\tau)+x(\sigma,\tau) = a(\sigma\tau).$$

Similarly the lower right corner of $\pi(\sigma)\pi(\tau)$ is equal to

$$d(\sigma)d(\tau)+b(\tau)c(\sigma) = d(\sigma)d(\tau)+x(\tau,\sigma) = d(\sigma\tau).$$

We now compute the lower left corner of $\pi(\sigma)\pi(\tau)$, which is given by

$$c(\sigma)a(\tau)+d(\sigma)c(\tau) = x(\rho,\sigma)a(\tau)+d(\sigma)x(\rho,\tau).$$

By applying (2b) to $(1,\rho,\sigma,\tau)$, we have

$$c(\sigma\tau) = x(\rho,\sigma\tau) = a(\tau)x(\rho,\sigma)+d(\sigma)x(\rho,\tau),$$

since $x(1,\sigma) = x(1,\tau) = 0$ by (2c). This shows that

$$c(\sigma\tau) = c(\sigma)a(\tau)+d(\sigma)c(\tau).$$

Similarly by applying (2b) to $(\sigma,\tau,1,\gamma)$, we have

$$b(\sigma\tau)x(\rho,\gamma) = x(\sigma\tau,\gamma) = a(\sigma)x(\tau,\gamma)+d(\tau)x(\sigma,\gamma) = (a(\sigma)b(\tau)+d(\tau)b(\sigma))x(\rho,\gamma),$$

which finishes the proof of the formula $\pi(\sigma)\pi(\tau) = \pi(\sigma\tau)$. Obviously, by definition, $\pi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and hence π is the desired representation.

Case 2. In this case, by (2b), we have $a(\sigma)a(\tau) = a(\sigma\tau)$ and $d(\sigma)d(\tau) = d(\sigma\tau)$ for all $\sigma,\tau \in G$. Then we simply put $\pi(\sigma) = \begin{pmatrix} a(\sigma) & 0 \\ 0 & d(\sigma) \end{pmatrix}$ which does the job.

We now prove Proposition 2. We consider the exact sequence:

$$0 \to \mathbf{I}/a\cap b \to \mathbf{I}/a\oplus\mathbf{I}/b \xrightarrow{\alpha} \mathbf{I}/(a+b) \to 0$$
$$a \mapsto a \bmod a \oplus a \bmod b$$
$$a\oplus b \mapsto a-b \bmod a+b.$$

We consider the pseudo-representation $\pi = \pi(a)\oplus\pi(b)$ with values in $\mathbf{I}/a\oplus\mathbf{I}/b$. The function $\alpha\circ\mathrm{Tr}(\pi)$ vanishes identically on Σ. Since this function is continuous on G and Σ is dense in G, $\alpha\circ\mathrm{Tr}(\pi)$ vanishes on G. Thus $\mathrm{Tr}(\pi)$ has values in $\mathbf{I}/a\cap b$. If we write $\pi = (a, d, x)$, then

$$a(\sigma) = 2^{-1}(\mathrm{Tr}(\pi(\sigma))-\mathrm{Tr}(\pi(\sigma c))),\ d(\sigma) = 2^{-1}(\mathrm{Tr}(\pi(\sigma))+\mathrm{Tr}(\pi(\sigma c)))$$
$$\text{and } x(\sigma,\tau) = a(\sigma\tau)-a(\sigma)a(\tau).$$

Thus π itself has values in $\mathbf{I}/a\cap b$ and gives the desired pseudo-representation.

§7.6. Examples of Λ-adic forms

In this section, we briefly discuss some examples of ordinary and non-ordinary Λ-adic cusp forms. We will not give detailed proofs but satisfy ourselves with indicating the source where one can find proofs. We start with the lowest weight cusp form of $SL_2(\mathbf{Z})$, which is the Ramanujan Δ function. The function Δ spans $\mathcal{S}_{12}(SL_2(\mathbf{Z}))$ and is a normalized eigenform. Then it is known by computation that $\Delta\,|\,T(p) = \tau(p)\Delta$ with $\tau(p) \in \mathbf{Z}_p^\times\cap\mathbf{Z}$ for $11 \le p \le 1021$. Thus writing as α the unique p-adic unit root of $X^2-\tau(p)+p^{11} = 0$ for those primes, we know that $f = \Delta(z)-\alpha^{-1}p^{11}\Delta(pz)$ is a normalized eigenform of level p and $f\,|\,T(p) = \alpha f$, i.e. f is ordinary. Then, if $|\tau(p)|_p = 1$, the fact that $\mathcal{S}_{12}^{\mathrm{ord}}(\Gamma_0(p);\mathbf{Q}_p) = \mathbf{Q}_p f$ follows from [M, Th.4.6.17 (2)]. In general, we have

$$\dim\mathcal{S}_k^{\mathrm{ord}}(\Gamma_0(p);\mathbf{Q}_p) = \dim\mathcal{S}_k^{\mathrm{ord}}(SL_2(\mathbf{Z});\mathbf{Q}_p) \quad \text{(Proposition 7.2.2).}$$

Thus $\mathbf{h}_{12}^{\mathrm{ord}}(\Gamma_0(p);\mathbf{Z}_p) \cong \mathbf{Z}_p$ via $T(n) \mapsto \tau(n)$ which is the eigenvalue of $T(n)$ for Δ. This implies $\mathbf{h}^{\mathrm{ord}}(\omega^{12};\Lambda)/P_{12}\mathbf{h}^{\mathrm{ord}}(\omega^{12};\Lambda) \cong \mathbf{Z}_p$. Since $\mathbf{h}^{\mathrm{ord}}(\omega^{12};\Lambda)$ is a Λ-algebra, we have the structural morphism $\iota : \Lambda \to \mathbf{h}^{\mathrm{ord}}(\omega^{12};\Lambda)$. Then by the Nakayama lemma, we know that ι is surjective. As we have already seen (Theorem 3.5), $\mathbf{h}^{\mathrm{ord}}(\omega^{12};\Lambda)$ is Λ-free, and hence ι is an isomorphism. Thus there exists a unique ordinary Λ-adic normalized eigenform F_Δ spanning $\mathbf{S}^{\mathrm{ord}}(\omega^{12};\Lambda)$ such that $F_\Delta(u^{12}-1) = \Delta(z)-\alpha^{-1}p^{11}\Delta(pz)$ as long as $|\tau(p)|_p = 1$ holds. Since 12 is the least weight k for which $\mathcal{S}_k(SL_2(\mathbf{Z})) \neq 0$, $\mathbf{h}^{\mathrm{ord}}(\chi;\Lambda) = 0$ for $p = 2, 3, 5$ and 7 for all χ.

In the text, we have only discussed Λ-adic forms of level p^∞. If we introduce an auxiliary level N prime to p, there are abundant examples. A formal q-expansion $F \in \Lambda[[q]]$ is called a Λ-adic form of level Np^∞ and of character χ for a finite

order character χ of $(\mathbf{Z}/Np\mathbf{Z})^\times$, if for almost all positive integers k, $F(u^k-1) \in \mathcal{M}_k(\Gamma_0(Np^\alpha),\chi\omega^{-k};\mathcal{O})$ for some fixed α. Then we define the notions of Λ-adic cusp forms, Λ-adic ordinary forms, etc. in the same manner as in §7.1. The first example of this type is the Λ-adic cusp forms associated with imaginary quadratic fields (given by theta series). We thus fix an imaginary quadratic extension $M/\mathbf{Q}$. Then there are abundant arithmetic Hecke characters λ such that $\lambda((\alpha)) = \alpha^{k-1}$ for $\alpha \equiv 1 \bmod c$ for some ideal c, where $k \geq 1$ is a positive integer. The largest ideal c in the integer ring r of M with this property is called the conductor of λ. Then it is well known (see [M, Th.4.8.2]) that there exists a modular form

$$(1) \qquad f_\lambda = \sum_a \lambda(a) q^{N(a)} \in \mathcal{M}_k(\Gamma_0(DN(c)),\chi\tilde{\lambda}),$$

where D is the discriminant of $M/\mathbf{Q}$, $\chi(m) = \left(\frac{-D}{m}\right)$ is the Jacobi symbol and $\tilde{\lambda}(m) = \lambda((m))/m^{k-1}$ for integers m. This form is known to be a cusp form if λ is non-trivial (in particular if $k > 1$). Then f_λ is a normalized eigenform and for primes l, $a(l,f) = 0$ if lr is a prime ideal, $a(l,f) = \lambda(\mathfrak{l})+\lambda(\bar{\mathfrak{l}})$ if $lr = \mathfrak{l}\bar{\mathfrak{l}}$ with $\mathfrak{l} \neq \bar{\mathfrak{l}}$ and $\mathfrak{l}\bar{\mathfrak{l}}+c = r$, $a(l,f) = \lambda(\bar{\mathfrak{l}})$ if $\mathfrak{l} \supset Dc$. Here if $\mathfrak{l} \supset c$, we agree to put $\lambda(\mathfrak{l}) = 0$. Let p be a prime ideal of M given by $\{x \in r \mid |x|_p < 1\}$ for the p-adic absolute value of $\overline{\mathbf{Q}}_p$. We fix one character λ modulo cp for an ideal c prime to p such that $\lambda((\alpha)) = \alpha$ if $\alpha \equiv 1 \bmod cp$. Then we take $K = \mathbf{Q}_p(\lambda)$ and its p-adic integer ring $\mathcal{O}$. We decompose $\mathcal{O}^\times = W_K \times \mu_K$ so that W_K is $\mathbf{Z}_p$-free and μ_K is a finite group. We then write the projection map of $\mathcal{O}^\times$ onto W_K as $x \mapsto \langle x \rangle$. First we suppose that $pr = p\bar{p}$ with two distinct prime ideals p and $\bar{p}$. Then the subgroup W_M of W_K topologically generated by $\langle\lambda(a)\rangle$ for all ideals a prime to p is isomorphic to the additive group $\mathbf{Z}_p$ and the index $p^\gamma = (W_M:W) < \infty$. Here we consider $W = 1+p\mathbf{Z}_p$ as a subgroup of W_M by first regarding W as a subgroup of $r_p^\times$ and then applying the map: $z \mapsto \langle\lambda(z)\rangle$. Note that this is in fact the natural inclusion map of W into $\mathbf{Q}_p(\lambda)$. The exponent $\gamma = 0$ if the class number of M is prime to p. We fix a generator w of W_M so that $w^{p^\gamma} = u$. Then we consider the ring $\mathbf{I} = \mathcal{O}[[Y]]$ containing the ring $\Lambda = \mathcal{O}[[X]]$ with the relation $(1+Y)^{p^\gamma} = (1+X)$. Then we consider the series

$$(2a) \qquad F_\lambda(Y;q) = \sum_a \lambda(a)\langle\lambda(a)\rangle^{-2}(1+Y)^{s(a)}q^{N(a)} \text{ if } pr = p\bar{p} \text{ with } p \neq \bar{p},$$

where a runs over all ideals prime to p and $s(a) = log(\langle\lambda(a)\rangle)/log(w)$, i.e. $w^{s(a)} = \langle\lambda(a)\rangle$. Then we know that $(1+Y)^{s(a)}|_{Y=w^{k-1}} = w^{ks(a)} = \langle\lambda(a)\rangle^k$. Noting

that the Hecke character λ_k modulo cp given by $\lambda_k(a) = \lambda(a)\langle\lambda(a)\rangle^{k-2}$ has in fact values in $\overline{\mathbf{Q}}$, we get

$$\text{(2b)} \qquad F_\lambda(w^k-1;q) = f_{\lambda_k} \in \mathcal{S}_k(\Gamma_0(DN(c)p),\chi\tilde{\lambda}\omega^{2-k};\mathcal{O}).$$

Here it is easy to compute $\tilde{\lambda}_k = \chi\tilde{\lambda}\omega^{2-k}$. If we substitute ζw^k-1 (instead of w^k-1) for X in $F_\lambda(X;q)$ for a p^γ-th root of unity ζ, we have

$$\text{(2c)} \qquad F_\lambda(\zeta w^k-1;q) = f_{\varepsilon\lambda_k} \in \mathcal{S}_k(\Gamma_0(DN(c)p),\chi\tilde{\lambda}\omega^{2-k};\mathcal{O}),$$

where ε is the finite order character of the ideal class group $Cl_M(1)$ given by $\varepsilon(a) = \zeta^{s(a)}$.

Since $P_k = X-(u^k-1) = \prod_\zeta(Y-(\zeta w^k-1))$ in $\mathbf{I}$, we know that F_λ is an $\mathbf{I}$-adic form of level $DN(c)$ and of character $\chi\tilde{\lambda}\omega^2$. Since $\varepsilon\lambda_k(\bar{p})$ is a p-adic unit and since the eigenvalue of $T(p)$ for $f_{\varepsilon\lambda_k}$ is given by $\varepsilon\lambda_k(\bar{p})$, F_λ is ordinary. If one chooses λ so that λ_1 is trivial (this is always possible), then we see that

$$f_{\lambda_1} = \sum_a q^{N(a)} = \sum_{n=1}^\infty \sigma_{1,\chi}(n)q^n - \sum_{n=1}^\infty \sigma_{1,\chi}(n)q^{np} = E_1(\chi)(z)-E_1(\chi)(pz).$$

Thus $F_\lambda(w-1) = E(\chi\omega)(u-1)$ where $E(\chi\omega)(X;q)$ is the Λ-adic Eisenstein series such that $E(\chi\omega)(u^k-1) = E_k(\chi\omega^{1-k})$ or $E_k(\chi)(z)-E_k(\chi)(pz)$ according as ω^{1-k} is non-trivial or not. Then, for example, supposing $W_M = W$, we have a strange Λ-adic form $E(X;q) = \dfrac{E(\chi\omega)-F_\lambda}{X-(u-1)}$. This implies

$$E\,|\,T(n) = \frac{a(n,E(\chi\omega))E(\chi\omega)-a(n,F_\lambda)F_\lambda}{X-(u-1)} = \frac{a(n,E(\chi\omega))-a(n,F_\lambda)}{X-(u-1)}E(\chi\omega)+a(n,F_\lambda)E.$$

Note that $\dfrac{a(n,E(\chi\omega))-a(n,F_\lambda)}{X-(u-1)} \in \Lambda$ and is non-vanishing at $u-1$. Thus on $\mathbf{M}^{ord}(\chi\omega;\Lambda)/P_1\mathbf{M}^{ord}(\chi\omega;\Lambda)$, $T(n)$ acts non-semi-simply. On the other hand, the action of Hecke operators $T(n)$ for n prime to Dp on $\mathcal{M}_1(\Gamma_0(Dp),\chi\omega)$ is semi-simple, because the same argument as in the proof of Theorem 5.3.2 obviously works. This shows that inside $\mathcal{O}[[q]]$, the image of specialization of $\mathbf{M}^{ord}(\chi\omega;\Lambda)$ under $F \mapsto F(u-1)$ is larger than the space of classical ordinary forms $\mathcal{M}_1^{ord}(\Gamma_0(Dp),\chi\omega;\mathcal{O})$.

Now we assume that p is inert or ramified in M. For simplicity we assume that $p \neq 2$. We have a surjective group homomorphism $\varphi : Cl_M(cp^\infty) \to W_M$ given by $\varphi(x) = \langle\lambda(x)\rangle$. On $Cl_M(cp^\infty)$, there is the natural action of complex conjugation c which leaves the maximal torsion subgroup of $Cl_M(cp^\infty)$ stable,

and hence c acts on the image W_M by $\varphi(x)^c = \varphi(x^c)$. This action may not coincide with the usual Galois action of c on $\mathbf{Q}(\lambda)$. Then $W_M \cong \mathbf{Z}_p^2$ and thus we have two generators w_1 and w_2 of W_M. We then may assume that $w_1 = u$ and $w_2 = w$ with $w^c = w^{-1}$ for complex conjugation c. We then write $\langle\lambda(a)\rangle = u^{s(a)}w^{t(a)}$ and define

(3a) $F_\lambda(X,Y;q) = \sum_a \lambda(a)\langle\lambda(a)\rangle^{-2}(1+X)^{s(a)}(1+Y)^{t(a)}q^{N(a)} \in \mathcal{O}[[X,Y]][[q]]$.

This is not really a Λ-adic form but, so to speak, an $\mathcal{O}[[X,Y]]$-adic form. That is, we have, for a pair (ζ,ζ') of p-power roots of unity

(3b) $F_\lambda(\zeta u^k-1,\zeta' w^k-1) = f_{\varepsilon\lambda_k} \in \mathcal{S}_k(\Gamma_0(DN(c)p^{2\max(\beta,1)}),\breve{\varepsilon}\chi\breve{\lambda}\omega^{2-k};\mathcal{O})$,

where $\varepsilon(a) = \zeta^{s(a)}\zeta'^{t(a)}$ is a finite order character with conductor p^β. Since $a(p,f_{\lambda_k})$ is either 0 or a p-adic non-unit, the family of modular forms $\{f_{\varepsilon\lambda_k}\}$ will never be ordinary.

These Λ-adic forms constructed out of imaginary quadratic fields are called Λ-adic forms with *complex multiplication* or of *CM type*. As is clear from the above examples, there exist $\mathbf{I}$-adic forms having values in a non-trivial extension $\mathbf{I}$ of Λ.

There are examples of Λ-adic forms without complex multiplication. We start from a primitive finite order character λ_1 modulo c of the imaginary quadratic field or real quadratic field M. We continue to write r for the integer ring of M. Then, even in the case of real M, if $\lambda_1(\alpha) = -1$ for $\alpha \in r$ with the congruence $\alpha \equiv 1 \bmod c$ and $\alpha^\sigma \equiv -1 \bmod c$ for a non-trivial automorphism σ of M, f_λ as in (1) is a cusp form in $\mathcal{S}_1(\Gamma_0(DN(c)),\breve{\lambda}\chi)$ for the discriminant D of M and the Jacobi symbol $\chi(m) = \left(\frac{|D|}{m}\right)$([M, Th.4.8.3]). Suppose that

(4a) p is a divisor of $DN(c)$ (resp. D) if M is real (resp. complex);

(4b) There exists a prime factor p of p in r such that p^σ is prime to c,

where $\sigma = c$ when M is imaginary. Then we see that $f_{\lambda_1} | T(p) = \lambda(p^\sigma)f_{\lambda_1}$ and hence f_{λ_1} is ordinary because $\lambda(p^\sigma)$ is a root of unity. When $p | D$, there are no ordinary Λ-adic forms with complex multiplication. When M is real quadratic, the modular forms associated with real quadratic fields do not exist in weight higher than 1. However by Theorem 7.3.7, we can lift f_{λ_1} to an $\mathbf{I}$-adic normalized eigenform F which is not of CM type.

We know from [M, Th.4.2.11 and Th.4.2.7] that

(5) $$\dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(4))) = 0$$

and for odd p, $\dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(p))) = \frac{p-6}{12} - \frac{1}{4}\left(\frac{-1}{p}\right) - \frac{1}{3}\left(\frac{-3}{p}\right)$.

It is also known that T(p) is invertible on $\mathcal{S}_2(\Gamma_0(p))$ and has only eigenvalues ±1 ([M, Th.4.6.17 (2)]). Thus in this special case, we have

$$\mathcal{S}_2(\Gamma_0(p);\mathcal{O}) = \mathcal{S}_2^{\mathrm{ord}}(\Gamma_0(p);\mathcal{O}).$$

Then by Theorem 3.3, we know

Theorem 1. *For odd primes* p, *we have*

$$\mathrm{rank}_\Lambda(\mathbf{h}^{\mathrm{ord}}(\omega^2;\Lambda)) = \mathrm{rank}_\Lambda(\mathbf{S}^{\mathrm{ord}}(\omega^2;\Lambda)) = \frac{p-6}{12} - \frac{1}{4}\left(\frac{-1}{p}\right) - \frac{1}{3}\left(\frac{-3}{p}\right).$$

The above dimension formula is due to Dwork when $p \equiv 1 \bmod 12$ [K4, p.140]. By the above formula $\mathrm{rank}_\Lambda(\mathbf{h}^{\mathrm{ord}}(\omega^2;\Lambda))$ grows linearly as the prime p grows. This is the only case where we know the exact rank of the space of ordinary Λ-adic forms in a systematic way. There are several numerical examples computed by Maeda for Λ-adic forms. We refer to [Md] and [H2] for these examples. In particular, in [Md] Maeda gives a criterion in terms of generalized Bernoulli numbers for having non-trivial Λ-adic forms without complex multiplication which are congruent to Λ-adic modular forms with complex multiplication. Such a congruence is very important in studying the Iwasawa theory of imaginary quadratic fields and CM fields. We refer to [HT1-3] for such applications in Iwasawa's theory.

Chapter 8. Functional equations of Hecke L-functions

In this chapter, after giving a brief summary of the notion of adeles of number fields, we prove the functional equations of Hecke L-functions. For further study of adeles and class field theory, we recommend [W1] and [N].

§8.1. Adelic interpretation of algebraic number theory

Let us start with the explanation of the adele ring of $\mathbf{Q}$ denoted by $\mathbf{A}$. To define the topological ring $\mathbf{A}$, we consider the module $\mathbf{Q}/\mathbf{Z}$ and its ring $\mathrm{End}(\mathbf{Q}/\mathbf{Z})$ of additive endomorphisms. Let $\mathbf{Q}/\mathbf{Z}[p^\infty]$ be the subgroup of $\mathbf{Q}/\mathbf{Z}$ consisting of elements killed by some power of p for a prime p of $\mathbf{Z}$. Then by definition, for any two distinct primes p and q, $\mathbf{Q}/\mathbf{Z}[p^\infty]\cap\mathbf{Q}/\mathbf{Z}[q^\infty] = \{0\}$ and hence $\oplus_p\mathbf{Q}/\mathbf{Z}[p^\infty] \subset \mathbf{Q}/\mathbf{Z}$. Let us show that this inclusion is in fact surjective. For any given rational number r, we expand r into the standard p-adic expansion $\sum_{n=-m}^{\infty} c_n p^n$ defined in §1.3 and put $[r]_p = \sum_{n=-m}^{-1} c_n p^n$ (the p-fraction part). Since $r-[r]_p \in \mathbf{Z}_p\cap\mathbf{Q}$, p does not appear in the denominator of $r-[r]_p$. Repeating this process of taking out the p-fraction part from r for all prime factors of the denominator of r, we know that $r-\sum_p[r]_p \in \mathbf{Z}$ and hence $r = \sum_p[r]_p$ in $\mathbf{Q}/\mathbf{Z}$. Since $[r]_p \in \mathbf{Q}/\mathbf{Z}[p^\infty]$, we know that $\oplus_p\mathbf{Q}/\mathbf{Z}[p^\infty] = \mathbf{Q}/\mathbf{Z}$. The above process can be applied to p-adic numbers $r \in \mathbf{Q}_p$. Then $r \mapsto [r]_p$ plainly induces an isomorphism: $\mathbf{Q}_p/\mathbf{Z}_p \cong \mathbf{Q}/\mathbf{Z}[p^\infty]$. Thus identifying $\mathbf{Q}_p/\mathbf{Z}_p$ with $\mathbf{Q}/\mathbf{Z}[p^\infty]$, we have

$$\mathbf{Q}/\mathbf{Z} \cong \oplus_p\mathbf{Q}_p/\mathbf{Z}_p. \tag{1}$$

This in particular shows that $\mathrm{End}(\mathbf{Q}/\mathbf{Z}) \cong \prod_p\mathrm{End}(\mathbf{Q}_p/\mathbf{Z}_p)$. The multiplication by elements of $\mathbf{Z}_p$ induces a morphism $\iota : \mathbf{Z}_p \to \mathrm{End}(\mathbf{Q}_p/\mathbf{Z}_p)$, i.e., $\iota_p(z)(z') = zz'$. We now show that ι is a surjective isomorphism. Obviously it is an injection. Note that the submodule $\mathbf{Q}_p/\mathbf{Z}_p[p^r]$ killed by p^r is isomorphic to $\mathbf{Z}/p^r\mathbf{Z}$ via $x \mapsto p^r x$. Since the endomorphism of $\mathbf{Z}/p^r\mathbf{Z}$ is determined by its value at 1, we see that $\mathrm{End}(\mathbf{Q}_p/\mathbf{Z}_p[p^r]) \cong \mathbf{Z}/p^r\mathbf{Z}$ via $\varphi \mapsto \rho(\varphi) = p^r\varphi(p^{-r})$. If $\varphi_r \in \mathrm{End}(\mathbf{Q}_p/\mathbf{Z}_p[p^r])$ is the restriction of $\varphi \in \mathrm{End}(\mathbf{Q}_p/\mathbf{Z}_p)$, then $\{\rho(\varphi_r)\}_r$ is coherent so that $\rho(\varphi_r) \equiv \rho(\varphi_s) \bmod p^s$ if $r \geq s$. Then the map $\rho : \mathrm{End}(\mathbf{Q}_p/\mathbf{Z}_p) \to \mathbf{Z}_p$ given by $\rho(\varphi) = \varprojlim_m \rho(\varphi_r) \in \mathbf{Z}_p$ gives the inverse of ι. This shows that

$$\mathrm{End}(\mathbf{Q}_p/\mathbf{Z}_p) \cong \mathbf{Z}_p \text{ and } \mathrm{End}(\mathbf{Q}/\mathbf{Z}) \cong \hat{\mathbf{Z}} = \prod_p \mathbf{Z}_p. \tag{2a}$$

For any finite subgroup X of $\mathbf{Q}/\mathbf{Z}$, we put

$$A(X) = \{a \in \mathrm{End}(\mathbf{Q}/\mathbf{Z}) \mid aX = 0\}.$$

Then obviously $\mathrm{End}(\mathbf{Q}/\mathbf{Z})/A(X) \cong \mathrm{End}(X)$. Declaring $\{A(X)\}_X$ to be a fundamental system of neighborhoods of 0 in $\mathrm{End}(\mathbf{Q}/\mathbf{Z})$, we give the structure of a topological ring on $\mathrm{End}(\mathbf{Q}/\mathbf{Z})$. This is the weakest topology that the quotient topology of $\mathrm{End}(\mathbf{Q}/\mathbf{Z})/A(X) \cong \mathrm{End}(X)$ is discrete, and hence it is a topology of the projective limit $\mathrm{End}(\mathbf{Q}/\mathbf{Z}) \cong \varprojlim_X \mathrm{End}(X)$. Thus $\mathrm{End}(\mathbf{Q}/\mathbf{Z})$ is a compact ring, which is isomorphic to $\hat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$ as topological ring. We define the finite part $\mathbf{A}_f$ of the adele ring $\mathbf{A}$ to be the subring of $\prod_p \mathbf{Q}_p$ generated by $\mathbf{Q}$ and $\hat{\mathbf{Z}}$. Here $\mathbf{Q}$ is embedded diagonally into $\prod_p \mathbf{Q}_p$ by $\mathbf{Q} \ni a \mapsto (\cdots a,a,a,\cdots) \in \prod_p \mathbf{Q}_p$. We give the structure of a locally compact ring on $\mathbf{A}_f$ so that $\hat{\mathbf{Z}}$ is an open compact subgroup of $\mathbf{A}_f$ and the topology of $\mathbf{A}_f$ induces the topology on $\hat{\mathbf{Z}}$. We define the adele ring $\mathbf{A}$ to be $\mathbf{A}_f \times \mathbf{R}$ and give the product topology on it. Then $\mathbf{A}$ is a locally compact ring. If $x \in \prod_p \mathbf{Q}_p$ satisfies $x_p \in \mathbf{Z}_p$ for almost all p (i.e. for all but finitely many p), we can cancel the denominator of x by multiplying a rational integer m, i.e., $mx \in \prod_p \mathbf{Z}_p$. Thus $x \in \mathbf{A}_f$. It is obvious that $x_p \in \mathbf{Z}_p$ for almost all p if $x \in \mathbf{A}_f$. Then we know that

$$\text{(2b)} \qquad \mathbf{A}_f = \prod{}'_p \mathbf{Q}_p = \{x \in \prod{}_p \mathbf{Q}_p \mid x_p \in \mathbf{Z}_p \text{ for almost all } p\}.$$

Thus $\mathbf{A}_f$ is the restricted direct product of $\mathbf{Q}_p$ with respect to $\mathbf{Z}_p$. This is the definition of $\mathbf{A}_f$ usually found in the literature. Now we shall see that $\mathbf{A}_f = \hat{\mathbf{Z}}+\mathbf{Q}$. For any $x \in \mathbf{A}_f$, the above definition using the restricted direct product shows that $[x] = \sum_p [x_p]_p$ is actually a finite sum and is a rational fraction. Then $x-[x] \in \hat{\mathbf{Z}}$ showing $\mathbf{A}_f = \hat{\mathbf{Z}}+\mathbf{Q}$. In particular, we have

$$\text{(2c)} \qquad \mathbf{A}_f = \hat{\mathbf{Z}}+\mathbf{Q} \text{ and } \mathbf{A}_f/\hat{\mathbf{Z}} \cong \mathbf{Q}/(\hat{\mathbf{Z}} \cap \mathbf{Q}) = \mathbf{Q}/\mathbf{Z}.$$

The multiplicative group $\mathbf{A}^\times$ is called the idele group of $\mathbf{Q}$. Since $\mathbf{Z}$ is a principal ideal domain, for any $x \in \mathbf{A}_f^\times$, we can write $x_p = up^{e(p)}$ with $u \in \mathbf{Z}_p^\times$. Since primes p with $e(p) \neq 0$ are finitely many, $\{x\} = \prod_p p^{e(p)}$ is a positive rational number and hence $x\{x\}^{-1} \in \hat{\mathbf{Z}}^\times$, which shows

$$\text{(3a)} \qquad \mathbf{A}^\times = \hat{\mathbf{Z}}^\times \mathbf{Q}^\times \mathbf{R}_+^\times,$$

where $\mathbf{R}_+^\times = \{x \in \mathbf{R} \mid x > 0\}$. Since $\mathbf{Q} \subset \mathbf{A}$ via $\mathbf{Q} \ni \alpha \mapsto (\alpha,\alpha,\ldots,\alpha) \in \mathbf{A}$, $\mathbf{A}$ is naturally a $\mathbf{Q}$-algebra. Consider a small open interval $U_\varepsilon = (-\varepsilon,\varepsilon)$ for $\varepsilon > 0$ in $\mathbf{R}$. Then $O = \hat{\mathbf{Z}} \times U_\varepsilon$ is an open neighborhood of 0 in $\mathbf{A}$. We see that $\mathbf{Q} \cap O = \mathbf{Z} \cap U_\varepsilon = \{0\}$ if $0 < \varepsilon < 1$. Thus we have found an open neighborhood O of 0 in $\mathbf{A}$ such that $\mathbf{Q} \cap O = \{0\}$. Note that

$$\mathbf{A}/\mathbf{Q} \cong \{(\hat{\mathbf{Z}} \times \mathbf{R})+\mathbf{Q}\}/\mathbf{Q} \cong (\hat{\mathbf{Z}} \oplus \mathbf{R})/\{(\hat{\mathbf{Z}} \oplus \mathbf{R}) \cap \mathbf{Q}\} \cong (\hat{\mathbf{Z}} \oplus \mathbf{R})/\mathbf{Z} \cong \hat{\mathbf{Z}} \times (\mathbf{R}/\mathbf{Z}),$$

which is a compact set. Thus

(3b) $\mathbf{Q}$ is a discrete subring of $\mathbf{A}$ and $\mathbf{A}/\mathbf{Q}$ is compact.

For a number field F (i.e. a finite extension $F/\mathbf{Q}$), we simply put $F_{\mathbf{A}} = F\otimes_{\mathbf{Q}}\mathbf{A}$. Then we have the ring embedding $F \ni a \mapsto a\otimes 1 \in F_{\mathbf{A}}$ and hence $F_{\mathbf{A}}$ is an F-algebra. The trace map $\mathrm{Tr}_{F/\mathbf{Q}} : F \to \mathbf{Q}$ induces the $\mathbf{A}$-linear map $\mathrm{Tr}_{F/\mathbf{Q}}\otimes\mathrm{id} : F_{\mathbf{A}} \to \mathbf{A}$, which is again denoted by $\mathrm{Tr}_{F/\mathbf{Q}}$ and is called the (adelic) trace map. Fixing a basis $\{\omega_i\}$ of F over $\mathbf{Q}$, we identify $F \cong \mathbf{Q}^{[F:\mathbf{Q}]}$ as a vector space, which induces an isomorphism $F_{\mathbf{A}} \cong \mathbf{A}^{[F:\mathbf{Q}]}$ of $\mathbf{A}$-modules. This identification gives a natural topology on $F_{\mathbf{A}}$, under which $F_{\mathbf{A}}$ is a locally compact topological ring. Obviously the topology of $F_{\mathbf{A}}$ does not depend on the choice of the basis. In particular,

(3c) F is a discrete subring of $F_{\mathbf{A}}$ and $F_{\mathbf{A}}/F \cong \hat{O}\times F_\infty/O$ is compact,

where we put $\hat{O}$ for $O\otimes_{\mathbf{Z}}\hat{\mathbf{Z}}$ for the integer ring O of F. Since $\mathbf{A} = \mathbf{A}_f\times\mathbf{R}$, we have $F_{\mathbf{A}} = F_{\mathbf{A}_f}\times F_\infty$ with $F_{\mathbf{A}_f} = F\otimes_{\mathbf{Q}}\mathbf{A}_f$ and $F_\infty = F\otimes_{\mathbf{Q}}\mathbf{R}$. Thus we can write $x = (x_f, x_\infty)$ with the finite part $x_f \in F_{\mathbf{A}_f}$ and the infinite part $x_\infty \in F_\infty$. Let I be the set of all field embeddings of F into $\mathbf{C}$. Then $\mathrm{Aut}(\mathbf{C})$ acts on I from the right via natural composition. Then the set of archimedean places $\mathbf{a}$ is defined to be the set $I/\langle c\rangle$, where $\langle c\rangle$ is the group of order 2 generated by complex conjugation c. Each $\sigma \in \mathbf{a}$ gives rise to a complex absolute value $|\ |_\sigma$ on F by $|a|_\sigma = |a^\sigma|$ for any representative $\sigma \in I$. Then writing $I(\mathbf{R})$ for the subset of I consisting of real embeddings and $I(\mathbf{C}) = I\text{-}I(\mathbf{R})$, i.e., the set of embeddings whose image is not contained in $\mathbf{R}$. We put $\mathbf{a}(\mathbf{R}) = I(\mathbf{R})$ and $\mathbf{a}(\mathbf{C}) = I(\mathbf{C})/\langle c\rangle$. Then as seen in (1.1.5b), $F_\infty = \mathbf{R}^{\mathbf{a}(\mathbf{R})}\times\mathbf{C}^{\mathbf{a}(\mathbf{C})}$. Similarly $\hat{O} = \prod_p O_p$, where p runs over all prime ideals of O. The unit group $F_{\mathbf{A}}^\times$ of $F_{\mathbf{A}}$ is called *the idele group* of F, whose elements are called ideles of F. We give the topology on $F_{\mathbf{A}}^\times$ so that the system of neighborhoods of 1 is given as follows. Let $\hat{O}^\times(m)$ be the kernel of the natural map $\prod_p O_p^\times \to (O/m)^\times$ for all ideals m of O. Then a fundamental system of neighborhoods is given by

$$\{\hat{O}^\times(m)\times U \mid m \text{ an ideal of } O,\ U \text{ a neighborhood of } 1 \text{ in } F_\infty^\times\}.$$

Thus $F_{\mathbf{A}}^\times$ is a locally compact group. The elements of $F_{\mathbf{A}}^\times$ are called ideles. The topology of $F_{\mathbf{A}}^\times$ is stronger than the one induced from the adele ring $F_{\mathbf{A}}$. In fact, the neighborhood of 0 of $F_{\mathbf{A}}$ is given by $\hat{O}(m)\times V$ for the kernel $\hat{O}(m)$ of the natural map of additive group $\prod_p O_p \to (O/m)$ and a neighborhood V of 0 in F_∞. One sees easily that $\{1+\hat{O}(m)\times V\}\cap F_{\mathbf{A}}^\times \supset \hat{O}^\times(m)\times(1+V)$ but they are never equal.

Exercise 1. Show that $\{1+\hat{O}(m)\times V\}\cap F_{\mathbf{A}}^\times \neq \hat{O}^\times(m)\times(1+V)$.

In the same manner as in (3a), we see that

(4a) $$F_{A_f}{}^{\times} = \{x \in \prod_p F_p \mid x_p \in O_p \text{ for almost all } p\}.$$

From this, writing $x_p O_p = p^{e(p)}$, we know that $e(p) = 0$ for almost all p. Thus the ideal $xO = \prod_p p^{e(p)}$ makes sense as a fractional ideal of F. Thus we have a natural homomorphism of groups

(4b) $$F_{A_f}{}^{\times} \to I \quad \text{given by} \quad x \mapsto xO.$$

Obviously this map is surjective. By abusing symbols, we write xO for $x_f O$ when $x \in F_A{}^{\times}$. We now define the adele norm $|x|_A$ by $|x_f|_{A_f} \times |x_\infty|_\infty$ for $|x|_{A_f} = \prod_p |x_p|_p$ and $|x_\infty|_\infty = \prod_{\sigma \in a(R)} |x_\sigma|_\sigma \times \prod_{\sigma \in a(C)} |x_\sigma|_\sigma{}^2$. We normalize $|\varpi_p|_p = N(p)^{-1}$ for the prime element ϖ_p of O_p. Then for $a \in F^{\times}$, we see that

$$|a|_\infty = \prod_{\sigma \in a(R)} |a^\sigma|_\sigma \times \prod_{\sigma \in a(C)} |a^\sigma|_\sigma{}^2 = \prod_{\sigma \in I} |a^\sigma| = |N(a)|.$$

On the other hand, writing the prime factorization of aO as $aO = \prod_p p^{e(p)}$, we see from (1.2.2b) that

$$|a|_{A_f} = \prod_p N(p^{e(p)})^{-1} = N(aO)^{-1} = |N(a)|^{-1}.$$

By this we know the following product formula:

(5) $$|a|_A = 1 \quad \text{for all } a \in F^{\times}.$$

Put $F_A^{(1)} = \{x \in F_A{}^{\times} \mid |x|_A = 1\}$. Then by the product formula, we see that $F_A^{(1)} \supset F^{\times}$.

Theorem 1. *$F^{\times}$ is a discrete subgroup of $F_A^{(1)}$ and $F_A^{(1)}/F^{\times}$ is a compact group, where the system of neighborhoods of 1 of the quotient group $F_A^{(1)}/F^{\times}$ is given by the images of the neighborhoods of 1 in $F_A^{(1)}$.*

Proof. The set of normalized absolute values of F, i.e.

$$\{|\ |_p,\ |\ |_\sigma \mid p\text{: prime ideals},\ \sigma \in a\},$$

is called the set of places of F. When we do not care much about the difference of finite or infinite places, we just write v to indicate a place of F. When we write p (resp. σ), it indicates a finite (resp. archimedean) place. Let a be an idele and define

$$V(a) = \{x \in A_F \mid |x_v|_v \le |a_v|_v \text{ for all } v\}.$$

Then we claim that the following assertion is equivalent to Corollary 1.2.1:

(6) for any idele with sufficiently large $|a|_A$, $V(a)\cap F^\times \neq \emptyset$.

To see this, let $\mathfrak{a} = aO$. Since $\mathfrak{a} = \{x \in F \mid |x|_v \le |a_v|_v\}$, we see $\mathfrak{a} = V(a)F_\infty \cap F$. Thus we only need to show that

$$\{x \in \mathfrak{a} \mid |x^\sigma| \le |a_\sigma| \text{ for all } \sigma \in \mathbf{a}\} \neq \{0\}.$$

Since $\alpha(V(a)\cap F^\times) = V(\alpha a)\cap F^\times$ and $|a|_A = |\alpha a|_A$ for $\alpha \in F^\times$, we may assume that $\mathfrak{a}$ is an integral ideal. Then by Corollary 1.2.1, there exists a constant $C > 0$ independent of $\mathfrak{a}$ such that if $|a_\infty|_\infty = \prod_{\sigma\in I}|a^\sigma| \ge CN(\mathfrak{a})$, then there exists $0 \neq \alpha \in \mathfrak{a}$ ($\Leftrightarrow |\alpha_f|_A \le |a_f|_A$) such that $|\alpha^\sigma| \le |a_\sigma|$ (i.e. $|\alpha^\sigma|_\sigma \le |a_\sigma|_\sigma$ for all σ). Since $N(\mathfrak{a}) = |a_f|_A^{-1}$, $|a|_A \ge C$ if and only if $|a_\infty|_A \ge C|a_f|_A^{-1} = CN(\mathfrak{a})$. This shows (6). Now we shall prove the theorem. We already know that F is discrete in F_A (3c). Since $F_A^\times$ has a stronger topology than F_A, the induced topology on $F^\times$ from $F_A^\times$ is stronger than the topology induced from F_A. Since the discrete topology is the strongest, $F^\times$ is discrete in $F_A^\times$. Take an idele c such that $|c|_A \ge C$. Then for arbitrary $a \in F_A^{(1)}$, $|ca^{-1}|_A \ge C$. Thus we can find by (6) an element $\alpha \in F^\times$ such that $\alpha \in a^{-1}cV(1) = V(a^{-1}c)$. That is, $\alpha a \in cV(1)$. Since αa is again in $F_A^{(1)}$, applying the above argument to $(\alpha a)^{-1}$, we can find $\beta \in F^\times$ such that $\beta \in \alpha acV(1)$ or $\beta(\alpha a)^{-1} \in cV(1)$. Thus $\beta = \beta(\alpha a)^{-1}\alpha a \in cV(1)cV(1)$ which is contained in $c^2V(1)$. Since $c^2V(1)$ is compact and $F^\times$ is discrete, $c^2V(1)\cap F^\times$ is compact and discrete and is therefore finite. Writing $c^2V(1)\cap F^\times = \{\beta_1, \ldots, \beta_m\}$, we see that $(\alpha a)^{-1} \in \bigcup_{i=1}^m \beta_i^{-1}cV(1)$ for any $a \in F_A^{(1)}$. Now we put

$$B = cV(1)\cup\bigcup_{i=1}^m \beta_i^{-1}cV(1).$$

Then $\alpha a \in B$ and $(\alpha a)^{-1} \in B$. Since B is a compact subset of F_A, it is easy to see that $B^* = \{x \in B \mid x^{-1} \in B\}$ is a compact set of $F_A^\times$. In fact, for each v, $|x|_v$ for $x \in B^*$ is bounded from above and from below, i.e. $\exists M_v > 0$ such that $|x_v|_v \le M_v$ and $|x|_v \ge M_v^{-1}$ because x and $x^{-1} \in B$. These M_v can be taken to be 1 for almost all v. Thus, we see that $F^\times B^* \supset F_A^{(1)}$ and B^* is a compact set of $F_A^\times$. Thus $F_A^{(1)}/F^\times$ is compact.

Corollary 1. *Let I be the group of all fractional ideals of F and $\mathcal{P}$ be the subgroup of principal ideals. Then we have*

$$I/\mathcal{P} \cong F_A^\times/F^\times\hat{O}^\times F_\infty^\times \cong F_A^{(1)}/F_A^{(1)}\cap F^\times\hat{O}^\times F_\infty^\times$$

which is a finite group.

Proof. To any idele a, we have associated an ideal $a\mathcal{O} = a\hat{\mathcal{O}} \cap F$. This correspondence induces a surjective homomorphism of groups $\rho : F_A{}^\times \to I$. We see easily that $\rho^{-1}(\mathcal{P}) = F^\times \hat{\mathcal{O}}^\times F_\infty^\times$. This shows the first isomorphism. Since $F_A{}^\times = F_A^{(1)} F^\times \hat{\mathcal{O}}^\times F_\infty^\times$ by definition, we have the second isomorphism. Since $F^\times \hat{\mathcal{O}}^\times F_\infty^\times$ is an open subgroup of $F_A{}^\times$, the middle term is a discrete group. Since $F_A^{(1)}$ is a compact group, the last term is a compact group. Thus $I/\mathcal{P}$ is a discrete compact group and hence is finite. This gives another proof of the finiteness of the ideal classes.

Corollary 2 (Dirichlet-Hasse). *Let* S *be a finite set of places. Let* $U(S) = \{x \in F_A{}^\times \mid |x|_v = 1 \text{ for all } v \notin S\}$ *and* $\mathcal{O}(S)^\times = U(S) \cap F^\times$. *Then if* S *contains* **a**, *i.e.* S *contains all infinite places, then* $\mathcal{O}(S)^\times \cong \mu(F) \times \mathbf{Z}^{s-1}$ *for* $s = \#(S)$, *where* $\mu(F)$ *is the group of roots of unity in* F, *and* **Z** *is considered as an additive group.*

Note that $\mathcal{O}(S_\infty)^\times = \mathcal{O}^\times$ and hence the above corollary includes Dirichlet's theorem about units as a special case.

Proof. Consider the group homomorphism

$$\theta : F_A{}^\times \ni a \mapsto (\log |x|_v)_{v \in S} \in \mathbf{Z}^{s-r} \times \mathbf{R}^r,$$

where r is the number of infinite places and we have normalized *log* at each place so that the above map has values in **Z** at the finite places. Then $\mathrm{Ker}(\theta) = U(\varnothing)$. Thus $U(S)/U(\varnothing) \cong \mathbf{Z}^{s-r} \times \mathbf{R}^r$. Since for the set of infinite places S_∞, $U(S_\infty) F_A^{(1)} = F_A{}^\times$, we see that

$$U(S)/F_A^{(1)} \cap U(S) \cong F_A{}^\times / F_A^{(1)} \cong \mathbf{R}.$$

Thus $F_A^{(1)} \cap U(S)/U(\varnothing) \cong \mathbf{Z}^{s-r} \times \mathbf{R}^{r-1}$. On the other hand,

$$F_A^{(1)} \cap U(S)/\mathcal{O}(S)^\times U(\varnothing) \cong F_A^{(1)} \cap F^\times U(S)/F^\times U(\varnothing)$$

is compact but $F^\times U(S)/F^\times U(\varnothing) \cong \mathcal{O}(S)^\times / \mathcal{O}(\varnothing)^\times$ is discrete. Thus

$$F_A^{(1)} \cap U(S)/\mathcal{O}(S)^\times U(\varnothing) \cong (\mathbf{R}/\mathbf{Z})^{r-1} \times G$$

for a finite group G and $\mathcal{O}(S)^\times/\mathcal{O}(\varnothing)^\times \cong \mathbf{Z}^{s-1}$. By Lemma 1.2.3, we see that $\mathcal{O}(\varnothing)^\times = \mu(F)$. This shows the result.

§8.2. Hecke characters as continuous idele characters

In this section, we show that each ideal Hecke character λ uniquely induces a continuous character of $F_A{}^\times/F^\times$ such that $\lambda(x) = \lambda(x\mathcal{O})$ if $x_c = 1$ for the conductor c of λ. Here $x_c = (x_p)_{p\supset c}$. Let F be a number field and I be the set of all embeddings of F into $\overline{\mathbf{Q}}$. Let $\mathcal{O}$ be the integer ring of F and m be a non-trivial ideal of $\mathcal{O}$. Write $I(m)$ for the group of all fractional ideals of F prime to m. Let F_v be the completion of F at v and $\mathcal{O}_v$ (resp. m_v) be the closure of $\mathcal{O}$ (resp. m) in F_v. (We use the symbol p_v to indicate the prime ideal of $\mathcal{O}$ corresponding to v and also its closure in $\mathcal{O}_v$ if v is a finite place). We define $U_v(m) = \{\alpha \in \mathcal{O}_v \mid \alpha \equiv 1 \bmod m_v\}$. Thus if $m_v = p_v{}^e$, then $U_v(m) = \{\alpha \in \mathcal{O}_v \mid |\alpha-1|_v \le N(p)^{-e}\}$, a closed disk of radius $N(p)^{-e}$ centered at 1, and $U_v(m) = \mathcal{O}_v{}^\times$ if p_v is prime to m. We define

$$U(m) = \prod_{v \text{ finite}} U_v(m) \text{ and } F_\infty = F\otimes_{\mathbf{Q}}\mathbf{R} = \mathbf{R}^{a(R)}\times\mathbf{C}^{a(C)},$$

$$F_{\infty+} = \{x = (x_v) \in F_\infty^\times \mid x_v > 0 \text{ if } v \text{ is real}\},$$

$$P(m) = F^\times\cap\{x \in F_A{}^\times \mid x_p \in U_v(m) \text{ if } p \mid m \text{ and } x_\infty \in F_{\infty+}\}$$
$$= \{\alpha \in F^\times \mid \alpha \in U_v(m) \text{ if } p_v \text{ divides } m \text{ and } \alpha^\sigma > 0 \text{ if } \sigma \text{ is real}\}.$$

Here the intersection is taken in the idele group $F_A{}^\times$. Let $\mathcal{P}(m)$ be the subgroup in $I(m)$ consisting of principal ideals spanned by elements $\alpha \in P(m)$. Then the ray class group $Cl(m)$ modulo m is defined by the following exact sequence:

$$1 \to \mathcal{P}(m) \to I(m) \to Cl(m) \to 1.$$

We have another exact sequence

$$1 \to E(m) \to P(m) \to \mathcal{P}(m) \to 1,$$

where

$$E(m) = F^\times\cap U(m)F_{\infty+}$$
$$= \{\alpha \in \mathcal{O}^\times \mid \alpha \in U_v(m) \text{ if } p_v \text{ divides } m \text{ and } \alpha^\sigma > 0 \text{ if } \sigma \text{ is real}\}.$$

Let $x = (x_v) \in F_A{}^\times$ be an idele such that $x_v = 1$ if either v is infinite or $m_v \ne \mathcal{O}_v$ (i.e. p_v divides m). Then $x_v\mathcal{O}_v = p_v{}^{e(v)}$ and $e(v) = e(x_v) = 0$ for almost all v including those v appearing in m. Then we defined a fractional ideal $x\mathcal{O}$ in F by $x\mathcal{O} = \prod_v p_v{}^{e(v)}$. This gives a group homomorphism of

$$F_A(m) = \{x \in F_A^\times \mid x_v = 1 \text{ if either } v \text{ is infinite or } m_v \neq O_v\}$$

into $I(m)$.

Lemma 1. *We have the following two exact sequences:*

(1) $$1 \to F^\times U(m)F_{\infty+} \to F_A^\times \to \mathrm{Cl}(m) \to 1,$$

(2) $$1 \to U(m) \cap F_A(m) \to F_A(m) \to I(m) \to 1.$$

Proof. We first prove the exactness of the second sequence. The projection map is given by $x \mapsto xO$. If $a = \prod_v p_v^{e(v)}$ is an element of $I(m)$, then $e(v) = 0$ if p_v divides m. Since O_v is a valuation ring, every ideal is principal, and hence we have $p_v^{e(v)} = x_v O_v$ for some $x_v \in F_v^\times$. We define x_v as above if v is finite and p_v is prime to m. We simply put $x_v = 1$ if either v is infinite or p_v divides m. Then $a = xO$ and thus the map $F_A(m) \to I(m)$ is surjective. If $xO = O$, then $e(x_v) = 0$ for all v and hence $x \in U(O)$. Since $x_v = 1$ if either v is infinite or p_v divides m by the definition of $F_A(m)$, we see that $x \in U(m) \cap F_A(m)$ if $xO = O$. This shows the exactness of the second sequence. Since $uxO = xO$ for $u \in U(m)F_{\infty+}$, we also know the exactness of

(3) $$1 \to U(m)F_{\infty+} \to U(m)F_A(m)F_{\infty+} \to I(m) \to 1.$$

By definition, we have

$$U(m)F_A(m)F_{\infty+} = \{x \in F_A^\times \mid x_p \in U_v(m) \text{ if } p \mid m \text{ and } x_\infty \in F_{\infty+}\},$$

and hence $U(m)F_A(m)F_{\infty+} \cap F^\times = P(m)$. Thus we see

$$\mathrm{Cl}(m) = I(m)/\mathcal{P}(m) = U(m)F_A(m)F_{\infty+}/U(m)F_{\infty+}P(m),$$

because $\mathcal{P}(m) = P(m)/E(m)$ and $E(m)$ is contained in $U(m)F_{\infty+}$. By definition, $F^\times$ is dense in $F_m^\times = \prod_{p \mid m} F_p^\times$. Thus, for each idele $x \in F_A^\times$, there exists $\alpha \in F^\times$ such that $(\alpha^{-1}x)_m \in \prod_p O_p^\times$. That is, $\alpha^{-1}xO$ is prime to m. Thus we can find $y \in U(m)F_A(m)F_{\infty+}$ such that $\alpha^{-1}xO = yO$. That is, $\alpha^{-1}xy^{-1} \in U(O)F_{\infty+}$. Since

$$U(O)/U(m) = \prod_{p_v \mid m}(O_v^\times/U_v(m)) \cong \prod_{p_v \mid m}(O_v/m_v)^\times \cong (O/m)^\times,$$

we can find $\gamma \in O$ such that $\gamma \equiv \alpha^{-1}xy^{-1} \bmod U(m)$, and hence $x \in \gamma\alpha y U(m)$. Therefore $F_A^\times = F^\times U(m)F_A(m)F_{\infty+}$. Since

$$U(m)F_A(m)F_{\infty+} \cap F^\times = P(m),$$

we see that

$$F_A^\times/F^\times U(m)F_{\infty+} \cong F^\times U(m)F_A(m)F_{\infty+}/F^\times U(m)F_{\infty+}$$
$$\cong U(m)F_A(m)F_{\infty+}/\{F^\times \cap F_A(m)U(m)F_{\infty+}\}U(m)F_{\infty+} \cong \mathrm{Cl}(m).$$

This shows the exactness of the first sequence.

Let λ^* be a Hecke character modulo m; that is, λ^* is a character of $I(m)$ such that $\lambda^*((\alpha)) = \alpha^\xi$ if $\alpha \in P(m)$, where $\xi = \sum_\sigma \xi_\sigma \sigma \in \mathbf{Z}[I]$ and $\alpha^\xi = \prod_\sigma \alpha^{\sigma\xi\sigma}$ for $\alpha \in F^\times$.

Theorem 1 (Weil). *There exists a unique continuous character* $\lambda : F_A^\times/F^\times U(m) \to \mathbf{C}^\times$ *such that* $\lambda(x) = \lambda^*(xO)$ *if* $x \in F_A(m)$ *and* $\lambda(x_\infty) = x_\infty^{-\xi} = \prod_\sigma x^{-\sigma\xi\sigma}$ *if* $x_\infty \in F_{\infty+}$, *where* $x^\sigma = x_v$ *and* $x^{\sigma c} = \bar{x}_v$ *for* $\sigma = \sigma_v$ *and complex conjugation* c.

Proof. By the exact sequence (3), we know that

$$I(m) \cong U(m)F_A(m)F_{\infty+}/U(m)F_{\infty+} = U(m)F_A(m)/U(m).$$

Thus we can define a character $\lambda : U(m)F_A(m) \to \mathbf{C}^\times$ by $\lambda(x) = \lambda^*(xO)$ for $x \in U(m)F_A(m)$. We extend this character λ to $U(m)F_A(m)F_{\infty+}$ by $\lambda(x) = \lambda^*(x_f O)x^{-\xi}$ where $x^{-\xi} = \prod_\sigma x^{-\sigma\xi\sigma}$ and x_f is the projection of x to $U(m)F_A(m)$. Here note that $x_f O = xO$. Thus for $\alpha \in P(m) = U(m)F_A(m)F_{\infty+} \cap F^\times$,

$$\lambda(\alpha x) = \lambda^*(\alpha x_f O)(\alpha x)^{-\xi} = \lambda^*((\alpha))\lambda^*(x_f O)\alpha^{-\xi}x^{-\xi} = \lambda^*(x_f O)x^{-\xi} = \lambda(x).$$

Now we extend this character to $F_A^\times = F^\times U(m)F_A(m)F_{\infty+}$ by $\lambda(\gamma x) = \lambda(x)$ if $\gamma \in F^\times$ and $x \in U(m)F_A(m)F_{\infty+}$. This is well defined. Indeed, if $\gamma x = \delta y$ for $x,y \in U(m)F_A(m)F_{\infty+}$ and $\gamma,\delta \in F^\times$, then

$$F \ni \gamma^{-1}\delta = y^{-1}x \in U(m)F_A(m)F_{\infty+} \text{ and } \gamma\delta^{-1} \in P(m).$$

Then $\lambda(\gamma x) = \lambda(x) = \lambda(\gamma^{-1}\delta y) = \lambda(y)$ because $\lambda(\alpha x) = \lambda(x)$ if $\alpha \in P(m)$. This shows the existence of λ. The uniqueness is obvious because $F_A^\times = F^\times U(m)F_A(m)F_{\infty+}$.

Exercise 1. Show the continuity of λ as above. (A sequence $x_n \in F_A^\times$ converges to x if and only if for any ideal a of O and $\varepsilon > 0$, there exists a positive number M such that if $n > M$ and $m > M$, then $x_n - x_m \in U(a)F_{\infty+}$ and $|x_n - x_m|_v < \varepsilon$ for all infinite v.)

Exercise 2. Show that if $\xi = 0$, then λ^* is a character of $\mathrm{Cl}(m)$ and λ is just the pullback of $\lambda^* : \mathrm{Cl}(m) \to \mathbf{C}^\times$ by the isomorphism

$$F_A{}^\times/F^\times U(m)F_{\infty+} \cong \mathrm{Cl}(m) \text{ given in Lemma 1.}$$

Exercise 3. Let λ be as in the theorem.
(i) Show that $\lambda(x)$ is contained in a finite extension K of F for all $x \in F_A(m)$.
(ii) Enlarging K if necessary, we suppose that K contains all conjugates of F over $\mathbf{Q}$. Fix one finite place v of K and write p (resp. $|\ |_v$) for its residual characteristic (resp. the v-adic absolute value on K). Then show that every place w of F over p is given in such a way that $|x|_w = |x^\sigma|_v$ for some $\sigma \in I$. Write this place as $w(\sigma)$.
(iii) If $w = w(\sigma)$, then $\sigma : F \to K$ extends to $\sigma : F_w \to K_v$ by continuity. Define for $x \in F_p{}^\times = (F \otimes_{\mathbf{Q}} \mathbf{Q}_p)^\times = \prod_{w|p} F_w{}^\times$, $x^\xi = \prod_\sigma x^{-\sigma\xi\sigma}$ where $x^\sigma = (x_{w(\sigma)})^\sigma$. Then show that there is a unique continuous character $\lambda_p : F_A{}^\times/F^\times U(m)F_{\infty+} \to K_v$ such that $\lambda_p(x) = \lambda^*(xO)$ if $x \in F_A(mp)$ and $\lambda_p(x_p) = \lambda(x_p)x_p{}^{-\xi}$ for all $x_p \in F_p{}^\times$.

Now for a given character $\lambda : F_A{}^\times/F^\times U(m)F_{\infty+} \to \mathbf{C}^\times$ such that $\lambda(x_\infty) = x_\infty{}^{-\xi}$, we can recover a Hecke character λ^* by putting $\lambda^*(xO) = \lambda(x)$ for $x \in F_A(m)$. In fact, if $xO = yO$ for x and y in $F_A(m)$, then $xy^{-1} \in U(m)$ and hence $\lambda(xy^{-1}) = 1$, that is $\lambda^*(xO) = \lambda^*(yO)$. If $\alpha \in P(m)$, then $\lambda^*((\alpha)) = \lambda(\alpha^m)$ for the projection α^m of α to $F_A(m)$. On the other hand, the projection α_m of α to $\prod_{v|m} F_v$ is contained in $U(m)$ because $U(m)F_A(m)F_{\infty+} \cap F^\times = P(m)$. Thus $\lambda(\alpha_m) = 1$. On the other hand, $\lambda(\alpha_\infty) = \alpha^{-\xi}$. Since λ is trivial on $F^\times$, we see $1 = \lambda(\alpha) = \lambda(\alpha_m)\lambda(\alpha^m)\lambda(\alpha_\infty) = \lambda^*((\alpha))\alpha^{-\xi}$ and hence $\lambda^*((\alpha)) = \alpha^\xi$ if $\alpha \in P(m)$. Thus the correspondence $\lambda \leftrightarrow \lambda^*$ is bijective for a given infinity type ξ and for a given defining ideal m; that is, we have

Corollary 1. *The correspondence of Hecke characters:* $\lambda \leftrightarrow \lambda^*$ *is bijective for a given ideal* m *and the infinity type* ξ. (The same statement is true for the p-adic version of Hecke character λ_p given in Exercise 3 (iii).)

Hereafter we identify ideal characters and idele characters and study continuous characters $\lambda : F_A{}^\times/F^\times U(m) \to \mathbf{C}^\times$ with $\lambda(x_\infty) = x_\infty{}^{-\xi}$ for $\xi \in \mathbf{Z}[I]$ instead of ideal characters.

Exercise 4. Let m and n be two ideals. Show that $U(m)U(n) = U(m+n)$.

For a given Hecke character λ as above, if λ is trivial on $U(m)$ and $U(n)$, then by Exercise 4, λ is trivial on $U(m+n)$. Thus there exists a largest ideal c such that λ is trivial on $U(c)$. This ideal c is called the conductor of λ.

We now study additive characters of F_A. We start with the simplest case of $\mathbf{A}$. Pick a prime p. Considering the p-fraction part $[z]_p$ of $z \in \mathbf{Z}_p$, we define the standard additive character

$$(4) \quad e_p : \mathbf{Q}_p \to \mathbf{T} = \{z \in \mathbf{C} \mid |z| = 1\} \text{ by } e_p(z) = \exp(-2\pi\sqrt{-1}\,[z]_p).$$

For any finite idele $x \in \mathbf{A}_f$, we define $e_f(x) = \prod_p e_p(x_p) = \exp(-2\pi\sqrt{-1}\,\Sigma_p[x_p]_p)$. This is well defined additive character since for almost all p $x_p \in \mathbf{Z}_p$ and hence $e_p(x_p) = 1$. We define $e_\infty(x_\infty) = \exp(2\pi\sqrt{-1}\,x_\infty)$. Thus we have an additive character $e : \mathbf{A} \to \mathbf{C}$ given by $e(x) = e_f(x_f)e(x_\infty)$. If α is a rational number, then

$$\alpha - \textstyle\sum_p [\alpha]_p \in \hat{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}.$$

Therefore

$$e(\alpha) = \exp(-2\pi\sqrt{-1}\,\Sigma_p[\alpha]_p)\exp(2\pi\sqrt{-1}\,\alpha) = \exp(2\pi\sqrt{-1}\,(\alpha - \Sigma_p[\alpha]_p)) = 1.$$

Namely e is trivial on $\mathbf{Q}$ and hence is a non-trivial additive character of $\mathbf{A}/\mathbf{Q}$.

Theorem 2. *For any number field* F, *there exists a non-trivial additive character*

$$e = e_F : F_A/F \to \mathbf{T}.$$

Proof. We have explicitly constructed $e = e_Q$ when $F = \mathbf{Q}$. For a general number field F, we simply define e_F by $e_F(x) = e_Q(\mathrm{Tr}_{F/Q}(x))$. Since the trace map sends elements in F onto $\mathbf{Q}$, e_F is a non-trivial additive character of F_A/F.

§8.3. Self-duality of local fields

We fix a place v of F and consider the completion $K = F_v$. Let $\mathbf{T} = \{z \in \mathbf{C} \mid |z| = 1\}$, which is a multiplicative group. We want to show that the group of continuous additive characters $\mathrm{Hom}_{\mathrm{conti}}(K,\mathbf{T})$ of K is canonically isomorphic to K. We start proving this first assuming $K = \mathbf{R}$. If $\alpha : \mathbf{R} \to \mathbf{T}$ is a continuous homomorphism, we consider its kernel $L = \mathrm{Ker}(\alpha)$, which is a closed subgroup of $\mathbf{R}$. Suppose that it has an accumulation point x. Then x itself belongs to L, and we can pick $y \in L$ arbitrarily near to 0 but not equal to 0. In other words, $z = y - x$ is arbitrarily near to 0 but not equal to 0. Then $\mathbf{Z}z$ is a subgroup of L whose adjacent elements have distance $|z|$. Since we can make $|z| \to 0$ keeping z in L, we know L is dense in $\mathbf{R}$. Since L is closed, $L = \mathbf{R}$ and α is the zero map. Thus for non-trivial α, L is a discrete subgroup of $\mathbf{R}$. Let z be the element in $L - \{0\}$ with the minimum distance to 0. Then by the euclidean algorithm, for each $x \in L$, we can find $q \in \mathbf{Z}$ so that

$x \in [qz,(q+1)z)$. Then $x-qz \in L$ has absolute value smaller than z, and hence by the minimality of the distance between z and 0, we know that $x = qz$. Namely $L = \mathbf{Z}z$. Since the homomorphism $\varphi : x \mapsto \exp(2\pi\sqrt{-1}\,z^{-1}x)$ has the same kernel as α, there is a unique automorphism $\beta : \mathbf{T} \cong \mathbf{T}$ such that $\alpha = \beta\circ\varphi$. First we fix the lifting $\iota : \mathbf{T}-\{-1\} \to (-\frac{1}{2},\frac{1}{2})$ by $\iota(\exp(2\pi\sqrt{-1}\,x)) = x$ for x with $|x| < \frac{1}{2}$. Since β is an automorphism, β sends a small neighborhood U of 0 onto another neighborhood U' of 0. We take a still smaller neighborhood W in U so that $W+W \subset U$. Thus $\beta'(x) = \iota(\beta(\exp(2\pi\sqrt{-1}\,x)))$ is a well defined additive map on $W_0 = \iota(W)$, which is a small neighborhood of 0 in $\mathbf{R}$. Since any additive map on $W_0\cap\mathbf{Q}$ is induced by a linear map $x \mapsto bx$ for some $b \in \mathbf{R}$, the continuity of β' tells us that β' coincides with $x \mapsto bx$ for some $b \in \mathbf{R}$ in a small neighborhood W_0. Then by the linearity of β, we see that $\beta(\exp(2\pi\sqrt{-1}\,x)) = \exp(2\pi\sqrt{-1}\,bx)$, which is an automorphism of $\mathbf{T}$, and hence $b = \pm 1$. This shows that $\alpha(x) = \exp(\pm 2\pi\sqrt{-1}\,z^{-1}x)$. We have shown the surjectivity of the natural map $\mathbf{R} \ni b \mapsto e_b \in \mathrm{Hom}_{\mathrm{conti}}(\mathbf{R},\mathbf{T})$ given by $e_b(x) = \exp(2\pi\sqrt{-1}\,bx)$. The injectivity of this map is obvious. Thus we have

$$\mathrm{Hom}_{\mathrm{cont}}(\mathbf{R},\mathbf{T}) \cong \mathbf{R} \quad \text{via} \quad e_b \leftrightarrow b.$$

By this, $\mathrm{Hom}_{\mathrm{cont}}(\mathbf{R}^2,\mathbf{T}) \cong \mathbf{R}^2$ and hence $\mathrm{Hom}_{\mathrm{cont}}(\mathbf{C},\mathbf{T}) \cong \mathbf{C}$. We can check that this isomorphism is induced by $e_b \leftrightarrow b$ for e_b given by $e_b(x) = \exp(2\pi\sqrt{-1}\,\mathrm{Tr}_{\mathbf{C}/\mathbf{R}}(bx))$. We now extend this result to any finite place v. For that, we recall the duality theory of locally compact groups. Let G be a locally compact abelian group. We consider its dual group $G^* = \mathrm{Hom}_{\mathrm{cont}}(G,\mathbf{T})$ and on it we put the topology of uniform convergence on every compact subset of G. Thus a sequence of characters $\alpha_n : G \to \mathbf{T}$ is convergent to a character α if α_n converges to α uniformly on any compact subset X of G. Let $\mathbf{e} : K \to \mathbf{T}$ be the additive character defined in the previous section, i.e.

$$\mathbf{e}(x) = \exp(-2\pi\sqrt{-1}\,[\mathrm{Tr}_{K/\mathbf{Q}_p}(x)]) \text{ if the residual characteristic of } v \text{ is } p$$

and

$$\mathbf{e}(x) = \exp(2\pi\sqrt{-1}\,[\mathrm{Tr}_{K/\mathbf{R}}(x)]) \text{ if } v \text{ is infinite,}$$

where $[x]$ is the p-fractional part of x. Then we can define a pairing $(\ ,\ ) : K \times K \to \mathbf{T}$ by $(x,y) = \mathbf{e}(xy)$. Then we want to prove

Proposition 1. *The above pairing induces* $\mathrm{Hom}_{\mathrm{cont}}(K,\mathbf{T}) \cong K$.

Before proving the proposition, we prove a preliminary lemma:

Lemma 1. *Identify* $\mathbf{T}$ *with* $\mathbf{R}/\mathbf{Z}$ *and let* I_k *be the image of the interval* $(-\frac{1}{3k}, \frac{1}{3k})$ *in* $\mathbf{T}$ *for positive integers* k. *If a homomorphism* α *of a group* G *into* $\mathbf{T}$ *satisfies* $I_1 \supset \alpha(G)$, *then* $\alpha = 0$.

There are two consequences of this lemma:

(i) *If* G *has a system of neighborhoods of the identity consisting of (open) subgroups* H, *then any continuous homomorphism* $\alpha : G \to \mathbf{T}$ *becomes trivial on a sufficiently small open subgroup* H.

(ii) *If* G *is compact, then* G^* *is discrete.* In fact, if a continuous character α_n of G converges to α in G^*, then the convergence is uniform on G (because G itself is compact) and α-α_n has values in I_1 on G for sufficiently large n. This means $\alpha_n = \alpha$ and thus G^* is discrete.

We add one more remark:
(iii) *If* G *is discrete, then* G^* *is compact,* because G^* is easily seen to be the closed subspace of compact space $\mathbf{T}^G$, which is the set of all functions of G having values in $\mathbf{T}$.

Proof (Pontryagin). We claim that if $jt \in I_1$ for all $j = 1,2,3,\ldots, k$, then $t \in I_k$. We prove this by induction on k. If $k = 1$, the assertion is trivially true. Suppose that the assertion is true for k-1 and try to prove the case of k. Choose a representative x of t in $(-\frac{1}{3(k-1)}, \frac{1}{3(k-1)})$. If x is already in $(-\frac{1}{3k}, \frac{1}{3k})$, there is nothing to prove. Thus we may suppose that $|x| \in [\frac{1}{3k}, \frac{1}{3(k-1)})$. Then $|kx| \in [\frac{1}{3}, \frac{k}{3(k-1)})$. This interval is inside $[0,1)$ and hence $kt \in I_1$ means that $kx \in (-\frac{1}{3}, \frac{1}{3})$ and hence $x \in (-\frac{1}{3k}, \frac{1}{3k})$, which means $t \in I_k$. Now let us prove the lemma. If $\alpha(G)$ is contained in I_1, then $\alpha(kg) = k\alpha(g) \in I_1$ for any positive integer k and any $g \in G$. Thus $I_k \supset \alpha(G)$ for all k, which means that $\alpha(G) = 0$ because $\bigcap_k I_k = \{0\}$.

Proof of Proposition 1. We may suppose that v is a finite place over a rational prime p. First assume that $K = \mathbf{Q}_p$. If $\phi \in \mathrm{Hom}_{\mathrm{cont}}(\mathbf{Q}_p, \mathbf{T})$, then for a sufficiently small neighborhood V of 0 in $\mathbf{Q}_p$, $I_1 \supset \phi(V)$ by continuity of ϕ. We can take the subgroup $p^r\mathbf{Z}_p$ as V. Thus $I_1 \supset \phi(p^r\mathbf{Z}_p)$ and hence by the lemma, $\phi(p^r\mathbf{Z}_p) = 0$. Since for any $x \in \mathbf{Q}_p$, we can find a sufficiently large exponent k such that $p^k x \in p^r\mathbf{Z}_p$, we see $p^k\phi(x) = \phi(p^k x) = 0$. Thus identifying $\mathbf{T}$ with $\mathbf{R}/\mathbf{Z}$ via $x \mapsto \exp(2\pi\sqrt{-1}\,x)$, the value of continuous character is contained in the image of fractions whose denominator is a p-power, i.e. $\mathbf{T}_p = \mathbf{Q}_p/\mathbf{Z}_p \supset \phi(\mathbf{Q}_p)$

(see (1.1)). Thus what we need to show is $\mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p,\mathbf{T}_p) \cong \mathbf{Q}_p$ under the pairing $(x,y) = xy \bmod \mathbf{Z}_p$, because any continuous homomorphism $\phi : \mathbf{Q}_p \to \mathbf{T}_p$ is $\mathbf{Z}_p$-linear. Thus $\mathbf{Q}_p$ is sent into $\mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p,\mathbf{T}_p)$ via $x \mapsto \phi_x$ for $\phi_x(y) = (xy \bmod \mathbf{Z}_p)$. Since $\mathbf{T}_p$ is divisible (i.e. for any $y \in \mathbf{T}_p$, we can find $x \in \mathbf{T}_p$ such that $px = y$), applying the functor $\mathrm{Hom}_{\mathbf{Z}_p}(*,\mathbf{T}_p)$, we have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{Z}_p & \longrightarrow & \mathbf{Q}_p & \longrightarrow & \mathbf{T}_p & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \to & \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{T}_p,\mathbf{T}_p) & \to & \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p,\mathbf{T}_p) & \underset{\delta}{\to} & \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Z}_p,\mathbf{T}_p) & \to & 0, \end{array}$$

where both rows are exact ((1.1.1a)), α takes $z \in \mathbf{Z}_p$ to multiplication by z on $\mathbf{T}_p = \mathbf{Q}_p/\mathbf{Z}_p$, $\beta(x) = \phi_x$ and γ takes $t \in \mathbf{T}_p$ to the unique homomorphism ϕ such that $\phi(1) = t$. The surjectivity of δ can be proven as follows. If $\phi : \mathbf{Z}_p \to \mathbf{T}_p$ is a $\mathbf{Z}_p$-linear map, then we can extend it to $p^{-r}\mathbf{Z}_p$ by putting $\phi(p^{-r}) = x_r$ for x_r in $\mathbf{T}_p$ such that $p^r x_r = \phi(1)$. Thus ϕ is extensible to $p^{-r}\mathbf{Z}_p$ for any r and hence extensible to $\mathbf{Q}_p$. By definition, γ is an isomorphism. Thus we only need to show that α is an isomorphism in order to show that β is an isomorphism. If $\alpha(x) = 0$, then multiplication of x on $p^{-r}\mathbf{Z}_p/\mathbf{Z}_p \cong \mathbf{Z}_p/p^r\mathbf{Z}_p$ is zero and hence x is divisible by p^r for arbitrary r. This shows that $x = 0$ and hence α is injective. If $\phi : \mathbf{T}_p \to \mathbf{T}_p$ is a $\mathbf{Z}_p$-linear map, then ϕ induces a map $\phi_r : p^{-r}\mathbf{Z}_p/\mathbf{Z}_p \to p^{-r}\mathbf{Z}_p/\mathbf{Z}_p$. Thus $\phi_n \in \mathrm{End}(\mathbf{Z}/p^r\mathbf{Z}) \cong \mathbf{Z}/p^r\mathbf{Z}$. Since ϕ_r induces ϕ_s if $r > s$, as an element of $\mathbf{Z}/p^r\mathbf{Z}$, $\phi_r \equiv \phi_s \bmod p^s$. Picking an integer x_n such that $x_n \equiv \phi_n \bmod p^n$ for each n, the sequence $\{x_n\}$ converges to $x \in \mathbf{Z}_p$ because $|x_r - x_s|_p \le p^{-s}$ if $r > s$. By definition $\alpha(x) = \phi$. Thus α is surjective and hence the assertion follows when $K = \mathbf{Q}_p$. By this we know $\mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p{}^r,\mathbf{T}_p) \cong \mathbf{Q}_p{}^r$ via the pairing $(x,y) = \sum_{j=1}^r x_j y_j \bmod \mathbf{Z}_p$. Now we treat the general case. Identify K with $\mathbf{Q}_p{}^r$ by choosing a basis $\{v_1,\ldots,v_r\}$ over $\mathbf{Q}_p$. We can also identify the $\mathbf{Q}_p$-dual vector space K^* of K with K via the pairing $\langle x,y\rangle = \mathrm{Tr}_{K/\mathbf{Q}_p}(xy)$. Thus by choosing the dual basis $v_j{}^*$ of K (i.e. $\langle v_k,v_j{}^*\rangle = \delta_{kj}$), we can identify K with $\mathbf{Q}_p{}^r$. Then by the above argument, we know that $\mathrm{Hom}_{\mathrm{cont}}(K,\mathbf{T}_p) \cong K$ via the pairing $(x,y) = \exp(2\pi\sqrt{-1}\,\mathrm{Tr}_{K/\mathbf{Q}_p}(xy))$. This shows the proposition.

Theorem 1. *Define a pairing* $(\ ,\ ) : F_A \times F_A \to \mathbf{T}$ *by* $(x,y) = \mathbf{e}(xy)$ *for the adelic standard additive character* $\mathbf{e} : F_A/F \to \mathbf{T}$. *Then this pairing induces an isomorphism* $F_A \cong \mathrm{Hom}_{\mathrm{cont}}(F_A,\mathbf{T})$.

Proof. Since $F_A = F_{A_f} \times F_\infty$ and F_∞ is a product of finitely many copies of $\mathbf{R}$ and $\mathbf{C}$, we only need to prove the self-duality for F_{A_f}. Since $n\hat{O}$ for positive integers n gives a system of neighborhoods of 0 in F_{A_f}, for any continuous homomorphism $\phi : F_{A_f} \to \mathbf{T} = \mathbf{R}/\mathbf{Z}$, we can find n so that $\phi(n\hat{O}) = 0$ by using Lemma 1. Thus we know that $\mathbf{Q}/\mathbf{Z} \supset \phi(F_{A_f})$. We first assume that $F = \mathbf{Q}$. As seen in (1.1) and (1.3b), $\mathbf{e}_f : A_f/\mathbf{Z}_f \cong \oplus_p(\mathbf{Q}_p/\mathbf{Z}_p) \cong \mathbf{Q}/\mathbf{Z}$. Using the commutative diagram analogous to the one in the proof of Proposition 1,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{\mathbf{Z}} & \longrightarrow & A_f & \longrightarrow & \oplus_p \mathbf{T}_p & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \to & \mathrm{Hom}(\mathbf{Q}/\mathbf{Z}, \mathbf{Q}/\mathbf{Z}) & \to & \mathrm{Hom}(A_f, \mathbf{Q}/\mathbf{Z}) & \underset{\delta}{\to} & \mathrm{Hom}(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) & \to & 0, \end{array}$$

we know that $\mathrm{Hom}(A_f, \mathbf{Q}/\mathbf{Z}) \cong A_f$. This shows the assertion for $\mathbf{Q}$. Now we can take a basis v_j of O over $\mathbf{Z}$; then $F \cong \mathbf{Q}^d$ and $O \cong \mathbf{Z}^d$ $(d = [F:\mathbf{Q}])$ via this basis. Then we see that $F_{A_f} \cong A_f^d$. The character $\mathbf{e}$ takes, by definition, F_{A_f} into $\mathbf{Q}/\mathbf{Z}$ (in fact $\mathbf{e} = \mathbf{e}_\mathbf{Q} \circ \mathrm{Tr}$ for the trace map $\mathrm{Tr} : F_{A_f} \to A_f$). Thus we know from the same argument as in the proof of Proposition 1 that $\mathrm{Hom}(F_{A_f}, \mathbf{Q}/\mathbf{Z}) \cong F_{A_f}$ via the pairing induced from $\mathbf{e}$. This finishes the proof.

By Lemma 1 and the above proof of the theorem, for each non-trivial continuous character $\phi : F_v \to \mathbf{T}$ (resp. $\phi : F_A \to \mathbf{T}$), there is a fractional ideal $p_v^{-\delta}$ in F_v (resp. ϑ^{-1} in F) maximal among the ideals a with $\phi(a) = 1$. The inverse of this ideal is called the different of ϕ. If $\mathbf{e}$ is the standard character, then the inverse of the different of $\mathbf{e}$ is the dual lattice of O under the pairing $(x,y) = \mathrm{Tr}_{F/\mathbf{Q}}(xy)$ and hence is the different inverse ϑ^{-1} in the classical sense. If $\phi(x) = \mathbf{e}(ax)$ for all $x \in F_A$, then the different for ϕ is given by $a\vartheta$.

Since the pairing $(\ ,\ )$ on F_A is continuous under the topology on F_A, the isomorphism of Theorem 1 is in fact an isomorphism of topological groups.

Exercise 1. Show that the isomorphism of Proposition 1 is continuous if $F = \mathbf{Q}_p$.

§8.4. Haar measures and the Poisson summation formula

To prove the functional equation for Hecke L-functions of number fields, we need the theory of Fourier transform on a locally compact abelian group G, which we explain now. We assume the following conditions.

(1a) *There is a continuous pairing* $(\ ,\ ) : G \times G \to \mathbf{T} = \{z \in \mathbf{C} \mid |z| = 1\}$

which induces an isomorphism $G \cong \mathrm{Hom}_{\mathrm{cont}}(G,\mathbf{T})$ (on the right-hand side, we put the topology of uniform convergence on all compact subsets of G and this isomorphism has to be an isomorphism of topological groups).

(1b) G *has a cocompact discrete subgroup* Γ. Here the word "cocompact" means that G/Γ is compact.
(1c) *The orthogonal complement* $\Gamma^* = \{x^* \in G \mid (x^*,x) = 1 \text{ for all } x \in \Gamma\}$ *is again a cocompact discrete subgroup of* G.

In fact, the third condition is superfluous and it is known that it follows from (1a,b) (see the remark after Lemma 3.1). In our application, G will be a vector space over $\mathbf{R}$ or the adele ring F_A. Let us check the conditions (1a,b,c) for a real vector space $V \cong \mathbf{R}^r$. Let $S : V \times V \to \mathbf{R}$ be any non-degenerate inner product and L be a lattice of V. Then L is a discrete subgroup of V and by choosing a basis $\{v_1,\ldots,v_r\}$ of L over $\mathbf{Z}$, we can identify L with $\mathbf{Z}^r$. Since the v_j's form a basis of V over $\mathbf{R}$, we can identify V with $\mathbf{R}^r$ via this basis. Then $V/L \cong (\mathbf{R}/\mathbf{Z})^r$ is compact. Now we define $(\ ,\ ) : V \times V \to S$ by $(x,y) = \exp(2\pi\sqrt{-1}\,S(x,y))$. Then

$$\begin{aligned} L^* &= \{x^* \in V \mid (x^*,x) = 1 \quad \text{for all} \quad x \in L\} \\ &= \{x^* \in V \mid S(x^*,x) \in \mathbf{Z} \quad \text{for all} \quad x \in L\}. \end{aligned}$$

Then L^* is the dual lattice generated by the dual basis v_i^* such that $S(v_i^*,v_j) = \delta_{ij}$. Thus L^* is again a lattice and is discrete and cocompact. When $G = F_A$, we can take F as a discrete subgroup of F_A.

On the group G, there exists a Haar measure $d\mu$ with values in $\mathbf{R}$, which satisfies the following conditions:

(2a) μ *is defined on a complete additive class containing all compact subsets of* G (e.g. a union of countably many compact subsets is measurable);
(2b) $0 \le \mu(K) < +\infty$ *for all compact subsets* K *of* G ($\mu(K) > 0$ if the interior of K is not empty),

$$\mu(U) = \mathrm{Sup}_{U \supset K \text{ compact}} \mu(U) \textit{ for all open sets } U \textit{ and}$$
$$\mu(X) = \mathrm{Inf}_{U \supset X,\, U \text{ open}} \mu(U) \textit{ for all measurable subsets } X;$$

(2c) $\mu(x+X) = \mu(X)$ *for all measurable subsets* X *and* $x \in G$.

Under the conditions (2a,b,c), the Haar measure is unique up to a constant multiple. The uniqueness is intuitively obvious because if K is a disjoint union of K' and $x+K'$, then $\mu(K') = \mu(K)/2$. In this way, if one fixes a compact neighborhood of 1 with positive measure, by subdividing it, the measures of all compact subsets are uniquely determined. The condition (2c) implies the equality

(3) $$\int_G f(x+y)d\mu(x) = \int_G f(x)d\mu(x)$$

for any integrable function f with respect to μ. When G is a real vector space, the Haar measure on V is a constant multiple of the Lebesgue measure induced by the identification $G \cong \mathbf{R}^r$.

Now we fix the Haar measure μ on G and consider the Hilbert space $L_2(G/\Gamma)$ of L_2-functions on G/Γ. In fact, by taking the fundamental domain K of Γ in G so that $\overline{K}$ is compact and the complement of $\overline{K}$ is open, the measure μ induces a measure on K, which gives a Haar measure on G/Γ. By multiplying by a suitable constant, we may assume that $\int_{G/\Gamma} d\mu(x) = 1$. The L_2 space $L_2(G/\Gamma)$ is the space of functions $f : G/\Gamma \to \mathbf{C}$ which are square integrable; i.e, $\int_{G/\Gamma} |f(x)|^2 d\mu(x) < +\infty$. Thus we can define the positive definite hermitian inner product on $L_2(G/\Gamma)$ by

$$\langle f,g\rangle = \int_{G/\Gamma} \overline{f(x)}\, g(x)d\mu(x).$$

For $\gamma^* \in \Gamma^*$, we consider the character $\psi = \psi_{\gamma^*} : G \to \mathbf{T}$ given by $\psi_{\gamma^*}(x) = (\gamma^*,x)$. Then for $\gamma \in \Gamma$, $\psi(x+\gamma) = (\gamma^*,x)(\gamma^*,\gamma) = \psi(x)$ because $(\gamma^*,\gamma) = 1$. Thus ψ is a continuous character of G/Γ. Since G/Γ is compact and ψ is continuous, we know that $\psi \in L_2(G/\Gamma)$. Moreover

$$\langle \psi,\psi\rangle = \int_{G/\Gamma} d\mu(x) = 1.$$

Since $G \cong \mathrm{Hom}_{\mathrm{cont}}(G, \mathbf{T})$, if $\gamma^*,\delta^* \in \Gamma^*$ and $\gamma^* \neq \delta^*$, then for some $y \in G$, $\psi_{\gamma^*}(y) \neq \psi_{\delta^*}(y)$. On the other hand, we consider an operator $T_y : L_2(G/\Gamma) \to L_2(G/\Gamma)$ given by $T_y f(x) = f(y+x)$. Then we see from (3) that

$$\langle T_y f,g\rangle = \int_{G/\Gamma} \overline{f(y+x)}\, g(x)d\mu(x) = \int_{G/\Gamma} \overline{f(x)}\, g(x-y)d\mu(x) = \langle f,T_{-y}g\rangle.$$

This implies

$$\psi_{\gamma^*}(y)^{-1}\langle \psi_{\gamma^*},\psi_{\delta^*}\rangle = \langle T_y\psi_{\gamma^*},\psi_{\delta^*}\rangle = \psi_{\delta^*}(y)^{-1}\langle \psi_{\gamma^*},T_{-y}\psi_{\delta^*}\rangle$$

and hence $\langle \psi_{\gamma^*},\psi_{\delta^*}\rangle = 0$ if $\gamma^* \neq \delta^*$. Moreover it is known (see [P]) that

(4) ψ_{γ^*} for $\gamma^* \in \Gamma^*$ gives an orthonormal basis of $L_2(G/\Gamma)$.

Thus, any $f \in L_2(G/\Gamma)$ is expanded into the L_2-convergent series

$$f = \sum_{\gamma^* \in \Gamma^*} c(\gamma^*)\psi_{\gamma^*} \quad \text{for} \quad c(\gamma^*) = \langle \psi_{\gamma^*},f\rangle.$$

Exercise 1. By applying the functor $\mathrm{Hom}(*, \mathbf{T})$ to the exact sequence of abelian groups $0 \to M \to N \to L \to 0$, we have naturally another sequence

$$(5) \qquad 0 \to \hat{L} \to \hat{N} \to \hat{M} \to 0,$$

where $\hat{M}$ denotes $\mathrm{Hom}(M, \mathbf{T})$ for any abelian group M. Show that the sequence (5) is exact. For the surjectivity of the last arrow: For each $\alpha \in \hat{M}$, consider the set A of pairs (X,ξ) consisting of subgroup X of N and a homomorphism $\xi : X \to \mathbf{T}$ such that $\xi|_\Gamma = \alpha$. Put an order $(X,\xi) > (X',\xi')$ on A when $X \supset X'$ and $\xi|_{X'} = \xi'$. Then by Zorn's lemma, there exists a maximal element (X,ξ) in A. Show that $X = N$ and the image of ξ in $\hat{M}$ is α.

Now we define the Fourier transform for any integrable function f on G by

$$(6) \qquad \mathcal{F}(f)(y) = \mathcal{F}_\Gamma(f)(y) = \int_G f(x)(x,y)d\mu(x).$$

Since $|(x,y)| = 1$, the above integral is always convergent if f is integrable.

Theorem 1 (the Poisson summation formula). *Suppose that*
(i) f *is a continuous function on* G *integrable with respect to* μ,
(ii) $\sum_{\gamma\in\Gamma} f(x+\gamma)$ *and* $\sum_{\gamma^*\in\Gamma^*} \mathcal{F}(f)(x+\gamma^*)$ *are both absolutely and locally uniformly convergent. Then we have*

$$\sum_{\gamma\in\Gamma} f(x+\gamma) = \sum_{\gamma^*\in\Gamma^*} \mathcal{F}(f)(\gamma^*)(-x,\gamma^*).$$

In particular,

$$\sum_{\gamma\in\Gamma} f(\gamma) = \sum_{\gamma^*\in\Gamma^*} \mathcal{F}(f)(\gamma^*).$$

Proof. The function $\Phi(x) = \sum_{\gamma\in\Gamma} f(x+\gamma)$ is invariant under translation by the elements of Γ. Thus we may consider Φ as a function on G/Γ. Since G/Γ is compact, Φ is square integrable. Thus we can expand

$$\Phi(x) = \sum_{\gamma^*\in\Gamma^*} c(\gamma^*)\psi_{\gamma^*}(x) \quad \text{for} \quad c(\gamma^*) = \langle\psi_{\gamma^*},\Phi\rangle.$$

Let K be the fundamental domain of G/Γ we have already chosen. Then

$$\begin{aligned}\langle\psi_{\gamma^*},\Phi\rangle &= \int_{G/\Gamma}(-\gamma^*,x)\Phi(x)d\mu(x) = \int_{G/\Gamma}(-\gamma^*,x)\textstyle\sum_{\gamma\in\Gamma} f(x+\gamma)d\mu(x)\\ &= \textstyle\sum_{\gamma\in\Gamma}\int_{G/\Gamma}(-\gamma^*,x)f(x+\gamma)d\mu(x) = \int_{\cup_\gamma K+\gamma}(-\gamma^*,x)f(x)d\mu(x)\\ &= \int_G(-\gamma^*,x)f(x)d\mu(x) = \mathcal{F}(f)(-\gamma^*).\end{aligned}$$

Thus we have

$$\sum_{\gamma\in\Gamma} f(x+\gamma) = \sum_{\gamma^*\in\Gamma^*} \mathcal{F}(f)(-\gamma^*)(x,\gamma^*) = \sum_{\gamma^*\in\Gamma^*} \mathcal{F}(f)(\gamma^*)(-x,\gamma^*).$$

Since the convergence is locally uniform, the above identity is not only in the L_2-space but the actual identity of the two functions valid everywhere.

§8.5. Adelic Haar measures

Now we want to construct explicitly the Haar measure on F_A and $F_A^\times$. When v is infinite, F_v is $\mathbf{C}$ or $\mathbf{R}$ and thus we have the Lebesgue measure dx on F_v. The Haar measure on the multiplicative group $F_v^\times$ in this case is given by $|x|^{-1}dx$ when v is real and $d\mu_v^\times(z) = |x^2+y^2|^{-1}dxdy$ (writing $z = x+\sqrt{-1}\,y$) when v is complex. Now we treat the case where v is finite. We only need to make explicit the integration of locally constant functions on F_v for finite v under the Haar measure. A function f on a topological group G is called locally constant if for any $x \in G$, there exists an open neighborhood V of x such that f is constant on V. Thus for a given $x \in V$, the set $\{y \in G \mid f(y) = f(x)\}$ is an open set. In particular, any locally constant function is continuous. To know the volume of open compact subsets of the Haar measure on $\mathcal{O}_v$, we may assume that $\mu(\mathcal{O}_v) = 1$. Since $\{p_v^j\}_{j=1,2,\dots}$ gives a system of neighborhoods of 0 and $\mathcal{O}_v = \bigcup_a a+p_v^j$ is a disjoint union of open subsets, where a runs over a representative set for $\mathcal{O}_v/p_v^j$. Thus we must have

$$N(p_v)^j\mu_v(p_v^j) = \#(\mathcal{O}_v/p_v^j)\mu_v(p_v^j) = \sum_a \mu_v(a+p_v^j) = \mu_v(\mathcal{O}_v) = 1.$$

This shows that for any generator ϖ_v of p_v

$$\mu_v(a+p_v^j) = N(p_v)^{-j} = |\varpi_v|_v^j. \tag{1}$$

Of course this formula is valid for all $a \in F_v$ and $i \in \mathbf{Z}$ (not necessarily positive). If $f : F_v \to \mathbf{C}$ is a locally constant function, then as already remarked, the set $f^{-1}(f(x)) = \{y \in F_v \mid f(y) = f(x)\}$ is an open set for a given x. Thus we can write, for $f(x) = c$, $f^{-1}(c) = \bigcup_a(a+p_v^{i(a)})$ as a disjoint union. Then formally

$$\int_{F_v} f(x)d\mu_v(x) = \sum_{c\in f(F_v)} c\mu_v(f^{-1}(c))$$

$$\text{and } \mu_v(f^{-1}(c)) = \sum_a \mu_v(a+p_v^{i(a)}) = \sum_a N(p_v)^{-i(a)}.$$

If the above sum is absolutely convergent, then f is called integrable. In particular, if f is compactly supported, that is, the closure of the set $\{x \in F_v \mid f(x) \neq 0\}$ (which is called the support of f) is compact, then f is integrable. We then have the property (4.2a-c) for this Haar measure. Similarly we can define the multiplicative Haar measure $d\mu^\times$ by

(2) $$\mu_v^\times(a+p_v^j) = 1/(O_v^\times:1+p_v^j) = \begin{cases} 1 & \text{if } j = 0, \\ N(p_v)^{-j+1}(N(p_v)-1)^{-1} & \text{if } j > 0 \end{cases}$$

for $a \in O_v^\times$. Since $a+p_v^j = a(1+p_v^j)$ and the subgroups $\{1+p_v^j\}_{j>0}$ give a system of neighborhoods, the same argument as in the additive case shows the invariance property of $\mu_v^\times$.

Exercise 1. (i) Show that $\{x \in F_v \mid f(x) \neq 0\}$ is closed if f is compactly supported and v is finite.
(ii) Show that for any locally constant function f whose support is in $F_v^\times$,
$$\int_{F_v^\times} f(x)d\mu_v^\times(x) = N(p_v)(N(p_v)-1)^{-1}\int_{F_v} f(x)\,|x|_v^{-1}d\mu_v(x).$$
(Reduce the problem to the formula $\mu_v^\times(a+p_v^i) = (1-N(p_v)^{-1})^{-1}\,|a|_v^{-1}\mu_v(a+p_v^i)$.)
(iii) Show that for any compactly supported locally constant function f on F_v and $a \neq 0$, $\int_{F_v} f(ax)d\mu_v(x) = |a|_v^{-1}\int_{F_v} f(x)d\mu_v(x)$ (use (ii)).

We now define the Haar measure on F_A. For each fractional ideal $\mathfrak{a}$, we write $\hat{\mathfrak{a}}$ for the closure of $\mathfrak{a}$ in F_{A_f}, which coincides with $\prod_{v \text{ finite}} \mathfrak{a}_v$. First, on F_{A_f}, we define the additive measure μ_f and the multiplicative measure $\mu_f^\times$ by

$$\mu(a+\mathfrak{a}) = N(\mathfrak{a})^{-1} \text{ for each fractional ideal } \mathfrak{a} \text{ in } F,$$
$$\mu^\times(aU(\mathfrak{a})) = (U(O):U(\mathfrak{a}))^{-1} = (\#(O/\mathfrak{a})^\times)^{-1} \text{ for each ideal } \mathfrak{a} \text{ in } O.$$

Since $\{U(\mathfrak{a})\}_{\mathfrak{a}}$ (resp. $\{\hat{\mathfrak{a}}\}_{\mathfrak{a}}$) gives a system of neighborhoods on $A_f^\times$ (resp. A_f), we can verify that μ_f and $\mu_f^\times$ are well defined. Let μ_∞ (resp. $\mu_\infty^\times$) be the additive (resp. multiplicative) Haar measure on F_∞ induced by the Lebesgue measure as already defined. Then if a function is of the form $\phi(x) = \phi_f(x_f)\phi_\infty(x_\infty)$ with a locally constant function ϕ_f on F_{A_f} and an integrable function f_∞ on F_∞, then the integration under the Haar measure $\mu = \mu_f \otimes \mu_\infty$ (resp. $\mu^\times = \mu^\times_f \otimes \mu^\times_\infty$) can be computed by

$$\int_{F_A^\times} \phi(x)d\mu^\times(x) = \int_{F_{A_f}^\times} \phi_f(x_f)d\mu_f^\times(x_f) \times \int_{F_\infty^\times} \phi_\infty(x_\infty)d\mu_\infty^\times(x_\infty),$$
$$\int_{F_A^\times} \phi(x)d\mu(x) = \int_{F_{A_f}} \phi_f(x_f)d\mu_f(x_f) \times \int_{F_\infty} \phi_\infty(x_\infty)d\mu_\infty(x_\infty).$$

Exercise 2. Show that $\mu_f = \otimes_{v \text{ finite}}\mu_v$. First show that the problem is reduced to proving $\mu_f(\hat{\mathfrak{a}}) = \prod_{v \text{ finite}}\mu_v(\mathfrak{a}_v)$ for all integral ideals $\mathfrak{a}$ and then show that the infinite product of the right-hand side is in fact a finite product and gives the volume of the left-hand side.

Examples of integrals: *Orthogonality relations* (Lemma 2.3.1): Let χ and λ be continuous characters (with values in $\mathbf{T}$) on $G = \mathcal{O}_v^\times$ or a_v. Let μ be a Haar measure on G. Then

$$\int_G \chi\lambda(x)d\mu(x) = \begin{cases} 0 & \text{if } \chi \neq \lambda^{-1}, \\ \mu(G) & \text{if } \chi = \lambda^{-1}. \end{cases}$$

Proof. Since $\chi\lambda$ is continuous, it becomes trivial on a sufficiently small subgroup H of finite index by Lemma 3.1. Thus we see

$$(3) \qquad \int_G \chi\lambda(x)d\mu(x) = \sum_{x\in G/H}\int_H \chi\lambda(xh)d\mu(xh) = \mathrm{vol}(H)\sum_{x\in G/H}\chi\lambda(x).$$

By Lemma 2.3.1, we see that

$$\sum_{x\in G/H}\chi\lambda(x) = \begin{cases} 0 & \text{if } \chi \neq \lambda^{-1}, \\ (G:H) & \text{if } \chi = \lambda^{-1}. \end{cases}$$

Then the assertion follows from the fact that $\mu(G) = \mu(H)(G:H)$.

Gauss sum. Let χ be a continuous character of $F_v^\times$ and ϕ be a non-trivial additive character of F_v. Let $\varpi^{-r}\mathcal{O}_v = \vartheta_v^{-1}$ be the different inverse of ϕ for a generator ϖ of p_v (i.e. $\varpi^{-r}\mathcal{O}_v$ is the maximal fractional ideal in F_v such that $\phi(\varpi^{-r}\mathcal{O}_v) = 1$) and $\varpi^f\mathcal{O}_v$ be the conductor of χ (i.e. $\varpi^f\mathcal{O}_v$ is the maximal ideal such that $\chi(1+\varpi^f\mathcal{O}_v) = 1$ if χ is non-trivial on $\mathcal{O}_v^\times$ and $m = 0$ if χ is trivial on $\mathcal{O}_v^\times$). When $f > 0$, we consider the integral

$$(4a) \qquad |\varpi^r|_v\chi(\varpi^{r+f})\int_{\varpi^{-r-f}\mathcal{O}_v^\times}\chi\phi(x)d\mu(x).$$

This is a Gauss sum. In fact, by the variable change: $x \mapsto \varpi^{-f-r}x$, we see

$$\begin{aligned} &|\varpi^r|_v\chi(\varpi^{r+f})\int_{\varpi^{-r-f}\mathcal{O}_v^\times}\chi\phi(x)d\mu(x) = \chi(\varpi^{r+f})\,|\pi^{-f}|_v\int_{\mathcal{O}_v^\times}\chi\phi(\varpi^{-f-r}x)d\mu(x) \\ &= |\varpi^{-f}|_v\int_{\mathcal{O}_v^\times}\chi(x)\phi(\varpi^{-f-r}x)d\mu(x) = |\varpi^{-f}|_v\sum_{x \bmod \varpi^f}\chi(x)\int_{x+\varpi^f\mathcal{O}_v}\phi(\varpi^{-r-f}y)d\mu(y) \\ &= |\varpi^{-f}|_v\sum_{x \bmod \varpi^f}\chi(x)\int_{\mathcal{O}_v}\phi(\varpi^{-r-f}(x+\varpi^f y))d\mu(\varpi^f y) = \sum_{x \bmod \varpi^f}\chi(x)\phi(\varpi^{-r-f}x), \end{aligned}$$

which is visibly a Gauss sum. We only integrate $\chi\phi$ on $\varpi^{-f-r}\mathcal{O}_v^\times$ but the same integral on $\varpi^m\mathcal{O}_v^\times$ vanishes if $m \neq -f-r$. In fact, we have

$$(4b) \qquad \int_{\varpi^m\mathcal{O}_v^\times}\chi\phi(x)d\mu(x) = 0 \quad \text{if} \quad m \neq -r-f \quad \text{and} \quad f > 0.$$

Proof. We see that

$$\int_{\varpi^m O_v^\times}\chi\phi(x)d\mu(x) = |\varpi^m|_v\int_{O_v^\times}\chi\phi(\varpi^m x)d\mu(x)$$
$$= \chi(\varpi^m)|\varpi^m|_v\int_{O_v^\times}\chi(x)\phi(\varpi^m x)d\mu(x).$$

First suppose that $m < -r-f$. Then the above integral is equal to

$$\chi(\varpi^m)|\varpi^m|_v\sum_{x \bmod \varpi^f}\chi(x)\int_{x+\varpi^f O_v}\phi(\varpi^m y)d\mu(y).$$

We then compute

$$\int_{\varpi^f O_v}\phi(\varpi^m(x+y))d\mu(y) = |\varpi^f|_v\phi(\varpi^m x)\int_{O_v}\phi(\varpi^{m+f}y)d\mu(y).$$

Since $m+f < -r$, $y \mapsto \phi(\varpi^{m+f}y)$ is a non-trivial additive character. Hence by (3), we see the right-hand side of the above integral vanishes. Thus we have the vanishing of (4b). Now we suppose that $m > -r-f$. Then

$$\int_{O_v^\times}\chi(x)\phi(\varpi^m x)d\mu(x) = \sum_{x \bmod \varpi^{f-1}}\int_{x+\varpi^{f-1}O_v}\chi(y)\phi(\varpi^m y)d\mu(y)$$
$$= \sum_{x \bmod \varpi^{f-1}}\int_{x+\varpi^{f-1}O_v}\chi(x(1+\varpi^{f-1}y))\phi(\varpi^m x(1+\varpi^{f-1}y))d\mu(x(1+\varpi^{f-1}y))$$
$$= \sum_{x \bmod \varpi^{f-1}}|x\varpi^{f-1}|_v\phi(\varpi^m x)\chi(x)\int_{\varpi^{f-1}O_v}\chi(1+\varpi^{f-1}y)d\mu(y).$$

Since $\int_{\varpi^{f-1}O_v}\chi(1+\varpi^{f-1}y)d\mu(y) = \mu(\varpi^f O_v)\sum_{y\in 1+\varpi^{f-1}O_v/1+\varpi^{f-1}O_v}\chi(y)$
$$= \mu(\varpi^f O_v)\int_{1+\varpi^{f-1}O_v}\chi(y)d\mu^\times(y) = 0 \quad \text{by (3)},$$

the vanishing of the integral we wanted follows.

Integrals at ∞. Write I for the set of all embeddings of F into $\mathbf{C}$. We consider the inner product $S : F\times F \to \mathbf{Q}$ given by $\mathrm{Tr}_{F/\mathbf{Q}}(xy)$. This inner product extends to $V = F_\infty$ as a real bilinear form. We identify F_∞ with $\mathbf{R}^{\mathbf{a}(\mathbf{R})}\times\mathbf{C}^{\mathbf{a}(\mathbf{C})}$. Then for each $\alpha \in F$, the image of α in V is given by $(\alpha^\sigma)_{\sigma\in \mathbf{a}(\mathbf{C})\cup\mathbf{a}(\mathbf{R})}$. We consider the function $\psi_y(v) = \exp(-\pi\sum_{\sigma\in I}y_\sigma|v_\sigma|^2)$ for $y_\sigma \in \mathbf{R}_+$ with $y_\sigma = y_{\sigma c}$ for complex conjugation c, where for $\sigma \in \mathbf{a}(\mathbf{C})$, we agree to write $v_{\sigma c}$ for $\bar{v}_\sigma$. Then we see that for any polynomial $P(v)$, $\psi_P(v) = P(v)\psi(v)$ is integrable on V and we have

Lemma 1. *Let* du *be the usual Lebesgue measure on* V. *Then*

(5a) $$\int_{F_\infty}\psi_y(u)\mathbf{e}(\mathrm{Tr}_{F/\mathbf{Q}}(uv))du = 2^{-t}N(y)^{-1/2}\psi_{y^{-1}}(v),$$

where $\mathbf{e}(x) = \exp(2\pi\sqrt{-1}x)$, $t = \#(\Sigma(\mathbf{C}))$ *and* $N(y) = \prod_{\sigma\in I}y_\sigma$. *Moreover let* $0 \le \eta \in \mathbf{Z}[I]$ *such that* $\eta_\sigma = 0$ *or* 1 *for* $\sigma \in \mathbf{a}(\mathbf{R})$ *and* $\eta_\sigma\eta_{\sigma c} = 0$ *for* $\sigma \in \mathbf{a}(\mathbf{C})$. *Then we have*

(5b) $$\int_{F_\infty} u^\eta \psi_y(u) e(\mathrm{Tr}_{F/Q}(uv))du = 2^{-t} N(y)^{-1/2} y^{-\eta} i^{\{\eta\}} v^{\eta c} \psi_{y^{-1}}(v),$$

where $\{\eta\} = \sum_{\sigma\in I}\eta_\sigma \in \mathbf{Z}$.

Proof. Note that $\mathrm{Tr}_{F/Q}(uv) = \sum_{\sigma\in \mathbf{a}(\mathbf{R})} u_\sigma v_\sigma + \sum_{\sigma\in \mathbf{a}(\mathbf{C})}(u_\sigma v_\sigma + \bar{u}_\sigma \bar{v}_\sigma)$. Thus the problem is reduced to the computation of

(5c) $$\int_{-\infty}^{\infty} \exp(-\pi y u^2) e(uv) du \quad \text{and} \quad \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \exp(-2\pi y u\bar{u}) e(uv + \bar{u}\bar{v}) du.$$

The first integral is equal to $\sqrt{y}^{-1}\exp(-\pi x^2/y)$, and the second follows from the first immediately. We obtain the last assertion via the differentiation by $\left(\frac{\partial}{\partial v}\right)^\eta = \prod_{\sigma\in I}\left(\frac{\partial}{\partial v_\sigma}\right)^{\eta_\sigma}$ of the first formula (5a).

Exercise 3. Give a detailed explanation of the computation of the integral (5b,c).

§8.6. Functional equations of Hecke L-functions

In this section, we prove the functional equation for Hecke L-functions via the method of Tate-Iwasawa. We basically follow the treatment in [W1,VII.5]. We first deal with the Fourier transform of standard functions on F_v or F_A. For a finite place v, a function f on F_v is called standard if it is locally constant and compactly supported. For a infinite place v, a function f is called a standard function if

$$f(x) = cx^A \exp(-\pi x^2) \text{ for a constant } c \text{ and } A = 0 \text{ or } 1 \text{ when } F_v = \mathbf{R},$$
$$f(x) = cx^A \bar{x}^B \exp(-2\pi |x|^2) \text{ for a constant } c \text{ and}$$
$$\text{integers } A \geq 0 \text{ and } B \geq 0 \text{ with } AB = 0 \text{ when } F_v = \mathbf{C}.$$

A function f on F_A is called standard if $f(x) = \prod_v f_v(x_v)$ for a standard function f_v on F_v for all v and f_v is a characteristic function of $\mathcal{O}_v$ for almost all v. Let G be either F_A or F_v. Let $\mathbf{e} : G \to \mathbf{T}$ be the standard additive character. We define a pairing $(\ ,\ ) : G\times G \to \mathbf{T}$ by $(x,y) = \mathbf{e}(xy)$. Then we already know that under this pairing, we have $G \cong \mathrm{Hom}_{\mathrm{cont}}(G,\mathbf{T})$. Let μ be the additive Haar measure defined in the previous section. We modify μ as follows. Define μ'_v by $2\mu_v$ if $v \in \mathbf{a}(\mathbf{C})$, $\mu'_v = \mu_v$ for $v \in \mathbf{a}(\mathbf{R})$ and $\mu'_v = |\varpi^r|_v^{1/2}\mu_v$ for finite places v, where we write the local different $\vartheta_v = \varpi^r \mathcal{O}_v$ for a prime element ϖ of $\mathcal{O}_v$. Then we define $\mu' = \otimes\mu'_v$ as the Haar measure on F_A. We will see later $\int_{F_A/F} d\mu' = 1$. We now define the Fourier transform of standard functions by

$$\mathcal{F}(f)(y) = \int_G f(x)(x,y)d\mu'(x).$$

When $G = F_v$ for a finite place v, then f is compactly supported and hence integrable. Thus $\mathcal{F}(f)$ is a well defined function on F_v because $|(x,y)| = 1$. When v is infinite, any standard function is integrable and thus the Fourier transform is again well defined. When $G = F_A$, then by definition of standard functions, $f(x) = f_\infty(x_\infty)f_f(x_f)$ and f_f is compactly supported and f_∞ is integrable. Then we see

$$\int_G f(x)(x,y)d\mu'(x) = \int_{F_\infty} f_\infty(x)(x_\infty,y_\infty)d\mu'_\infty(x_\infty)\int_{F_{A_f}} f(x_f)(x_f,y_f)d\mu'_f(x_f)$$

and each integral of the right-hand side is well defined and hence the Fourier transform is a well defined function on F_A. We also know that if $G = F_A$ and $f = \prod_v f_v$ is a standard function, then

$$\mathcal{F}(f) = \prod_v \mathcal{F}(f_v).$$

Thus the computation of Fourier transform of standard functions is reduced to local computation on F_v for each place v. As seen in §5, we already know that

$$(1) \qquad \mathcal{F}(f_v) = \int_{\mathbf{R}} x^A \exp(-\pi x^2)(x,y)d\mu'(x) = \sqrt{-1}^{\,A} y^A \exp(-\pi y^2) \text{ if } F_v = \mathbf{R},$$

$$\mathcal{F}(f_v) = \int_{\mathbf{C}} x^A \bar{x}^B \exp(-2\pi|x|^2)(x,y)d\mu'(x)$$
$$= \sqrt{-1}^{\,A+B} y^B \bar{y}^A \exp(-2\pi|y|^2) \text{ if } F_v = \mathbf{C}.$$

Thus we compute the Fourier transform on F_v for finite places v. Let π be a generator of the maximal ideal of $\mathcal{O}_v$ and $\varpi^r\mathcal{O}_v = \vartheta_v$ be the different of $\mathbf{e}$. First we take the characteristic function $\Phi = \Phi_v$ of $\mathcal{O}_v$. Then we claim

$$(2) \qquad \mathcal{F}(\Phi)(y) = |\varpi^r|_v^{1/2}\Phi(\varpi^r y).$$

Let us prove this. Note that the additive character $y \mapsto \mathbf{e}(xy)$ is trivial on $\mathcal{O}_v$ if and only if $x \in \varpi^{-r}\mathcal{O}_v$. Thus the orthogonality relation tells us that

$$\int_{F_v} \Phi(x)(x,y)d\mu(x) = \int_{\mathcal{O}_v} \mathbf{e}(xy)d\mu(x) = \begin{cases} 1 & \text{if } x \in \varpi^{-r}\mathcal{O}_v, \\ 0 & \text{if } x \notin \varpi^{-r}\mathcal{O}_v, \end{cases}$$

which shows (2), because $\mu'_v = |\varpi^r|_v^{1/2}\mu_v$. Since $r = 0$ for almost all v, $\mathcal{F}(\Phi_v) = \Phi_v$ for almost all v. If f is a standard function on F_A, then $f = \prod_v f_v$ and $f_v = \Phi_v$ for almost all v, and we know from (1) and (2) that $\mathcal{F}(f) = \prod_v \mathcal{F}(f_v)$ is again a standard function.

Now we take a continuous multiplicative character λ of $F_v^\times$ and assume that λ is non-trivial on $\mathcal{O}_v^\times$. Thus if $\varpi^f\mathcal{O}_v$ is the conductor of λ, then $f > 0$ ($\varpi^f\mathcal{O}_v$ is by definition the maximal ideal such that $\lambda(1+\varpi^f\mathcal{O}_v) = 1$). Let Φ_λ be the locally constant function defined as follows:

$$\Phi_\lambda(x) = \begin{cases} \lambda^{-1}(x) & \text{if } x \in \mathcal{O}_v^\times, \\ 0 & \text{if } x \notin \mathcal{O}_v^\times. \end{cases}$$

Then defining $\kappa = \kappa_v = |\varpi^f|_v^{-1/2}\int_{\mathcal{O}_v^\times}\lambda^{-1}(x)e(\varpi^{-r-f}x)d\mu(x)$, we have

$$\mathcal{F}(\Phi_\lambda)(y) = |\varpi^{f+r}|_v^{1/2}\lambda(\varpi^{r+f})\kappa_v\Phi_{\lambda^{-1}}(\varpi^{r+f}y). \tag{3}$$

In fact, by the computation of the Gauss sum, we already know that

$$\begin{aligned} &\int_{F_v}\Phi_\lambda(x)(x,y)d\mu(x) = \int_{\mathcal{O}_v^\times}\lambda^{-1}(x)e(xy)d\mu(x) \\ &= |y|_v^{-1}\int_{y\mathcal{O}_v^\times}\lambda^{-1}(y^{-1}x)\phi(x)d\mu(x) = |y|_v^{-1}\lambda(y)\int_{y\mathcal{O}_v^\times}\lambda^{-1}(x)\phi(x)d\mu(x) \\ &= \begin{cases} 0 & \text{if } y\mathcal{O}_v^\times \neq \varpi^{-r-f}\mathcal{O}_v^\times, \\ |\varpi^{f+r}|_v^{1/2}\lambda(\varpi^{r+f}y)\kappa_v & \text{if } y\mathcal{O}_v^\times = \varpi^{-r-f}\mathcal{O}_v^\times, \end{cases} \end{aligned}$$

which shows (3). By (3), we know that $\lambda(\varpi^{r+f})\kappa_v$ is determined independently of the choice of ϖ since the Fourier transform has nothing to do with the choice of ϖ. This number is called the local factor (or local root number) of λ and it is not so difficult to show that $|\kappa_v| = 1$ by using the Fourier inversion formula (see Exercise 2.3.5, Corollary 1, and the proof of Theorem 1 below).

Let Φ be a standard function and Φ' be its Fourier transform. Consider another function $\Phi_z(x) = \Phi(zx)$ for $z \in F_A^\times$, which is again a standard function. Then by definition,

$$\mathcal{F}(\Phi_z)(y) = \int_{F_A}\Phi(zx)e(xy)d\mu'(x) = \int_{F_A}\Phi(x)e(xz^{-1}y)d\mu'(z^{-1}x) = |z|_A^{-1}\Phi'(z^{-1}y).$$

This formula will be useful. Let $\lambda : F_A^\times/F^\times U(c) \to \mathbf{C}^\times$ be a Hecke character of conductor c and of infinity type $\xi = \sum_\sigma \xi_\sigma\sigma$. We may assume that λ has values in $\mathbf{T}$ by dividing λ by a suitable power of the norm character $\omega_s(x) = |x|_A^s$ (in fact, if $x_\infty = 1$, then $|x|_A^s = N(x\mathcal{O})^{-s}$ and $L(s,\lambda\omega_t) = L(t+s,\lambda)$).

Exercise 1. Show the existence of ω_s with the above property, i.e. show that there exists $s \in \mathbf{C}$ such that $|\lambda(x)| = |x|_A^s$.

Let λ_v be the restriction of λ to $F_v^\times$. If $F_v = \mathbf{R}$ and $\sigma : F \to \mathbf{R}$ is the corresponding field embedding, then $\lambda_v(x) = x^{\xi\sigma}|x|^{-\xi\sigma} = x^{-A_v}|x|^{A_v}$ for $A_v = 0$ or 1 according to the parity of ξ_σ. If $F_v = \mathbf{C}$, then $\lambda_v(x) = x^{-A_v}\bar{x}^{-B_v}|x|^{A_v+B_v}$ for integers $A_v \geq 0$, $B_v \geq 0$ and $A_vB_v = 0$, because λ has values in $\mathbf{T}$.

Exercise 2. Show that if $\chi : \mathbf{C}^\times \to \mathbf{C}^\times$ is a continuous character, then there exist integers $A \geq 0$, $B \geq 0$ and $AB = 0$ and a complex number $s \in \mathbf{C}$ such that $\chi(x) = x^{-A}\bar{x}^{-B}|x|^{2s}$.

Take an idele b such that $b\mathcal{O} = c\vartheta$ for the absolute different ϑ of F and $b_\infty = 1$. Then for each v, we may assume that $b_v = \varpi^{f+r}$ in the above computation. We then define a standard function attached to λ by $\Phi_\lambda = \prod\Phi_{\lambda_v}$ as follows. If λ_v is trivial on $\mathcal{O}_v^\times$ (this is the case for almost all v), we put $\Phi_{\lambda_v} = \Phi_v$ (the characteristic function of $\mathcal{O}_v$) and if λ_v is non-trivial on $\mathcal{O}_v^\times$, Φ_{λ_v} is as in (3) and if v is real,

$$\Phi_{\lambda_v}(x) = x^{A_v}\exp(-\pi x^2),$$

and if v is complex, then

$$\Phi_{\lambda_v}(x) = x^{A_v}\bar{x}^{B_v}\exp(-2\pi|x|^2).$$

Thus by (1), (2) and (3), we have

$$\mathcal{F}(\Phi_\lambda)(y) = \kappa|b|_A^{1/2}\Phi_{\lambda^{-1}}(by), \tag{4}$$

where $\kappa = \prod_v\kappa_v$ and κ_v is as in (3) if λ_v is non-trivial on $\mathcal{O}_v^\times$, $\kappa_v = 1$ if λ_v is trivial on $\mathcal{O}_v^\times$ and $\kappa_v = \sqrt{-1}^{A_v}$ for v real and $\kappa_v = \sqrt{-1}^{A_v+B_v}$ for v complex.

Now we define for any standard function Φ the zeta integral:

$$Z(s,\lambda;\Phi) = \int_{F_A^\times}\Phi(x)\lambda(x)|x|_A^s d\mu^\times(x). \tag{5}$$

By definition, $Z(s,\lambda;\Phi) = \prod_v\int_{F_v^\times}\Phi_v(x_v)\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x_v)$. Now we compute this integral locally and show that it is essentially the Hecke L-function $L(s,\lambda)$. We start computing the integral for finite places v. First suppose that Φ_v is the characteristic function of $\mathcal{O}_v$ and λ_v is trivial on $\mathcal{O}_v^\times$. Then

$$\begin{aligned}\int_{F_v^\times}\Phi_v(x_v)\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x) &= \sum_{j=0}^\infty \int_{\varpi^j\mathcal{O}_v^\times}\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x_v) \\ &= \sum_{j=0}^\infty \lambda^*(p_v)^j N(p_v)^{-js}\int_{\mathcal{O}_v^\times}d\mu^\times{}_v = (1-\lambda^*(p_v)N(p_v)^{-s})^{-1},\end{aligned} \tag{6}$$

which is the Euler factor of $L(s,\lambda)$ at p_v. For other finite places v, $\mathrm{Supp}(\Phi_v)$ is contained in $\varpi^{-n}\mathcal{O}_v$ for a sufficiently large n. Thus taking the characteristic function χ of this set, we have, for a sufficiently large constant M, $|\Phi_v(x)\lambda_v(x)|x|_v^s| < M\chi(x)|x|_v^\sigma$ for $\sigma = \mathrm{Re}(s)$. Then

$$\text{(7a)}\qquad \left|\int_{F_v^\times}\Phi_v(x_v)\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x)\right| < M\int_{F_v^\times}\chi(x_v)|x_v|_v^\sigma d\mu^\times{}_v(x)$$
$$= M\sum_{j=-n}^{\infty} N(p_v)^{-js} = MN(p_v)^{ns}(1-N(p_v)^{-s})^{-1}.$$

If $\Phi_v = \Phi_{\lambda_v}$ in (3), we can compute $\int_{F_v^\times}\Phi_v(x_v)\lambda_v(x_v)|x_v|_v^s d\mu_v(x)$ explicitly. In fact, we see that

$$\text{(7b)}\qquad \int_{F_v^\times}\Phi_{\lambda_v}(x_v)\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x) = \int_{\mathcal{O}_v^\times} d\mu^\times{}_v(x) = 1$$

because $\Phi_{\lambda_v} = \lambda_v^{-1}$ on $\mathcal{O}_v^\times$ and 0 outside. Anyway we have

$$\text{(8a)}\qquad \left|\int_{F_{A_f}^\times}\Phi(x)\lambda(x)|x|_A^s d\mu_f^\times(x)\right| \le M\zeta_F(\sigma) \text{ for } \sigma = \mathrm{Re}(s),$$

which is convergent if $\sigma > 1$. We conclude that

$$\text{(8b)}\qquad \int_{F_{A_f}^\times}\Phi_\lambda(x)\lambda(x)|x|_A^s d\mu_f^\times(x) = \prod_v(1-\lambda^*(p_v)N(p_v)^{-s})^{-1} = L(s,\lambda).$$

Now we compute the integral at infinite places. Since the standard function $\Phi_v(x)$ is equal to either $x^A\exp(-\pi x^2)$ or $x^A\bar{x}^B\exp(-2\pi|x|^2)$ according as $F_v = \mathbf{R}$ or $\mathbf{C}$, Φ_v decreases exponentially if $|x| \to +\infty$. Thus if $\mathrm{Re}(s)$ is sufficiently large, the integral

$$\int_{F_v^\times}\Phi_v(x_v)\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x)$$

converges absolutely if $\mathrm{Re}(s)$ is sufficiently large. Thus $Z(s,\lambda;\Phi)$ is a well defined analytic function of s if $\mathrm{Re}(s)$ is sufficiently large. Now we compute $\int_{F_v^\times}\Phi_v(x_v)\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x)$ for $\Phi_v = \Phi_{\lambda_v}$. First assume that $F_v = \mathbf{R}$ and $\lambda_v(x) = x^{-A}|x|^A$. Then $\Phi_v = x^A\exp(-\pi x^2)$ and we have

$$\text{(9a)}\qquad \int_{F_v^\times}\Phi_v(x_v)\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x) = \int_{-\infty}^{\infty}\exp(-\pi x^2)|x|^{s+A-1}dx$$
$$= \int_0^\infty \exp(-\pi y)y^{(s+A/2)-1}dy = \pi^{-(s+A)/2}\Gamma((s+A)/2) = G_{\lambda_v}(s).$$

When $F_v = \mathbf{C}$ and $\lambda_v(x) = x^{-A}\bar{x}^{-B}|x|^{A+B}$,

(9b) $$\int_{F_v^\times}\Phi_v(x_v)\lambda_v(x_v)|x_v|_v^s d\mu^\times{}_v(x)$$
$$= \int_{F_v^\times}\exp(-2\pi|x|^2)|x^2+y^2|^{s+(A+B)/2-1}dxdy$$
$$= 2^{-1}(2\pi)^{1-(s+(A+B)/2)}\Gamma(s+(A+B)/2) = 2^{-1}G_{\lambda_v}(s).$$

We put $G_{\lambda_\infty}(s) = \prod_{v \text{ infinite}} G_{\lambda_v}(s)$. Then we have

(9c) $$\int_{F_\infty^\times}\Phi_{\lambda_\infty}(x_\infty)\lambda_\infty(x_\infty)|x_\infty|_\infty^s d\mu^\times{}_\infty(x) = 2^{-t}G_{\lambda_\infty}(s).$$

Thus finally we see that

(10) $$Z(s,\lambda;\Phi_\lambda) = 2^{-t}G_{\lambda_\infty}(s)L(s,\lambda) \text{ if } \mathrm{Re}(s) > 1.$$

Until now we have only used the fact that λ is a continuous character of $F_A^\times/U(c)$. Hereafter we suppose that $\lambda(F^\times) = 1$ and prove the functional equation. Let Φ be a standard function on F_A and Φ' be its Fourier transform. Since F_A/F is known to be compact and F is a discrete subgroup of F_A (1.3c), we can apply the Poisson summation formula in §4 to this situation. We first review the formula. Let $F^\perp = \{x \in F_A \mid (x,F) = 1\}$. Then $F^\perp \cong \mathrm{Hom}_{\mathrm{cont}}(F_A/F,\mathbf{T})$. Since F_A/F is compact, $F^\perp$ is a discrete subgroup of F_A by identifying F_A with $\mathrm{Hom}_{\mathrm{cont}}(F_A,\mathbf{T})$ (Lemma 3.1 and Theorem 3.1). Since the standard character $\mathbf{e}$ is trivial on F, $(\eta,\xi) = \mathbf{e}(\eta\xi) = 1$ for ξ and η in F. Thus F is contained in $F^\perp$. Thus $F^\perp/F$ is a discrete subgroup of F_A/F. Since F_A/F is compact, $F^\perp/F$ must be discrete and compact. Thus $F^\perp/F$ is a finite group. Let $x \in F^\perp - F$ and suppose $Nx \in F$ (such an integer $N > 0$ always exists because $F^\perp/F$ is finite). Since F is a field of characteristic 0, we can find $y \in F$ such that $Ny = Nx$. Thus $x-y$ is killed by N in F_A. Since F_A is torsion-free, $x = y$, a contradiction. Thus $F^\perp = F$. Let G be a locally compact abelian group. We suppose that there is a pairing $(\ ,\ ): G\times G \to \mathbf{T}$ under which $G \cong \mathrm{Hom}_{\mathrm{cont}}(G,\mathbf{T})$. Let Γ be a discrete cocompact subgroup and $\Gamma^* = \{x \in G \mid (x,\Gamma) = 1\}$. Then Γ^* is again a discrete cocompact subgroup. Let μ be a Haar measure on G. Let K be a fundamental domain of G/Γ and normalize μ so that $\int_K d\mu = 1$. Then the Poisson summation formula reads

$$\sum_{\gamma\in\Gamma} f(\gamma) = \sum_{\gamma^*\in\Gamma^*}\mathcal{F}(f)(\gamma^*)$$

if both sides are absolutely convergent and the Fourier transform $\mathcal{F}(f)$ with respect to μ and $(\ ,\ )$ is well defined (i.e. f is continuous and integrable on G). Let us apply this formula for $f = \Phi$ and $G = F_A$, $\Gamma = \Gamma^* = F$. Thus we need to

show that $\int_{F_A/F} d\mu' = 1$. By (1.3c), we have a canonical isomorphism $\hat{O}\times F_\infty/O$. Thus $\int_{F_A/F} d\mu = \int_{F_\infty/O} d\mu_\infty$. Let $\{\omega_1,\ldots,\omega_d\}$ $(d = [F:\mathbf{Q}])$ be a basis of O over $\mathbf{Z}$. We identify $F_\infty = \mathbf{C}^{a(C)}\times\mathbf{R}^{a(R)}$ and $\mathbf{C}$ with $\mathbf{R}^2$ taking the basis $(1,\sqrt{-1})$. Thus ω_j can be considered as a vector in $F_\infty = (\mathbf{R}^2)^{a(C)}\times\mathbf{R}^{a(R)}$ whose component at each $\sigma \in \mathbf{a}$ is given as follows: For $\sigma \in \mathbf{a}(\mathbf{C})$, $(\mathrm{Re}(\omega_j^\sigma),\mathrm{Im}(\omega_j^\sigma))$ and for $\sigma \in \mathbf{a}(\mathbf{R})$, ω_j^σ. Then

$$\int_{F_\infty/O} d\mu_\infty = |\det(\omega_1,\ldots,\omega_d)| = 2^{-t}|D|^{1/2} = 2^{-t}|N(\vartheta)|^{1/2}.$$

This shows that μ' on F_A is the right choice, i.e., $\int_{F_A/F} d\mu' = 1$.

Theorem 1. *Let Φ be a standard function on F_A and Φ' be its Fourier transform. Then the function $s \mapsto Z(s,\lambda;\Phi)$ defined by (5) when the integral is convergent can be continued analytically as a meromorphic function on the whole complex plane. It satisfies the following functional equation:*

$$Z(s,\lambda;\Phi) = Z(1-s,\lambda^{-1};\Phi').$$

If one specializes Φ in the theorem to Φ_λ, we derive from (4) and (10) the following result:

Corollary 1. *$L(s,\lambda)$ can be continued to a meromorphic function on the whole s-plane and satisfies the following functional equation:*

$$G_{\lambda_\infty}(s)L(s,\lambda) = \kappa\lambda(b)\lambda_\infty(-1)(|D|N(c))^{(1/2)-s}G_{\lambda_\infty^{-1}}(1-s)L(1-s,\lambda^{-1}),$$

where c is the conductor of λ, D is the absolute discriminant of F, b is the idele fixed in (3) and κ is the root number for λ.

Before proving the theorem, we start with the following lemma in [W1, VII.5]. We can decompose $F_A^\times/F^\times = (F_A^{(1)}/F^\times)\times\mathbf{R}_+$ via $x \mapsto (x_f(x_\infty|x|_A^{-1/[F:Q]}), |x|_A)$. We know that $(F_A^{(1)}/F^\times)$ is a compact group (Theorem 1.1).

Lemma 1 ([W1, VII.5]). *Let F_1 be a measurable function on $\mathbf{R}_+$ with $0 \le F_1 \le 1$. Moreover suppose that there exists an interval $[t_0,t_1]$ in $\mathbf{R}_+$ such that $F_1(x) = 1$ if $x < t_0$ and $F_1(x) = 0$ if $x > t_1$. Then the integral $f(s) = \int_0^\infty F_1(x)x^{s-1}dx$ is absolutely convergent for $\mathrm{Re}(s) > 0$. The function $f(s)$ can be continued analytically in the whole s-plane as a meromorphic function. Moreover $f(s)-s^{-1}$ is an entire function. If $F_1(x)+F_1(x^{-1}) = 1$ for all $x \in \mathbf{R}_+$, then $f(s)+f(-s) = 0$.*

Proof (A. Weil). First take as F_1 the function ϕ such that $\phi(x) = 0$ if $x > 1$ and $\phi(x) = 1$ if $x < 1$. Then $f(s) = \int_0^1 x^{s-1}dx = [x^s/s]_0^1 = s^{-1}$ if $\mathrm{Re}(s) > 0$ and the assertion is obvious. For general F_1, we see that

$$f(s)-s^{-1} = \int_0^\infty (F_1-\phi)(x)x^{s-1}dx.$$

Since $F_1-\phi$ is a bounded measurable function with compact support on $\mathbf{R}_+$, the above integral is (locally) uniformly and absolutely convergent for all s, which gives an entire function of s. Note that $\phi(x)+\phi(x^{-1}) = 1$. If $F_1(x)+F_1(x^{-1}) = 1$, then $F_2 = F_1-\phi$ satisfies $F_2(x^{-1}) = -F_2(x)$. Thus replacing x by x^{-1} in the above integral, we see $f(-s)-(-s)^{-1} = -f(s)+s^{-1}$. This shows that $f(-s) = -f(s)$.

Proof of the theorem. We already know that the integral

$$Z(s,\lambda;\Phi) = \int_{F_A^\times}\Phi(x)\lambda(x)|x|_A^s d\mu^\times(x)$$

is absolutely convergent if $\mathrm{Re}(s) > 1$. Let F_1 be a continuous function as in the lemma and define F_0 by $F_0+F_1 = 1$. Thus $0 \le F_j \le 1$ and $F_0(x) = 0$ if $x < t_0$ and $F_1(x) = 0$ if $x > t_1$. Take arbitrary $B > 1$. Then, for any $\sigma \in \mathbf{R}$ with $\sigma < B$, we see that $x^\sigma F_0(x) \le t_0^{\sigma-B}x^B$. We define

$$Z_j(s,\lambda;\Phi) = \int_{F_A^\times}\Phi(x)\lambda(x)|x|_A^s F_j(|x|_A)d\mu^\times(x).$$

Then writing $\sigma = \mathrm{Re}(s)$, we have

$$\int_{F_A^\times}|\Phi(x)|\,|x|_A^\sigma F_0(|x|_A)d\mu^\times(x) \le t_0^{\sigma-B}\int_{F_A^\times}|\Phi(x)|\,|x|_A^B d\mu^\times(x).$$

Thus this integral is absolutely convergent for all s since $B > 1$. Thus $Z_0(s,\lambda;\Phi)$ is an entire function of s. Now replacing λ by λ^{-1}, s by $1-s$, Φ by Φ' and F_0 by the function $x \mapsto F_1(x^{-1})$, by the same argument as above, we have an entire function of s defined on the whole s-plane,

$$Z'_0(1-s,\lambda^{-1};\Phi') = \int_{F_A^\times}\Phi'(x)\lambda^{-1}(x)|x|_A^{1-s}F_1(|x|_A^{-1})d\mu^\times(x).$$

Let $\Phi_z(x) = \Phi(zx)$ for $z \in F_A^\times$. Then the Fourier transform of Φ_z is given by $|z|_A^{-1}\Phi'_{z^{-1}}$ as already remarked. We now write, choosing a fundamental domain X of $F_A^\times/F^\times$, $F_A^\times = \bigcup_{\xi\in F-\{0\}}\xi X$. Then

$$Z_j(s,\lambda;\Phi) = \int_{F_A^\times}\Phi(x)\lambda(x)|x|_A^s F_j(|x|_A)d\mu^\times(x)$$

$$= \sum_{\xi\in F-\{0\}}\int_X \Phi(\xi x)\lambda(x)|x|_A^s F_j(|x|_A)d\mu^\times(x)$$
$$= \int_{F_A^\times/F^\times}\sum_{\xi\in F-\{0\}}\Phi(\xi x)\lambda(x)|x|_A^s F_j(|x|_A)d\mu^\times(x).$$

Similarly, we have

$$Z'_0(1-s,\lambda^{-1};\Phi') = \int_{F_A^\times/F^\times}\sum_{\xi\in F-\{0\}}\Phi'(\xi x)\lambda^{-1}(x)|x|_A^{1-s}F_1(|x|_A^{-1})d\mu^\times(x).$$

By the Poisson summation formula, we see that

$$\Phi(0)+\sum_{\xi\in F-\{0\}}\Phi(\xi x) = \sum_{\xi\in F}\Phi_x(\xi) = |x|_A^{-1}\sum_{\xi\in F}\Phi'(\xi x^{-1})$$
$$= |x|_A^{-1}\{\Phi'(0)+\sum_{\xi\in F-\{0\}}\Phi'(\xi x^{-1})\}.$$

Thus we see that

$$Z_1(s,\lambda;\Phi) = \int_{F_A^\times/F^\times}\sum_{\xi\in F-\{0\}}\Phi'(\xi x^{-1})\lambda(x)|x|_A^{s-1}F_1(|x|_A)d\mu^\times(x)$$
$$+ \int_{F_A^\times/F^\times}\{\Phi'(0)|x|_A^{-1}-\Phi(0)\}\lambda(x)\,|\,x\,|_A{}^sF_1(|x|_A)d\mu^\times(x).$$

By the variable change $x\mapsto x^{-1}$, the first integral equals $Z'_0(1-s,\lambda^{-1};\Phi')$ and thus

$$Z_1(s,\lambda;\Phi)-Z'_0(1-s,\lambda^{-1};\Phi')$$
$$= \int_{F_A^\times/F^\times}\{\Phi'(0)\,|\,x\,|_A{}^{-1}-\Phi(0)\}\lambda(x)|x|_A^s F_1(\,|\,x\,|_A)d\mu^\times(x).$$

Now we use the fact that $F_A^\times/F^\times = K\times\mathbf{R}_+$ for a compact group $K = F_A^{(1)}/F^\times$. Write $\lambda = \lambda_1\lambda_2$ as a product of characters of K and $\mathbf{R}_+$. Since $log : \mathbf{R}_+\cong\mathbf{R}$ and $\mathrm{Hom}_{cont}(\mathbf{R},\mathbf{T})\cong\mathbf{R}$, $\lambda_2(x) = |\,x\,|_A{}^t$ for some $t\in\sqrt{-1}\mathbf{R}$. Then we have

$$Z_1(s,\lambda;\Phi)-Z'_0(1-s,\lambda^{-1};\Phi') = Z_1(s+t,\lambda_1;\Phi)-Z'_0(1-s-t,\lambda_1{}^{-1};\Phi').$$

Thus we may assume that $t = 0$. Then

$$Z_1(s,\lambda;\Phi)-Z'_0(1-s,\lambda^{-1};\Phi') = \int_K\lambda d\mu^\times\int_{\mathbf{R}_+}\{\Phi'(0)-\Phi(0)x\}x^{s-2}F_1(x)dx.$$

Since K is compact, $c(\lambda) = \int_K\lambda d\mu^\times$ is a constant and vanishes if $\lambda\neq 1$ on K. Anyway, by Lemma 1,

$$Z_1(s,\lambda;\Phi)-Z'_0(1-s,\lambda^{-1};\Phi') = c(\lambda)(\Phi'(0)f(s-1)-\Phi(0)f(s))$$

for a meromorphic function $f(s)$ satisfying the following conditions: (i) $f(s)-s^{-1}$ is entire and (ii) $f(s)+f(-s) = 0$. Since $Z(s,\lambda;\Phi) = Z_0(s,\lambda;\Phi)+Z_1(s,\lambda;\Phi)$, the

above fact shows the analytic continuation of $Z(s,\lambda;\Phi)$ because $Z'_0(1-s,\lambda^{-1};\Phi')$ is entire. Moreover we have

$$Z(s,\lambda;\Phi) = Z_0(s,\lambda;\Phi) + Z'_0(1-s,\lambda^{-1};\Phi') + c(\lambda)(\Phi'(0)f(s-1)-\Phi(0)f(s)).$$

Since f is an odd function, we know the functional equation

$$Z(s,\lambda;\Phi) = Z(1-s,\lambda^{-1};\Phi')$$

because of the Fourier inversion formula $\mathcal{F}\mathcal{F}(\Phi)(x) = \Phi(-x)$. We have not proven the inversion formula yet but for the special function Φ_λ it is obvious by (3).

We now give a sketch of a proof of the inversion formula when v is finite (a similar argument works also for $\mathbf{R}$ or $\mathbf{C}$). Let f be a standard function and $\Phi_n(x) = \Phi_0(\pi^n x)$ be the characteristic function of $\varpi^{-n}\mathcal{O}_v$. Then we compute for $G = F_v$

$$\mathcal{F}\mathcal{F}(f)(z) = \int_G\int_G f(x)(x,y)d\mu'(x)(y,z)d\mu'(y).$$

We already know that $\mathcal{F}(\Phi_n)(x) = |\pi|_v^{-n}\Phi_0(\pi^{r-n}x)$ by (2). Instead of the above integral, we compute

$$\begin{aligned}\int_G\int_G\Phi_n(y)f(x)(x,y)d\mu(x)(y,z)d\mu(y) &= \int_G\int_G\Phi_n(y)(y,x+z)d\mu(y)f(x)d\mu(x)\\ &= \int_G\mathcal{F}(\Phi_n)(x+z)f(x)d\mu(x) = |\varpi|_v^{-n}\int_G\Phi_0(\pi^{r-n}x)f(x-z)d\mu(x)\\ &\overset{\pi^{-n}x \mapsto x}{=} \int_G\Phi_0(\varpi^r x)f(\pi^n x-z)d\mu(x).\end{aligned}$$

By taking the limit as $n \to \infty$, we see that

$$f(-z)|\varpi|_v^{-r} = f(-z)\int_G\Phi_0(\varpi^r x)d\mu(x) = |\varpi|_v^{-r}\mathcal{F}\mathcal{F}(f)(z),$$

because the difference of μ and μ' is $|\varpi^r|_v^{1/2}$. This shows the result.

Exercise 3. Show that $\sum_{\xi\in F}\Phi(\xi)$ is absolutely convergent when $F = \mathbf{Q}$.

When λ is the trivial character, we see that $\Phi_\lambda(x) = \Phi_f(x_f)\Phi_\infty(x_\infty)$ for the characteristic function Φ_f of $\hat{O}$ and $\Phi_\infty(x_\infty) = \exp(-\pi\sum_{\sigma\in I}|x_\infty{}^\sigma|^2)$. Thus $\Phi(0) = 1$ and by (4), $\mathcal{F}(\Phi_\lambda)(0) = |D|^{-1/2}\Phi_\lambda(0) = |D|^{-1/2}$. Thus we have $\Phi'(0) = |D|^{-1/2}$. By the proof of the theorem, we see that

$$\mathrm{Res}_{s=1}Z(s,\lambda;\Phi_\lambda) = \int_K\lambda d\mu^\times\Phi'(0) \qquad (K = F_A^{(1)}/F^\times).$$

We now compute $\int_K \lambda d\mu^\times$. By Corollary 1.1, we see that

$$\int_K \lambda d\mu^\times = h(F)\int_{K'} \lambda d\mu^\times \quad \text{for} \quad K' = F_A^{(1)} \cap F^\times \hat{O}^\times F_\infty^\times / F^\times,$$

where $h(F)$ is the class number of F. It is then plain that $K' \cong X/E$ for $X = \{x \in F_\infty^\times \mid N(x) = 1\}$ where E is the subgroup of $\mathcal{O}^\times$ consisting of totally positive units. We then consider the logarithm map in (1.2.7) $l : F_\infty^\times \to \mathbf{R}^{\mathbf{a}}$. We decompose the Haar measure on $\mathbf{C}$ so that $dxdy = rdrd\theta$ for $r = |z|^2$ for $z \in \mathbf{C}$ and the Haar measure $d\theta$ on $\mathbf{T}$. Then we see easily that

$$\mathrm{vol}(l(X)/l(E)) = \int_{l(X)/l(E)} dr = |R| = R_\infty,$$

where $R = \det((l_i(\varepsilon^{(j)}))_{i,j})$ for a basis $\{\varepsilon_1, \ldots, \varepsilon_s\}$ $(s = \#(\mathbf{a})\text{-}1)$ of the torsion-free part of E. Note that the kernel Y of l can be written as $(\{\pm 1\}^{\mathbf{a}(\mathbf{R})} \times \mathbf{T}^{\mathbf{a}(\mathbf{C})})/\mu(F)$ for the group $\mu(F)$ of roots of unity in F. Then we have

$$\int_Y d\theta = 2^r (2\pi)^t / w \quad \text{for} \quad w = \#\mu(F) \quad (r = \#(\mathbf{a}(\mathbf{R})) \text{ and } t = \#(\mathbf{a}(\mathbf{C}))).$$

Thus $\int_K \lambda d\mu^\times = \dfrac{2^r (2\pi)^t R_\infty h(F)}{w}$, and we obtain

Corollary 2 (Residue formula). *We have*

$$\mathrm{Res}_{s=1} \zeta_F(s) = \frac{2^r (2\pi)^t R_\infty h(F)}{w |D|^{1/2}}.$$

Chapter 9. Adelic Eisenstein series and Rankin products

In this chapter, first we shall give an adelic interpretation of modular forms and then we will compute the Fourier expansion of adelic Eisenstein series for GL(2) over $\mathbf{Q}$. After this computation, we will know that the Eisenstein series has analytic continuation with respect to the variable s. Using this fact, we will show the analytic continuability of the Rankin product and its functional equations.

§9.1. Modular forms on $GL_2(F_A)$

Hereafter, we assume that F is a totally real field. We start from the definition of modular forms on the group $GL_2(F_A)$, which consists of invertible 2×2 matrices with coefficients in F_A. We use the notation of Chapter 5. In particular, $\mathcal{H}$ denotes the upper half complex plane. We put, identifying F_∞ with $\mathbf{R}^I$ for the set of real embeddings I of F,

$$G_{\infty+} = \{x \in GL_2(F_\infty) = GL_2(\mathbf{R})^I \mid \det(x_\sigma) > 0 \text{ for all } \sigma \in I\}.$$

Then we can let the group $G_{\infty+}$ act on $\mathcal{Z} = \mathcal{H}^I$ via linear fractional transformations $x(z) = (x_\sigma(z_\sigma))_{\sigma\in I}$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \dfrac{az+b}{cz+d}$. We put

$$C_{\infty+} = \{x \in G_{\infty+} \mid x(\mathbf{i}) = \mathbf{i}\} \text{ for } \mathbf{i} = (\sqrt{-1}, \ldots, \sqrt{-1}) \in \mathcal{Z}.$$

Exercise 1. Show that for $\alpha \in GL_2(\mathbf{R})$ with $\det(\alpha) > 0$, $\alpha(i) = i$ ($i = \sqrt{-1}$) if and only if there exist $t \in \mathbf{R}^\times$ and $\theta \in \mathbf{R}$ such that $\alpha = t\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Especially $C_{\infty+} = \mathbf{R}^\times SO_2(\mathbf{R})$.

For $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $z \in \mathcal{H}$, we put $j(\alpha,z) = (cz+d)$. Then we see easily that $j(\alpha\beta,z) = j(\alpha,\beta(z))j(\beta,z)$. Thus if $\alpha(i) = \beta(i) = i$, then $j(\alpha\beta,i) = j(\alpha,i)j(\beta,i)$ and the map $\alpha \mapsto j(\alpha,i)$ is a group homomorphism of $\mathbf{R}^\times SO_2(\mathbf{R})$ into $\mathbf{C}^\times$. In fact, $j(\alpha,i) = te^{i\theta}$ if $\alpha = t\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. We define $j_k(x,z) = \prod_\sigma j(x_\sigma,z_\sigma)^k$ for each positive integer k, $x \in G_{\infty+}$ and $z \in \mathcal{Z}$, and $|j(x,z)|^s = \prod_\sigma |j(x_\sigma,z_\sigma)|^s$ for $s \in \mathbf{C}$. Then the map $x \mapsto j_k(x,\mathbf{i})$ is a group homomorphism of $C_{\infty+}$ into $\mathbf{C}^\times$.

We consider the open compact subgroup

$$S = GL_2(\hat{O}) = \prod_p GL_2(O_p)$$

of $GL_2(F_A)$ and its subgroup of finite index, for each integral ideal m

$$S(m) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S \mid c \in m\hat{O} = \prod_p m_p\right\}.$$

For a given character $\chi : Cl(m) = F_A^\times/F^\times U(m)F_{\infty+} \to \mathbf{T}$, a continuous function $f : GL_2(F_A) \to \mathbf{C}$ is called an adelic modular form (in a weak sense) of weight k, of character χ and of level m if it satisfies the following condition:

(M1) $f(\alpha xu) = \chi_m(u)f(x)j_k(u_\infty,\mathbf{i})^{-1}$ for all $u \in S(m)C_{\infty+}$ and $\alpha \in GL_2(F)$,

where $\chi_m(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \prod_{v \mid m}\chi_v(d_v)$. Modular forms play the role of Hecke characters for the group GL(2) in place of GL(1). In fact, any Hecke character $\lambda : F_A^\times = GL_1(F_A) \to \mathbf{C}^\times$ for a general number field F satisfies the condition $\lambda(\alpha xu) = \lambda(x)u_\infty^{-\xi}$ for $\alpha \in F^\times = GL_1(F)$ and $u \in U(m)F_{\infty+}$ for its infinity type ξ, which is an analog of (M1).

We can define, from the modular form f and a given element $t \in GL_2(F_{A_f})$ as above, a function $f_t : \mathcal{Z} \to \mathbf{C}$ as follows: for $z = x+\mathbf{i}y \in \mathcal{Z}$ $(x, y \in F_\infty)$, we pick one element $u_\infty \in G_{\infty+}$ so that $u_\infty(i) = z$, for example, $u_\infty = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$ satisfies the requirement. This in particular shows that $G_{\infty+} = B_{\infty+}C_{\infty+}$, where

$$B_\infty = \left\{\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \middle| \; x \in F_\infty,\; 0 < y \in F_{\infty+}^\times\right\}.$$

We put $f_t(z) = f(tu_\infty)j_k(u_\infty,\mathbf{i})$. This definition of $f_t(z)$ does not depend on the choice of u_∞. In fact, if $u_\infty(i) = u'_\infty(i)$, then $u_\infty^{-1}u'_\infty(i) = i$ and hence $c = u_\infty^{-1}u'_\infty \in C_{\infty+}$. That is, $u_\infty c = u'_\infty$ and

$$f(tu'_\infty)j_k(u'_\infty,\mathbf{i}) = f(tu_\infty c)j_k(u_\infty c,\mathbf{i}) = f(tu_\infty)j_k(c,\mathbf{i})^{-1}j_k(c,\mathbf{i})j_k(u_\infty,\mathbf{i}) = f_t(z).$$

Now put $\Gamma_t = GL_2(F)\cap t^{-1}S(N)tG_{\infty+}$. Then Γ_t is a subgroup of $GL_2(F)$, and if $t = 1$,

$$\Gamma_1 = \{\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(O) \mid c \in m \text{ and } \det(\alpha) \in F_{\infty+}\}.$$

In particular, if $F = \mathbf{Q}$, then

$$\Gamma_1 = \Gamma_0(m) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \mid c \in m\}.$$

We now show that f_t satisfies $f_t(\gamma(z)) = \chi^*(d)f_t(z)j_k(\gamma,z)$ for $\gamma \in \Gamma_t$ if t is of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, where χ^* is the ideal character associated to the idele character χ. Thus f_t is a modular form on $\mathcal{Z}$ for the discrete subgroup Γ_t in the classical sense: if $\gamma \in \Gamma_t$, then

$$f_t(\gamma(z)) = f(t\gamma_\infty u_\infty)j_k(\gamma_\infty u_\infty, \mathbf{i})$$

since $\gamma_\infty u_\infty(\mathbf{i}) = \gamma(z)$. The adele matrix γ_∞ has non-trivial components only at infinity and t is concentrated on finite places. Thus $\gamma t t^{-1}\gamma_f^{-1}t = \gamma\gamma_f^{-1}t = \gamma_\infty t = t\gamma_\infty$. Moreover $t^{-1}\gamma_f^{-1}t \in S(m)$ and we know that

$$\begin{aligned} f_t(\gamma(z)) &= f(t\gamma_\infty u_\infty)j_k(\gamma_\infty u_\infty, \mathbf{i}) = f(\gamma t t^{-1}\gamma_f^{-1}tu_\infty)j_k(\gamma_\infty u_\infty, \mathbf{i}) \\ &= \chi_m(d)^{-1}f(tu_\infty)j_k(\gamma_\infty, z)j_k(u_\infty, \mathbf{i}) = \chi_m(d)^{-1}f_t(z)j_k(\gamma, z). \end{aligned}$$

Note that $1 = \chi(d) = \chi_m(d)\chi^*((d))$ for the ideal character χ^* associated to the idele character χ. Thus $\chi_m(d)^{-1} = \chi^*(d)$. Similar computation shows that for more general $\alpha \in GL_2(F)$ with $\det(\alpha) \gg 0$ (the symbol "$\gg$" means that $\det(\alpha)$ is totally positive, i.e. $\det(\alpha)^\sigma > 0$ for all $\sigma \in I$), we have

$$\text{(1a)} \qquad f_t(\alpha(z))j_k(\alpha, z)^{-1} = f_{\alpha_f^{-1}t}(z).$$

Thus to one modular form f on $GL_2(F_A)$, we can attach a system of classical modular forms $\{f_t\}$. This system is basically parametrized by the double coset space:

$$GL_2(F)\backslash GL_2(F_A)/S(m)G_{\infty+} \cong GL_2^+(F)\backslash GL_2(F_{A_f})/S(m)$$

which is an analog of the class group $Cl(m) = F^\times\backslash F_A^\times/U(m)F_{\infty+}$. In fact, it is known that if $\{a_i\}_{i=1,\dots,h}$ is a representative set of $Cl(1)$ in $F_A^\times$, then

$$\text{(1b)} \qquad GL_2(F_A) = \bigcup_{i=1}^h GL_2(F)\begin{pmatrix} a_i & 0 \\ 0 & 1 \end{pmatrix}S(m)G_{\infty+} \text{ (approximation theorem).}$$

Thus each modular form on $GL_2(F_A)$ corresponds to a set of h classical modular forms on $\mathcal{Z}$. We now impose the following holomorphy condition on f:

(M2) $\quad f_t$ *is a holomorphic function on* $\mathcal{Z}$ *for all* $t \in GL_2(F_{A_f})$.

Let us give a proof of (1b): Consider $L_f = \hat{\mathcal{O}}^2$ and $L = \mathcal{O}^2$ as lattices in the column vector space $V = F^2$. For each $x \in GL_2(F_{A_f})$, $xL = xL_f \cap V$ is a lattice of V. We first show that there is a vector $0 \neq y \in xL$ such that $xL/\mathcal{O}y$ is torsion-free. Take one non-trivial vector $y \in xL$. The places v such that the image $y(v)$ of y in $xL/p_v xL$ is zero are finitely many (note that $y(v) = 0$ if and only if $xL/\mathcal{O}y$ has non-trivial p_v-torsion). Let Z be the set of such places. We choose $z \in xL$ so that the image $z(v)$ in $xL/p_v xL$ is non-zero for every $v \in Z$. We may assume that z and y are linearly independent over F. Then the images of z and y in $xL/p_v xL$ are linearly independent for almost all places v. Let Y be the finite set of places v where the images of z and y in $xL/p_v xL$ are not linearly independent. Thus we can write $z(v) = \lambda(v)y(v)$ for $v \in Y$ with

$\lambda(v) \in \mathcal{O}_v/p_v$. Since $\mathcal{O}_v/p_v$ has at least two elements, we can find $b \in \mathcal{O}$ such that $(b \bmod p_v) \neq \lambda(v)$ for all $v \in Y$ (by Chinese remainder theorem). Then put $t = z\text{-}by$. Then if $v \in Y$, then $t(v) = t \bmod p_v xL \neq 0$ by the choice of b. If v is in Z, then $t(v) = z(v) \neq 0$ by our choice of z. If v is in neither Z nor Y, then z and y are linearly independent in $xL/p_v xL$ and hence $t(v) \neq 0$. Thus $xL/\mathcal{O}t$ is without torsion. Thus we may assume that $xL/\mathcal{O}y$ is torsion-free from the first. Since $xL/\mathcal{O}y$ can be embedded into F, it is isomorphic to an ideal $\mathfrak{a}$ of $\mathcal{O}$, which is projective because $\mathcal{O}$ is a Dedekind domain ([Bour1, VII.4.10]). Thus $xL \cong \mathfrak{a}t \oplus \mathcal{O}y$ for an ideal $\mathfrak{a}$ and $t \in xL$. Take $a \in F_{A_f}$ such that $a\mathcal{O} = \mathfrak{a}$, and write $a = \beta a_i$ with β in F and for some i (we can choose the parity of β arbitrarily at infinite places by changing i if necessary). Then, writing the matrix $\alpha = \begin{pmatrix} \beta t_1 & y_1 \\ \beta t_2 & y_2 \end{pmatrix}$ for $t = \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}$ and $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, we see that $\alpha \begin{pmatrix} a_i & 0 \\ 0 & 1 \end{pmatrix} L_f = xL_f$. We may further assume that $\det(\alpha) \gg 0$ by choosing a suitable parity of β. Thus $x = \alpha \begin{pmatrix} a_i & 0 \\ 0 & 1 \end{pmatrix} u$ for $u \in S$ since $S = \{x \in GL_2(F_{A_f}) \mid xL_f = L_f\}$. This shows (1) for $m = \mathcal{O}$. For general m, we can easily approximate u as above by $\gamma \in b^{-1}Sb \cap GL_2^+(F)$ for $b = \begin{pmatrix} a_i & 0 \\ 0 & 1 \end{pmatrix}$ so that $\gamma u \in S(m)$. This is a special case of the strong approximation theorem but it is not so hard to verify it in this case. When $F = \mathbf{Q}$, we have already proven the strong approximation theorem as Lemma 6.1.1 and its proof applies to the general case.

Now we define the Fourier expansion of modular forms. Since any modular form f on $GL_2(F_A)$ has a prearranged move under the left translation by $GL_2(F)$ and the right translation by $S(m)C_{\infty+}$, by (M1), it is determined by the value on the subgroup

$$B(F_A)_+ = \{b \in B(F_A) \mid \det(b_\infty) \gg 0\},$$

where for any $\mathbf{Q}$-algebra A, we put

$$B(A) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \, a \in (A \otimes_{\mathbf{Q}} F)^\times \text{ and } b \in A \otimes_{\mathbf{Q}} F \right\}.$$

Let f be a modular form as in (1). We write simply $f(y,x) = f\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right)$. Now for $u \in F_A$, we consider a unipotent matrix $\alpha(u) = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$. Then $\alpha(u)\begin{pmatrix} y & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y & x+u \\ 0 & 1 \end{pmatrix}$. In particular, if $\xi \in F$, then $\tau(\xi) \in GL_2(F)$ and thus $f(y,x+\xi) = f\left(\alpha(u)\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right) = f(y,x)$. Thus $f(y,x)$ is translation invariant under F in the variable x. Thus for a fixed y, we can consider $x \mapsto f(y,x)$ as a

continuous function on F_A/F (which is of C^∞-class in $x_\infty \in F_\infty$). The group F_A/F is a compact additive group. Thus we can expand $f(y,x)$ into an adelic Fourier expansion on F_A/F (see §8.4); namely,

$$f(y,x) = \sum_\phi c(y,\phi)\phi(x),$$

where ϕ runs over all additive characters $\phi \in \mathrm{Hom}_{\mathrm{cont}}(F_A/F,\mathbf{T})$ and

$$c(y,\phi) = \int_{F_A/F} f(y,x)\phi(-x)d\mu(x).$$

Here the additive Haar measure μ is normalized so that $\mu(F_A/F) = 1$. We already know that $\mathrm{Hom}_{\mathrm{cont}}(F_A/F,\mathbf{T}) \cong F$ so that each character of F_A/F is given by $x \mapsto e(\xi x)$ for the standard character $e : F_A/F \to \mathbf{T}$. Thus we can write this expansion as

$$f(y,x) = \sum_{\xi\in F} c(y,\xi)e(\xi x) \quad \text{for } x \in F_A.$$

Let us verify several properties of this expansion. Since f is invariant under right multiplication by the matrix $\alpha = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}$ with $u \in U$, we see that $f(uy,x) = f\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\alpha\right) = f(y,x)$. This shows that $c(uy,\xi) = c(y,\xi)$. Thus

(2) $\qquad c(y,\xi)$ depends only on the ideal $y\mathcal{O}$ and y_∞.

Similarly $f(\eta y, \eta x) = f(y,x)$ for $\eta \in F^\times$, and thus

(3) $\qquad c(\eta y,\xi) = c(y,\xi\eta)$ for $\xi \in F$, $0 \neq \eta \in F$.

Let $\vartheta = d\mathcal{O}$ $(d \in F_{A_f}{}^\times)$ be the different of $F/\mathbf{Q}$. Thus $d^{-1}\hat{\mathcal{O}}$ is the maximal additive subgroup in $\mathbf{A}_f$ of the form $x\hat{\mathcal{O}}$ so that $e_f(x\hat{\mathcal{O}}) = 1$. Now for $u \in \hat{\mathcal{O}}$, $\alpha(u) = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in S(m)$, we know that $f(y,x+uy) = f(y,x)$. Therefore $c(y,\xi) = c(y,\xi)e(\xi uy)$ for all $u \in \hat{\mathcal{O}}$. This implies that if $c(y,\xi) \neq 0$, $\xi y \in d^{-1}\hat{\mathcal{O}}$; in other words,

(4) $\qquad \xi dy\mathcal{O}$ is an integral ideal if $c(y,\xi) \neq 0$.

Now we compute the function $f_t : \mathcal{Z} \to \mathbf{C}$ for $t = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ with a fixed $a \in \mathbf{A}_f$. Write $\mathfrak{a} = a\mathcal{O}$ for the corresponding ideal. Then for $z = x_\infty + y_\infty \mathbf{i} \in \mathcal{Z}$, taking $\begin{pmatrix} y_\infty & x_\infty \\ 0 & 1 \end{pmatrix}$ as u_∞, we see that

(5a) $$f_t(z) = f(ay_\infty, x_\infty) = \sum_{\xi \in a^{-1}} c(ay_\infty, \xi)\exp(2\pi\sqrt{-1}\,\mathrm{Tr}(\xi x_\infty)).$$

Especially, if f_t is a holomorphic function, then $\frac{\partial}{\partial \bar{z}_\sigma} = \frac{\partial}{\partial x_\sigma} + i\frac{\partial}{\partial y_\sigma}$ kills each term and hence $\frac{\partial}{\partial y_\sigma} c(ay_\infty, \xi) = -2\pi\xi^\sigma c(ay_\infty, \xi)$. Thus $c(ay_\infty, \xi)$ is a constant multiple of $\exp(-2\pi\mathrm{Tr}(\xi y_\infty))$. We write this constant as $c(\xi d a)$; thus $c(ay_\infty, \xi) = c(\xi d a)\exp(-2\pi\mathrm{Tr}(\xi y_\infty))$. We now show that $c(\xi d a) = 0$ unless $\xi^\sigma \geq 0$ for all σ when $F \neq \mathbf{Q}$. For that we pick one $\xi \neq 0$ which is not totally positive. We then define $[\xi] = \{\sigma \in I \mid \xi^\sigma < 0\}$, which is not empty. Fix one element $\sigma \in [\xi]$ and take a totally positive unit ε such that $\varepsilon^\sigma > 1$ for σ and $\varepsilon^\tau < 1$ for all $\tau \neq \sigma$. We can always find such a unit (see the proof of Dirichlet's unit theorem, Theorem 1.2.3). Then

$$\begin{aligned} c(\xi d a) &= \int_{F_A/F} f(1,x)\psi(-\xi x)d\mu(x)\exp(2\pi\mathrm{Tr}_{F/Q}(\xi)) \\ &= \int_{F_A/F} f(1,x)\psi(-\xi\varepsilon^n x)d\mu(x)\exp(2\pi\mathrm{Tr}_{F/Q}(\xi\varepsilon^n)) \\ &\leq \int_{F_A/F} |f(1,x)|\, d\mu(x)\exp(2\pi\mathrm{Tr}_{F/Q}(\xi\varepsilon^n)). \end{aligned}$$

Note that $\xi^\sigma\varepsilon^{\sigma n} \to -\infty$ as $n \to \infty$ and $\xi^\tau\varepsilon^{\tau n} \to 0$ as $n \to \infty$. Thus we know that $\exp(2\pi\mathrm{Tr}_{F/Q}(\xi\varepsilon^n)) \to 0$ as $n \to \infty$. This in particular shows that $c(\xi d a) = 0$ unless $\xi^\sigma \geq 0$ for all $\sigma \in I$. When $F = \mathbf{Q}$, this argument does not work and we need to impose the following condition:

(M3) f_t *has Fourier expansion of the following form:*

$$f_t(z) = \sum_{n \geq 0} a_n \exp(2\pi\sqrt{-1}\,nz) \text{ for all } t \in GL_2(F_{A_f}),$$

where n runs over a lattice of $\mathbf{Q}$. As for the constant term $a_0 = a_0(f_t)$, if we restrict t to be $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$ ($y \in F_{A_f}^\times$, $x \in F_A$), it is a function of y, and hence we write $a_0(y)$. Since f is invariant under left multiplication by $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ ($\alpha \in F^\times$) and under right multiplication by $\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}$ for $u \in \hat{O}^\times$, the function $y \mapsto a_0(y)$ factors through $F_{A_f}^\times/F^\times\hat{O}^\times$, which is the absolute class group. Thus we can define new functions $n \mapsto a(n;f)$ by $a(n;f) = c(\xi d a)$ if $n = \xi d a$ for $\xi \in F_+$ and $n \mapsto a_0(n;f)$ by $a_0(n;f) = a_0(yd^{-1})$ if $n = yO$. We denote by $\mathbf{M}_k(m,\chi)$ for the space of functions satisfying the conditions (M1-3). Then $f \in \mathbf{M}_k(m,\chi)$ has adelic Fourier expansion of the following type:

(5b) $$f(y,x) = a(y\vartheta;f)+\sum_{\xi\in F_+} a(\xi y\vartheta;f)e(\sqrt{-1}\,\xi y_\infty)e(\xi x),$$

where $n \mapsto a(n;f) \in \mathbf{C}$ is a function of fractional ideals vanishing outside integral ideals and $n \mapsto a_0(n;f)$ factors through the ideal class group of F. The space of cusp forms $\mathbf{S}_k(m,\chi)$ is the subspace of $\mathbf{M}_k(m,\chi)$ consisting of functions $f \in \mathbf{M}_k(m,\chi)$ satisfying the following cuspidal condition for the standard Haar measure $d\mu$ on F_A/F:

(S) $$\int_{F_A/F} f\left(\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}x\right)d\mu(u) = 0 \quad \text{for all} \quad x \in GL_2(F_A).$$

This just means the vanishing of the constant term of f_t for all t. Since $f_t|\alpha = f_{\alpha_f^{-1}t}$ for $\alpha \in GL_2(F)$ with $\det(\alpha) \in F_+$, this simply implies that f_t is a cusp form for all t.

When $F = \mathbf{Q}$, we know from (1b) that $GL_2(\mathbf{A}) = GL_2(\mathbf{Q})S(m)G_{\infty+}$ since $\mathbf{A}^\times = \mathbf{Q}^\times U(1)\mathbf{R}_+^\times$ (8.1.3a). We already know that f_t for $t = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ gives a homomorphic modular form in $\mathcal{M}_k(\Gamma_0(m),\chi^*)$ since $Cl(m) \cong (\mathbf{Z}/m)^\times$ and the character χ^* can be considered as a Dirichlet character. Conversely, starting from $\phi \in \mathcal{M}_k(\Gamma_0(m),\chi^*)$ and writing each $x \in GL_2(\mathbf{A})$ as αu with $\alpha \in GL_2(\mathbf{Q})$ and $u \in S(m)G_{\infty+}$, we define $f: GL_2(\mathbf{A}) \to \mathbf{C}$ by $f(x) = \chi_m(u)\phi(z)j_k(u_\infty,\mathbf{i})^{-1}$ for $z = u_\infty(\mathbf{i})$. We need to show that f is a well defined element in $\mathbf{M}_k(m,\chi)$. If $x = \alpha u = \alpha' u'$, then

$$GL_2(\mathbf{Q}) \ni \gamma = \alpha'^{-1}\alpha = u'u^{-1} \in S(m)G_{\infty+}$$

and hence $\gamma \in GL_2(\mathbf{Q})\cap S(m)G_{\infty+} = \Gamma_0(m)$. Then we see that

$$\chi_m(u')\phi(u'_\infty(\mathbf{i}))j_k(u'_\infty,\mathbf{i})^{-1} = \chi_m(\gamma u)\phi(\gamma(z))j_k(\gamma u_\infty,\mathbf{i})^{-1}$$
$$= \chi_m(u)\chi^*(\gamma)^{-1}\phi(\gamma(z))j_k(\gamma,z)^{-1}j_k(u_\infty,\mathbf{i})^{-1} = \chi_m(u)\phi(z)j_k(u_\infty,\mathbf{i})^{-1}.$$

Thus f(x) is well defined independently of the choice of α and u. It is obvious from (5.1.1a,b) that $f \in \mathbf{M}_k(m,\chi)$ and $f_1 = \phi$. Thus

(6) $\mathbf{M}_k(m,\chi) \cong \mathcal{M}_k(\Gamma_0(m),\chi^*)$ and $\mathbf{S}_k(m,\chi) \cong \mathcal{S}_k(\Gamma_0(m),\chi^*)$ via $f \mapsto f_1$.

In this sense, we can take $\mathbf{M}_k(m,\chi)$ as a generalization of the space $\mathcal{M}_k(\Gamma_0(m),\chi)$ for general totally real field F.

We have, for $t = \begin{pmatrix}a & 0\\ 0 & 1\end{pmatrix}$ and $f \in \mathbf{M}_k(m,\chi)$

(7) $\quad f_t(z) = \sum_{0 \ll \xi \in a^{-1}d^{-1}} c(\xi\vartheta a)\exp(2\pi\sqrt{-1}\,\mathrm{Tr}(\xi z))$ for $c(a) \in \mathbf{C}$.

In particular, when $F = \mathbf{Q}$ and $a = 1$, the above expansion has the usual form: $\sum_{n=0}^{\infty} c(n)\exp(2\pi\sqrt{-1}\,nz)$. In general,

$$c(y,\xi) = c(y\xi,1) = c(\xi dy\mathcal{O})\exp(-2\pi\mathrm{Tr}(\xi y)).$$

Thus we may regard the Fourier coefficient $c(a)$ as a function of integral ideals $a \mapsto c(a)$. The L-function of f is then defined by $L(s,f) = \sum_a c(a)N(a)^{-s}$. This function is known to have an analytic continuation and a functional equation similar to Hecke L-functions. These L-functions are first investigated in detail by Hecke and have now become very important tools in number theory. Of course, when $F = \mathbf{Q}$, this L-function is nothing but the one studied in §5.5. In this book, however, we do not go into details of the theory of such L-functions. We list [JL], [G] and [W3] as standard textbooks for this subject. Instead, we introduce now the Eisenstein series as an example of these modular forms and try to give some account of how to compute the Fourier coefficients of Eisenstein series when $F = \mathbf{Q}$ in the following section. Let $\Gamma = GL_2(F) \cap t^{-1}U(m)tG_{\infty+}$ for the above t. Thus

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(F) \mid a, d \in \mathcal{O},\ c \in am,\ d \in a^{-1},\ ad\text{-}bc \in E \right\},$$

where E is the group of all totally positive units in $\mathcal{O}^{\times}$. Let

$$\Gamma_{\infty} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c = 0 \right\}.$$

Then $j(\gamma,z)^k = (N(d)/|N(d)|)^k$ if $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma_{\infty}$. Thus we see $j(\gamma\delta,z)^k = j(\gamma,\delta(z))^k j(\delta,z)^k = (N(d)/|N(d)|)^k j(\delta,z)^k$ for $\gamma \in \Gamma_{\infty}$. Now we put for a character $\chi : (\mathcal{O}/m)^{\times} \to \mathbf{T}$ such that $\chi(\varepsilon) = (N(\varepsilon)/|N(\varepsilon)|)^k$

(8) $$E_{\Gamma}(z,s,\chi) = y^s \sum_{\gamma \in \Gamma_{\infty}\backslash\Gamma} \chi(\delta) j(\delta,z)^{-k} |j(\delta,z)|^{-2s},$$

where $\chi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \chi(d)$. Then this series is absolutely convergent if $\mathrm{Re}(s) > 1-(k/2)$ (see §§2.5 and 2.8, where we expressed Eisenstein series in terms of Shintani zeta functions) and $E_{\Gamma}(\gamma(z)) = \chi(\gamma)^{-1}E_{\Gamma}(z)j(\gamma,z)^k$ for $\gamma \in \Gamma$ by definition. We now interpret this definition in adelic language. In the adelic case, the object corresponding to the congruence subgroup Γ is $GL_2(F)$, and that of Γ_{∞} is $B_{\infty} = \mathcal{O}^{\times}B(F)$, where

$$B(F) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in F^\times \text{ and } b \in F \right\}.$$

Let $\chi : Cl(m) = F_A{}^\times/F^\times U(m)F_{\infty+} \to \mathbf{T}$ be a character and suppose that $\chi(x_\infty) = (N(x_\infty)/|N(x_\infty)|)^k$. We define the following functions on $GL_2(F_A)$:

$$(9) \quad \eta(x) = \begin{cases} |y|_A & \text{if } x = \begin{pmatrix} y & b \\ 0 & 1 \end{pmatrix} au \ (a \in F_A{}^\times \text{ and } u \in S(m)C_{\infty+}), \\ 0 & \text{otherwise} \end{cases}$$

and

$$\chi^\#\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{cases} \prod_{v \mid m} \chi_v(d_v) & \text{if } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in B(F_A)S(m)G_{\infty+}, \\ 0 & \text{otherwise.} \end{cases}$$

These functions are well defined. To see this, let $L_f = \hat{O}^2$ (column vectors). Then, if $\begin{pmatrix} y & b \\ 0 & 1 \end{pmatrix} au = \begin{pmatrix} y' & b' \\ 0 & 1 \end{pmatrix} a'u'$ as above, then looking at the second row of $a\begin{pmatrix} y & b \\ 0 & 1 \end{pmatrix} uL_f = a'\begin{pmatrix} y' & b' \\ 0 & 1 \end{pmatrix} u'L_f$ which only depends on a and a' because $uL_f = u'L_f$, we know $a\hat{O} = a'\hat{O}$. Thus $|a_f|_A = |a'_f|_A$. By taking the determinants of both sides, we then conclude that $|y_f|_A = |y'_f|_A$. On the other hand, $\mathrm{Im}(x_\infty(\mathbf{i})) = y_\infty = y'_\infty$, which shows that $|y|_A = |y'|_A$. Similarly $\chi^\#$ is well defined. By the product formula $|\xi|_A = 1$ for $\xi \in F^\times$ (8.1.5), we know that $\eta(\gamma x) = \eta(x)$ if $\gamma \in B_\infty$. We also see that $\chi^\#(\gamma x)j(\gamma x_\infty,\mathbf{i})^{-k} = \chi^\#(x)j(x_\infty,\mathbf{i})^{-k}$ for all $\gamma \in B_\infty$.

Exercise 2. Suppose that $\chi(x_\infty) = (N(x_\infty)/|N(x_\infty)|)^k$. Then show that $\chi^\#(\gamma x)j(\gamma x_\infty,\mathbf{i})^{-k} = \chi^\#(x)j(x_\infty,\mathbf{i})^{-k}$ for all $\gamma \in B_\infty$.

We define

$$E^*(x,s,\chi) = \textstyle\sum_{\gamma \in B_\infty \backslash GL_2(F)} \chi^\#(\gamma x)\eta(\gamma x)^s j_{-k}(\gamma x_\infty,\mathbf{i}).$$

Suppose that $x_f = t = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. Then $\gamma t \in B(F_A)S(m)G_{\infty+}$ if and only if $\chi^\#(\gamma t)\eta(\gamma t) \neq 0$. Write $\gamma = \begin{pmatrix} * & * \\ c & d \end{pmatrix}$, then if $\chi^\#\eta(\gamma x) \neq 0$, there exists $s \in S(m)$ with $s = \begin{pmatrix} * & * \\ ca & d \end{pmatrix}$. Thus $c \in a^{-1} = a^{-1}O$, $d \in O$ and $ca+dO = O$. This shows that we can find $e \in O$ and $f \in a^{-1}$ such that $cf\text{-}de = 1$. Namely $\delta = \begin{pmatrix} e & f \\ c & d \end{pmatrix} \in \Gamma$. One can easily show that this correspondence

$$B_\infty\backslash\{\gamma \mid \gamma t \in B(F_A)S(m)G_{\infty+}\} \ni \gamma \mapsto \delta \in \Gamma_\infty\backslash\Gamma$$

is bijective and thus each term of the summation of E_Γ and E^* can be naturally identified. Moreover by the above computation, writing $(\gamma t)_f = b_f s_f$ as above for $b \in B(A_F)$, we see that $\eta((\gamma t)_f) = |\det(b_f s_f)|_A = |\det(\gamma_f)|_A |a|_A$. On the other hand, $\eta((\gamma x)_\infty) = \mathrm{Im}(\gamma x_\infty(\mathbf{i})) = |j(\gamma, x_\infty(\mathbf{i}))|^{-2} |\det(\gamma_\infty)|_A \eta(x_\infty)$. Thus

$$\text{(10a)} \qquad \begin{aligned} \eta(\gamma t) &= |j(\gamma, x_\infty(\mathbf{i}))|^{-2} |\det(\gamma_\infty)|_A \mathrm{Im}(x_\infty(\mathbf{i})) |\det(\gamma_f)|_A |a|_A \\ &= |a|_A \mathrm{Im}(x_\infty(\mathbf{i})) |j(\gamma, x_\infty(\mathbf{i}))|^{-2}. \end{aligned}$$

Thus we know that

$$\text{(10b)} \qquad E^*(tx_\infty, s, \chi) j(x_\infty, \mathbf{i})^k = |a|_A^s E_\Gamma(x_\infty(\mathbf{i}), s, \chi^{*-1}),$$

because $\chi^*((d))\chi(d_m) = \chi(d) = 1$ for the ideal character χ^* associated with χ. This shows the convergence and we now know E^* corresponds to E_Γ naturally.

By definition, we have $E^*(\gamma x, s, \chi) = E^*(x, s, \chi)$ for $\gamma \in GL_2(F)$ and $E^*(ux, s, \chi) = \chi(u)E^*(x, s, \chi)$ for $u \in \hat{O}^\times$. Thus for $z \in F_{A_f}^\times$, the modular form $\chi^{-1}(z)|z|_A^k E^*(zx, s, \chi)$ depends only on the class of z modulo $\hat{O}^\times F^\times$. Note that $F_{A_f}^\times / \hat{O}^\times F^\times \cong F_A^\times / \hat{O}^\times F^\times F_\infty^\times$ which is isomorphic to the absolute ideal class group Cl of F. We now define

$$\text{(11)} \qquad \begin{aligned} &\mathbf{E}_k(x, s, \chi) = \mathbf{E}_{k,m}(x, s, \chi) = L_m(k+2s, \chi^{-1}) \textstyle\sum_{z \in \mathrm{Cl}} \chi^{-1}(z) |z|_A^k E^*(zx, s, \chi) \\ &\text{and } \mathbf{G}_k(x, s, \chi) = \mathbf{G}_{k,N}(x, s, \chi) = \chi(\det(x))\mathbf{E}_k(x\tau_f, s, \chi^{-1}), \end{aligned}$$

where $\tau = \begin{pmatrix} 0 & -1 \\ m & 0 \end{pmatrix}$ with a finite idele m such that $mO = \mathfrak{m}$ and $L_m(s, \chi^{-1}) = \sum_{\mathfrak{n}} \chi^{-1}(\mathfrak{n}) N(\mathfrak{n})^{-s}$ in which the sum is taken over $\mathfrak{n}$ prime to $\mathfrak{m}$. Note that for $z' \in F_A^\times$, we have

$$\begin{aligned} \textstyle\sum_{z \in \mathrm{Cl}} \chi^{-1}(z) |z|_A^k E^*(zz'x, s, \chi) &= \textstyle\sum_{z \in \mathrm{Cl}} \chi^{-1}(zz'^{-1}) |zz'^{-1}|_A^k E^*(zx, s, \chi) \\ &= \chi(z') |z'|_A^{-k} \textstyle\sum_{z \in \mathrm{Cl}} \chi^{-1}(z) E^*(zx, s, \chi). \end{aligned}$$

Thus $\mathbf{E}_k$ satisfies (M1) for $\chi_k : z \mapsto \chi(z)|z|_A^{-k}$. Using the fact that

$$\tau \begin{pmatrix} a & b \\ mc & d \end{pmatrix} \tau^{-1} = \begin{pmatrix} d & -c \\ -mb & a \end{pmatrix},$$

we conclude easily that $\mathbf{G}_k$ also satisfies (M1) for χ_k. We now state the principal result:

Theorem 1 (Hecke-Shimura). *Let* χ *be a finite order Hecke character modulo* m. *Define a function on the set of fractional ideals by* $\sigma_{m,\chi}(a) = \sum_{\mathfrak{b}\supset a}\chi(\mathfrak{b})N(\mathfrak{b})^m$ *and* $\sigma'_{m,\chi}(a) = \sum_{\mathfrak{b}\supset a}\chi(a/\mathfrak{b})N(\mathfrak{b})^m$ *if* a *is integral and otherwise* $\sigma_{m,\chi}(a) = \sigma'_{m,\chi}(a) = 0$. *Here we understand* $\chi(a) = 0$ *if* a and m *have a non-trivial common factor. Let* k *be a positive integer such that* $\chi(x_\infty) = \dfrac{N(x_\infty)^k}{|N(x_\infty)|^k}$. *Then* $\mathbf{E}_{k,m}(x,s,\chi)$ *and* $\mathbf{G}_{k,m}(x,s,\chi)$ *can be continued to meromorphic functions in* s *so that there exists a non-zero entire function* f *in* s *such that* $f(s)\mathbf{G}_k(x,s,\chi)$ *and* $f(s)\mathbf{E}_k(x,s,\chi)$ *are entire. Moreover they are finite at* $s = 0$, *and except when* $k = 2$, $F = \mathbf{Q}$, *and* χ *is trivial, we have*

$$\mathbf{G}_{k,m}\left(\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}, 1\text{-}k, \chi\right) = C'\{2^{-[F:\mathbf{Q}]}L_m(1\text{-}k,\chi) + \sum_{0\ll\xi\in F}\sigma_{k\text{-}1,\chi}(\xi dy\mathcal{O})e(i\xi_\infty y_\infty)e(\xi x)\},$$

and if $m \neq \mathcal{O}$,

$$\mathbf{G}_{k,m}\left(\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}, 0, \chi\right) = C\{\delta_{k,1}2^{-[F:\mathbf{Q}]}L_m(0,\chi) + \sum_{0\ll\xi\in F}\sigma'_{k\text{-}1,\chi}(\xi dy\mathcal{O})e(i\xi_\infty y_\infty)e(\xi x)\},$$

where C *and* C' *are non-zero constants depending on* k *and* m. *In the exceptional case when* $F = \mathbf{Q}$, χ *is trivial and* $k = 2$, $\mathbf{G}_{2,m}(x,0,\mathrm{id})$ *is non-holomorphic.*

Here $e(i\xi_\infty y_\infty)e(\xi x_\infty) = \exp(2\pi i\mathrm{Tr}(\xi z))$ for $z = x_\infty + iy_\infty$ and $i = \sqrt{-1}$. We will prove this theorem for $F = \mathbf{Q}$ in the following two sections. A proof for the general fields F can be found in [Sh9] and [H8, §6].

§9.2. Fourier expansion of Eisenstein series

In this section, we assume that $F = \mathbf{Q}$ and compute the Fourier coefficients of Eisenstein series. I follow Shimura [Sh2, 7, 9] in this computation, which can be generalized to bigger groups (e.g. symplectic and unitary groups as was done in [Sh9]). We exploit the fact that our group is GL(2) to simplify the computation in many places. We restate the definition of the Eisenstein series when $F = \mathbf{Q}$. Let N be a positive integer. We change the notation here and the ideal $N\mathbf{Z}$ plays the role of m in the previous section. We first prove Theorem 1.1 when $N > 1$. We will later remove this assumption to include the special case of $N = 1$. Let $\chi : (\mathbf{Z}/N\mathbf{Z})^\times = \mathrm{Cl}(N) \to \mathbf{C}^\times$ be a Dirichlet character with $\chi(-1) = (-1)^k$ $(0 < k \in \mathbf{Z})$. We define two functions $\eta,\chi^\# : \mathrm{GL}_2(\mathbf{A}) \to \mathbf{C}$ by

$$\eta(x) = \begin{cases} |y|_A & \text{if } x = \begin{pmatrix} y & b \\ 0 & 1 \end{pmatrix} au \ (u \in S(N)C_{\infty+} \ a \in A^\times), \\ 0 & \text{otherwise,} \end{cases}$$

$$\chi^\#\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{cases} \Pi_{p|N}\chi_p(d_p) & \text{if } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in B(A)S(N)G_{\infty+}, \\ 0 & \text{otherwise.} \end{cases}$$

Then the function $x \mapsto \chi^\#\eta(x)^s j(x_\infty,i)^{-k}$ is invariant under left multiplication by elements in $B = \{\pm\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbf{Q}^\times, b \in \mathbf{Q}\}$. Then

$$E^*(x,s,\chi) = \sum_{\gamma\in B\backslash GL_2(\mathbf{Q})}\chi^\#(\gamma x)\eta(\gamma x)^s j(\gamma_\infty x_\infty,i)^{-k}$$
$$= \sum_{\gamma\in B_+\backslash GL_2(\mathbf{Q})_+}\chi^\#(\gamma x)\eta(\gamma x)^s j(\gamma_\infty x_\infty,i)^{-k},$$

where $GL_2(\mathbf{Q})_+ = \{\alpha \in GL_2(\mathbf{Q}) \mid \det(\alpha) > 0\}$ and $B_+ = B\cap GL_2(\mathbf{Q})_+$. Put $\varepsilon = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We compute the Fourier expansion of $E(x,s) = E^*(x\varepsilon_f^{-1},s,\chi)$ and later relate it to the Eisenstein series $G_k(x,s,\chi)$ in the theorem. Note that $E(\gamma x,s) = E(x,s)$ for all $\gamma \in GL_2(\mathbf{Q})$, and hence $E(x,s)$ has a Fourier expansion. We define its Fourier coefficients for $\xi \in F$ by

$$b(\xi,w,s) = \int_{A/\mathbf{Q}} E(\alpha(x)w,s)e(-\xi x)d\mu(x),$$

where $w \in A^\times B(A)$, μ is the additive Haar measure on $A/\mathbf{Q}$ such that $\mu(A/\mathbf{Q}) = 1$ and $\alpha(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$. We observe that

$$b(\xi,w,s) = \int_{A/\mathbf{Q}} E(\alpha(x)w,s)e(-\xi x)d\mu(x) = \int_{A/\mathbf{Q}} E^*(\alpha(x)w\varepsilon_f^{-1},s)e(-\xi x)d\mu(x)$$
$$= \int_{A/\mathbf{Q}}\sum_{\gamma\in B_{\infty+}\backslash GL_2(\mathbf{Q})_+}\chi^\#(\gamma\alpha(x)w\varepsilon_f^{-1})\eta(\gamma\alpha(x)w\varepsilon_f^{-1})^s j(\gamma_\infty(\alpha(x)w)_\infty,i)^{-k}e(-\xi x)d\mu(x).$$

Suppose that $w \in A^\times B(A)_+$. Then the non-triviality of

$$\chi^\#(\gamma\alpha(x)w\varepsilon_f^{-1})\eta(\gamma\alpha(x)w\varepsilon_f^{-1})^s$$

means that $\gamma\alpha(x)w\varepsilon_f^{-1} \in B(A)S(N)G_{\infty+}$ and $\gamma\alpha(x)w \in B(A)S(N)G_{\infty+}\varepsilon_f$. Since $u \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \bmod N$ for all $u \in S(N)$, if we write $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $c \neq 0$. Thus $\gamma = \begin{pmatrix} c^{-2}\det(\gamma) & c^{-1}a \\ 0 & 1 \end{pmatrix} c\varepsilon\alpha(c^{-1}d)$. That is, $\gamma \in B_{\infty+}\mathbf{Q}^\times\varepsilon U$ for $U = \{\alpha(x) \mid x \in \mathbf{Q}\}$. Thus $B_+\backslash B_+\mathbf{Q}^\times\varepsilon U \cong \mathbf{Q}_+\varepsilon U$. Hence we see that

$$b(\xi,w,s) = \int_{A/Q} \sum_{\gamma\in Q_+,\delta\in Q} \chi^{\#}(\varepsilon\gamma\alpha(x+\delta)w\varepsilon_f^{-1})\eta(\varepsilon\gamma\alpha(x+\delta)w\varepsilon_f^{-1})^s j(\gamma_\infty(\alpha(x+\delta)w)_\infty,i)^{-k}e(-\xi x)d\mu.$$

We now prove a lemma, which shows that the above summation with respect to $\gamma \in \mathbf{Q}$ is in fact reduced to the summation over a fractional ideal of $\mathbf{Q}$.

Lemma 1. *Write* $w = \alpha(x)a\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} = a\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$ *for* $a \in \mathbf{A}^\times$. *Then we have* $(\varepsilon w\varepsilon^{-1})_f \in B(\mathbf{A}_f)S(N)$ *(i.e.* $\chi^{\#}(\varepsilon w\varepsilon_f^{-1}) \neq 0$*) if and only if*

$$x \in a^{-1}N\hat{\mathbf{Z}},\ a \in y^{-1}\hat{\mathbf{Z}} \text{ and } ax\mathbf{Z}+ay\mathbf{Z} = \mathbf{Z}.$$

Proof. By computation, we see that $(\varepsilon w\varepsilon^{-1})_f = \begin{pmatrix} a & 0 \\ -ax & ay \end{pmatrix}_f$. From this, $\begin{pmatrix} a & 0 \\ -ax & ay \end{pmatrix}_f \in B(\mathbf{A})S(N)$ implies $ax \in N\hat{\mathbf{Z}}$, $ay \in \hat{\mathbf{Z}}$ and $ax\hat{\mathbf{Z}}+ay\hat{\mathbf{Z}} = \hat{\mathbf{Z}}$ ($\Leftrightarrow ax\mathbf{Z}+ay\mathbf{Z} = \mathbf{Z}$). On the other hand, if $ax \in N\hat{\mathbf{Z}}$, $ay \in \hat{\mathbf{Z}}$ and $ax\hat{\mathbf{Z}}+ay\hat{\mathbf{Z}} = \hat{\mathbf{Z}}$, then we can find $t,s \in \hat{\mathbf{Z}}$ such that $axt+ays = 1$ and $u = \begin{pmatrix} s & t \\ -ax & ay \end{pmatrix} \in S(N)$ and

$$(\varepsilon w\varepsilon^{-1})_f u^{-1} = \begin{pmatrix} a^2y & -at \\ 0 & 1 \end{pmatrix} \in B(\mathbf{A}), \tag{1}$$

which shows the converse.

Applying the above lemma to $\gamma\alpha(x+\delta)\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}$ (instead of w itself) for a given $\gamma \in y^{-1}\mathbf{Z}$, we see that

$$\chi^{\#}(\varepsilon\gamma\alpha(x+\delta)w\varepsilon_f^{-1}) \neq 0 \Leftrightarrow \gamma(x+\delta) \in N\hat{\mathbf{Z}} \text{ and } \gamma(x+\delta)\hat{\mathbf{Z}}+\gamma y\hat{\mathbf{Z}} = \hat{\mathbf{Z}}.$$

Let $\Phi = \Phi_\gamma : \mathbf{A}_f \to \mathbf{C}$ be the following function depending on γ and y: $\Phi(x) = \prod_p \Phi_p(x_p)$ and Φ_p is the characteristic function of $N\mathbf{Z}_p$ if $\gamma y_p\mathbf{Z}_p = \mathbf{Z}_p$ and Φ_p is a characteristic function of $\mathbf{Z}_p^\times$ if $p\mathbf{Z}_p \supset \gamma y_p\mathbf{Z}_p$. Thus if $N\hat{\mathbf{Z}}+\gamma y\hat{\mathbf{Z}} = \hat{\mathbf{Z}}$ (i.e. $\gamma y\mathbf{Z}$ is prime to N), then $\chi^{\#}(\varepsilon\gamma\tau(x+\delta)w\varepsilon_f^{-1}) \neq 0$ if and only if $\Phi(\gamma(x+\delta)) = 1$. Thus we see that

$$\begin{aligned} b(\xi,w,s) &= \int_{A/Q} \sum_{\gamma\in Q_+,\delta\in Q} \chi^{\#}(\varepsilon\gamma\alpha(x+\delta)w\varepsilon_f^{-1})\Phi_\gamma(\gamma(x+\delta))\,\eta(\varepsilon\gamma\alpha(x+\delta)w\varepsilon_f^{-1})^s \\ &\qquad \times j(\gamma_\infty(\alpha(x+\delta)w)_\infty,i)^{-k}e(-\xi x)d\mu(x) \\ &= \sum_{0<\gamma\in y^{-1}\mathbf{Z}} \int_A \chi^{\#}(\varepsilon\gamma\alpha(x)w\varepsilon_f^{-1})\Phi(\gamma x)\eta(\varepsilon\gamma\alpha(x)w\varepsilon_f^{-1})^s j(\gamma_\infty(\alpha(x)w)_\infty,i)^{-k}e(-\xi x)d\mu(x), \end{aligned}$$

where γ runs over $y^{-1}\mathbf{Z}\cap\mathbf{R}_+$ such that $\gamma y\mathbf{Z}+N\mathbf{Z}=\mathbf{Z}$. By (1), we can compute $\chi^{\#}(\varepsilon\gamma\alpha(x)w\varepsilon_f^{-1})\eta(\varepsilon\gamma\alpha(x)w\varepsilon_f^{-1})$ explicitly:

Lemma 2. *Suppose that* $\Phi(\gamma x)=1$ *and* $\gamma x\mathbf{Z}+\gamma y\mathbf{Z}=\mathbf{Z}$ *for* $\gamma\in\mathbf{Q}_+$ *and* $y\in\mathbf{A}^\times$. *Then we have for* $w=\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix}$ *and* $z=x_\infty+\sqrt{-1}\,y_\infty\in\mathcal{H}$

$$\eta(\varepsilon\gamma\alpha(x)w\varepsilon_f^{-1})=|\gamma_f^2y|_{\mathbf{A}}|z|^{-2} \text{ and } \chi^{\#}(\varepsilon\gamma\alpha(x)w\varepsilon_f^{-1})=\prod_{p|N}\chi_p(\gamma_p y_p).$$

Therefore, for $\chi_N(\gamma y)=\prod_{p|N}\chi_p(\gamma_p y_p)$

$$b(\xi,\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix},s)=\sum_{0<\gamma\in y^{-1}\mathbf{Z}}\int_{\mathbf{A}}\Phi(\gamma x)\chi_N(\gamma y)|\gamma_f^2y|_{\mathbf{A}}^s(\gamma_\infty z)^{-k}|z|^{-2s}e(-\xi x)d\mu(x)$$
$$=\chi(y)\sum_{0<\gamma\in y^{-1}\mathbf{Z}}\chi^{-1}(\gamma y\mathbf{Z})\gamma^{2s-k}|y_f|_{\mathbf{A}}^s\int_{\mathbf{A}}\Phi(\gamma x)z^{-k}|y_\infty|^s|z|^{-2s}e(-\xi x)d\mu(x),$$

because $\chi(\gamma^{(N)}y^{(N)})\chi_N(\gamma y)=\chi(y)$ and $\chi(\gamma^{(N)}y^{(N)})=\chi(\gamma y\mathbf{Z})$ as the ideal character (where $y^{(N)}\prod_{p|N}y_p=y$).

Now we compute the following two integrals:

$$b_f(\xi,\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix},s)=\chi(y)\sum_{0<\gamma\in y^{-1}\mathbf{Z}}\chi^{-1}(\gamma y\mathbf{Z})\gamma^{2s-k}|y_f|_{\mathbf{A}}^s\int_{\mathbf{A}_f}\Phi(\gamma x)e(-\xi x)d\mu_f(x) \text{ and}$$
$$y^{-s}b_\infty(\xi,\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix},s)=\int_{-\infty}^{\infty}(x+iy)^{-k}|x+iy|^{-2s}\exp(-2\pi i\xi x)dx.$$

Then of course, $b(\xi,\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix},s)=b_f(\xi,\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix},s)b_\infty(\xi,\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix},s)$. We first compute the finite part of the integral. First suppose that $\gamma y_p\mathbf{Z}_p=\mathbf{Z}_p$ ($\Leftrightarrow \gamma\mathbf{Z}_p=y_p^{-1}\mathbf{Z}_p$). Then

$$\int_{\mathbf{Q}_p}\Phi(\gamma x_p)e_p(-\xi x_p)d\mu_p(x)=|\gamma|_p^{-1}\int_{\mathbf{Q}_p}\Phi(x)e_p(-\xi\gamma^{-1}x_p)d\mu_p(x)$$
$$=|\gamma|_p^{-1}\int_{N\mathbf{Z}_p}e_p(-\xi\gamma^{-1}x)d\mu_p(x)=|\gamma^{-1}N|_p\int_{\mathbf{Z}_p}e_p(-\xi\gamma^{-1}Nx)d\mu_p(x)$$
$$=\begin{cases}|y_pN|_p & \text{if } \xi\gamma^{-1}N\in\mathbf{Z}_p \text{ (i.e. } \xi\in N^{-1}y_p^{-1}\mathbf{Z}_p),\\ 0 & \text{otherwise.}\end{cases}$$

Next suppose that $p\mathbf{Z}_p\supset\gamma y_p\mathbf{Z}_p$ ($\Leftrightarrow y_p^{-1}\mathbf{Z}_p\supset\gamma p^{-1}\mathbf{Z}_p$) (in particular, p is prime to N). Then we have

$$\int_{\mathbf{Q}_p}\Phi(\gamma x)e_p(-\xi x)d\mu_p(x)=|\gamma|_p^{-1}\int_{\mathbf{Q}_p}\Phi(x)e_p(-\xi\gamma^{-1}x)d\mu_p(x)$$
$$=|\gamma|_p^{-1}\int_{\mathbf{Z}_p^\times}e_p(-\xi\gamma^{-1}x)d\mu_p(x)=|\gamma|_p^{-1}\sum_a\int_{a+p\mathbf{Z}_p}e_p(-\xi\gamma^{-1}x)d\mu_p(x)=0$$

if $x \mapsto e_p(\xi\gamma^{-1}x)$ is non-trivial on $p\mathbf{Z}_p$, i.e. $\xi\gamma^{-1} \notin p^{-1}\mathbf{Z}_p$. Thus we may assume that $\xi \in y_p^{-1}\mathbf{Z}_p$. Then

$$\int_{Q_p}\Phi(\gamma x)e_p(-\xi x)d\mu_p(x) = \sum_{r\in\gamma^{-1}Z_p^\times/y_pZ_p} e_p(-\xi r)\int_{a+y_pZ_p} e_p(-\xi x)d\mu_p(x)$$
$$= |y_p|_p\sum_{r\in\gamma^{-1}Z_p^\times/y_pZ_p} e_p(-\xi r).$$

Thus we know that if $\xi \in y^{-1}N^{-1}\mathbf{Z}$, then

$$b_f(\xi,\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix},s) = \chi(y) \sum_{0<\gamma\in y^{-1}Z}\chi^{-1}(\gamma yZ)\gamma^{2s-k}|y_f|_A^{s+1}N^{-1}\sum_{r\in\gamma^{-1}NZ_f^\times/yNZ_f} e(-\xi r)$$
$$= \chi(y)|y_f|_A^{-s-k+1}N^{-1} \sum_{0<\gamma\in y^{-1}Z}\chi^{-1}(\gamma yZ)|(\gamma y)_f|_A^{2s+k}\sum_{r\in(Z/\gamma yZ)^\times}\exp(-2\pi i\xi rN/\gamma).$$

To compute this sum, we introduce the Möbius function μ on the set of ideals with values in $\{\pm1,0\}$. Let $\lambda : \mathbf{Z} \to \mathbf{C}$ be any Dirichlet character and consider the L-function

$$L(s,\lambda) = \prod_p(1-\lambda(p)p^{-s})^{-1} = \sum_{n=1}^\infty \lambda(n)n^{-s}.$$

Then write $L(s,\lambda)^{-1}$ in the form of a Dirichlet series $\sum_{n=1}^\infty\mu(n)\lambda(n)n^{-s}$. Then

$$\sum_{n=1}^\infty \mu(n)\lambda(n)n^{-s} = \prod_p(1-\lambda(p)p^{-s}) = L(s,\lambda)^{-1}$$

and hence $\mu(1) = 1$, $\mu(p) = -1$ for a prime p and $\mu(p_1p_2\cdot\cdots\cdot p_r) = (-1)^r$ for distinct primes p_j and $\mu(n) = 0$ if n has a square factor. For any positive integer m, by the above definition, we see that

$$\prod_{p|m}(1+\mu(p)p^{-s}) = \sum_{0<d|m}\mu(d)d^{-s}.$$

In particular, if we specialize $s = 0$, then we see that

$$\sum_{0<d|m}\mu(d) = \begin{cases} 1 & \text{if } m = 1, \\ 0 & \text{if } m > 1. \end{cases}$$

Thus for positive integers m and n,

$$\sum_{r\in(Z/mZ)^\times}\exp(-2\pi irn/m) = \sum_{r\in(Z/mZ)}\exp(-2\pi irn/m)\sum_{0<d|(r,m)}\mu(d).$$

We want to interchange the two summations: for each divisor d of m, the r with $d|(r,m)$ is just the multiples of d; thus such an r runs over the set

$$\{d, 2d, \ldots, (m/d)d\}.$$

Thus

$$\sum_{r\in(\mathbf{Z}/m\mathbf{Z})}\exp(-2\pi irn/m)\sum_{0<d\,|\,(r,m)}\mu(d) = \sum_{0<d\,|\,m}\mu(d)\sum_{j=1}^{m/d}\exp(-2\pi ijdn/m)$$
$$= \sum_{d\,|\,m}\mu(m/d)\sum_{j=1}^{d}\exp(-2\pi ijn/d) \text{ by } d\mapsto m/d.$$

Note that by the orthogonality relation of characters of $\mathbf{Z}/d\mathbf{Z}$

$$\sum_{j=1}^{d}\exp(-2\pi ijn/d) = \begin{cases} 0 & \text{if } n \text{ is not divisible by } d, \\ d & \text{if } d\,|\,n. \end{cases}$$

This shows that

$$\sum_{r\in(\mathbf{Z}/m\mathbf{Z})}\exp(-2\pi irn/m)\sum_{0<d\,|\,(r,m)}\mu(d) = \sum_{0<d\,|\,(m,n)}\mu(m/d)d.$$

From this fact, we conclude that

$$b_f(\xi,\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix},s)$$
$$= \chi(y)\,|\,y_f\,|_{\mathbf{A}}^{-s-k+1}N^{-1}\sum_{0<\gamma\in y^{-1}\mathbf{Z}}\chi^{-1}(\gamma y\mathbf{Z})\,|\,(\gamma y)_f\,|_{\mathbf{A}}^{2s+k}\sum_{r\in(\mathbf{Z}/\gamma y\mathbf{Z})^\times}\exp(-2\pi i\xi rNy/\gamma y)$$
$$= \chi(y)\,|\,y_f\,|_{\mathbf{A}}^{-s-k+1}N^{-1}\sum_{\mathbf{Z}\supset\gamma y\mathbf{Z}}\chi^{-1}(\gamma y\mathbf{Z})\,|\,(\gamma y)_f\,|_{\mathbf{A}}^{2s+k}\sum_{0<d\,|\,(\gamma y,\xi Ny)}\mu(\gamma y\mathbf{Z}/d)d$$
$$= \chi(y)\,|\,y_f\,|_{\mathbf{A}}^{-s-k+1}N^{-1}\sum_{n=1}^{\infty}\chi^{-1}(n)n^{-2s-k}\sum_{0<d\,|\,(n,\xi Ny)}\mu(n/d)d.$$

We again want to interchange the two summations as above. For each divisor $0<d$ of $\xi N/\gamma$, n runs through all positive multiples md of d. Thus

$$\sum_{n=1}^{\infty}\chi^{-1}(n)n^{-2s-k}\sum_{0<d|(n,\xi N/\gamma)}\mu(n/d)d = \sum_{d\,|\,\xi N/\gamma}\sum_{m=1}^{\infty}\chi^{-1}(md)(md)^{-2s-k}d\mu(m)$$
$$= \sum_{0<d\,|\,\xi N/\gamma}\chi^{-1}(d)d^{-2s-k+1}\sum_{m=1}^{\infty}\mu(m)\chi^{-1}(m)m^{-2s-k}$$
$$= L(2s+k,\chi^{-1})^{-1}\sum_{0<d\,|\,\xi N/\gamma}\chi^{-1}(d)d^{-2s-k+1}$$
$$= \begin{cases} L(2s+k,\chi^{-1})^{-1}\sum_{0<d\,|\,\xi N/\gamma}\chi^{-1}(d)d^{-2s-k+1} & \text{if } \xi\neq 0, \\ L(2s+k,\chi^{-1})^{-1}L(2s+k-1,\chi^{-1}) & \text{if } \xi = 0. \end{cases}$$

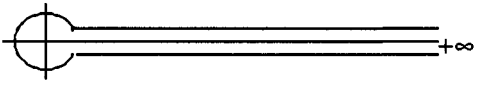
We now know that

$$(2)\qquad L(2s+k,\chi^{-1})b_f(\xi,\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix},s)$$
$$= \chi(y)\,|\,y_f\,|_{\mathbf{A}}^{-s-k+1}N^{-1}\times\begin{cases} \sum_{d\mathbf{Z}\supset\xi Ny\mathbf{Z}}\chi^{-1}(d)d^{-2s-k+1} & \text{if } \xi\neq 0, \\ L(2s+k-1,\chi^{-1}) & \text{if } \xi = 0. \end{cases}$$

Now we compute $y^{-s}b_\infty(\xi,\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix},s) = \int_{-\infty}^{\infty}(x+iy)^{-k}\,|\,x+iy\,|^{-2s}\exp(-2\pi i\xi x)dx$.

Consider the function $\zeta(z;\alpha,\beta) = \int_0^\infty e^{-zx}(x+1)^{\alpha-1}x^{\beta-1}dx$ for $z\in\mathbf{C}$ with $\mathrm{Re}(z)>0$ and $\alpha,\beta\in\mathbf{C}$. Here for $z\in\mathbf{C}^\times$ $z^\alpha = |\,z\,|^\alpha e^{i\alpha\theta}$ writing

$z = |z|e^{i\theta}$ with $-\pi < \theta \le \pi$. Then one knows that this integral is convergent if $\mathrm{Re}(\beta) > 0$ by a standard estimate. The divergence of the integral when $\mathrm{Re}(s) \le 0$ is caused by the singularity at 0 of the integrand. Thus by converting the integral into a contour integral on

$P(\varepsilon)$: 

for sufficiently small $\varepsilon > 0$, we can avoid the singularity at 0 and have an integral expression for $(e^{2\pi i\beta}-1)\zeta(z;\alpha,\beta)$, which is convergent for all $\beta \in \mathbf{C}$:

$$(e^{2\pi i\beta}-1)\zeta(z;\alpha,\beta) = z^{-\beta}\int_{P(\varepsilon)}(1+z^{-1}t)^{\alpha-1}t^{\beta-1}e^{-t}dt \quad \text{(see §2.2).}$$

Thus the function $(e^{2\pi i\beta}-1)\zeta(z;\alpha,\beta)$ is holomorphic on the whole space $H' \times \mathbf{C} \times \mathbf{C}$, where $H' = \{z \in \mathbf{C} \mid \mathrm{Re}(z) > 0\}$. By using the well known formula: $\Gamma(\beta)\Gamma(1-\beta) = 2\pi i(e^{\pi i\beta}-e^{-\pi i\beta})^{-1}$, we know that

$$\omega(z;\alpha,\beta) = z^{\beta}\Gamma(\beta)^{-1}\zeta(z;\alpha,\beta) = \frac{e^{-\pi i\beta}}{2\pi i}\Gamma(1-\beta)\int_{P(\varepsilon)}(1+z^{-1}t)^{\alpha-1}t^{\beta-1}e^{-t}dt$$

is also holomorphic on $H' \times \mathbf{C}^2$. When $\beta = 0$, by computing the residue of $(1+z^{-1}t)^{\alpha-1}t^{\beta-1}e^{-t}$ at $t = 0$ (see the computation in Exercise 2.2.1), we know that $\omega(z;\alpha,0) = 1$. On the other hand, when $\alpha = 1$,

$$\int_{P(\varepsilon)}(1+z^{-1}t)^{\alpha-1}t^{\beta-1}e^{-t}dt = \int_{P(\varepsilon)}t^{\beta-1}e^{-t}dt = (e^{2\pi i\beta}-1)\Gamma(\beta) \quad \text{(see (2.2.2)).}$$

Thus we again obtain $\omega(z;1,\beta) = 1$ by $\Gamma(\beta)\Gamma(1-\beta) = 2\pi i(e^{\pi i\beta}-e^{-\pi i\beta})^{-1}$. Actually we will prove the following functional equation in Lemma 3.1 (see [Sh6]):

$$\omega(z;1-\beta,1-\alpha) = \omega(z;\alpha,\beta);$$

and the above evaluation follows if one knows either $\omega(z;1,\beta) = 1$ or $\omega(z;\alpha,0) = 1$.

Lemma 3. *We have*

$$y^{-s}b_\infty(\xi,\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix},s) = \int_{-\infty}^{\infty}(x+iy)^{-k}\,|x+iy|^{-2s}\exp(-2\pi i\xi x)dx$$

$$= \begin{cases} i^{-k}(2\pi)^{k+s}\Gamma(k+s)^{-1}(2y)^{-s}\xi^{k+s-1}e^{-2\pi\xi y}\omega(4\pi\xi y;k+s,s) & \textit{if } \xi > 0, \\ i^{-k}(2\pi)^{s}\Gamma(s)^{-1}(2y)^{-s-k}|\xi|^{s-1}e^{-2\pi|\xi|y}\omega(4\pi|\xi|y;s,k+s) & \textit{if } \xi < 0, \\ i^{-k}(2\pi)^{k+2s}\Gamma(k+s)^{-1}\Gamma(s)^{-1}\Gamma(k+2s-1)(4\pi y)^{1-k-2s} & \textit{if } \xi = 0. \end{cases}$$

We will give a proof of this lemma later. By admitting this lemma, we now write down, for $\Gamma_{\mathbf{C}}(s) = (2\pi)^{-s}\Gamma(s)$,

$$\text{(3a)}\quad L(2s+k,\chi)\chi(y)E^*(\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}\varepsilon_f^{-1},s,\chi^{-1})$$

$$= i^{-k}2^{-s}\{\frac{2\pi}{N}(2\,|\,y\,|_A)^{1-k-s}\frac{\Gamma(2s+k-1)L(2s+k-1,\chi)}{\Gamma(k+s)\Gamma(s)}$$

$$+\frac{N^{-s-k}}{\Gamma_C(s+k)}\sum_{n=1}^{\infty}|(ny)_f|_A^{-s-k+1}\sigma_{-2s-k+1,\chi}(ny\mathbf{Z})e(\frac{nz+(nx)_f}{N})\omega(4\pi\frac{ny_\infty}{N};k+s,s)$$

$$+(2\,|\,y\,|_A)^{-k}\frac{N^{-s}}{\Gamma_C(s)}\sum_{n=1}^{\infty}|(ny)_f|_A^{1-s}\sigma_{-2s-k+1,\chi}(ny\mathbf{Z})e(-\frac{n\bar{z}+(nx)_f}{N})\omega(4\pi\frac{ny_\infty}{N};s,k+s)\},$$

where $\sigma_{s,\chi}(y\mathbf{Z}) = \sum_{d\mathbf{Z}\supset y\mathbf{Z}}\chi(d)d^s$ and $z = x_\infty+iy_\infty$. Let $\tau = \begin{pmatrix} 0 & -1 \\ N & 0\end{pmatrix}$. Then we see from $\chi((-N)_f) = \chi((-N)_\infty)^{-1} = (-1)^k$, $E^*(zx) = \chi(z)\,|\,z\,|_A^{-k}E^*(x)$ and

$$(-N^{-1})_f\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}\tau_f = \begin{pmatrix} y_f & Nx_f \\ 0 & 1\end{pmatrix}\begin{pmatrix} y_\infty & Nx_\infty \\ 0 & 1\end{pmatrix}\varepsilon_f^{-1}$$

that

$$\text{(3b)}\quad G_k(\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix},s,\chi) = (-1)^kN^kL(2s+k,\chi)\chi(y)E^*((-N^{-1})_f\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}\tau_f,s,\chi^{-1})$$

$$= (-N)^kL(2s+k,\chi)\chi(y)E^*(\begin{pmatrix} y_f & Nx_f \\ 0 & 1\end{pmatrix}\begin{pmatrix} y_\infty & Nx_\infty \\ 0 & 1\end{pmatrix}\varepsilon_f^{-1},s,\chi^{-1})$$

$$= i^k2^{-s}N^{-s}\{2\pi(2\,|\,y\,|_A)^{1-k-s}\frac{\Gamma(k+2s-1)L(2s+k-1,\chi)}{\Gamma(k+s)\Gamma(s)}$$

$$+\Gamma_C(s+k)^{-1}\sum_{n=1}^{\infty}|(ny)_f|_A^{-s-k+1}\sigma_{-2s-k+1,\chi}(ny\mathbf{Z})e(nz+(nx)_f)\omega(4\pi ny_\infty;k+s,s)$$

$$+\Gamma_C(s)^{-1}(2\,|\,y\,|_A)^{-k}\ \sigma_{-2s-k+1,\chi}(ny\mathbf{Z})e(-n\bar{z}-(nx)_f)\omega(4\pi ny_\infty;s,k+s)\}.$$

The explicit Fourier expansion (3a,b) shows the analytic continuability of $\mathbf{E}_k$ and $\mathbf{G}_k$ because we already know the meromorphy of $L(s,\chi)$ and by an estimate similar to (5.1.4a,b), we easily know the convergence of the Fourier expansion for all $s \in \mathbf{C}$ as long as the constant term is finite. Writing $m\mathbf{Z}$ $(0 < m \in \mathbf{Z})$ for $ny\mathbf{Z}$, we see that

$$|(ny)_f|_A^{1-k-s}\sigma_{-2s-k+1,\chi}(ny\mathbf{Z})\,|_{s=0} = m^{k-1}\sum_{0<d\,|\,m}\chi(d)d^{1-k}$$

$$= \sum_{0<d\,|\,m}\chi(d)(m/d)^{k-1} \overset{m/d\mapsto d}{=} \sum_{0<d\,|\,m}\chi(m/d)d^{k-1} = \sigma'_{k-1,\chi}(m).$$

Noting that

$$\{\Gamma(2s)/\Gamma(s)\}\,|_{s=0} = 2^{-1} \text{ and } \mathrm{Res}_{s=0}L(2s+1,\chi) = 2^{-1}\delta_{\chi,\mathrm{id}}\prod_{p\,|\,N}(1-p^{-1}),$$

we now know from the above formula and (3b) that for $0 < k \in \mathbf{Z}$, $C = \sqrt{-1}^k(k-1)!^{-1}(2\pi)^k$ and for $u_z = \begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}$

$$\text{(4a)}\quad G_k(u_z,0,\chi) = C\left\{\frac{\delta_{k,1}L_L(0,\chi)}{2} - \frac{\delta_{k,2}\delta_{\chi,\mathrm{id}}\varphi(L)}{L(8\pi|y|_A)} + \sum_{n=1}^{\infty}\sigma'_{k-1,\chi}(n)e(nz)\right\},$$

and for $C' = \sqrt{-1}^k 2^k N^{k-1}\pi$

$$\text{(4b)}\qquad G_k(u_z,1-k,\chi) = C'\left\{\frac{L_L(1-k,\chi)}{2} + \sum_{n=1}^{\infty}\sigma_{k-1,\chi}(n)e(nz)\right\},$$

where $\delta_{k,j}$ is the Kronecker symbol and $\delta_{\chi,\mathrm{id}} = 1$ or 0 according as $\chi = \mathrm{id}$ or not, $\varphi(L) = \#((\mathbf{Z}/L\mathbf{Z})^\times)$ and $L_L(s,\chi) = \{\prod_{p|L}(1-\chi(p)p^{-s})\}L(s,\chi)$.

Now we assume that $N = 1$ and hence $\chi = \mathrm{id}$. The only difference in computation from the case when $N > 1$ is that for $w \in \mathbf{A}^\times B(\mathbf{A})_+$, the non-triviality of $\chi^\#(\gamma\alpha(x)w\varepsilon_f^{-1})\eta(\gamma\alpha(x)w\varepsilon_f^{-1})^s$ does not necessarily mean that $c \neq 0$ for $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix}$. Since we have $\gamma = \begin{pmatrix} c^{-2}\det(\gamma) & c^{-1}a \\ 0 & 1\end{pmatrix}c\varepsilon\tau(c^{-1}d)$ if $c \neq 0$, we have

$$GL_2(\mathbf{Q})_+ = B_+\mathbf{Q}^\times \cup B_+\mathbf{Q}^\times\varepsilon U \quad \text{(disjoint)}.$$

Thus we have an extra factor coming from $B_+\mathbf{Q}^\times$ in the computation of $b(\xi,w,s)$:

$$b(\xi,u_z,s) = \int_{A/Q}\eta(u_z)^s\psi(-\xi x)d\mu$$
$$+ \int_{A/Q}\sum_{\gamma\in Q_+,\delta\in Q}\chi^\#(\varepsilon\gamma\alpha(x+\delta)w\varepsilon_f^{-1})\eta(\varepsilon\gamma\alpha(x+\delta)w\varepsilon_f^{-1})^s j(\gamma_\infty(\alpha(x+\delta)w)_\infty,i)^{-k}\psi(-\xi x)d\mu.$$

Note that, by the formula $\int_{A/Q}d\mu = 1$ (see §8.6),

$$\int_{A/Q}\eta(u_z)^s\psi(-\xi x)d\mu = |y|_A^s\int_{A/Q}\psi(-\xi x)d\mu = \delta_{\xi,0}|y|_A^s.$$

Thus we have, for $\sigma_s(n) = \sigma_{s,\mathrm{id}}(n)$

$$\text{(5a)}\ G_{k,1}(u_z,s,\mathrm{id}) = \zeta(k+2s)|y|_A^s + i^k 2^{-s}\{2\pi(2|y|_A)^{1-k-s}\frac{\Gamma(k+2s-1)\zeta(2s+k-1)}{\Gamma(k+s)\Gamma(s)}$$
$$+\Gamma_C(s+k)^{-1}\sum_{n=1}^{\infty}|(ny)_f|_A^{1-s-k}\sigma_{-2s-k+1}(ny\mathbf{Z})e(nz)e((nx)_f)\omega(4\pi ny_\infty;k+s,s)$$
$$+\Gamma_C(s)^{-1}(2|y|_A)^{-k}\sum_{n=1}^{\infty}|(ny)_f|_A^{1-s}\sigma_{-2s-k+1}(ny\mathbf{Z})e(-n\bar{z})e(-(nx)_f)\omega(4\pi ny_\infty;s,k+s)\},$$

and by the functional equation for the Riemann zeta function, we have for $C = \sqrt{-1}^k(k-1)!^{-1}(2\pi)^k$ and $C' = \sqrt{-1}^k 2^k\pi$

$$\text{(5b)}\quad C^{-1}G_{k,1}(x,0,\mathrm{id}) = 2^{-1}\zeta(1-k)+\delta_{k,2}(2\pi|y|_A)^{-1}+\sum_{n=1}^{\infty}\sigma_{k-1,\chi}(n)e(nz)$$
$$= C'^{-1}G_{k,1}(x,1-k,\mathrm{id}).$$

This finishes the proof of the theorem. We note here a byproduct of our computation:

Theorem 1. *Let the notation be as above. Then* $\Gamma_C(s+k)G_{k,N}(x,s,\chi)$ *is entire if* $\mathrm{Re}(s) > -1-\frac{k}{2}$ *and* χN^k *is non-trivial. When* χ *is trivial and* $k = 0$, *it is entire if* $\mathrm{Re}(s) > \frac{2-k}{2}$. *The singularities of this function are at most simple poles.*

We now prove Lemma 3. Following the argument given in [Sh6], we show that

$$(6) \qquad \begin{aligned} b(\xi,y;\alpha,\beta) &= \int_{-\infty}^{\infty}(x+iy)^{-\alpha}(x-iy)^{-\beta}\exp(-2\pi i\xi x)dx \\ &= i^{\beta-\alpha}(2\pi)^{\alpha}\Gamma(\alpha)^{-1}(2y)^{-\beta}\xi^{\alpha-1}\omega(4\pi y\xi;\alpha,\beta) \text{ if } \xi > 0. \end{aligned}$$

The case where $\xi \le 0$ can be dealt with similarly. Then the lemma is the special case where $\alpha = k+s$ and $\beta = s$. We have

$$\begin{aligned} b(\xi,y;\alpha,\beta) &= \int_{-\infty}^{\infty}(x+iy)^{-\alpha}(x-iy)^{-\beta}\exp(-2\pi i\xi x)dx \\ &= \int_{-\infty}^{\infty}(i(y-ix))^{-\alpha}(-i(y+ix))^{-\beta}\exp(-2\pi i\xi x)dx \\ &= i^{\beta-\alpha}\int_{-\infty}^{\infty}(y-ix)^{-\alpha}(y+ix)^{-\beta}\exp(-2\pi i\xi x)dx. \end{aligned}$$

Here note that $a = y-ix \in H'$ (i.e. $\mathrm{Re}(a) > 0$). Recall the formula in Exercise 2.4.2:

$$\int_0^{\infty} e^{-au}u^{s-1}du = a^{-s}\Gamma(s) \text{ if } a \in H' \text{ and } \mathrm{Re}(s) > 0.$$

Thus $(y-ix)^{-\alpha} = \Gamma(\alpha)^{-1}\int_0^{\infty}\exp(-(y-ix)u)u^{\alpha-1}du$ if $\mathrm{Re}(\alpha) > 0$. Using this formula, we obtain

$$(7) \quad \begin{aligned} b(\xi,y;\alpha,\beta) &= i^{\beta-\alpha}\Gamma(\alpha)^{-1}\int_{-\infty}^{\infty}\exp(-2\pi i\xi x)\int_0^{\infty}\exp(-(y-ix)u)u^{\alpha-1}du(y+ix)^{-\beta}dx \\ &= i^{\beta-\alpha}\Gamma(\alpha)^{-1}\int_{-\infty}^{\infty}\int_0^{\infty}\exp(-2\pi i\xi x-(y-ix)u)u^{\alpha-1}(y+ix)^{-\beta}dudx \\ &= i^{\beta-\alpha}\Gamma(\alpha)^{-1}\int_0^{\infty}\exp(-uy)u^{\alpha-1}\int_{-\infty}^{\infty}\exp(ix(u-2\pi\xi))(y+ix)^{-\beta}dxdu. \end{aligned}$$

Now by putting $f(x) = (y+ix)^{-\beta}$, we consider the inner integral

$$\int_{-\infty}^{\infty}\exp(ix(u-2\pi\xi))(y+ix)^{-\beta}dx = \int_{-\infty}^{\infty}\exp(2\pi ix\frac{u-2\pi\xi}{2\pi})(y+ix)^{-\beta}dx = \mathcal{F}(f)(\frac{u-2\pi\xi}{2\pi}).$$

Here $\mathcal{F}(f)$ denotes the Fourier transform of f. On the other hand, we also know that

$$(*) \qquad (y+ix)^{-\beta} = \Gamma(\beta)^{-1}\int_0^\infty \exp(-(y+ix)u)u^{\beta-1}du.$$

Now define a function $g : \mathbf{R} \to \mathbf{C}$ by

$$g(u) = \begin{cases} \exp(-yu)u^{\beta-1} & \text{if } u > 0, \\ 0 & \text{if } u \le 0. \end{cases}$$

Then, by $(*)$, we see that

$$f(x) = (y+ix)^{-\beta} = \Gamma(\beta)^{-1}\int_0^\infty \exp(-2\pi ix\frac{u}{2\pi})g(u)du = \Gamma(\beta)^{-1}\mathcal{F}(g)(\frac{-u}{2\pi}).$$

Thus $\mathcal{F}(f)(x) = 2\pi\Gamma(\beta)^{-1}\mathcal{F}\mathcal{F}(g)(2\pi x) = 2\pi\Gamma(\beta)^{-1}g(-2\pi x)$ by the Fourier inversion formula. Thus we obtain

$$\int_{-\infty}^\infty e^{ix(u-2\pi\xi)}(y+ix)^{-\beta}dx = \begin{cases} 2\pi\Gamma(\beta)^{-1}\exp(-y(u-2\pi\xi))(u-2\pi\xi)^{\beta-1} & \text{if } u > 2\pi\xi, \\ 0 & \text{otherwise.} \end{cases}$$

We plug this in (3) and then obtain

$$b(\xi,y;\alpha,\beta) = i^{\beta-\alpha}(2\pi)\Gamma(\alpha)^{-1}\Gamma(\beta)^{-1}\int_{\pi\xi}^\infty \exp(-2yv)(v+\pi\xi)^{\alpha-1}(v-\pi\xi)^{\beta-1}dv.$$

By the simple variable change $(v-\pi\xi)/2\pi\xi \mapsto t$, we obtain the desired formula.

§9.3. Functional equation for Eisenstein series

Hereafter we always assume $F = \mathbf{Q}$. Assuming that χ is primitive modulo N (allowing the case $\chi = \mathrm{id}$ and $N = 1$), we now look at the explicit Fourier expansion of $\mathbf{G}_k(x,s,\chi)$ given in (2.3b) to know whether there is a functional equation for Eisenstein series $\mathbf{E}_k$ and $\mathbf{G}_k$. We know from (1.9) that

$$\mathbf{E}_{k,N}(x_\infty,s,\chi)j(x_\infty,i)^k = L_N(k+2s,\chi^{*-1})E_\Gamma(z,s,\chi) \quad \text{for} \quad z = x_\infty(i),$$

where $\Gamma = \Gamma_0(N)$ and $E_\Gamma(z,s,\chi) = y^s\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\chi^{*-1}(\delta)j(\delta,z)^{-k}|j(\delta,z)|^{-2s}$. Note that $\Gamma_\infty\backslash\Gamma \cong R/\{\pm1\}$ via $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \mapsto (cN,d)$ for

$$R = \{(cN,d) \in \mathbf{Z}^2 \mid cN\mathbf{Z}+d\mathbf{Z} = \mathbf{Z}\}.$$

Thus, regarding χ^* as a Dirichlet character on $(\mathbf{Z}/N\mathbf{Z})^\times$,

$$E_\Gamma(z,s,\chi) = 2^{-1}y^s\sum_{(cN,d)\in R}\chi^{*-1}(d)(cNz+d)^{-k}|cNz+d|^{-2s}.$$

Note that $R\times\mathbf{N} \cong \{(mN,n) \mid (m,n) \in \mathbf{Z}^2\}$ via $(cN,d)\times t \mapsto (tcN,td)$. Thus

$$\begin{aligned} E'_{k,N}(z,s,\chi) &= y^s\sum_{(mN,n)\neq(0,0)}\chi^{*-1}(n)(mNz+n)^{-k}|mNz+n|^{-2s} \\ &= y^s\sum_{t=1}^\infty \sum_{(cN,d)\in R}\chi^{*-1}(td)(tcNz+td)^{-k}|tcNz+td|^{-2s} \\ &= 2L(2s+k,\chi^{-1})E_\Gamma(z,s,\chi) = 2\mathbf{E}_{k,N}(x_\infty,s,\chi)j(x_\infty,i)^k. \end{aligned}$$

Let $\tau = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Then $\tau^{-1} = -N^{-1}\tau$ and we have

$$\begin{aligned} E'_{k,N}(z,s,\chi)\,|_k\tau &= N^{k-1}E'_N(\tfrac{-1}{Nz},s,\chi)(Nz)^{-k} = 2N^{k-1}\mathbf{E}_{k,N}(\tau_\infty x_\infty,s,\chi)j(x_\infty,i)^k \\ &= 2N^{k-1}\mathbf{E}_{k,N}(\tau x_\infty \tau_f^{-1},s,\chi)j(x_\infty,i)^k = 2N^{k-1}\mathbf{E}_{k,N}(x_\infty\tau_f^{-1},s,\chi)j(x_\infty,i)^k \\ &= 2N^{k-1}\chi(-N_f^{-1})\mathbf{E}_{k,N}(x_\infty\tau_f,s,\chi)j(x_\infty,i)^k = 2N^{-1}(-1)^k\mathbf{G}_{k,N}(x_\infty,s,\chi)j(x_\infty,i)^k. \end{aligned}$$

Now we have, for $\Gamma_C(s) = (2\pi)^{-s}\Gamma(s)$,

$$\begin{aligned} (1)\qquad & \Gamma_C(s+k)\Gamma_C(s)\mathbf{G}_k(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix},s,\chi) = \delta_{\chi,\mathrm{id}}\Gamma_C(s+k)\Gamma_C(s)\zeta(k+2s)\,|\,y\,|_A^s \\ & +i^k(2N)^{-s}\{(2\,|\,y\,|_A)^{1-k-s}\Gamma_C(k+2s-1)L(2s+k-1,\chi) \\ & +\Gamma_C(s)\sum_{n=1}^{\infty}|(ny)_f|_A^{1-k-s}\,\sigma_{-2s-k+1,\chi}(nyZ)e(nz+(nx)_f)\omega(4\pi ny_\infty;k+s,s) \\ & +\Gamma_C(s+k)(2\,|\,y\,|_A)^{-k}\sum_{n=1}^{\infty}|(ny)_f|_A^{1-s}\,\sigma_{-2s-k+1,\chi}(nyZ)e(-n\bar{z}-(nx)_f)\omega(4\pi ny_\infty;s,k+s)\}. \end{aligned}$$

The idea is to compute the Fourier expansion of $\mathbf{E}_k$ directly and relate it to $\mathbf{G}_k(x,1-k-s,\chi)$. Here we assume that χ is a primitive character modulo N allowing the identity character when $N = 1$. We know, for $z = x_\infty(i)$,

$$\mathbf{E}_{k,N}(x_\infty,s,\chi)j(x_\infty,i)^k = 2^{-1}y^s\sum_{(mN,n)\neq(0,0)}\chi^{*-1}(n)(mNz+n)^{-k}\,|\,mNz+n\,|^{-2s}.$$

Since we have shown in the previous section how to compute the adelic Fourier expansion of $\mathbf{G}_k$, here we shall give a computation in a classical way:

$$\begin{aligned} \mathbf{E}_k(x_\infty,s,\chi) &= 2^{-1}y^s\sum_{(mN,n)\neq(0,0)}\chi^{*-1}(n)(mNz+n)^{-k}\,|\,mNz+n\,|^{-2s} \\ &= y^sL(k+2s,\chi^{*-1})+\frac{1}{N^{k+2s}}\sum_{b\in(Z/NZ)^\times}\chi^{*-1}(b)\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}(mz+\frac{b}{N}+n)^{-k}\,|\,mz+\frac{b}{N}+n\,|^{-2s} \\ &= y^sL(k+2s,\chi^{*-1})+N^{-k-2s}\sum_{b\in(Z/NZ)^\times}\chi^{*-1}(b)\sum_{m=1}^{\infty}S(mz+\frac{b}{N};k+s,s), \end{aligned}$$

where $S(z;\alpha,\beta) = \sum_{m\in Z}(z+m)^{-\alpha}(\bar{z}+m)^{-\beta}$ $(\alpha,\beta\in \mathbf{C})$. For each $z\in \mathbf{C}$ and $s\in \mathbf{C}$, we define $z^s = |\,z\,|^s e^{is\theta}$ writing $z = |\,z\,|e^{i\theta}$ with $-\pi < \theta \le \pi$. We compute the Fourier transform of $\varphi(y;\alpha,\beta;x) = (x+iy)^{-\alpha}(x-iy)^{-\beta}$. Note that $S(z;\alpha,\beta) = \varphi(y;\alpha,\beta;x+m)$ for $z = x+iy$. We have by the Poisson summation formula (Theorem 8.4.1)

$$S(z;\alpha,\beta) = \sum_{n\in Z}e(nx)B(y,n;\alpha,\beta)$$

where $$B(y,\xi;\alpha,\beta) = \int_{-\infty}^{\infty} e(-\xi x)\varphi(y;\alpha,\beta;x)dx.$$

Exercise 1. To justify the use of the Poisson summation formula, show:
(i) If $\mathrm{Re}(\alpha+\beta) \geq 1$, $\varphi(y;\alpha,\beta;x)$ is continuous and bounded as a function of x and is integrable; (ii) $\sum_{n\in Z} |B(y,n+x;\alpha,\beta)|$ is convergent locally uniformly in x. (You may use Lemma 2.3 and Lemma 2 below.)

By Lemma 2.3, we have, for $z = x+iy \in \mathcal{H}$

$$\begin{aligned}
(2)\qquad E_k\left(\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix},s,\chi\right) &= y^s L(k+2s,\chi^{*-1}) \\
&\quad + N^{-k-2s} \sum_{b\in(Z/NZ)^\times} \chi^{*-1}(b) \sum_{m=1}^{\infty}\sum_{n\in Z} e(mnx+\frac{nb}{N})B(my,n;k+s,s) \\
&= y^s L(k+2s,\chi^{*-1}) + N^{-k-2s} i^{-k}(2\pi)^s \\
&\quad \times\{(2\pi)^{k+s}\Gamma(k+s)^{-1}\Gamma(s)^{-1}\Gamma(k+2s-1)(4\pi y)^{1-k-s} \sum_{b\in(Z/NZ)^\times}\chi^{*-1}(b)\sum_{m=1}^{\infty} m^{1-k-2s} \\
&\quad + \frac{2^{-s}(2\pi)^k}{\Gamma(k+s)} \sum_{n>0}\sum_{b\in(Z/NZ)^\times}\chi^{*-1}(b)e(\frac{nb}{N})\sum_{m=1}^{\infty} e(mnx)\frac{n^{k+s-1}}{m^s}e^{-2\pi mny}\omega(4\pi mny;k+s,s) \\
&\quad + \frac{2^{-s-k}y^{-k}}{\Gamma(s)} \sum_{n>0}\sum_{b\in(Z/NZ)^\times}\chi^{*-1}(b)e(-\frac{nb}{N})\sum_{m=1}^{\infty} e(-mnx)\frac{n^{s-1}}{m^{s+k}}e^{-2\pi mny}\omega(4\pi mny;s,k+s)\} \\
&= y^s L(k+2s,\chi^{-1}) + 2^{-s}N^{-k-2s}i^{-k}\delta_{\chi,\mathrm{id}}\{\frac{\Gamma(2s+k-1)L(2s+k-1,\chi^{-1})}{\Gamma_C(k+s)\Gamma_C(s)}2^s(4\pi y)^{1-k-s} \\
&\quad + \Gamma_C(k+s)^{-1}G(\chi^{-1})\sum_{n=1}^{\infty} n^{-s}\sigma_{k+2s-1,\chi}(n)e(nz)\omega(4\pi ny;k+s,s) \\
&\quad + (2y)^{-k}\Gamma_C(s)^{-1}G(\chi^{-1})\chi(-1)\sum_{n=1}^{\infty} n^{-s-k}\sigma_{k+2s-1,\chi}(n)e(-n\bar{z})\omega(4\pi ny;s,k+s)\}.
\end{aligned}$$

Here we have used Lemma 2.3.2 to obtain the last equality. Now we replace s in (1) by $1-k-s$ and compute for $z = x+iy \in \mathcal{H}$

$$\begin{aligned}
\Gamma_C(1-s)\Gamma_C(1-k-s)G_k\left(\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix},1-k-s,\chi\right) &= \delta_{\chi,\mathrm{id}}\Gamma_C(1-s)\Gamma_C(1-k-s)\zeta(2-k-2s)|y|_A{}^s \\
&\quad + i^k N^{s+k-1}2^{k+s-1}\{(2y)^s\Gamma_C(1-k-2s)L(2s+k-1,\chi) \\
&\quad + \Gamma_C(1-k-s)\sum_{n=1}^{\infty} n^{-s}\sigma_{k+2s-1,\chi}(n)e(nz)\omega(4\pi ny;1-s,1-k-s) \\
&\quad + \Gamma_C(1-s)(2y)^{-k}\sum_{n=1}^{\infty} n^{-s-k}\sigma_{k+2s-1,\chi}(nyZ)e(-n\bar{z})\omega(4\pi ny_\infty;1-k-s,1-s)\}.
\end{aligned}$$

We will prove the functional equation $\omega(z;1-\beta,1-\alpha) = \omega(z;\alpha,\beta)$ later. Then, noting the facts that $\Gamma(s+1) = s\Gamma(s)$ and $\chi(-1) = (-1)^k$, we know that

$$\begin{aligned}
i^{-k}(2N)^{1-s-k}\Gamma_C(1-s)G_{k,N}(w,1-k-s,\chi) - 2^s N^{k+2s} i^k \Gamma_C(s+k)G(\chi^{-1})^{-1}E_{k,N}(w,s,\chi) \\
= c(s)y^s + d(s)y^{1-k-s}
\end{aligned}$$

for suitable meromorphic functions $c(s)$ and $d(s)$ of s. Since we know that $\mathbf{G}_k$ and $\mathbf{E}_k$ are both modular forms of weight k and of character χ. Then we see for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ that

$$\begin{aligned} &c(s)y^s\,|cz+d|^{-2s-k}+d(s)y^{1-k-s}\,|cz+d|^{2s+k-2} \\ &= (c(s)y^s+d(s)y^{1-k-s})\,|_k\gamma = \chi(\gamma)(c(s)y^s+d(s)y^{1-k-s}). \end{aligned}$$

By choosing γ and $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_0(N)$ suitably, we can make

$$\begin{vmatrix} |cz+d|^{-2s-k} - \chi(\gamma) & |cz+d|^{-2s+k-2} - \chi(\gamma) \\ |c'z+d'|^{-2s-k} - \chi(\gamma') & |c'z+d'|^{-2s+k-2} - \chi(\gamma') \end{vmatrix} \neq 0 \text{ for almost all } s.$$

This implies $c(s) = d(s) = 0$ for all s. Since $GL_2(\mathbf{A}) = GL_2(\mathbf{Q})S(N)G_{\infty+}$, the above identity between $\mathbf{E}_k$ and $\mathbf{G}_k$ holds all over $GL_2(\mathbf{A})$. That is, we have

Theorem 1. *Suppose that χ is a primitive character modulo N (we allow the trivial character when $N = 1$). Then we have*

$$\Gamma_{\mathbf{C}}(s+k)\mathbf{E}_{k,N}(w,s,\chi) = \chi_\infty(-1)G(\chi^{-1})2^{1-2s-k}N^{1-3s-2k}\Gamma_{\mathbf{C}}(1-s)\mathbf{G}_{k,N}(w,1-k-s,\chi).$$

Exercise 2. *Show the functional equation for $L(s,\chi)$ using Theorem 1.*

We need to prove

Lemma 1. *We have* $\qquad \omega(z;1-\beta,1-\alpha) = \omega(z;\alpha,\beta).$

Proof. By definition, $\zeta(z;\alpha,\beta) = \int_0^\infty e^{-zx}(x+1)^{\alpha-1}x^{\beta-1}dx$, which converges absolutely for arbitrary $\alpha \in \mathbf{C}$ if $\mathrm{Re}(\beta) > 0$ and $\mathrm{Re}(z) > 0$. We compute

$$\Gamma(\alpha)\zeta(z;1-\alpha,\beta) = \int_0^\infty e^{-zx}\Gamma(\beta)(x+1)^{-\alpha}x^{\beta-1}dx = \int_0^\infty e^{-zx}\int_0^\infty e^{-u(x+1)}u^{\alpha-1}du\,x^{\beta-1}dx,$$

because $\Gamma(\alpha)(x+1)^{-\alpha} = \int_0^\infty e^{-u(x+1)}u^{\alpha-1}du$ if $\mathrm{Re}(\alpha) > 0$ (Exercise 2.4.2). From Fubini's theorem, we see that

$$\begin{aligned} \Gamma(\alpha)\zeta(z;1-\alpha,\beta) &= \int_0^\infty e^{-u}u^{\alpha-1}\int_0^\infty e^{-x(z+u)}x^{\beta-1}dxdu = \Gamma(\beta)\int_0^\infty e^{-u}u^{\alpha-1}(z+u)^{-\beta}du \\ &\overset{u\to zu}{=} \Gamma(\beta)z^{\alpha-\beta}\int_0^\infty e^{-zu}u^{\alpha-1}(u+1)^{-\beta}du = \Gamma(\beta)z^{\alpha-\beta}\zeta(z;1-\beta,\alpha). \end{aligned}$$

This implies the functional equation of ω because $\omega(z;\alpha,\beta) = z^\beta\Gamma(\beta)^{-1}\zeta(z;\alpha,\beta)$. Now we prove the following estimate for our later use:

Lemma 2. *For any given compact subset* T *in* $\mathbf{C}^2$, *we can find two positive real numbers* A *and* B *such that if* $(\alpha,\beta) \in T$ *and* $y \in \mathbf{R}_+$, *then*

$$|\omega(y;\alpha,\beta)| \le A(1+y^{-B}).$$

Proof. We have $\zeta(y;\alpha,\beta+1) = \int_0^\infty e^{-yx}(x+1)^{\alpha-1}x^\beta dx$. Using the formulas

$$e^{-yx} = \frac{d}{dx}(-y^{-1}e^{-yx}),\ \frac{d}{dx}\{(x+1)^{\alpha-1}x^\beta\} = (\alpha-1)(x+1)^{\alpha-2}x^\beta+\beta(x+1)^{\alpha-1}x^{\beta-1},$$

we perform the integration by parts and obtain

$$\zeta(y;\alpha,\beta+1) = [-y^{-1}e^{-yx}(x+1)^{\alpha-1}x^\beta]_0^\infty+y^{-1}(\alpha-1)\zeta(y;\alpha-1,\beta+1)+y^{-1}\beta\zeta(y;\alpha,\beta).$$

If $\mathrm{Re}(\beta) > 0$, $[-y^{-1}e^{-yx}(x+1)^{\alpha-1}x^\beta]_0^\infty = 0$ and thus we have

$$\beta\zeta(y;\alpha,\beta) = y\beta\zeta(y;\alpha,\beta+1)+(1-\alpha)\beta\zeta(y;\alpha-1,\beta+1).$$

Interpreting this using ω, we get

$$\omega(y;\alpha,\beta) = \omega(y;\alpha,\beta+1)+(1-\alpha)y^{-1}\omega(y;\alpha-1,\beta+1). \tag{3}$$

Iterating this formula n times, we have

$$\begin{aligned}\omega(y;\alpha,\beta) &= \textstyle\sum_{k=0}^n \binom{n}{k}(1-\alpha)(2-\alpha)\cdot\cdots\cdot(k-\alpha)y^{-k}\omega(y;\alpha-k,\beta+n) \\ &= \textstyle\sum_{k=0}^n (-1)^k\binom{n}{k}\frac{\Gamma(\alpha)}{\Gamma(\alpha-k)}y^{-k}\omega(y;\alpha-k,\beta+n).\end{aligned} \tag{4}$$

Now we choose a positive integer n so that $\mathrm{Re}(\alpha-1) \le n$ for all $(\alpha,\beta) \in T$. Then for $x \in \mathbf{R}_+$, $|(1+x)^{\alpha-1}| \le (1+x)^n = \sum_{k=0}^n\binom{n}{k}x^k$. Thus if $\mathrm{Re}(\beta) > 0$ for all $(\alpha,\beta) \in T$, we have

$$\begin{aligned}|\omega(y;\alpha,\beta)| &\le |\Gamma(\beta)^{-1}y^\beta\textstyle\int_0^\infty e^{-yx}(x+1)^{\alpha-1}x^{\beta-1}dx| \\ &\le |\Gamma(\beta)|^{-1}y^{\mathrm{Re}(\beta)}\textstyle\int_0^\infty e^{-yx}(1+x)^n x^{\mathrm{Re}(\beta)-1}dx \\ &= \textstyle\sum_{k=0}^n \binom{n}{k}|\Gamma(\beta)|^{-1}y^{\mathrm{Re}(\beta)}\int_0^\infty e^{-yx}x^{k+\mathrm{Re}(\beta)-1}dx \\ &= |\Gamma(\beta)|^{-1}\textstyle\sum_{k=0}^n \binom{n}{k}\Gamma(k+\mathrm{Re}(\beta))y^{-k}.\end{aligned}$$

From this the assertion of the lemma is clear. When there exists $(\alpha,\beta) \in T$ such that $\mathrm{Re}(\beta) \le 0$, we choose a sufficiently large integer n so that $\mathrm{Re}(\beta+n) > 0$ for all $(\alpha,\beta) \in T$. Then by (4), the proof in this case is reduced to the case already treated.

From the computation of the Fourier expansion we have done, we can at least determine the form of the Fourier expansion of $\mathbf{E}_k$ at various cusps. That is, we see that

$$E'_{k,N}(z,s,\chi) = \sum_{b \bmod N} \chi^{*-1}(b) E'_{k,N}(z,s;(0,b)),$$

where $E'_N(z,s;(a,b)) = y^s \sum_{(m,n)\equiv(a,b) \bmod N,\ (m,n)\neq(0.0)} (mz+n)^{-k} \,|\, mz+n \,|^{-2s}$ for $(a,b) \in (\mathbf{Z}/N\mathbf{Z})^2$. We also see easily that for $\gamma \in SL_2(\mathbf{Z})$

$$E'_{k,N}(z,s;(a,b)) \,|_k \gamma = E'_{k,N}(z,s;(a,b)\gamma).$$

Thus the Fourier expansion of $E'_{k,N}(z,s;(a,b))$ at the cusp $\gamma(\infty)$ is given by the Fourier expansion of $E'_{k,N}(z,s;(a,b)\gamma)$. Thus we only need to compute $E'_{k,N}(z,s;(a,b))$ for general (a,b). First writing

$$E'_{k,N}(z,s;(a,b)) = y^s N^{-k-2s} \sum_{m\equiv a \bmod N,\ m\neq 0} S(\frac{mz+b}{N};k+s,s)$$

and then applying the Poisson summation formula to $S(\frac{mz+b}{N};k+s,s)$, we have

$$E'_{k,N}(z,s;(a,b)) = c(s)y^s + d(s)y^{1-k-s} + \sum_{n=1}^{\infty} a_{n/N}(s) e(nz/N) \omega(4\pi ny/N;k+s,s)$$
$$+ \sum_{n=1}^{\infty} b_{n/N}(s) e(-n\bar{z}/N) \omega(4\pi ny/N;k+s,s),$$

where $c(s)$ and $d(s)$ are meromorphic functions of s and $a_{n/N}$ and $b_{n/N}$ are entire functions of s. Moreover, as long as s stays in a compact subset $|a_{n/N}(s)| \leq A'n^A$ and $|b_{n/N}(s)| \leq B'n^B$ for suitable positive real numbers A, A', B, B'. This shows

Lemma 3. *For any given compact subset* T *in* $\mathbf{R}$ *and* $\gamma \in SL_2(\mathbf{Z})$, *there exist positive numbers* A *and* B *such that if* $\chi \neq \mathrm{id}$

$$\left| \mathbf{E}_k(z,s,\chi) \,|_k \gamma \right| \leq A(1+y^{-B}) \text{ as } y \to \infty \text{ as long as } x = \mathrm{Re}(z) \in T$$

and if $\chi = \mathrm{id}$, *the above estimate holds if* $T \subset \mathbf{R} - \{\frac{1-k}{2}\}$.

Exercise 3. Compute explicitly the Fourier expansion at ∞ of $E'_{k,N}(z,s;(a,b))$.

We now make the following definition. For a C^∞-function $f : \mathcal{H} \to \mathbf{C}$ satisfying $f|_k\gamma = f$ for all $\gamma \in \Gamma$ for a congruence subgroup Γ of $SL_2(\mathbf{Z})$,

(5a) f is called *slowly increasing* if for any $\alpha \in SL_2(\mathbf{Z})$, there exist positive numbers A and B such that $|f|_k\alpha(z)| \leq A(1+y^{-B})$ as $y \to \infty$;
(5b) f is called *rapidly decreasing* if for any $B \in \mathbf{R}$ and $\alpha \in SL_2(\mathbf{Z})$, there exists a positive constant A such that $|f|_k\alpha(z)| \leq A(1+y^B)$ as $y \to \infty$.

Thus if f is slowly increasing, then for every $\alpha \in SL_2(\mathbf{Z})$, $f|_k\alpha$ has polynomial growth in y as $y \to \infty$. If $f|_k\alpha(z)$ for every $\alpha \in SL_2(\mathbf{Z})$ decreases exponentially with respect to y as $y \to \infty$, f is rapidly decreasing. If g and f are both of weight k for Γ and f (resp. g) is rapidly decreasing (resp. slowly increasing), then $\Phi(z) = \bar{g}f(z)\mathrm{Im}(z)^k$ is Γ-invariant and rapidly decreasing at every cusp. Since every small neighborhood $D = \{z \in \Gamma_\infty\backslash H \mid \mathrm{Im}(z) > M\}$ of the cusp $i\infty$ is isomorphic to an open disk with variable q ($q = \exp(2\pi iz)$) and since such neighborhoods are transformed by an element $\alpha \in SL_2(\mathbf{Z})$ to neighborhoods of a given cusp, $|\Phi(z)|$ is a bounded function on $Y = \Gamma\backslash H$. Since Y has finite volume under $y^{-2}dxdy$, the inner product (f,g) is well defined. Let us record this fact:

(6) *If* f *and* g *are* C^∞*-class modular forms of weight* k *with respect to* Γ *and if* f *is rapidly decreasing and* g *is slowly increasing, then the integral defining the Petersson inner product* (f,g) *is absolutely convergent.*

§9.4. Analytic continuation of Rankin products

We start by introducing a slightly more general space of modular forms. Let χ be a finite order Hecke character modulo N and χ' be a character of $(\mathbf{Z}/N\mathbf{Z})^\times$. We define $\mathbf{M}_k(N;\chi,\chi')$ to be the space of functions **f** satisfying (M2-3) in §1 and the following replacement of (M1): for $u \in S(N)C_{\infty+}$ and $\alpha \in GL_2(F)$,

(M'1) $$\mathbf{f}(\alpha xu) = \chi'(u)\chi_N(u)\mathbf{f}(x)j_k(u_\infty,\mathbf{i})^{-1},$$

where $\chi_N(u)$ is as in (M1) in §1 and $\chi'\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \chi'((a^{-1}d)_N)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S(N)C_{\infty+}$. If $\mathbf{f} \in \mathbf{M}_k(N;\chi,\chi')$ satisfies the cuspidal condition (S) in §1, **f** is called a cusp form and we write $\mathbf{S}_k(N;\chi,\chi')$ for the subspace consisting of cusp forms in $\mathbf{M}_k(N;\chi,\chi')$. For each arithmetic Hecke character $\theta : \mathbf{A}^\times/\mathbf{Q}^\times U(M)\mathbf{R}_+ \to \mathbf{C}^\times$ of finite order and $\mathbf{f} \in \mathbf{M}_k(N;\chi,\chi')$, we define a new function

$$\mathbf{f}\otimes\theta : GL_2(\mathbf{A}) \to \mathbf{C} \text{ by } \mathbf{f}\otimes\theta(x) = \theta(\det(x))\mathbf{f}(x).$$

Then it is plain that $\mathbf{f}\otimes\theta \in \mathbf{M}_k([M,N];\chi\theta^2,\chi'\theta_M^{-1})$, where [M,N] is the least common multiple of N and M and θ_M is the restriction of θ to $\mathbf{Z}_M^\times = \prod_{p|M}\mathbf{Z}_p^\times$. Note that any character χ' can be lifted uniquely to a finite order Hecke character θ of $\mathbf{A}^\times/\mathbf{Q}^\times U(N)\mathbf{R}_+$ so that $\chi' = \theta_N$. Then the association $\mathbf{f} \mapsto \mathbf{f}\otimes\theta$ induces a map $\otimes\theta : \mathbf{M}_k(N;\chi,\chi') \to \mathbf{M}_k(N;\chi\theta^2)$ whose inverse is given by $\otimes\theta^{-1}$. Thus we have

(1) $$\otimes\theta : \mathbf{M}_k(N;\chi,\theta_N) \cong \mathbf{M}_k(N;\chi\theta^2).$$

One can of course define the space $\mathbf{M}_k(m;\chi,\chi')$ for GL(2) over a totally real field for a character $\chi' : (\mathcal{O}/m)^\times \to \mathbf{C}^\times$. However in this case, χ' may not be liftable to an arithmetic Hecke character θ, and even if the lifting is possible, θ may not be uniquely determined. Although we can construct a theory similar to the one presented here in the general case (see [H8]), this difficulty certainly adds more technicality in the treatment. This is the one of the reasons why we assumed that $F = \mathbf{Q}$ here.

Now we look into the Fourier expansion of $f \in \mathbf{M}_k(N;\chi,\chi')$. We take the finite order Hecke character θ such that $\theta_N = \chi'$. Then $f\otimes\theta$ has the following Fourier expansion:

$$f\otimes\theta\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right) = a_0(y\mathbf{Z};f\otimes\theta)+\sum_{\xi\in\mathbf{Q}_+} a(\xi y\mathbf{Z};f\otimes\theta)e(i\xi y_\infty)e(\xi x).$$

Thus applying $\otimes\theta^{-1}$, we find for $y \in \mathbf{A}^\times_+ = \mathbf{A}_f^\times\mathbf{R}_+$ that

$$\begin{aligned} f\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right) &= \theta(y)^{-1}f\otimes\theta\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right) \\ &= \theta^{-1}(y_f)a_0(y\mathbf{Z};f\otimes\theta)+\sum_{\xi\in\mathbf{Q}_+}\theta^{-1}(\xi y_f)a(\xi y\mathbf{Z};f\otimes\theta)e(i\xi y_\infty)e(\xi x). \end{aligned}$$

Here we have used the fact that $\theta((\xi y)_f) = \theta(\xi y) = \theta(y) = \theta(y_f)$ for $y \in \mathbf{A}^\times_+$ and $\xi \in \mathbf{Q}_+$. Thus let us put

(2) $$a(y;f) = \theta^{-1}(y_f)a(y\mathbf{Z};f\otimes\theta) \text{ and } a_0(y;f) = \theta^{-1}(y_f)a_0(y\mathbf{Z};f\otimes\theta).$$

Then the function of ideles $y \mapsto a(y;f)$ no longer factors through ideals but really depends on the finite part of the idele y and satisfies

(3a) $$a(uy;f) = \theta_N^{-1}(u_N)a(y;f\otimes\theta) \text{ for } u \in U(1) = \hat{\mathbf{Z}}^\times.$$

This shows the restriction of $a(*;f)$ to ideles in

$$(\mathbf{A}_f^{(N)})^\times = \{x \in \mathbf{A}_f^\times \mid x_p = 1 \text{ if } p \mid N\}$$

factors through the ideals prime to N (thus $f \in \mathbf{M}_k(N;\chi,\chi')$ with non-trivial N' is a GL(2)-analog of Hecke characters with non-trivial conductor). As for the constant term, we have

(3b) $$a_0(\alpha uy;f) = \chi'^{-1}(u)a(y;f) \text{ for } u \in U(1) = \hat{\mathbf{Z}}^\times \text{ and } \alpha \in \mathbf{Q}_+.$$

Thus the function $y \mapsto a_0(y;f)$ factors through $\mathbf{A}_f^\times/U(N) \cong Cl(N)$ instead of $CL(1)$ for $f\otimes\theta$. Now there is another operation. Let θ be a primitive Dirichlet character of $(\mathbf{Z}/C\mathbf{Z})^\times$ $(2 < C \in \mathbf{Z})$. Then choose a representative set R in $\mathbf{Z}_C^\times = \prod_{p|C}\mathbf{Z}_p^\times$ modulo $C\mathbf{Z}_C$ and define for $f \in \mathbf{M}_k(N;\chi,\chi')$,

$$\text{(4a)} \qquad f\,|\,\theta(x) = C^{-1}G(\theta)\sum_{r\in R}\theta^{-1}(r)f(x\alpha(r/C)) \text{ for } \alpha(r/C) = \begin{pmatrix}1 & r/C\\ 0 & 1\end{pmatrix}.$$

Then for $u = \begin{pmatrix}a & 0\\ 0 & b\end{pmatrix} \in S([C,N])$, $u\alpha(r/C) = \alpha(ab^{-1}r/C)u$ and thus

$$f\,|\,\theta(xu) = C^{-1}G(\theta)\sum_{r\in R}\theta^{-1}(r)f(xu\alpha(r/C)) = C^{-1}G(\theta)\sum_{r\in R}\theta^{-1}(r)f(x\alpha(ab^{-1}r/C)u)$$
$$= \chi_N(b)\chi'_N(a^{-1}b)C^{-1}G(\theta)\sum_{r\in R}\theta^{-1}(a^{-1}br)f(x\alpha(r/C)) = \chi_N(b)\chi'_N\theta_C(a^{-1}b)f\,|\,\theta(x).$$

Note that $S([C^2,N])$ is generated by the u's as above, $\alpha(v)$ for $v \in \mathbf{Z}_C$ $(\mathbf{Z}_C = \prod_{p|C}\mathbf{Z}_p)$ and $w \in S(1)$ with $w \equiv 1 \bmod C^2$. Since $w\alpha(r/C) = \alpha(r/C)w'$ with $w' \in S(N)$ for the w's as above, we know that

$$\text{(4b)} \qquad f\,|\,\theta \in \mathbf{M}_k([C^2,N];\chi,\chi'\theta).$$

We compute the Fourier expansion of $f\,|\,\theta$:

$$CG(\theta)^{-1}f\,|\,\theta\left(\begin{pmatrix}y & x\\ 0 & 1\end{pmatrix}\right) = a_0(y;f)\sum_{r\in R}\theta^{-1}(r) + \sum_{\xi\in Q_+}a(\xi y,f)e(i\xi y_\infty)e(\xi x)\sum_{r\in R}\theta^{-1}(r)e(\frac{\xi r}{C}).$$

Here note that by the definition of $\mathbf{e}$ (8.2.4), $\mathbf{e}(\frac{\xi yr}{C}) = \exp(-2\pi i[\xi yr/C])$ for the fractional part $[\xi yr/C]$ of $\xi yr/C$ in $\mathbf{Q}_C^\times = \prod_{p|C}\mathbf{Q}_p^\times$. Hence $\sum_{r\in R}\theta^{-1}(r)e(\frac{\xi yr}{C})$ $= \theta(-\xi y)G(\theta^{-1}) = \theta(\xi y)C^{-1}G(\theta)$ (see (4.2.6a)) if $\xi y\mathbf{Z}$ is prime to $C\mathbf{Z}$ and otherwise it vanishes. This shows $a(y;f\,|\,\theta) = \theta(y_C)a(y;f)$ and $a_0(y;f\,|\,\theta) = 0$. Thus we have

$$\text{(4c)} \qquad f\,|\,\theta\left(\begin{pmatrix}y & x\\ 0 & 1\end{pmatrix}\right) = \sum_{\xi\in Q_+}\theta((\xi y)_C)a(\xi y;f)e(i\xi y_\infty)e(\xi x),$$

where we consider θ is supported on $\mathbf{Z}_C^\times$ extended 0 outside $\mathbf{Z}_C^\times$.

Let χ be a finite order character of $\mathbf{A}^\times/U(N)\mathbf{Q}_{\infty+} \cong (\mathbf{Z}/N\mathbf{Z})^\times$. We write χ^* for the associated Dirichlet character modulo N. When confusion is unlikely, we write χ for χ^*. We pick a $\mathbf{Z}[\chi]$-algebra homomorphism

$$\lambda : \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]) \to \mathbf{C}$$

and consider its normalized eigenform $f = \sum_{n=1}^{\infty}\lambda(T(n))q^n \in \mathcal{S}_k(\Gamma_0(N),\chi^*)$. We may write the corresponding cusp form $\mathbf{f} \in \mathbf{S}_k(N,\chi)$ as

$$\mathbf{f}\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right) = \sum_{\xi\in \mathbf{Q}_+} a(\xi y\mathbf{Z};\mathbf{f})e(\xi x)e(i\xi y_\infty) \quad \text{for } a(n\mathbf{Z};\mathbf{f}) = \lambda(T(n)).$$

Similarly we take another normalized eigenform $\mathbf{g} \in \mathbf{M}_l(J,\psi)$ associated with a $\mathbf{Z}[\psi]$-algebra homomorphism $\varphi : \mathbf{h}_l(\Gamma_0(J),\psi;\mathbf{Z}[\psi]) \to \mathbf{C}$. Then we define the L-function of $\lambda\otimes\varphi\otimes\omega$ for an arithmetic Hecke character ω (of $\mathbf{Q}$) as in (7.4.2):

$$\begin{aligned}(5)\qquad L(s,\lambda\otimes\varphi\otimes\omega) &= L(2s+2-k-l,\chi\psi\omega^2)\sum_{n=1}^{\infty}\lambda(T(n))\varphi(T(n))\omega^*((n))n^{-s}\\ &= L(2s+2-k-l,\chi\psi\omega^2)\sum_{n=1}^{\infty} a(n;\mathbf{f})a(n;\mathbf{g})\omega^*((n))n^{-s},\end{aligned}$$

which is an Euler product of degree 4 (see the proof of Lemma 5.4.2). Now taking the product $\Psi(x) = (\overline{\mathbf{f}(x)j_k(x_\infty,i)})((\mathbf{g}\,|\,\omega)(x)j_l(x_\infty,i))$ as a function on $GL_2(\mathbf{A})$, we consider the integral

$$(6)\qquad Z(s,\mathbf{f},\mathbf{g},\omega) = \int_{\mathbf{A}^\times_+/\mathbf{Q}_+}\int_{\mathbf{A}/\mathbf{Q}}\Psi\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right)d\mu(x)\omega(y)\,|\,y\,|_{\mathbf{A}}^s d\mu^\times(y),$$

where $d\mu$ and $d\mu^\times$ are the additive and multiplicative Haar measures discussed in §8.5. Disregarding the convergence of the integral, it is formally well defined. We will look into the convergence later and for the moment concentrate on computing it formally in terms of Dirichlet series. Let C be the conductor of ω and write Φ for the characteristic function of $\mathbf{Z}_C^\times$ in $\mathbf{Q}_C^\times$. Then we see that

$$a(y;\mathbf{f})^c a(y;\mathbf{g}\,|\,\omega)\omega(y) = \Phi(y_C)a(y;\mathbf{f})^c a(y;\mathbf{g})\omega(y^{(C)}),$$

where $a(y;\mathbf{f})^c = \overline{a(y;\mathbf{f})}$ and $y^{(C)} = yy_C^{-1}$ for $y \in \mathbf{A}^\times_+$. Then by the orthogonality relation (8.4.4):

$$\int_{\mathbf{A}/\mathbf{Q}} e(\xi x)d\mu(x) = \begin{cases} 0 & \text{if } \xi \neq 0, \\ 1 & \text{if } \xi = 0, \end{cases}$$

we have, for $\mathbf{A}^\times_+ = \mathbf{A}_f^\times\times\mathbf{R}_+$ ($\mathbf{R}_+ = \{x \in \mathbf{R}\,|\,x > 0\}$) and $\mathbf{Q}_+ = \mathbf{Q}\cap\mathbf{R}_+$,

$$Z(s,\mathbf{f},\mathbf{g},\omega) = \sum_{\xi,\eta}\int_{\mathbf{A}_+^\times/\mathbf{Q}_+}\int_{\mathbf{A}/\mathbf{Q}} a(\xi y;\mathbf{f})^c\, a(\eta y;\mathbf{g}\,|\,\omega)e((\xi-\eta)x)d\mu(x)e(i(\xi+\eta)y_\infty)\omega(y)\,|\,y\,|_{\mathbf{A}}^s d\mu^\times(y)$$

$$\begin{aligned}
&(\omega(\xi y) = \omega(y)) \\
&= \int_{\mathbf{A}_+^\times/\mathbf{Q}_+} \sum_{\xi\in\mathbf{Q}_+} \Phi((\xi y)_C) a(\xi y;\mathbf{f})^c a(\xi y;\mathbf{g}) e(2i\xi y_\infty)\omega(\xi y)\,|\,\xi y\,|_{\mathbf{A}}^s d\mu^\times(y) \\
&= \int_{\mathbf{A}_+^\times} \Phi(y_C) a(y;\mathbf{f})^c a(y;\mathbf{g})\omega(y)\,|\,y\,|_{\mathbf{A}}^s e(2iy_\infty) d\mu^\times(y) \\
&= \int_{\mathbf{A}_f^\times} \Phi(y_C) a(y_f;\mathbf{f})^c a(y_f;\mathbf{g})\omega(y_f)\,|\,y_f\,|_{\mathbf{A}}^s d\mu_f^\times(y_f) \int_{\mathbf{R}_+} e(2iy_\infty) y_\infty^s d\mu^\times(y).
\end{aligned}$$

Thus we compute each integral, for $U = U(1)$

$$\begin{aligned}
&\int_{\mathbf{A}_f^\times} \Phi(y_C) a(y_f;\mathbf{f})^c a(y_f;\mathbf{g})\omega(y_f)\,|\,y_f\,|_{\mathbf{A}}^s d\mu_f^\times(y_f) \\
&\quad = \sum_{0<n\in\mathbf{Z}} n^{-s}\omega^*(n) \int_{nU} a(y_f;\mathbf{f})^c a(y_f;\mathbf{g}) d\mu_f^\times(y_f) \\
&\quad = \sum_{n=1}^{\infty} \omega^*(n)\lambda^c(T(n))\varphi(T(n))n^{-s} = L(2s+2-k-l,\chi^{-1}\psi\omega^2)^{-1} L(s,\lambda^c\otimes\varphi\otimes\omega)
\end{aligned}$$

and

$$\int_{\mathbf{R}_+} e(2iy_\infty) y_\infty^s d\mu^\times(y) = \int_0^\infty e^{-4\pi y} y^{s-1} dy = (4\pi)^{-s}\Gamma(s).$$

This shows

$$L(2s+2-k-l,\chi^{-1}\psi\omega^2) Z(s,f,g,\omega) = (4\pi)^{-s}\Gamma(s) L(s,\lambda^c\otimes\varphi\otimes\omega). \tag{7}$$

As already seen in §5.4, the series $\sum_{n=1}^\infty \omega^*(n)\lambda^c(T(n))\varphi(T(n))n^{-s}$ actually converges absolutely either if $\mathrm{Re}(s) > 1+\frac{k+l}{2}$ or if $\mathrm{Re}(s) > l+\frac{k}{2}$ according as $\mathbf{g}$ is a cusp form or $\mathbf{g}$ is not a cusp form. The integration over $\mathbf{A}/\mathbf{Q}$ needs no justification because $\mathbf{A}/\mathbf{Q}$ is compact and the series are uniformly convergent. As for the integration over $\mathbf{A}^\times/\mathbf{Q}^\times$, replacing each term in the summation by its absolute value, we can perform the interchange of summation and integration because we are dealing with series with positive terms. The resulting series with positive terms after the interchange of the integrals converges if $\mathrm{Re}(s)$ is sufficiently large. Then we apply the dominated convergence theorem of Lebesgue quoted in §2.4 to perform the same interchange without taking absolute value. Thus the identity (7) is valid if $\mathrm{Re}(s)$ is sufficiently large.

Now we compute the integral (6) differently. Recall that

$$\Psi(x) = (\overline{f(x)j_k(x_\infty,i)})((\mathbf{g}\,|\,\omega)(x)j_l(x_\infty,i)).$$

We consider a measure $dv = |\,y\,|_{\mathbf{A}}^{-1} d\mu^\times(y)\otimes d\mu(x)$ on

$$B(\mathbf{A})_+ = \left\{\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix} \in B(\mathbf{A})\,\middle|\, y_\infty > 0\right\}.$$

Since $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\alpha(u) = \alpha(yu)\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$ and $d\mu(yx) = |y|_A d\mu(y)$ (because $\int_{xZ_p} d\mu_p = |x|_p$ (8.5.1)), $b'^* d\mu_B(b) = d\mu_B(b'b) = d\mu_B(b)$, i.e. $d\mu_B$ is left invariant. Then we see, for $B(\mathbf{Q})_+ = B(\mathbf{A})_+ \cap B(\mathbf{Q})$, that

$$Z(s,f,g,\omega) = \int_{B(\mathbf{Q})_+\backslash B(\mathbf{A})_+} \Psi(b)\omega(\det(b))\eta(b)^{s+1} d\mu_B,$$

where $\eta(x)$ is as in (1.9...). Let $GL_2(\mathbf{A})_+ = \{x \in GL_2(\mathbf{A}) \mid \det(x_\infty) > 0\}$ and recall that $C_{\infty+} = \{x \in GL_2(\mathbf{R}) \mid \det(x) > 0 \text{ and } x(i) = i\}$. Now we choose a suitable Haar measure μ_L on $GL_2(\mathbf{A})_+$ depending on $S(L)$ as follows. Let S be any open compact subgroup of $GL_2(\mathbf{A}_f)$. Let $d\mu_\infty$ be the Haar measure on the compact group $C_{\infty+}/Z_\infty$ (for the center Z_∞ of $G_{\infty+}$) with volume 1 (note that $C_{\infty+}/Z_\infty \cong \mathbf{T}$ because $C_{\infty+} = SO_2(\mathbf{R})Z_\infty$). Then we define a measure μ_S on $B(\mathbf{A})_+SC_{\infty+}$ such that

$$\int_{B(\mathbf{A})_+SC_{\infty+}/Z_\infty} \varphi(x)d\mu_S(x) = \int_{B(\mathbf{A})_+}\int_{SC_{\infty+}/Z_\infty} \varphi(bu)d\mu_0(u)d\mu_B(b)$$

for all functions φ on $B(\mathbf{A})_+UC_{\infty+}$, where $d\mu_0$ is the tensor product measure on $SC_{\infty+}/Z_\infty$ of the Haar measure on the compact group S with volume 1 and the measure $d\mu_\infty$ on $C_{\infty+}/Z_\infty$. We take the measure on $GL_2(\mathbf{Q})_+\backslash GL_2(\mathbf{A})_+/SC_{\infty+}$ induced by this measure. In fact, by taking a fundamental domain $\mathcal{F}$ of $GL_2(\mathbf{Q})_+$ in $B(\mathbf{A})_+SC_{\infty+}/SC_{\infty+}$, we define

$$\int_{GL_2(\mathbf{Q})_+\backslash G(\mathbf{A})_+/SC_{\infty+}} f(x)d\mu_S(x) = \int_{\mathcal{F}} f(x)d\mu_S(x).$$

This is possible because of $GL_2(\mathbf{A})_+ = GL_2(\mathbf{Q})_+ \cdot B(\mathbf{A})_+ \cdot S \cdot C_{\infty+}$ (1.1b). The measure we have constructed depends on the choice of S in the following sense. If one takes an open compact subgroup S' of S, then for any right S-invariant function f,

$$\int_{GL_2(\mathbf{Q})_+\backslash G(\mathbf{A})_+/S'C_{\infty+}} f(x)d\mu_{S'}(x) = [S:S']\int_{GL_2(\mathbf{Q})_+\backslash G(\mathbf{A})_+/SC_{\infty+}} f(x)d\mu_S(x),$$

because $d\mu_0$ for S' is $d\mu_0$ for S multiplied by the index $[S;S']$. Let $E(S) = \mathbf{Q}^\times \cap SC_{\infty+}$ (which is either $\{\pm 1\}$ or $\{1\}$) and φ be a function on $B(\mathbf{Q})_+\backslash GL_{2+}(\mathbf{A})/SC_{\infty+}$ such that φ is supported by $B(\mathbf{A})_+SC_{\infty+} = B(\mathbf{A}_f)SG_{\infty+}$. Then we have

$$\text{(8a)} \quad \int_{GL_2(\mathbf{Q})_+\backslash G(\mathbf{A})_+/SC_{\infty+}} \sum_{\gamma \in E(S)B(\mathbf{Q})_+\backslash GL_2(\mathbf{Q})_+} \varphi(\gamma x)d\mu_S(x)$$
$$= \int_{E(S)B(\mathbf{Q})_+\backslash B(\mathbf{A})_+SC_{\infty+}/SC_{\infty+}} \varphi(x)d\mu_S(x) = \int_{B(\mathbf{Q})_+\backslash B(\mathbf{A})_+} \varphi(x)d\mu_B(x).$$

We know from (1) and (4b) that, for $\xi = \chi\psi^{-1}\omega^{-2}$,

$$\Psi(xu)\omega(\det(xu)) = \xi^\#(u)\Psi(x)\omega(\det(x)) \quad \text{for } u \in S(L)$$

where $L = [C^2,N,J]$ is the least common multiple of C^2, N and J. Thus $\xi^{\#}(x)\Psi(x)\omega(\det(x))$ is left $B(\mathbf{Q})_+$-invariant and right $S(L)C_{\infty+}$-invariant. Note that $\xi^{\#}(b)\Psi(b)\omega(\det(b)) = \Psi(b)\omega(\det(b))$ for $b \in B(\mathbf{A})_+$, and write $Y = GL_2(\mathbf{Q})_+\backslash GL_2(\mathbf{A})_+/SC_{\infty+}$. Applying (8a) to $S = S(L)$ and $E(S) = \{\pm 1\}$, we have, writing $d\mu_S$ as $d\mu_L$ and $\xi = \chi\psi^{-1}\omega^{-2}$,

$$\int_{B(\mathbf{Q})_+\backslash B(\mathbf{A})_+}\Psi(b)\omega(\det(b))\eta(b)^{s+1}d\mu_B$$
$$= \int_Y \sum_{\gamma\in\{\pm1\}B(\mathbf{Q})_+\backslash GL_2(\mathbf{Q})_+}\Psi(\gamma x)\omega(\det(\gamma x))\xi^{\#}(\gamma x)\eta(\gamma x)^{s+1}d\mu_L(x).$$

We now compute

$$\Psi(\gamma x) = (\mathbf{f}(\gamma x)j_k(\gamma x_\infty,i))^c((\mathbf{g}\,|\,\omega^{-1})(\gamma x)j_l(\gamma x_\infty,i)) =$$
$$\mathbf{f}(x)^c((\mathbf{g}\,|\,\omega^{-1})(x))j_k(\gamma x_\infty,i)^c j_l(\gamma x_\infty,i) = \mathbf{f}(x)^c((\mathbf{g}\,|\,\omega^{-1})(x))j(\gamma x_\infty,i)^{l-k}\,|\,j(\gamma x_\infty,i)\,|^{2k}.$$

Then we see from (1.11) and (1.10a) that for $w = \begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}$

(8b) $$L(2s+2-k-l,\chi^{-1}\psi\omega^2)Z(s,\mathbf{f},\mathbf{g},\omega)$$
$$= L(2s+2-k-l,\chi^{-1}\psi\omega^2)\int_Y \mathbf{f}^c(\mathbf{g}\,|\,\omega^{-1})(w)\omega(\det(w))$$
$$\times\sum_{\gamma\in\{\pm1\}B(\mathbf{Q})_+\backslash GL_2(\mathbf{Q})_+}\xi^{\#}(\gamma w)\eta(\gamma w)^{s+1}j(\gamma w_\infty,i)^{l-k}\,|\,j(\gamma w_\infty,i)\,|^{2k}d\mu_L(w)$$
$$= \int_Y \mathbf{f}^c(\mathbf{g}\,|\,\omega^{-1})(w)\omega(\det(w))L(2s+2-k-l,\chi^{-1}\psi\omega^2)E^*(w,s-k+1,\xi)\,|\,y\,|_{\mathbf{A}}{}^k d\mu_L(w)$$
$$= \int_Y \mathbf{f}^c(\mathbf{g}\,|\,\omega^{-1})(w)\omega(\det(w))\mathbf{E}_{k-l,L}(w,s-k+1,\xi)\,|\,y\,|_{\mathbf{A}}{}^k d\mu_L(w).$$

Here we claim that

(9) $$Y = GL_2(\mathbf{Q})_+\backslash GL_2(\mathbf{A})_+/S(L)C_{\infty+} \cong \Gamma_0(L)\backslash\mathcal{H} \text{ via } x_\infty \mapsto x_\infty(i).$$

In fact, if $x_\infty = \gamma x'_\infty u$ with $u \in C_{\infty+}$, then $\gamma \in S(L)G_{\infty+}\cap GL_2(\mathbf{Q}) = \Gamma_0(L)$. Therefore the above map is well defined and surjective. The injectivity follows from the fact that $GL_2(\mathbf{A})_+ = GL_2(\mathbf{Q})_+S(L)G_{\infty+}$ (1.1b). Thus the fundamental domain $\mathcal{F}$ we have taken in order to define $d\mu_L$ can be thought of as a fundamental domain of $\Gamma_0(L)\backslash\mathcal{H}$. Then our measure on Y is the familiar one, $y^{-2}dxdy$, by the definition of $d\mu_B$. Noting the fact $\eta\left(\begin{pmatrix} y_\infty & x_\infty \\ 0 & 1\end{pmatrix}\right) = y_\infty$, we know that

(10) $$L(2s+2-k-l,\chi^{-1}\psi\omega^2)Z(s,\mathbf{f},\mathbf{g},\omega) = 2^{-1}((\mathbf{g}\,|\,\omega)E'_{k-l,L}(s-k+1,\chi\psi^{-1}\omega^{-2}),\mathbf{f})_{\Gamma_0(L)},$$

where $(\ ,\ )_\Gamma$ is the Petersson inner product defined in §5.3 and $\mathbf{g}\,|\,\omega \in \mathcal{M}_\lambda(\Gamma_0(J),\psi\omega^2)$ (resp. $\mathbf{f} \in \mathcal{S}_k(\Gamma_0(N),\chi)$) is the modular (resp. cusp) form corresponding to $(\mathbf{g}\,|\,\omega)\otimes\omega$ (resp. $\mathbf{f}$). By Lemma 3.3, $E(z,s) =$

$E'_{k-l,L}(s-k+1,\chi\psi^{-1}\omega^{-2})$ has only polynomial growth as $y \to s \in \mathbf{P}^1(\mathbf{Q})$ (i.e. $E(z,s)$ is slowly increasing). The same fact is true for $g|\omega$ (see Section 5.3). Since f is rapidly decreasing (see (5.3.8a)), $\bar{f}(g|\omega)E(z,s)$ is also rapidly decreasing, and hence $((g|\omega)E'_{k-l,L}(s),f)$ converges absolutely for any s. Thus the function assigning $((g|\omega)E'_{k-l,L}(s),f)$ to s is a meromorphic function of s well defined for all s. In particular, when $k \neq l$, it is an entire function. This shows the analytic continuability of $L(2s+2-k-l,\chi^{-1}\psi\omega^2)Z(s,f,g,\omega)$. Thus we have

Theorem 1 (residue formula). *Let* $\lambda : \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]) \to \mathbf{C}$ *and* $\varphi : \mathbf{h}_l(\Gamma_0(J),\psi;\mathbf{Z}[\psi]) \to \mathbf{C}$ *be algebra homomorphisms with* $k \geq l$ *and let* ω *be a primitive Dirichlet character. Then* $L(s,\lambda^c\otimes\varphi\otimes\omega)$ *can be continued to a meromorphic function on the whole complex s-plane and is entire if* $\mathrm{Re}(s) > \frac{k+l}{2}$ *and if either* $\chi^{-1}\psi\omega^2 N^{k-l}$ *is non-trivial or* $\lambda(T(p)) \neq \omega(p)\varphi(T(p))$ *for at least one prime* p *outside* NJC. *If* $\lambda = \varphi$ *and if* χ *is primitive modulo* N, *the function* $L(s,\lambda^c\otimes\lambda)$ *has a simple pole at* $s = k$ *whose residue is given by*

$$\mathrm{Res}_{s=k}L(s,\lambda^c\otimes\lambda) = 2^{2k-1}\pi^{k+1}(k-1)!^{-1}N^{-1}\prod_{p|N}(1-p^{-1})(f,f)_{\Gamma_0(N)},$$

where $f \in \mathcal{S}_k(\Gamma_0(N),\chi)$ *whose Fourier expansion is given by*

$$f(z) = \sum_{n=1}^{\infty} \lambda(T(n))e(nz).$$

Proof. The first assertion for non-trivial $\chi^{-1}\psi\omega^2 N^{k-l}$ follows from Theorem 2.1 and the argument given above. Note that

$$\mathrm{Res}_{s=1}\mathbf{G}_{0,N}(x,s,\mathrm{id}) = \mathrm{Res}_{s=1}\mathbf{E}_{0,N}(x,s,\mathrm{id}) = \pi\prod_{p|N}(1-p^{-1}).$$

From this, we get, with a non-zero constant c,

$$\mathrm{Res}_{s=k}L(s,\lambda^c\otimes\varphi\otimes\omega) = c(g|\omega,f)_{\Gamma_0(L)}.$$

We know from (5.3.10) that $T(p)^* = \chi(p)^{-1}T(p)$, although we only proved this fact when N and J are powers of a prime in §5 (see [M, §4.5] for the general case). Thus

$$\omega(p)\varphi(T(p))(g|\omega,f) = (g|\omega|T(p),f) = (g|\omega,f|T(p)^*) = \chi(p)\lambda^c(T(p))(g|\omega,f).$$

Since $\lambda^c(T(p)) = \chi(p)^{-1}\lambda(T(p))$ (see (5.4.1) and [M, (4.6.17)]), if $\omega(p)\varphi(T(p)) \neq \lambda(T(p))$, $(g|\omega,f) = 0$. When $\lambda = \varphi$, we can easily compute c using the above residue formula of Eisenstein series and conclude with the residue formula in the theorem.

Returning to the integral expression (8b), the integrand

$$f^c(g\,|\,\omega^{-1})(w)\omega(\det(w))E_{k-l,L}(w,s-k+1,\xi)\,|\,y\,|_A{}^k$$

is the restriction of $\Sigma_{\gamma\in\{\pm1\}B(Q)_+\backslash GL_2(Q)_+}\Psi(\gamma x)\omega(\det(\gamma x))\xi^{\#}(\gamma x)\eta(\gamma x)^{s+1}$ to $B(A)$, which is left invariant under $GL_2(Q)$ and right invariant under $S(L)C_{\infty+}$. Note that the same fact is true for

$$f^c(g\,|\,\omega^{-1})(x)\omega(\det(x))\,|\det(x)\,|_A{}^kE_{k-l,L}(x,s-k+1,\xi).$$

This shows that

$$\begin{aligned}(11)\quad & L(2s+2-k-l,\chi^{-1}\psi\omega^2)Z(s,f,g,\omega)\\ &= \int_Y f^c(g\,|\,\omega^{-1})(x)\omega(\det(x))\,|\det(x)\,|_A{}^kE_{k-l,L}(x,s-k+1,\xi)d\mu_L(x).\end{aligned}$$

§9.5. Functional equations for Rankin products

In this section, we prove the functional equation for Rankin products which also establishes the holomorphy of the L-function $L(s,\lambda^c\otimes\varphi)$ if $\lambda\neq\varphi$. We follow the treatment given in [H5, I.9]. We start with algebra homomorphisms $\lambda : \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]) \to \mathbf{C}$ and $\varphi : \mathbf{h}_l(\Gamma_0(J),\psi;\mathbf{Z}[\psi]) \to \mathbf{C}$ and suppose:

(1a) $k \geq l$,

(1b) χ and ψ are primitive modulo N and J, respectively,

(1c) $\chi^{-1}\psi$ is primitive modulo L,

where L is the least common multiple of N and J. The first assumption (1a) is harmless, but the other two conditions impose a real restriction. To remove this assumption, the simplest way is the use of harmonic analysis on $GL_2(A)$ [J], although one can do that in classical way adding a large amount of technicality. The reason for this difficulty is that, without the conditions (1b,c), the L-function $L(s,\lambda^c\otimes\varphi)$ lacks some of the Euler factors (whose exact form can be predicted using Galois representations attached to modular forms discussed in §7.5; see [D1, (1.2.1)]) at places p dividing L, and thus we cannot expect a good functional equation without supplementing missing Euler factors. In [J, IV], all the Euler factors are defined in terms of admissible representations and are computed explicitly when the attached local representations are subquotients of an induced representation of a character of a Borel subgroup. Then the functional equation is proven for any automorphic L-functions of $GL(2)\times GL(2)$ in [J,§19] including $L(s,\lambda^c\otimes\varphi)$ treated here. The Euler factor for super-cuspidal local representations is recently computed in [GJ] (see also [Sch] and [H6]). Here we do not intend to be selfcontained. In fact, we shall use the semi-simplicity of $\mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Q}(\chi))$ (for example, [M, Th.4.6.13]), when χ is primitive modulo N, which is proven in the text as Theorem 5.3.2 when N is a prime power. Anyway, the proof in the

general case is basically the same as in the case of p-power level and is a good exercise after studying the proof in the special case.

Let $\mathbf{f}$ (resp. $\mathbf{g}$) be the normalized eigenform corresponding to λ and φ. We write f and g for the corresponding classical modular forms $\mathbf{f}_1$ and $\mathbf{g}_1$, respectively. We start with the integral expression

$$2^{-s}\Gamma_{\mathbf{C}}(s)L(s,\lambda^c\otimes\varphi) = \int_Y(\mathbf{f}^c\mathbf{g})(x)\mathbf{E}_{k-l,L}(x,s-k+1,\xi)\,|\det(x)|_{\mathbf{A}}{}^k d\mu_L(x),$$

where $Y = GL_2(\mathbf{Q})_+\backslash GL_2(\mathbf{A})_+/S(L)C_{\infty+} \cong \Gamma_0(L)\backslash\mathcal{H}$ and $\xi = \chi\psi^{-1}$. Applying the functional equation for Eisenstein series (Theorem 3.1): for $w = \begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}$

$$\begin{aligned}\Gamma_{\mathbf{C}}(s-l+1)&\mathbf{E}_{k-l,L}(w,s-k+1,\xi)\\ &= 2^{-2s+k+l-1}L^{-3s+k-2+2l}\xi_\infty(-1)G(\xi^{-1})\Gamma_{\mathbf{C}}(k-s)\mathbf{G}_{k-l,N}(w,l-s,\xi)\\ &= 2^{-2s+k+l-1}L^{-3s+k-2+2l}\xi_\infty(-1)G(\xi^{-1})\Gamma_{\mathbf{C}}(k-s)\xi(\det(w))\mathbf{E}_{k-l}(w\tau_L,l-s,\xi^{-1}),\end{aligned}$$

we have

$$\begin{aligned}(2a)\quad 2^{-s}&\Gamma_{\mathbf{C}}(s-l+1)\Gamma_{\mathbf{C}}(s)L(s,\lambda^c\otimes\varphi)\\ &=\int_Y\mathbf{f}^c\mathbf{g}(x)\Gamma_{\mathbf{C}}(s-l+1)\mathbf{E}_{k-l,L}(x,s-k+1,\xi)\,|\det(x)|_{\mathbf{A}}{}^k d\mu_L(x)\\ &= 2^{-2s+k+l-1}L^{-3s+k-2+2l}\xi_\infty(-1)G(\xi^{-1})\Gamma_{\mathbf{C}}(k-s)\\ &\quad\times\int_Y\bar{\mathbf{f}}\mathbf{g}(x_\infty)\xi(\det(x))\mathbf{E}_{k-l}(x\tau_L,l-s,\xi^{-1})\,|\det(x)|_{\mathbf{A}}{}^k d\mu_L(x)\\ &\overset{x\mapsto x\tau^{-1}}{=} 2^{-2s+k+l-1}L^{-3s+k-2+2l}\xi_\infty(-1)G(\xi^{-1})\Gamma_{\mathbf{C}}(k-s)\\ &\quad\times\int_Y\overline{\mathbf{f}(\tau_L^{-1}x)}\mathbf{g}(\tau_L^{-1}x)\mathbf{E}_{k-l}(x_\infty,l-s,\xi^{-1})\,|\det(\tau_L^{-1}x)|_{\mathbf{A}}{}^k d\mu_L(x).\end{aligned}$$

In order to avoid confusion between $\mathbf{f}(x)^c = \overline{\mathbf{f}(x)}$ (complex conjugation applied to the value $\mathbf{f}(x)$) and $\mathbf{f}^c(x)$ (complex conjugation applied to the Fourier coefficient, i.e., $a(n,\mathbf{f}^c) = a(n,\mathbf{f})^c$), we write the latter action as $\mathbf{f}_c$. Then we claim that

$$\mathbf{f}\,|\,\tau_N^{-1}(x) = \chi(\det(x))^{-1}\mathbf{f}(x\tau_N^{-1}) = N^{-k/2}W(\lambda)\mathbf{f}_c(x) \quad\text{and}\quad \mathbf{g}\,|\,\tau_J^{-1} = J^{-l/2}W(\varphi)\mathbf{g}_c$$

for the constants $W(\lambda)$ and $W(\varphi)$ with absolute value 1, where $\tau_N = \begin{pmatrix} 0 & -1 \\ N & 0\end{pmatrix} \in GL_2(\mathbf{A}_f)$. In fact, by the same computation as in (1.1a), we see that $(\mathbf{f}\,|\,\tau_N^{-1})_1 = f(\tau_N(z))j(\tau_N,z)^{-k}$ regarding τ_N on the right-hand side as an element in $GL_2(\mathbf{Q})$. Then Proposition 5.5.1 shows the fact when N is a p-power. A key point is that $T^*(p) = \tau_N T(p)\tau_N^{-1}$ for p outside N and $\tau_N S(N)\tau_N^{-1} = S(N)$. The general case follows from the semi-simplicity of the Hecke algebra $\mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Q}(\chi))$ by the same argument which proves

Proposition 5.5.1. Note that $\tau_L = \tau_N\beta$ with $\beta = \begin{pmatrix} M(\lambda) & 0 \\ 0 & 1 \end{pmatrix}$ for $M(\lambda)N = L$. Then $\mathbf{f}\,|\,\tau_L^{-1}(x) = \chi(\det(x))^{-1}(\mathbf{f}(x\beta^{-1}\tau_N^{-1})) = \mathbf{f}\,|\,\tau_N^{-1}(x\beta^{-1}) = N^{-k/2}\mathbf{f}_c(x\beta^{-1})$ using the fact that $1 = \chi(N) = \chi(N_f)\chi_\infty(N) = \chi(N_f)$. This shows that

$$a(n;\mathbf{f}\,|\,\tau_L^{-1}) = N^{-k/2}W(\lambda)a(n/M(\lambda),\mathbf{f})^c = N^{-k/2}W(\lambda)\lambda(T(n/M(\lambda)))^c \text{ and}$$
$$a(n;\mathbf{g}\,|\,\tau_L^{-1}) = J^{-l/2}W(\varphi)a(n/M(\varphi),\mathbf{g})^c = J^{-l/2}W(\varphi)\varphi(T(n/M(\varphi)))^c$$

for $M(\varphi) = L/J$. Thus (2a) is equal to, for $\beta' = \begin{pmatrix} M(\varphi) & 0 \\ 0 & 1 \end{pmatrix}$ and $w = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$,

$$\begin{aligned}
\text{(2b)}\quad & W(\lambda)^cW(\varphi)2^{-2s+k+l-1}L^{-3s+2k-2+2l}N^{-k/2}J^{-l/2}\xi_\infty(-1)G(\xi^{-1})\Gamma_C(k-s) \\
& \times\int_Y \mathbf{f}_c(w\beta^{-1})^c\mathbf{g}_c(w\beta'^{-1})E'_{k-l,L}(z,l-s,\xi^{-1})y^{k-2}dxdy \qquad (z = x+iy) \\
& = W(\lambda)^cW(\varphi)2^{-s}N^{-k/2}J^{-l/2}L^{-3s+2k-2+2l}\xi_\infty(-1)G(\xi^{-1})\Gamma_C(k-s)\Gamma_C(k+l-1-s) \\
& \quad \times L_L(k+l-2s,\chi\psi^{-1})\textstyle\sum_{n=1}^\infty \lambda(T(n/M(\lambda)))\varphi^c(T(n/M(\varphi)))n^{s+1-k-l},
\end{aligned}$$

where we agree that $\lambda(T(n)) = \varphi^c(T(n)) = 0$ if n is not an integer. Since L is the least common multiple of N and J and since $L = M(\lambda)N = M(\varphi)J$, $M(\lambda)$ and $M(\varphi)$ are mutually prime. Then $n/M(\lambda)$ and $n/M(\varphi)$ are both integers if and only if n is divisible by $M(\lambda)M(\varphi)$. Moreover $M(\lambda)\,|\,J$ and $M(\varphi)\,|\,N$, and hence we have $T(p^e) = T(p)^e$ for p dividing the level (see (5.3.4a) and [M, Lemma 4.5.7]). Therefore, we have

$$\lambda(T(nM(\varphi))) = \lambda(T(n))\lambda(T(M(\varphi))) \text{ and } \varphi(T(nM(\lambda))) = \lambda(T(n))\lambda(T(M(\lambda))).$$

Thus we see that

$$\begin{aligned}
\text{(2c)}\quad & \sum_{\substack{n=1 \\ n\mapsto M(\lambda)M(\varphi)n}}^\infty \lambda(T(n/M(\lambda)))\varphi^c(T(n/M(\varphi)))n^{-s} \\
& = (M(\lambda)M(\varphi))^{-s}\textstyle\sum_{n=1}^\infty \lambda(T(nM(\varphi)))\varphi^c(T(nM(\lambda)))n^{-s} \\
& = \lambda(T(M(\varphi)))\varphi^c(T(M(\lambda)))(M(\lambda)M(\varphi))^{-s}\textstyle\sum_{n=1}^\infty \lambda(T(n))\varphi^c(T(n))n^{-s}.
\end{aligned}$$

Combining (2a,b,c), we get

$$\begin{aligned}
& 2^{-s}\Gamma_C(s-l+1)\Gamma_C(s)L(s,\lambda^c\otimes\varphi) \\
& \quad = W(\lambda)^cW(\varphi)2^{-s}N^{-k/2}J^{-l/2}L^{-3s+2k-2+2l}\xi_\infty(-1)G(\xi^{-1})\lambda(T(M(\varphi)))\varphi^c(T(M(\lambda))) \\
& \qquad \times(M(\lambda)M(\varphi))^{s+1-k-l}\Gamma_C(k-s)\Gamma_C(k+l-1-s)L(k+l-1-s,\lambda\otimes\varphi^c).
\end{aligned}$$

Using the fact that $\xi(-1) = (-1)^{k-l}$, $W(\lambda^c)W(\lambda) = (-1)^k$ (Proposition 5.5.1), $M(\lambda) = L/N$ and $M(\varphi) = L/J$ and $W(\xi^{-1}) = G(\xi^{-1})/|G(\xi^{-1})| = G(\xi^{-1})L^{-1/2}$ (Exercise 2.3.5), we get

Theorem 1 (Functional equation). *Suppose (1a,b,c). Then for the least common multiple L of N and J, we have*

$$G_\infty(s)L(s,\lambda^c\otimes\varphi) = W(\lambda^c\otimes\varphi)(LNJ)^{-s+((k+l-1)/2)}G_\infty(k+l-1-s)L(k+l-1-s,\lambda\otimes\varphi^c),$$

where $G_\infty(s) = \Gamma_C(s-l+1)\Gamma_C(s)$ *and*

$$W(\lambda^c\otimes\varphi) = (-1)^l W(\lambda^c)W(\varphi)W(\chi^c\psi)\frac{\lambda(T(M(\varphi)))\varphi(T(M(\lambda)))^c}{M(\varphi)^{(k-1)/2}\ M(\lambda)^{(l-1)/2}}.$$

By our assumptions (1b,c), we know that $M(\lambda)\,|\,J$ and $M(\varphi)\,|\,N$. Under this circumstance, it is known that $|W(\lambda^c\otimes\varphi)| = 1$ (see [M, Th.4.6.17]). Since we know that $G_\infty(s)L(s,\lambda^c\otimes\varphi)$ is holomorphic if $\lambda \neq \varphi$ and

$$\mathrm{Re}(s-k+1) > \frac{l-k}{2} \iff \mathrm{Re}(s) > \frac{k+l-2}{2}$$

by Theorem 2.1. Since $k \geq l > 0$, this is enough to show that $G_\infty(s)L(s,\lambda^c\otimes\varphi)$ is entire on the whole s-plane if $\lambda \neq \varphi$. When $\lambda = \varphi$, by the same reasoning, the only singularity of $\Gamma_C(s-k+1)\Gamma_C(s)L(s,\lambda^c\otimes\lambda)$ is at $s = k$ and $k-1$. Thus we have

Corollary 1. *Suppose (1a,b,c). Then* $G_\infty(s)L(s,\lambda^c\otimes\varphi)$ *is an entire function of* s *unless* $\lambda = \varphi$. *If* $\lambda = \varphi$, $G_\infty(s)L(s,\lambda^c\otimes\lambda)$ *has two simple poles at* $s = k$ *and* $k-1$.

Chapter 10. Three variable p-adic Rankin products

In this chapter, we first prove Shimura's algebraicity theorem for Rankin product L-functions $L(s,\lambda\otimes\varphi)$. Then we construct three variable p-adic Rankin products extending the result obtained in §7.4. As for the algebraicity theorem, we follow the treatment in [Sh3], [Sh4] and also [H5, §6], [H7]. We only treat the case of $GL_2(\mathbf{Q})$. For further study of this type of algebraicity questions for the algebraic group $GL(2)$ over general fields, we refer to Shimura's papers [Sh5, Sh8, Sh11, Sh12] and [H8] for totally real fields and [H9] for fields containing CM fields. As for the p-adic L-functions, we generalize the method developed in [H7]. Another method of dealing with this problem can be found in [H5]. The general case of $GL(2)$ over totally real fields is treated in [H8]. There is one more method of getting p-adic continuation of $L(s,\lambda\otimes\varphi)$ along the cyclotomic line (i.e. varying s) found by Panchishkin [Pa].

§10.1. Differential operators of Maass and Shimura

We study here the differential operators δ_k introduced by Maaß and later studied by Shimura acting on C^∞-class modular forms f on $\mathcal{H}$: for a complex number k and for $y = \mathrm{Im}(z)$

(1a) $$\delta_k = \frac{1}{2\pi i}\left(\frac{\partial}{\partial z} + \frac{k}{2iy}\right) \text{ and } \delta_k^r = \delta_{k+2r-2}\cdot\cdots\cdot\delta_{k+2}\delta_k,\ \delta_k^0 f = f.$$

We also define

(1b) $$\varepsilon = -\frac{1}{2\pi i}y^2\frac{\partial}{\partial \bar{z}} \text{ and } d = \frac{1}{2\pi i}\frac{\partial}{\partial z}.$$

It is easy to check that

(1c) $$\delta_k f = y^{-k}d(y^k f) \text{ and } \delta_k^r = y^{-k-2r}(y^2 d y^{-2})^r y^{k+2}.$$

Now define a new "weight k" action (denoted by $f \mapsto f\|_k\alpha$) of $\alpha \in G_{\infty+}$ as follows:

$$f\|_k\alpha(z) = \det(\alpha)^{k/2}f(\alpha(z))j(\alpha,z)^{-k} = \det(\alpha)^{1-(k/2)}f|_k\alpha(z).$$

Then the operators δ_k and ε have the following automorphic property: if f is of C^r-class,

(2) $$\delta_k^r(f\|_k\alpha) = (\delta_k^r f)\|_{k+2r}\alpha \text{ and } \varepsilon^r(f\|_k\alpha) = (\varepsilon^r f)\|_{k-2r}\alpha \text{ for all } \alpha \in G_{\infty+}.$$

The proof is a simple computation. We only give a detail account for δ. We may assume that $\det(\alpha) = 1$ and need to prove $\delta_k(f\|_k\alpha) = (\delta_k f)\|_{k+2}\alpha$. Note that

$$\frac{\partial}{\partial z}\alpha(z) = j(\alpha,z)^{-2}, \text{ and}$$

$$\frac{\partial}{\partial z}j(\alpha,z)^{-k} = -kcj(\alpha,z)^{-k-1} \text{ and } y(\alpha(z)) = y(z)\,|j(\alpha,z)|^{-2}.$$

We see, writing $j = j(\alpha,z)$ and noting $y(\alpha(z)) = \frac{y}{j\bar{j}}$ that

$$2\pi i\{\delta_k(f\|_k\alpha)-(\delta_k^r f)\|_{k+2}\alpha\} = -kcf(\alpha(z))j^{-k-1}+\frac{kf(\alpha(z))}{2iy}j^{-k} - \frac{k}{2iy(\alpha(z))}f(\alpha(z))j^{-k-2}$$
$$= \frac{kf(\alpha(z))}{2iy}j^{-k}\left\{1-\left(\frac{2iyc}{cz+d}+\frac{c\bar{z}+d}{cz+d}\right)\right\} = 0.$$

Exercise 1. Prove the second formula of (2).

We now claim that the following two formulas holds:

$$(3)\quad \delta_k^r f = \sum_{j=0}^{r}\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(j+k)}(-4\pi y)^{j-r}d^j \text{ and } d^r f = \sum_{j=0}^{r}\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(j+k)}(4\pi y)^{j-r}\delta_k^j f.$$

Since the proof for these two formulas is basically the same, we only give an argument for the second formula. We proceed by induction on r. When $r = 1$, the right-hand side equals

$$k(4\pi y)^{-1}f+\delta_k f = \frac{kf}{4\pi y} + \frac{1}{2\pi i}\left(\frac{\partial}{\partial z}+\frac{k}{2iy}\right)f = df,$$

which shows the formula when $r = 1$. Now assume that $r > 0$ and that the formula is true for d^r. Then

$$d^{r+1}f = \frac{1}{2\pi i}\frac{\partial}{\partial z}\left(\sum_{j=0}^{r}\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(j+k)}(4\pi y)^{j-r}\delta_k^j f\right).$$

Note that $d = \delta_{k+2j}+\frac{k+2j}{4\pi y}$ and $d(4\pi y)^{j-r} = (r-j)(4\pi y)^{j-r-1}$. Thus

$$d^{r+1}f = \frac{1}{2\pi i}\frac{\partial}{\partial z}\left(\sum_{j=0}^{r}\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(j+k)}(4\pi y)^{j-r}\delta_k^j f\right)$$
$$= \sum_{j=0}^{r}\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(j+k)}\{(r-j)(4\pi y)^{j-r-1}\delta_k^j f+(4\pi y)^{j-r}\delta_k^{j+1}f+(k+2j)(4\pi y)^{j-r-1}\delta_k^j f\}.$$

The coefficient of $(4\pi y)^{j-(r+1)}\delta_k^j f$ is given by, when $1 \le j \le r$,

$$(r-j)\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(r+j)}+\binom{r}{j-1}\frac{\Gamma(r+k)}{\Gamma(j-1+k)}+(k+2j)\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(j+k)}$$
$$= \binom{r+1}{j}\frac{\Gamma(k+r+1)\{(r-j+1)(r-j)+(k+2j)(r+1-j)+j(k+j-1)\}}{(r+1)(k+r)\Gamma(k+j)} = \binom{r+1}{j}\frac{\Gamma(k+r+1)}{\Gamma(k+j)}.$$

When $j = 0$, it is given by

$$r\binom{r}{0}\frac{\Gamma(k+r)}{\Gamma(k)}+r\binom{r}{0}\frac{\Gamma(k+r)}{\Gamma(k)} = \binom{r+1}{0}\frac{\Gamma(k+r+1)}{\Gamma(k)}.$$

Similarly, when $j = r+1$, it is given by

$$\binom{r}{r}\frac{\Gamma(k+r)}{\Gamma(k+r)} = \binom{r+1}{r+1}\frac{\Gamma(k+r+1)}{\Gamma(k+r+1)}.$$

This shows the validity of (3).

Exercise 2. Give a detailed proof of the first formula of (3).

If f is a holomorphic function on $\mathcal{H}$ having q-expansion of the form

$$f(z) = \sum_{n=1}^{\infty} a(n/N;f)q^n \quad (q = e(z/N)) \text{ for a positive integer } N,$$

then as a power series of q, $f(q)$ converges absolutely on a small disk $D_r = \{\,|q| < r\}$. Taking a smaller disk D_ε, $f(q)/q$ gives a continuous function of q on the closure of D_ε which is compact. Hence $|f(q)/q|$ is bounded, i.e. $|f(z)| \le C\exp(-2\pi y/N)$ as $y \to \infty$ for a constant C. In other words, f decreases exponentially at $i\infty$. If f is a holomorphic cusp form for a congruence subgroup Γ of $SL_2(\mathbf{Z})$, the function f is therefore rapidly decreasing. Moreover $\frac{\partial^r f}{\partial z^r}$ is also exponentially decreasing as $y \to \infty$. Since $(\delta_k^r f)$ is a polynomial in $(4\pi y)^{-1}$ with holomorphic function coefficients as above, $(\delta_k^r f)$ still decreases exponentially as $y \to \infty$. Since $\delta_k^r(f\|_k\alpha) = (\delta_k^r f)\|_{k+2r}\alpha$, applying the above argument to $f\|_k\alpha$ for $\alpha \in SL_2(\mathbf{Z})$ in place of f, we know that $f\|_k\alpha$ decreases exponentially as $y \to \infty$. Thus we know that

(4a) $(\delta_k^r f)$ *is rapidly decreasing as a modular form for* Γ *of weight* $k+2r$ *if* f *is a holomorphic cusp form of weight* k *for* Γ.

Similarly we can prove that

(4b) $(\delta_k^r f)$ *is slowly increasing as a modular form for* Γ *of weight* $k+2r$ *if* f *is a holomorphic modular form of weight* k *for* Γ.

Let $f = \sum_{j=0}^{r}(4\pi y)^{-j}f_j$ be a C^∞-function on $\mathcal{H}$. Suppose that the functions f_j are all holomorphic. We claim that

(5a) $$f_j = 0 \text{ for all } j \text{ if } f = 0.$$

We prove this by induction on r (see [Sh10, §2]). When $r = 0$, there is nothing to prove. Applying $\frac{\partial}{\partial \bar{z}}$, we get $0 = \sum_{j=1}^{r}-(2\pi j\sqrt{-1})(4\pi y)^{-j-1}f_j$. Then dividing out by $(4\pi y)^{-2}$ and applying the induction assumption, we get $f_j = 0$ for $j > 0$. This shows, at the same time, $0 = f = f_0$. In particular,

$$\varepsilon f = (16\pi^2)^{-1}\sum_{j=1}^{r} j(4\pi y)^{-j+1}f_j.$$

Iterating this operation r times, we arrive, if f is of degree r in $(4\pi y)^{-1}$, at

(5b) $$\varepsilon^r f = c_r f_r \qquad \text{with } c_r = (16\pi^2)^{-r}r!.$$

In particular, if f is an arbitrary C^∞-function on $\mathcal{H}$ with $\varepsilon^{r+1}f = 0$, then $f_r = c_r^{-1}\varepsilon^r f$ is a holomorphic function, and $\varepsilon^r(f-(4\pi y)^{-r}f_r) = 0$ by (5b). Thus by induction on r, we see the following fact for a C^∞-function f on $\mathcal{H}$ ([Sh10, Prop.2.4]):

(5c) $\varepsilon^{r+1}f = 0 \Leftrightarrow$ *there exist holomorphic functions* f_j $(j = 1, 2, \ldots, r)$ *such that* $\sum_{j=0}^{r}(4\pi y)^{-j}f_j$,

where f_j is uniquely determined by f. Now we suppose that f is a modular form of weight $k+2r$ for a congruence subgroup Γ satisfying the equivalent conditions (5c). Then $f\|_{k+2r}\gamma = f$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ implies

$$\sum_{j=0}^{r}(4\pi y)^{-j}f_j = \sum_{j=0}^{r}((4\pi y)^{-j}f_j)\|_{k+2r}\gamma = \sum_{j=0}^{r}(4\pi y)^{-j}f_j(\gamma(z))(cz+d)^{-k-2r}\,|cz+d|^{2j}$$

$$= \sum_{j=0}^{r}(4\pi y)^{-j}f_j(\gamma(z))(cz+d)^{-k-2r+j}(c\bar{z}+d)^{j}$$

$$= \sum_{j=0}^{r}(4\pi y)^{-j}f_j(\gamma(z))(cz+d)^{-k-2r+j}\{c(z-2iy)+d\}^{j}$$

$$= \sum_{j=0}^{r}(4\pi y)^{-j}f_j(\gamma(z)) \sum_{m=0}^{j}\binom{j}{m}(cz+d)^{-k-2r+j+m}(-2icy)^{j-m}$$

$$= (4\pi y)^{-r}f_r\|_k\gamma + \sum_{m=0}^{r-1}(4\pi y)^{-m}\sum_{j=m}^{r-1}(2\pi i c^{-1})^{m-j}\binom{j}{m}f_j\|_{k+2r-j-m}\gamma.$$

Noting that the second sum in the last formula is a polynomial in $(4\pi y)^{-1}$ of degree less than r, we conclude from (5a) that $f_r\|_k\gamma = f_r$ for all $\gamma \in \Gamma$ comparing the coefficient in $(4\pi y)^{-r}$. Now by (3), $\frac{\Gamma(k)}{\Gamma(r+k)}(\delta_k^r f_r)$ is a C^∞-class modular form of weight $k+2r$ which is a polynomial in $(4\pi y)^{-1}$ of degree r whose coefficient in $(4\pi y)^{-r}$ is f_r. Thus $f-(\delta_k^r h_r)$ for $h_r = \frac{\Gamma(k)}{\Gamma(r+k)}f_r$ is of degree $r-1$. Repeating this process, we can write, if $k \geq 1$ and $r \geq 0$,

(6) $f = \sum_{j=0}^{r}\delta_{k+2r-2j}^{j}h_j$ if f satisfies (5c) ([Sh3], [Sh10, Prop.3.4]),

where h_j is a holomorphic modular form of weight $k+2r-2j$. The modular forms h_j are uniquely determined by f. In this argument proving (6), we implicitly assumed that $k \geq 1$; otherwise, $h_r = \frac{\Gamma(k)}{\Gamma(r+k)}f_r$ may not be well defined (i.e. $\frac{\Gamma(k)}{\Gamma(r+k)}$ may have a pole at non-positive integers k). Now we have by (2) $\varepsilon^{r+1}(f\|_{k+2r}\alpha) = (\varepsilon^{r+1}f)\|_{k-2}\alpha = 0$ for $\alpha \in GL_2(\mathbf{Q})\cap G_{\infty+}$ Then by (5c), we can write $f\|_{k+2r}\alpha = \sum_{j=0}^{r}\delta_{k+2r-2j}^{j}h'_j$ for holomorphic modular forms h'_j. On the other hand, by (2)

$$\sum_{j=0}^{r}\delta_{k+2r-2j}^{j}h'_j = f\|_{k+2r}\alpha = \left\{\sum_{j=0}^{r}\delta_{k+2r-2j}^{j}h_j\right\}\|_{k+2r}\alpha = \sum_{j=0}^{r}\delta_{k+2r-2j}^{j}(h_j\|_{k+2r-2j}\alpha).$$

By the uniqueness of h'_j, we see that $h'_j = h_j \|_{k+2r-2j}\alpha$. This shows that

(7) *f is slowly increasing (resp. rapidly decreasing) if and only if* h_j *is holomorphic at every cusp (resp. a cusp form).*

Let $\mathcal{N}_k^r(\Gamma_0(N),\chi)$ be the space of C^∞ modular forms f satisfying:

(N1) f *is slowly increasing;*

(N2) $\varepsilon^{r+1}f = 0$;

(N3) $f|_k\gamma = \chi(d)f$ *for* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$,

where χ is a Dirichlet character modulo N. We also consider the subspace $\mathcal{NS}_k^r(\Gamma_0(N),\chi)$ of $\mathcal{N}_k^r(\Gamma_0(N),\chi)$ consisting of rapidly decreasing forms. Modular forms in these spaces are called nearly holomorphic modular forms. We have proven

Theorem 1. *Suppose that* $r \geq 0$ *and* $k \geq 1$. *Then we have*

$$\mathcal{N}_{k+2r}^r(\Gamma_0(N),\chi) \cong \oplus_{j=0}^r \mathcal{M}_{k+2r-2j}(\Gamma_0(N),\chi),$$
$$\mathcal{NS}_{k+2r}^r(\Gamma_0(N),\chi) \cong \oplus_{j=0}^r \mathcal{S}_{k+2r-2j}(\Gamma_0(N),\chi).$$

The isomorphisms are given by $f \mapsto (h_j)$ *as in (6). Moreover these isomorphisms are equivariant under the "*$\|$*"-action of* $G_{\infty+}$.

We write the projection map $f \mapsto h_0$ as

(8a) $$H : \mathcal{N}_{k+2r}^r(\Gamma_0(N),\chi) \to \mathcal{M}_{k+2r}(\Gamma_0(N),\chi),$$

which is called the holomorphic projection. Since we have a Galois action $f \mapsto f^\sigma$ ($\sigma \in \mathrm{Aut}(\mathbf{C})$) taking $\mathcal{M}_k(\Gamma_0(N),\chi)$ to $\mathcal{M}_k(\Gamma_0(N),\chi^\sigma)$ (see §§5.3 and 5.4), we can define a Galois action on $\mathcal{N}_{k+2r}^r(\Gamma_0(N),\chi)$ so that f^σ corresponds (h_j^σ) under the isomorphism of Theorem 1. Then by definition, we in particular have, if $k \geq 1$ and $r \geq 0$,

(8b) $$H(f^\sigma) = (H(f))^\sigma \text{ for all } f \in \mathcal{N}_{k+2r}^r(\Gamma_0(N),\chi).$$

Note here that $d(\sum_{n=0}^\infty a_n q^n) = \sum_{n=0}^\infty n a_n q^n$, i.e. $d = q\frac{d}{dq}$. This implies $d(f^\sigma) = (df)^\sigma$ for the naive Galois action on q-expansion coefficients. By our definition, the monomial "$(4\pi y)^{-m}$" is invariant under the Galois action. Since δ_k is the sum of the multiplication by $-k(4\pi y)^{-1}$ and d, we see that

(8c) $$\delta_k(f^\sigma) = (\delta_k f)^\sigma \text{ for } f \in \mathcal{N}_{k+2r}^r(\Gamma_0(N),\chi).$$

We want to compute the adjoint of δ_k and ε under the Petersson inner product. We start with a general argument. Consider a compactly supported C^∞-function ϕ and a C^∞-function ψ. Let

$$E = 2y^2\frac{\partial}{\partial\bar{z}},\ \Delta = 2\{\frac{k}{2iy}+\frac{\partial}{\partial z}\},\ E_x = y^2\frac{\partial}{\partial x},\ E_y = iy^2\frac{\partial}{\partial y},$$
$$\text{and}\quad \Delta_x = \frac{\partial}{\partial x},\ \Delta_y = -i\{\frac{k}{y}+\frac{\partial}{\partial y}\}.$$

Then $E = E_x+E_y$ and $\Delta = \Delta_x+\Delta_y$. Writing $\psi^c(z) = (\psi(z))^c$ for complex conjugation c, we have, for $y(z) = \mathrm{Im}(z)$,

$$\frac{\partial\phi\psi^c y^k}{\partial x} = \frac{\partial\phi}{\partial x}\psi^c y^k+\phi\frac{\partial\psi^c}{\partial x}y^k = (\Delta_x\phi)\psi^c y^k+\phi(E_x\psi)^c y^{k-2},$$
$$\frac{\partial\phi\psi^c y^k}{\partial y} = \frac{\partial\phi}{\partial y}\psi^c y^k+k\phi\psi^c y^{k-1}+\phi\frac{\partial\psi^c}{\partial y}y^k = i(\Delta_y\phi)\psi^c y^k+i\phi(E_y\psi)^c y^{k-2}.$$

This shows

$$0 = [\phi\psi^c y^k]_{-\infty}^{\infty} = \int_{-\infty}^{\infty}\frac{\partial\phi\psi^c y^k}{\partial x}dx = \int_{-\infty}^{\infty}(\Delta_x\phi)\psi^c y^k dx+\int_{-\infty}^{\infty}\phi(E_x\psi)^c y^{k-2}dx,$$
$$0 = -i[\phi\psi^c y^k]_0^{\infty} = -i\int_0^{\infty}\frac{\partial\phi\psi^c y^k}{\partial y}dy = \int_0^{\infty}(\Delta_y\phi)\psi^c y^k dy+\int_0^{\infty}\phi(E_y\psi)^c y^{k-2}dy.$$

Thus we have the following adjoint formula:

$$\int_{\mathcal{H}}(\Delta\phi)\psi^c y^k dxdy = -\int_{\mathcal{H}}\phi(E\psi)^c y^{k-2}dxdy. \tag{9}$$

Let Γ be a congruence subgroup of $SL_2(\mathbf{Z})$. Let ϕ be a C^∞-class modular form of weight k. We take a sufficiently fine (locally finite) open covering $\Gamma\backslash\mathcal{H} = \bigcup_{j\in I}U_j$ on $\mathcal{H}$ so that U_j is simply connected. Let $\pi : \mathcal{H}\to\Gamma\backslash\mathcal{H}$ be the projection. We choose a connected component U_j^* in $\pi^{-1}(U_j)$. Thus π induces an isomorphism: $U_j^* \cong U_j$. Then we take a partition of unity of class C^∞: $1 = \sum_{j\in I}\chi_j$; here, χ_j is a C^∞-function with $\mathrm{Supp}(\chi_j) \subset U_j$. We regard χ_j as a function on U^*_j under the identification induced by π. Then $\chi_j\phi : U_j^* \to \mathbf{C}$ is a C^∞-function whose support is contained in U_j^*. Thus we can extend $\chi_j\phi$ to all $\mathcal{H}$ by 0 outside U_j^*. Then for any C^∞-class modular form ψ of weight k+2 for Γ, we see from (9) that

$$(\delta_k\phi,\psi) = \int_{\Gamma\backslash\mathcal{H}}(\delta_k\textstyle\sum_{j\in I}\chi_j\phi)\psi^c y^k dxdy = \sum_{j\in I}\int_{\mathcal{H}}\delta_k(\chi_j\phi)\psi^c y^k dxdy \tag{10}$$
$$= \textstyle\sum_{j\in I}\int_{\mathcal{H}}\chi_j\phi\varepsilon(\psi)^c y^{k-2}dxdy = (\phi,\varepsilon\psi)$$

as long as $\sum_{j\in I}\int_{\mathcal{H}}\delta_k(\chi_j\phi)\psi^c y^k dxdy$ is absolutely convergent. When either ϕ or ψ is rapidly decreasing and the other is slowly increasing, we can always choose the covering $\{U_j\}$ so that the above sum is absolutely convergent. Let us see that this is so. We take out a small neighborhood of each cusp in $\Gamma\backslash\mathcal{H}$ and write the rest as Y_0. Then Y_0 is relatively compact. We choose a closed neighborhood D_s of each cusp s so that $Y_0\cap D_s \neq \emptyset$, $\Gamma\backslash\mathcal{H} = \bigcup D_s \cup Y_0$ and $\iota : D_0 \cong S^1\times[M,\infty)$ (for sufficiently large $M > 0$) inducing $\iota_*(y^{-2}dxdy) = t^{-2}dtd\theta$ for the variable θ on S^1 and t on $[M,\infty)$. Here ι is given by an element α of $SL_2(\mathbf{Z})$ such that $\alpha(s) = i\infty$ (then $t = \mathrm{Im}(\alpha(z))$ and $\theta = \mathrm{Re}(\alpha(z))$). Now take a covering $S^1 = V_1\cup V_2$ so that V_i is isomorphic to an open interval. Then $U_{i,j} = U_{s,i,j} = V_i\times(M+j-\delta,M+j+\delta)$ for $(1/2) < \delta < 1$ covers D_s. If $F(t,\theta)$ decreases exponentially as $t \to \infty$, we see easily that $\sum_{i,j}\int_{U_{i,j}}Ft^{-2}dtd\theta$ converges absolutely. We then choose a finite open covering $Y_0 = \bigcup_\alpha U_\alpha$. Then the covering $\{U_{s,i,j}, U_\alpha\}$ does the job. Thus we have

Theorem 2. *Suppose either* $f \in \mathcal{N}_k^r(\Gamma_0(N),\chi)$ *or* $g \in \mathcal{N}_{k+2}^{r'}(\Gamma_0(N),\chi)$ *is rapidly decreasing. Then we have* $(\delta_k f,g) = (f,\varepsilon g)$.

Corollary 1. *Suppose that* $f \in \mathcal{S}_k(\Gamma_0(N),\chi)$ *and* $g \in \mathcal{N}_k^r(\Gamma_0(N),\chi)$. *If* $r < k/2$, *then* $(f,g) = (f,H(g))$.

Proof. Writing $g = H(g)+\sum_{j=1}^r \delta_{k-2j}^j h_j$, we see that $(f,\delta_{k-2j}^j h_j) = (\varepsilon f,\delta_{k-2j}^{j-1} h_j) = 0$ since $\varepsilon f = 0$. This implies $(f,g) = (f,H(g))$.

Now we see that

$$2\pi i\delta_{k+s}\left(\frac{(cz+d)^{-k}}{|cz+d|^{2s}}\right) = \frac{k+s}{(z-z^c)}(cz+d)^{-k}|cz+d|^{-2s}-(k+s)c(cz+d)^{-k-1}|cz+d|^{-2s}$$

$$= \frac{k+s}{(z-z^c)}(cz+d)^{-k}|cz+d|^{-2s}\{1-\frac{c(z-z^c)}{cz+d}\}$$

$$= \frac{k+s}{(z-z^c)}(cz+d)^{-k-1}(cz^c+d)|cz+d|^{-2s} = \frac{k+s}{(z-z^c)}(cz+d)^{-k-2}|cz+d|^{-2(s-1)}.$$

By (1c), we have $\delta_k f = y^{-k}d(y^k f)$ and hence

$$\delta_{k+s+2}((4\pi y)^{-1}f) = (4\pi)^{-1}y^{-k-s-2}d(y^{k+s+1}f) = (4\pi y)^{-1}\delta_{k+s+1}f. \tag{11}$$

Thus iterating the formula

$$\delta_{k+s}((cz+d)^{-k}|cz+d|^{-2s}) = (-4\pi y)^{-1}(k+s)(cz+d)^{-k-2}|cz+d|^{-2(s-1)}, \tag{12a}$$

we have

(12b) $\delta^r_{k+s}((cz+d)^{-k}|cz+d|^{-2s}) = (-4\pi y)^{-r}\frac{\Gamma(s+k+r)}{\Gamma(s+k)}(cz+d)^{-k-2r}|cz+d|^{-2(s-r)}$.

Recalling the definition in §9.3,

$$E'_{k,N}(z,s,\chi) = y^s\sum_{(mN,n)\neq(0,0)}\chi^{*-1}(n)(mNz+n)^{-k}|mNz+n|^{-2s},$$

we know that

(13) $$(-4\pi)^r\frac{\Gamma(s+k)}{\Gamma(s+k+r)}\delta^r_k(E'_{k,L}(z,s,\chi)) = E'_{k+2r,L}(z,s-r,\chi).$$

§10.2. The algebraicity theorem for Rankin products

We now recall (9.4.7) and (9.4.10):

(1) $$(4\pi)^{-s}\Gamma(s)L(s,\lambda^c\otimes\varphi) = 2^{-1}(gE'_{k-l,L}(s-k+1,\chi\psi^{-1}),f)_{\Gamma_0(L)},$$

where we have used the notation in §9.4, which we recall briefly: $\lambda : \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]) \to \mathbf{C}$ (resp. $\varphi : \mathbf{h}_l(\Gamma_0(J),\psi;\mathbf{Z}[\psi]) \to \mathbf{C}$) is a $\mathbf{Z}[\chi]$-algebra (resp. $\mathbf{Z}[\psi]$-algebra) homomorphism; f and g are associated normalized eigenforms, $f = \sum_{n=1}^{\infty}\lambda(T(n))q^n$ and $g = \sum_{n=1}^{\infty}\varphi(T(n))q^n$; L is the least common multiple of N and J. We consider the set $\mathcal{P}$ consisting of all $\mathbf{Z}[\chi']$-algebra homomorphisms $\lambda' : \mathbf{h}_k(\Gamma_0(N'),\chi';\mathbf{Z}[\chi']) \to \mathbf{C}$ varying N' and χ' but fixing k. For $\lambda' \in \mathcal{P}$, the integer N' is called the level of λ'. An element $\lambda : \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]) \to \mathbf{C} \in \mathcal{P}$ is called *primitive* if N is minimal among the levels of the homomorphisms in the following set:

$$\{\lambda' \in \mathcal{P} \mid \lambda'(T(p)) = \lambda(T(p)) \text{ for all but finitely many primes } p\}.$$

The primitive element λ as above is uniquely determined by λ' and is called a primitive homomorphism associated to λ'. The level of the primitive element λ is called the *conductor* of λ'. We note that

$$\lambda'(T(n)) = \lambda(T(n)) \text{ if } n \text{ is prime to the level of } \lambda'.$$

The modular form f associated to a primitive λ is called a primitive form. This notion of primitive forms coincides with the one given in [M,p.164], and we refer to [M, 4.6.12-14] for the proof of the above facts. We now assume that λ is primitive. If the reader is not familiar with the notion of primitive forms, he may make the stronger assumption that χ is primitive of conductor N; in this case, f is automatically primitive in the above sense [M, §4.6]. Under the assumption of primitivity, we have

(2) $$f^c\|_k\tau_N = W(\lambda^c)f \text{ for } W(\lambda^c) \in \mathbf{C}^\times \text{ with } W(\lambda^c)W(\lambda) = \chi(-1),$$

where $\tau_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. This assertion is proven in Proposition 5.5.1 when χ is primitive modulo p^r and $N = p^r$ for a prime p. A proof of the general case can be found in [M, Th.4.6.15]. Hereafter we simply write $(f,h)_L$ for $(f,h)_{\Gamma_0(L)}$. Then we have, for any smooth modular form h on $\Gamma_0(L)$ with character χ^* which is slowly increasing at every cusp of $\Gamma_0(L)$,

$$(3a) \qquad (h\|_k\tau_L, f\|_k\tau_L)_L = (h,f)_L.$$

This follows from the fact shown below (5.3.9): $(h\|_k\tau_L, f) = (h, f\|_k\tau_L{}^t)$ and $\tau_L{}^t = -\tau_L$. In particular,

$$W(\lambda)W(\lambda)^c(f,f)_N = (f\|_k\tau_N, f\|_k\tau_N)_N = (f,f)_N$$

and thus

$$(3b) \qquad W(\lambda)W(\lambda)^c = 1.$$

We write $T_{L/N} : \mathcal{M}_k(\Gamma_0(L),\chi^*) \to \mathcal{M}_k(\Gamma_0(N),\chi^*)$ for the adjoint of $[\Gamma_0(N)\beta\Gamma_0(L)]$ with $\beta = \begin{pmatrix} L/N & 0 \\ 0 & 1 \end{pmatrix}$. We use the same symbol $T_{L/N}$ to denote the corresponding operator $\mathbf{M}_k(L,\chi) \to \mathbf{M}_k(N,\chi)$. Thus

$$(3c) \qquad (h \mid T_{L/N}, f)_N = (h, f \mid [\Gamma_0(N)\beta\Gamma_0(L)])_L.$$

We see that

$$\beta\begin{pmatrix} a & b \\ Lc & d \end{pmatrix}\beta^{-1} = \begin{pmatrix} a & Lb/N \\ Nc & d \end{pmatrix} \text{ and hence } \Gamma_0(N) \supset \beta\Gamma_0(L)\beta^{-1}.$$

This implies that

$$\Gamma_0(N)\beta\Gamma_0(L) = \Gamma_0(N)\beta \text{ and } h \mid [\Gamma_0(N)\beta\Gamma_0(L)](z) = (L/N)^{k-1}h(Lz/N).$$

Then using these formulas, we have

$$\begin{aligned}
2(4\pi)^{-s}\Gamma(s)L(s,\lambda^c\otimes\varphi) &= (gE'_{k-l,L}(s-k+1,\chi\psi^{-1}),f)_L \\
&= ((g\|_l\tau_L)(E'_{k-l,L}(s-k+1,\chi\psi^{-1})\|_{k-l}\tau_L),f\|_k\tau_L)_L \\
&= ((g\|_l\tau_L)(E'_{k-l,L}(s-k+1,\chi\psi^{-1})\|_{k-l}\tau_L),f\|_k\tau_N\beta)_L \\
&= (L/N)^{1-(k/2)}((g\|_l\tau_L)(E'_{k-l,L}(s-k+1,\chi\psi^{-1})\|_{k-l}\tau_L),(f\|_k\tau_N) \mid [\Gamma_0(N)\beta\Gamma_0(L)])_L \\
&= (L/N)^{1-(k/2)}(\{(g\|_l\tau_L)(E'_{k-l,L}(s-k+1,\chi\psi^{-1})\|_{k-l}\tau_L)\} \mid T_{L/N}, f\|_k\tau_N)_N \\
&= L^{1-(k-l)/2}N^{(k/2)-1}J^{-l/2}W(\varphi)W(\lambda)^c \\
&\qquad \times(\{(g_c(Lz/J)(E'_{k-l,L}(s-k+1,\chi\psi^{-1})\|_{k-l}\tau_L)\} \mid T_{L/N}, f_c)_N,
\end{aligned}$$

where we have used the following formula:

$$g\|_l\tau_L = g\|_l\tau_J\|_l\begin{pmatrix} L/J & 0 \\ 0 & 1 \end{pmatrix} = (L/J)^{l/2}W(\varphi)g_c(Lz/J).$$

As seen in §§9.1 and 9.2 ((9.2.4a,b)), we can compute the Fourier expansion of $G_{k-l,L}(l-k+1,\xi)$ and $G_{k-l,L}(0,\xi)$ explicitly. To recall this, we put

$$E_L(\chi N^k) = 2^{-1}L_L(1-k,\chi) + \sum_{n=1}^{\infty}\sigma_{k-1,\chi}(n)e(nz),$$

$$G_L(\chi N^k) = \sum_{n=1}^{\infty}\sigma'_{k-1,\chi}(n)e(nz),$$

where the norm character N only has symbolic meaning but later we consider N to be the cyclotomic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then we have, for $C = i^k\dfrac{(2\pi)^k}{\Gamma(k)}$ and a Dirichlet character ξ modulo L

(4a) $\mathbf{G}_{k,L}(0,\xi) = C\{\delta_{k,1}2^{-1}L_L(0,\xi)-\delta_{k,2}\delta_{\xi,\mathrm{id}}(8\pi\,|\,y\,|_A)^{-1}\varphi(L)L^{-1}+G_L(\xi N^k)\}$,
and for $C' = i^k2^kL^{k-1}\pi$

(4b) $$\mathbf{G}_{k,L}(1-k,\xi) = C'\{\delta_{k,2}\delta_{L,1}(8\pi\,|\,y\,|_A)^{-1}+E_L(\xi N^k)\},$$

where $\delta_{k,j}$ is the Kronecker symbol and $\delta_{\xi,\mathrm{id}} = 1$ or 0 according as $\xi = \mathrm{id}$ or not. Now we write $h^* = \mathbf{h} : GL_2(\mathbf{A}) \to \mathbf{C}$ for the adelic modular form corresponding to h (see (M1) in §9.1), i.e.,

$\mathbf{h}(\alpha u) = \chi_L(u)h(u_\infty(i))j_k(u_\infty,i)^{-1}$ for $u \in S(L)G_{\infty+}$ and $\alpha \in GL_2(\mathbf{Q})$.
As seen in §9.3 (noting $h\|_k\tau_L = L^{1-(k/2)}h\,|_k\tau_L$), we have

(5a) $$(E'_{k,L}(z,s,\xi)\|_k\tau_L)^* = 2L^{-(k/2)}\xi(-1)\mathbf{G}_{k,L}(x,s,\xi^{-1}),$$
and by (1.13),

(5b) $$E'_{k-l,L}(z,s-r,\chi\psi^{-1}) = (-4\pi)^r\frac{\Gamma(s+k-l-2r)}{\Gamma(s+k-l-r)}\delta^r_{k-l-2r}E'_{k-l-2r,L}(z,s,\chi\psi^{-1}).$$

Solving the equations $s-r = m-k+1$ and $s = 1-k+l+2r$, we conclude from $W(\lambda)^c = \chi(-1)W(\lambda^c)$ that for an integer m with $l \le m = l+r \le \dfrac{k+l}{2}$

(6a) $$\begin{aligned}
&2(4\pi)^{-m}\Gamma(m)L(m,\lambda^c\otimes\varphi)\\
&\quad= (L/N)^{1-(k/2)}(\{(g\|_l\tau_L)(E'_{k-l,L}(m-k+1,\chi\psi^{-1})\|_{k-l}\tau_L)\}\,|\,T_{L/N,f}\|_k\tau_N)_N\\
&= (L/N)^{1-(k/2)}(-4\pi)^{m-l}\Gamma(m+1-l)^{-1}\\
&\quad\times(\{(g\|_l\tau_L)(\delta^{m-l}_{k+l-2m}(E'_{k+l-2m,L}(z,1-k-l+2m,\chi\psi^{-1})\|_{k+l-2m}\tau_L))\}\,|\,T_{L/N,f}\|_k\tau_N)_N\\
&= (L/N)^{1-(k/2)}(-4\pi)^{m-l}\Gamma(m+1-l)^{-1}\chi(-1)W(\lambda^c)\\
&\quad\times(\{(g\|_l\tau_L)(\delta^{m-l}_{k+l-2m}(E'_{k+l-2m,L}(z,1-k-l+2m,\chi\psi^{-1})\|_{k+l-2m}\tau_L))\}\,|\,T_{L/N,f_c})_N.
\end{aligned}$$

Now we note that
$$\begin{aligned}
&(E'_{k+l-2m,L}(z,1-k-l+2m,\chi\psi^{-1})\|_{k+l-2m}\tau_L)^*\\
&\qquad= 2\chi\psi^{-1}(-1)L^{-(k+l)/2+m}\mathbf{G}_{k+l-2m,L}(z,1-k-l+2m,\chi^{-1}\psi).
\end{aligned}$$
We see from (4b) for an integer $l \le m = l+r \le \dfrac{k+l}{2}$ that

(6b) $$\begin{aligned}
&\Gamma(m+1-l)\Gamma(m)L(m,\lambda^c\otimes\varphi)\\
&\quad= (L/N)^{1-(k/2)}2^{-1}(4\pi)^m\Gamma(m+1-l)\\
&\qquad\times(\{(g\|_l\tau_L)(E'_{k-l,L}(m-k+1,\chi\psi^{-1})\|_{k-l}\tau_L)\}\,|\,T_{L/N,f}\|_k\tau_N)_N\\
&\quad= \psi(-1)L^{m+1-k}N^{(k/2)-1}J^{-l/2}(-4\pi)^{m-l}(4\pi)^mW(\varphi)W(\lambda^c)\\
&\qquad\times(\{g(Lz/J)(\delta^{m-l}_{k+l-2m}\mathbf{G}_{k+l-2m,L}(z,1-k-l+2m,\chi^{-1}\psi))\}\,|\,T_{L/N,f^c})_N\\
&\qquad\quad= t(\{g(Lz/J)(\delta^{m-l}_{k+l-2m}E'_L(\chi^{-1}\psi N^{k+l-2m}))\}\,|\,T_{L/N,f^c})_N,
\end{aligned}$$

where $t = i^{k+l}2^{k-l+2m}\pi^{2m-l+1}L^{l-m}N^{(k/2)-1}J^{-l/2}W(\varphi)W(\lambda^c)$

and $E'_L(\chi^{-1}\psi N^{k+l-2m}) = \delta_{k+l-2m,2}\delta_{L,1}(8\pi|y|_A)^{-1}+E_L(\chi^{-1}\psi N^{k+l-2m})$.

Now we treat the other half of the critical values $L(m,\lambda^c\otimes\varphi)$ for m with $1+\frac{k+l}{2} \le m < k$. We solve the equations $s-r = m-k+1$ and $s = 0$ and get $m = k-1-r$ with $r \ge 0$. We have

$$\begin{aligned}
(7a)\quad & 2(4\pi)^{-m}\Gamma(m)L(m,\lambda^c\otimes\varphi) \\
&= (L/N)^{1-(k/2)}(\{(g\|_l\tau_L)(E'_{k-l,L}(m-k+1,\chi\psi^{-1})\|_{k-l}\tau_L)\}\,|\,T_{L/N},f\|_k\tau_N)_N \\
&= (L/N)^{1-(k/2)}(-4\pi)^{k-1-m}\frac{\Gamma(2m+2-k-l)}{\Gamma(m+1-l)} \\
&\qquad\times(\{(g\|_l\tau_L)(\delta^{k-1-m}_{2m+2-k-l}E'_{2m+2-k-l,L}(z,0,\chi\psi^{-1})\|_{2m+2-k-l}\tau_L)\}\,|\,T_{L/N},f\|_k\tau_N)_N,
\end{aligned}$$

where we have used the following formula:

$$E'_{k-l,L}(z,m-k+1,\chi\psi^{-1}) = (-4\pi)^{k-1-m}\frac{\Gamma(2m+2-k-l)}{\Gamma(m+1-l)}\delta^{k-1-m}_{2m+2-k-l}E'_{2m+2-k-l,L}(z,0,\chi\psi^{-1}).$$

Then we see from $W(\lambda)^c = \chi(-1)W(\lambda^c)$ that

$$\begin{aligned}
(7b)\quad & \Gamma(m+1-l)\Gamma(m)L(m,\lambda^c\otimes\varphi) \\
&= 2^{k-l+2m}i^{k+l}\pi^{2m+1-l}L^{l/2-m}N^{(k/2)-1}W(\lambda^c) \\
&\qquad\times(\{(g\|_l\tau_L)(\delta^{k-1-m}_{2m+2-k-l}G'_L(\chi^{-1}\psi N^{2m+2-k-l}))\}\,|\,T_{L/N},f_c)_N, \\
&= 2^{k-l+2m}i^{k+l}\pi^{2m+1-l}L^{l-m}N^{(k/2)-1}J^{-l/2}W(\varphi)W(\lambda^c) \\
&\qquad\times(\{g_c(Lz/J)(\delta^{k-1-m}_{2m+2-k-l}G'_L(\chi^{-1}\psi N^{2m+2-k-l}))\}\,|\,T_{L/N},f_c)_N,
\end{aligned}$$

where $G'_L(\xi N^k) = \delta_{k,1}2^{-1}L_L(0,\xi)-\delta_{k,2}\delta_{\xi,id}(8\pi|y|_A)^{-1}\varphi(L)L^{-1}+G_L(\xi)$.

Lemma 1. *Let* χ *be a Dirichlet character modulo* N. *Suppose that all the prime factors of* L *divide* N. *Then for all* $h \in \mathcal{M}_k(\Gamma_0(L),\chi)$ *and* $\sigma \in \mathrm{Aut}(\mathbf{C})$, *we have* $T_{L/N}(h)^\sigma = T_{L/N}(h^\sigma)$.

Proof. Since $T = T_{L/N}$ is the adjoint of $[\Gamma_0(N)\beta\Gamma_0(L)]$ for $\beta = \begin{pmatrix} L/N & 0 \\ 0 & 1\end{pmatrix}$, we see for two modular forms ϕ of weight k for $\Gamma = \Gamma_0(L)$ and ψ of weight k for $\Gamma' = \Gamma_0(N)$ that

$$\int_{\Gamma\backslash\mathcal{H}}\phi\psi\,|_k\beta y^{k-2}dxdy = \int_{\Gamma\backslash\mathcal{H}}\phi\,|\,T\psi y^{k-2}dxdy.$$

Using this formula, we compute T directly:

$$\begin{aligned}
\int_{\Gamma\backslash\mathcal{H}}\phi\psi\,|_k\beta y^{k-2}dxdy &= (L/N)^{k-1}\int_{\Gamma\backslash\mathcal{H}}\phi\psi(\beta(z))y^{k-2}dxdy \\
&= (L/N)^{-1}\int_{\beta\Gamma\beta^{-1}\backslash\mathcal{H}}\phi(\beta^{\iota}(z))\psi(z)y^{k-2}dxdy
\end{aligned}$$

$$= (L/N)^{-1}\sum_{\gamma\in \beta\Gamma\beta^{-1}\cap\Gamma'\backslash\Gamma'}\int_{\beta\Gamma\beta^{-1}\backslash\mathcal{H}}\phi(\beta^{\iota}(\gamma z))\psi(z)y^{k-2}dxdy$$
$$= \int_{\Gamma'\backslash\mathcal{H}}\sum_{\gamma\in \beta\Gamma\beta^{-1}\cap\Gamma'\backslash\Gamma'}\phi\,|_k\beta^{\iota}\gamma(z)\psi(z)y^{k-2}dxdy.$$

Thus we see that $\phi\,|\,T = \sum_{\gamma\in \beta\Gamma\beta^{-1}\backslash\Gamma'}\phi\,|_k\beta^{\iota}\gamma$. Note that $\beta\Gamma\beta^{-1}\cap\Gamma' = (\beta^{\iota})^{-1}\Gamma\beta^{\iota}\cap\Gamma'$

$$\beta\Gamma\beta^{-1}\cap\Gamma' = \{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma_0(N)\,|\,b \in (L/N)\mathbf{Z}\} = \beta\Gamma'\beta^{-1}\cap\Gamma'.$$

Thus choosing a common representative set R for

$$(\beta^{\iota})^{-1}\Gamma'\beta^{\iota}\cap\Gamma'\backslash\Gamma' \cong \beta\Gamma\beta^{-1}\cap\Gamma'\backslash\Gamma'$$

we have

$$\Gamma_0(L)\beta^{\iota}\Gamma_0(N) = \coprod_{\gamma\in R}\Gamma_0(L)\beta^{\iota}\gamma \text{ and } \Gamma_0(N)\beta^{\iota}\Gamma_0(N) = \coprod_{\gamma\in R}\Gamma_0(N)\beta^{\iota}\gamma.$$

This shows that the operator $T = T_{L/N}$ coincides with $T(L/N)$ on $\mathcal{M}_k(\Gamma_0(N),\chi)$ and, if all the prime divisors of L divide N, then T is equal to $T(L/N)$ on the larger space $\mathcal{M}_k(\Gamma_0(L),\chi)$. In fact, if all prime divisors of L divide N, for any $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix}$ in Γ', taking $0 \le u < L/N$ such that $au \equiv -b \bmod (L/N)$, we see that $\gamma\begin{pmatrix} 1 & u \\ 0 & 1\end{pmatrix} \in \beta\Gamma\beta^{-1}\cap\Gamma'$. Thus we can take $R = \left\{\begin{pmatrix} 1 & u \\ 0 & 1\end{pmatrix}\,\middle|\, 0 \le u < L/N\right\}$ as the common representative set, and we see $T_{L/N} = T(L/N)$: $a(n,f\,|\,T) = a(nL/N,f)$. This shows the lemma if all the prime divisors of L divide N.

The assertion of the above lemma is in fact true without assuming any condition. However, to prove it, we need a fairly long argument either from the theory of primitive forms [M, §4.6] (see [Sh3] for the actual argument) or from the cohomology theory studied in §7.2. We shall prove it in the general case by a cohomological argument. First we introduce the space of N-old forms. Since

$$\beta_t^{-1}\Gamma_0(N)\beta_t \supset \Gamma_0(Nt) \text{ for } \beta_t = \begin{pmatrix} t & 0 \\ 0 & 1\end{pmatrix} \text{ with } 0 < t \in \mathbf{Z},$$

for any modular form $f \in \mathcal{M}_k(\Gamma_0(N),\chi)$, we see that $f_t(z) = f(tz) = t^{1-k}f\,|\,\beta_t$ is an element of $\mathcal{M}_k(\Gamma_0(tN),\chi)$. Then we define the subspace $\mathcal{S}_k^N(\Gamma_0(L),\chi)$ of N-old forms in $\mathcal{S}_k(\Gamma_0(L),\chi)$ to be a subspace spanned by modular forms in the set: $\{f_t(z) = f(tz)\,|\,0 < t\,|\,L/N \text{ and } f \in \mathcal{S}_k(\Gamma_0(N),\chi)\}$.

Lemma 2. *Let χ be a Dirichlet character modulo N. Then for all $h \in \mathcal{S}_k^N(\Gamma_0(L),\chi)$ and $\sigma \in \mathrm{Aut}(\mathbf{C})$, we have* $T_{L/N}(h)^{\sigma} = T_{L/N}(h^{\sigma})$.

Proof. What we need to prove is $T_{L/N}(f_t)^{\sigma} = T_{L/N}(f_t^{\sigma})$ for any divisor t of L/N and all $f \in \mathcal{S}_k(\Gamma_0(N),\chi)$. Writing the operator $f \mapsto f\,|_k\beta_t$ as $[t]$, we see that $[L/N] = \prod_p[p^e]$ according to the prime decomposition $L/N = \prod_{p\,|\,L/N}p^e$. Then by definition of $T_{L/N}$, we have $T_{L/N} = \prod_{p\,|\,L/N}T_{p^e}$, where T_{p^e} is the adjoint of $[p^e] : \mathcal{S}_k(\Gamma_0(L/p^e),\chi) \to \mathcal{S}_k(\Gamma_0(L),\chi)$ which has the same effect as, for example, the adjoint of

$$[p^e] : \mathcal{S}_k(\Gamma_0(N),\chi) \to \mathcal{S}_k(\Gamma_0(Np^e),\chi).$$

Thus we may assume that L/N is a prime power without losing generality. Then $T_{p^e} = T_{p,e}\circ T_{p,e-1}\circ\cdots\circ T_{p,1}$, where $T_{p,j}$ is the adjoint of

$$[p] : \mathcal{S}_k(\Gamma_0(Np^{j-1}),\chi) \to \mathcal{S}_k(\Gamma_0(Np^j),\chi).$$

Thus we may assume that $e = 1$ because $f_{p^k} \mid T_{p,j} = f_{p^{k-1}}$ if $j > 0$ and $k > 0$. If $p \mid N$, the assertion is already proven by Lemma 1. Thus we may assume that $p \nmid N$. Then choosing $\tau \in SL_2(\mathbf{Z})$ by the strong approximation theorem (Lemma 6.1.1) so that $\tau \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \bmod p$ and $\tau \in \Gamma_0(N)$, we can take the following set as the representative set R as in the proof of Lemma 1:

$$R = \left\{\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \mid 0 \le u < p\right\} \cup \{\tau\}.$$

Then $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\tau \equiv \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \equiv \tau\beta_p \bmod p$ shows that $f \mid T_p = f \mid T_{N(p)}$ if $f \in \mathcal{S}_k(\Gamma_0(N),\chi)$. On the other hand, we see that

$$f_p \mid_k \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\tau = p^{1-k} f \mid_k \beta_p \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\tau = p^{k-1} f \mid_k \tau = p^{k-1} f,$$

$$\sum_{0\le u<p} f_p \mid \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = f.$$

This shows that $f_p \mid T_p = (1+p^{k-1})f$. This finishes the proof.

The following fact is a key to our argument:

Proposition 1. *Suppose that* $k \ge 2$. *Then the orthogonal projection*

$$\pi_\chi : \mathcal{S}_k(\Gamma_0(L),\chi) \to \mathcal{S}_k^N(\Gamma_0(L),\chi)$$

is rational; that is, we have $\pi_\chi\sigma(f^\sigma) = \{\pi_\chi(f)\}^\sigma$ *for all* $\sigma \in \mathrm{Aut}(\mathbf{C})$.

Proof. Note that $\beta_t\tau_L = t\tau_{L/t}$ for any divisor t of L. This shows that $\mathcal{S}(\chi) = \mathcal{S}_k^N(\Gamma_0(L),\chi)$ is stable under τ_L. Note that the Hecke operators $T(n)$ of level N and L are different on $\mathcal{S}_k(\Gamma_0(N),\chi)$ if n has a prime factor q such that q divides L but q is prime to N. To indicate this difference, we write $T_L(n)$ for Hecke operators of level L if necessary. We write $L = N_0L_0$ such that L_0 is prime to N and all the prime factors of N_0 divides N. If n and tL_0 are relatively prime, we see

$$a(m,f_t \mid T_L(n)) = \sum_{0<b\mid(m,n)} \chi_L(b)b^{k-1}a(\frac{mn}{b^2t},f) = a(m,(f \mid T_N(n))_t)$$

$$\Leftrightarrow f_t \mid T_L(n) = (f \mid T_N(n))_t$$

where the subscript "L" to χ is given to indicate that χ is a Dirichlet character modulo L (i.e. $\chi_L(b) = 0$ if b and L are not relatively prime). This follows from the two facts

$$t \mid mn/b^2 \Leftrightarrow t \mid m \text{ and } \chi_L(b) = 0 \Leftrightarrow \chi_N(b) = 0$$

under the assumption that n and N are relatively prime. When t is a prime power $q^r \mid L_0$ with $r \geq 1$, then

$$a(m,f_{q^r} \mid T_L(q)) = a(mq,f_{q^r}) = a(m/q^{r-1},f) = a(m,f_{q^{r-1}}).$$

If $r = 0$, $a(m,f \mid T_L(q)) = a(mq,f) = a(m,f \mid T_N(q))-\chi_N(q)q^{k-1}a(m,f_q)$. These facts show that $\mathcal{S}(\chi)$ is stable under $T_L(n)$ for all $n > 0$. Since $\mathcal{S}(\chi)$ is stable under τ_L and τ_L is an automorphism of $\mathcal{S}(\chi)$, $\mathcal{S}(\chi)$ is stable under $\tau_L T_L(n)\tau_L^{-1} = T_L(n)^*$ (= the adjoint of $T_L(n)$ under the Petersson inner product). Let $\mathcal{S}^\perp(\chi)$ be the orthogonal complement of $\mathcal{S}(\chi)$ in $\mathcal{S}_k(\Gamma_0(L),\chi)$ under the Petersson inner product. The stability of $\mathcal{S}(\chi)$ under $T_L(n)^*$ and $T_L(n)$ for all n shows the stability of $\mathcal{S}^\perp(\chi)$ under these operators. Then, for any $\mathbf{Q}(\chi)$-subalgebra A of $\mathbf{C}$, we let $\mathcal{h}^\perp(A)$ (resp. $\mathcal{h}(A)$) denote the A-algebra generated over A in $\mathrm{End}_{\mathbf{C}}(\mathcal{S}^\perp(\chi))$ (resp. $\mathrm{End}_{\mathbf{C}}(\mathcal{S}(\chi))$) by $T_L(n)$ for all n. By the duality between $\mathcal{S}_k(\Gamma_0(L),\chi;A)$ and $\mathbf{h}(A) = \mathbf{h}_k(\Gamma_0(L),\chi;A)$ (Theorem 6.3.2), we know that $\mathbf{h}(\mathbf{C}) = \mathcal{h}^\perp(\mathbf{C})\oplus\mathcal{h}(\mathbf{C})$ as an algebra direct sum. Now we can think of corresponding subspaces $H\mathcal{S}^\perp(A)$ and $H\mathcal{S}(A)$ in $H^1_P(\Gamma_0(L),L(n,\chi;A))$. Thus β_t induces a morphism

$$[\beta_t] = [\Gamma_0(N)\beta_t\Gamma_0(L)] : H^1_P(\Gamma_0(N),L(n,\chi;A)) \to H^1_P(\Gamma_0(L),L(n,\chi;A)),$$

and $H\mathcal{S}(A)$ is defined to be the sum of $\mathrm{Im}([\beta_t])$ over all positive divisors of L/N. Then from the fact that

$$H^1_P(\Gamma_0(N),L(n,\chi;\mathbf{Q}(\chi)))\otimes_{\mathbf{Q}(\chi)}\mathbf{C} = H^1_P(\Gamma_0(N),L(n,\chi;\mathbf{C})),$$

we know that $H\mathcal{S}(\mathbf{Q}(\chi))\otimes_{\mathbf{Q}(\chi)}\mathbf{C} = H\mathcal{S}(\mathbf{C})$. We can define $H\mathcal{S}^\perp(A)$ to be the orthogonal complement of $H\mathcal{S}(A)$ under the pairing (6.2.3a) in the full cohomology group $H^1_P(\Gamma_0(L),L(n,\chi;A))$. The formula (6.2.3b) then tells us that the Eichler-Shimura isomorphism induces isomorphisms of Hecke modules,

$$H\mathcal{S}^\perp(\mathbf{C}) \cong \mathcal{S}^\perp(\chi)\oplus\mathcal{S}^\perp(\chi^c)^c \text{ and } H\mathcal{S}(\mathbf{C}) \cong \mathcal{S}(\chi)\oplus\mathcal{S}(\chi^c)^c,$$

where, for example, $\mathcal{S}^\perp(\chi^c)^c = \{\overline{f(z)} \mid f \in \mathcal{S}^\perp(\chi^c)\}$ for complex conjugation c. This implies (see the proof of Theorem 6.3.2)

$$\mathcal{h}^\perp(\mathbf{C}) = \mathcal{h}^\perp(\mathbf{Q}(\chi))\otimes_{\mathbf{Q}(\chi)}\mathbf{C} \text{ and } \mathcal{h}(\mathbf{C}) = \mathcal{h}(\mathbf{Q}(\chi))\otimes_{\mathbf{Q}(\chi)}\mathbf{C}.$$

Thus again by the duality theorem, we know that

$$\mathcal{S}^\perp(\chi;\mathbf{Q}(\chi))\otimes_{\mathbf{Q}(\chi)}\mathbf{C} = \mathcal{S}^\perp(\chi),\ \mathcal{S}(\chi;\mathbf{Q}(\chi))\otimes_{\mathbf{Q}(\chi)}\mathbf{C} = \mathcal{S}(\chi) \text{ and}$$
$$\mathcal{S}_k(\Gamma_0(L),\chi;\mathbf{Q}(\chi)) = \mathcal{S}^\perp(\chi;\mathbf{Q}(\chi))\oplus\mathcal{S}(\chi;\mathbf{Q}(\chi)),$$

where $\mathcal{S}^\perp(\chi;A) = \mathcal{S}_k(\Gamma_0(L),\chi;A)\cap\mathcal{S}^\perp(\chi)$ and $\mathcal{S}(\chi;A) = \mathcal{S}_k(\Gamma_0(L),\chi;A)\cap\mathcal{S}(\chi)$. This shows the rationality of π_χ over $\mathbf{Q}(\chi)$. Now we want to show that for $\sigma \in \mathrm{Gal}(\mathbf{Q}(\chi)/\mathbf{Q})$, the following diagram is commutative:

$$(*)\qquad \begin{array}{ccc} \pi_\chi : \mathcal{S}_k(\Gamma_0(L),\chi;\mathbf{Q}(\chi)) & \to & \mathcal{S}_k(\Gamma_0(L),\chi;\mathbf{Q}(\chi)) \\ \downarrow \sigma & & \downarrow \sigma \\ \pi_{\chi^\sigma} : \mathcal{S}_k(\Gamma_0(L),\chi^\sigma;\mathbf{Q}(\chi)) & \to & \mathcal{S}_k(\Gamma_0(L),\chi^\sigma;\mathbf{Q}(\chi)). \end{array}$$

To see this, we consider the Galois action of $\sigma \in \mathrm{Gal}(\mathbf{Q}(\chi)/\mathbf{Q})$ on the $\Gamma_0(N)$-module $L(n,\chi;\mathbf{Q}(\chi))$, which induces an isomorphism

$$\sigma : H^1_P(\Gamma_0(N),L(n,\chi;\mathbf{Q}(\chi))) \cong H^1_P(\Gamma_0(N),L(n,\chi^\sigma;\mathbf{Q}(\chi))),$$

which in turn induces a $\mathbf{Q}$-algebra isomorphism

$$\sigma^* : \mathbf{h}_k(\Gamma_0(N),\chi^\sigma;\mathbf{Q}(\chi)) \cong \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Q}(\chi)).$$

Here σ^* takes $T(n)$ to $T(n) = \sigma^{-1}T(n)\sigma$ and coincides with σ^{-1} on $\mathbf{Q}(\chi)$. It is easy to check that $\langle h^{\sigma^*},f\rangle^\sigma = \langle h,f^\sigma\rangle$ for $h \in \mathbf{h}_k(\Gamma_0(N),\chi^\sigma;\mathbf{Q}(\chi))$ and $f \in \mathcal{S}_k(\Gamma_0(N),\chi;\mathbf{Q}(\chi))$, because σ^* takes $T(n)$ to $T(n)$. Then again by the duality, we know the commutativity of $(*)$, which shows the proposition.

Corollary 1. *For* $f \in \mathcal{N}^r_{k+2r}(\Gamma_0(L),\chi)$ $(k \geq 1$ *and* $r \geq 0)$ *and* $\sigma \in \mathrm{Aut}(\mathbf{C})$, *we have* $(f\,|\,T_{L/N})^\sigma = f^\sigma\,|\,T_{L/N}$.

Proof. Using Theorem 1.1, we can write

$$f = \sum_{j=0}^r \delta^j_{k+2r-2j} h_j \text{ with } h_j \in \mathcal{M}_{k+2r-j}(\Gamma_0(L),\chi).$$

Then, with the notation of the proof of Lemma 1, we see that

$$\begin{aligned} f\,|\,T_{L/N} &= \sum_{j=0}^r \sum_{\gamma\in R} (L/N)^{k+2r-1}(\delta^j_{k+2r-2j}h_j)\|_{k+2r}\beta^\iota\gamma \\ &= \sum_{j=0}^r \sum_{\gamma\in R} (L/N)^{2j}(\delta^j_{k+2r-2j}(L/N)^{k+2r-2j-1}\textstyle\sum_{\gamma\in R} h_j\|_{k+2r-2j}\beta^\iota\gamma) \\ &= \sum_{j=0}^r \sum_{\gamma\in R} (L/N)^{2j}(\delta^j_{k+2r-2j}(h_j\,|\,T_{L/N})). \end{aligned}$$

Note that $T_{L/N}$ is the adjoint of $[L/N] : \mathcal{S}_k(\Gamma_0(N),\chi) \to \mathcal{S}_k(\Gamma_0(L),\chi)$ and thus $\mathrm{Ker}(T_{L/N})$ contains $\mathrm{Ker}(\pi_\chi)$ in Proposition 1. Thus $T_{L/N} = T_{L/N}\circ\pi_\chi$. Then by Lemma 2 and Proposition 1, we see that

$$(h_j\,|\,T_{L/N})^\sigma = (\pi_\chi(h_j)\,|\,T_{L/N})^\sigma = (\pi_\chi(h_j^\sigma)\,|\,T_{L/N}) = h_j^\sigma\,|\,T_{L/N}.$$

Then by (1.8c), we know that

$$\begin{aligned} (f\,|\,T_{L/N})^\sigma &= \{\textstyle\sum_{j=0}^r \sum_{\gamma\in R} (L/N)^{2j}(\delta^j_{k+2r-2j}(h_j\,|\,T_{L/N}))\}^\sigma \\ &= \textstyle\sum_{j=0}^r \sum_{\gamma\in R} (L/N)^{2j}(\delta^j_{k+2r-2j}(h_j^\sigma\,|\,T_{L/N})) = f^\sigma\,|\,T_{L/N}. \end{aligned}$$

Now we shall prove the following algebraicity theorem for Rankin products:

Theorem 1 (Shimura [Sh3,4]). *Let* $\lambda : \mathbf{h}_k(\Gamma_0(N),\chi;\mathbf{Z}[\chi]) \to \mathbf{C}$ *(resp.* $\varphi : \mathbf{h}_l(\Gamma_0(J),\psi;\mathbf{Z}[\psi]) \to \mathbf{C}$*) be a* $\mathbf{Z}[\chi]$*-algebra (resp.* $\mathbf{Z}[\psi]$*-algebra) homomorphism and let* $f = \sum_{n=1}^{\infty}\lambda(T(n))q^n \in \mathcal{S}_k(\Gamma_0(N),\chi)$*. Suppose that* λ *and* φ *are both primitive. Then for all integers* m *with* $l \le m < k$*, we have*

$$S(m,\lambda^c\otimes\varphi) = (-1)^{m+l}\frac{\Gamma(m+1+l)\Gamma(m)L(m,\lambda^c\otimes\varphi)}{N^{(k/2)}J^{-l/2}W(\lambda^c)W(\varphi)(2\pi i)^{k-l+2m}\pi^{1-k}(f,f)} \in \overline{\mathbf{Q}}$$

and for all $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, $S(m,\lambda^c\otimes\varphi)^\sigma = S(m,\lambda^{\sigma c}\otimes\varphi^\sigma)$.

Proof. We write $(\ ,\ )$ for the Petersson inner product on $\mathcal{S}_k(\Gamma_0(N),\chi^c)$ and write $\langle\ ,\ \rangle : \mathbf{h}_k(\Gamma_0(N),\chi^c;\overline{\mathbf{Q}})\times\mathcal{S}_k(\Gamma_0(N),\chi^c;\overline{\mathbf{Q}}) \to \overline{\mathbf{Q}}$ for the pairing given by $\langle h,f\rangle = a(1,f\,|\,h)$. Under the primitivity assumption on λ, it is known that $\lambda^c : \mathbf{h}_k(\Gamma_0(N),\chi^c;\mathbf{Q}(\lambda^c)) \to \mathbf{Q}(\lambda^c)$ has a section in the category of $\mathbf{Q}$-algebras; i.e., there exists an algebra homomorphism $s : \mathbf{Q}(\lambda^c) \to \mathbf{h}_k(\Gamma_0(N),\chi^c;\mathbf{Q}(\lambda^c))$ such that $\lambda\circ s = \mathrm{id}$ and $B = \mathrm{Ker}(\lambda)$ is a $\mathbf{Q}$-subalgebra of $\mathbf{h}_k(\Gamma_0(N),\chi^c;\mathbf{Q}(\lambda^c))$. Thus $\mathbf{h}_k(\Gamma_0(N),\chi^c;\mathbf{Q}(\lambda^c)) = \mathbf{Q}(\lambda)1_{\lambda^c}\oplus B$ with an idempotent 1_{λ^c}. When χ is primitive (modulo N), $\mathbf{h}_k(\Gamma_0(N),\chi^c;\mathbf{Q}(\lambda^c))$ is semi-simple and thus this is obvious. The general case is shown in [M, Th.4.6.12]. We consider the linear form $l_\lambda : \phi \mapsto \langle 1_{\lambda^c},\phi\rangle$ on $\mathcal{S}_k(\Gamma_0(N),\chi^c;\overline{\mathbf{Q}})$. The action of σ on $L(n,\chi^c;\overline{\mathbf{Q}})$ induces an isomorphism $\sigma : H^1_P(\Gamma_0(N),L(n,\chi^c;\overline{\mathbf{Q}})) \to H^1_P(\Gamma_0(N),L(n,\chi^{c\sigma};\overline{\mathbf{Q}}))$. We see that $\sigma T(n)\sigma^{-1} = T(n)$ and thus induces an algebra isomorphism

$$\sigma : \mathbf{h}_k(\Gamma_0(N),\chi^c;\mathbf{Q}(\lambda^c)) \to \mathbf{h}_k(\Gamma_0(N),\chi^{\sigma c};\mathbf{Q}(\lambda^{\sigma c})).$$

Then we see by definition that $\langle h^\sigma,\phi^\sigma\rangle = \langle h,\phi\rangle^\sigma$. In particular, we have

$$\langle 1_{\lambda^c},\phi\rangle^\sigma = \langle 1_{\lambda^{\sigma c}},\phi^\sigma\rangle, \text{ i.e., } l_{\lambda^c}(\phi)^\sigma = l_{\lambda^{c\sigma}}(\phi^\sigma).$$

As a linear form, l_{λ^c} is the unique one satisfying $l_{\lambda^c}(\phi\,|\,T(n)) = \lambda(T(n))^c l_{\lambda^c}(\phi)$ and $l_{\lambda^c}(f_c) = 1$ because of the duality between the Hecke algebra and the space of modular forms (Theorem 6.3.2). We consider another linear form $\phi \mapsto (\phi,f_c)$. Since

$$(\phi\,|\,T(n),f_c) = (\phi,f_c\,|\,T(n)^*) = (\phi,\lambda(T(n))f_c) = \lambda(T(n))^c(\phi,f_c),$$

l_{λ^c} is a constant multiple of $\phi \mapsto (\phi,f_c)$, i.e. $l_{\lambda^c}(\phi) = C(\phi,f_c)$. We compute C. We see that $1 = l_{\lambda^c}(f_c) = c(f_c,f_c) = C(f,f)$ and thus

$$l_{\lambda^c}(\phi) = \frac{(\phi,f_c)}{(f,f)}.$$

Here the equality $(f_c,f_c) = (f,f)$ can be shown via the change of variable $z \mapsto -\bar{z}$. Writing

$$\phi = \begin{cases} H(g(Lz/J)(\delta^{k-1-2m}_{2m+2-k-l}G'_L(\chi^{-1}\psi N^{2m+2-k-l}))\,|\,T_{L/N}) & \text{if } 1+\frac{k-l}{2} \le m < k, \\ H(g(Lz/J)(\delta^{m-l}_{k+l-2m}E'_L(\chi^{-1}\psi N^{k+l-2m}))\,|\,T_{L/N}) & \text{if } l \le m \le \frac{k+l}{2}, \end{cases}$$

we know from the above formula that ϕ has algebraic Fourier coefficients and

$$L^{l-m}N^{-1}S(m,\lambda^c\otimes\varphi)^\sigma = \left(\frac{(\phi,f_c)}{(f,f)}\right)^\sigma = \frac{(\phi^\sigma,f^\sigma{}_c)}{(f^\sigma,f^\sigma)}.$$

Here we have used the fact $f_c{}^\sigma = (f^\sigma)_c$ shown after the proof of Corollary 5.4.3 when N is a prime power. The assertion in the general case also follows from the same argument by [M, Th.4.6.12 and (4.6.17)] under the primitivity assumption on λ. Then by Lemma 1 and (1.8b,c), we have, for $\xi = \chi^{-1}\psi$,

$$\phi^\sigma = \begin{cases} H(g^\sigma(Lz/J)(\delta^{k-1-2m}_{2m+2-k-l}G'_L(\xi^\sigma N^{2m+2-k-l}))\,|\,T_{L/N}) & \text{if } 1+\frac{k-l}{2} \le m < k, \\ H(g^\sigma(Lz/J)(\delta^{m-l}_{k+l-2m}E'_L(\xi^\sigma N^{k+l-2m}))\,|\,T_{L/N}) & \text{if } l \le m \le \frac{k+l}{2}. \end{cases}$$

This shows $L^{l-m}N^{-1}S(m,\lambda^c\otimes\varphi)^\sigma = L^{l-m}N^{-1}S(m,\lambda^{\sigma c}\otimes\varphi^\sigma)$, which proves the last assertion. The first assertion follows from the last assertion since $\mathbf{Q}(\chi^{-1}) \subset \mathbf{Q}(\lambda^c)$ and $\mathbf{Q}(\psi) \subset \mathbf{Q}(\varphi)$ because for example

$$\chi(p)p^{k-1} = \lambda(T(p)^2)-\lambda(T(p^2)) \quad \text{(see (5.3.4a) and §6.3).}$$

Applying the above theorem to the primitive algebra homomorphism $\varphi\otimes\omega : \mathbf{h}_l(\Gamma_0(J'),\psi\omega^2;\mathbf{Z}[\psi\omega^2]) \to \mathbf{C}$ for a Dirichlet character ω modulo C such that $\varphi\otimes\omega(T(n)) = \omega(n)\varphi(T(n))$ for all n prime to CJ, we have

Corollary 2. *Let the notation be as in the theorem. Then for each Dirichlet character* ω *modulo* C, *write* J' *for the level of the primitive algebra homomorphism* $\varphi\otimes\omega$ *associated to* $g\,|\,\omega$. *(*J' *is a divisor of the least common multiple of* J *and* C^2.*) Then we have, for all integers* m *with* $l \le m < k$,

$$S(m,\lambda^c\otimes\varphi\otimes\omega) = \frac{(-1)^{m+l}\Gamma(m+1+l)\Gamma(m)L(m,\lambda^c\otimes\varphi\otimes\omega)}{N^{(k/2)}J'^{-l/2}W(\lambda^c)W(\varphi\otimes\omega)(2\pi i)^{k-l+2m}\pi^{1-k}(f,f)} \in \overline{\mathbf{Q}},$$

and for all $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, $S(m,\lambda^c\otimes\varphi\otimes\omega)^\sigma = S(m,\lambda^{\sigma c}\otimes\varphi^\sigma\otimes\omega^\sigma)$.

§10.3. Two variable Λ-adic Eisenstein series

We fix a prime p and put $\mathbf{p} = 4$ if $p = 2$ and $\mathbf{p} = p$ otherwise. Let $\mathcal{O}$ be the integer ring of a finite extension K of $\mathbf{Q}_p$. Let ξ and χ be two Dirichlet characters modulo $\mathbf{p}$. We assume that $\chi(-1) = 1$. We agree to put in force the following convention:

$$\xi(n) = \chi(n) = 0 \quad \text{when} \quad p \mid n,$$

even if χ or ξ is trivial. We also consider the continuous character $\kappa = \kappa_X : W = 1+p\mathbf{Z}_p \to \Lambda^\times = \mathcal{O}[[X]]^\times$ given by $\kappa(z) = (1+X)^{s(z)}$ for $s(z)$ given by $u^{s(z)} = z$ $(u = 1+p)$. We have added the suffix "X" to κ because we want to write κ_Z for the "same" character having values in $\Lambda_Z = \mathcal{O}[[Z]]$ obtained from κ by replacing X by Z. We consider the following formal q-expansions:

$$E(\xi,\chi)(X,Z;q) = \sum_{n=1}^{\infty} \xi(n)\kappa_Z(\langle n\rangle)\sum_{0<b\mid n} b^{-1}\chi(b)\kappa_X(\langle b\rangle)q^n \in \mathcal{O}[[X,Z]][[q]],$$
$$E(\chi N^k)(q) = \sum_{n=1}^{\infty}\sum_{0<b\mid n} b^{k-1}\chi(b)q^n = E_p(\chi N^k)\mid \iota,$$
$$G(\chi N^k)(q) = \sum_{n=1}^{\infty}\sum_{0<b\mid n} b^{k-1}\chi(n/b)q^n = G_p(\chi N^k)\mid \iota = d^{k-1}E(\chi N^{2-k})(q),$$

where ι is the trivial character modulo p, $E_p(\chi N^k)$ is the q-expansion introduced in §10.2 and $\langle n\rangle = n\omega(n)^{-1} \in W$. Thus the operation $f\mid\iota$ is just taking out terms involving q^n for n divisible by p, i.e. $f\mid\iota = f-(f\mid T(p))(pz)$. This series has the following property:

(E1) $\quad E(\xi,\chi)(u^k-1,\varepsilon(u)u^r-1) = d^r(E(\chi\omega^{-k}N^k)\mid\varepsilon\xi\omega^{-r})$ for $k \geq 1$ and $r \geq 0$,

where $d = q\frac{d}{dq} = \frac{1}{2\pi i}\frac{\partial}{\partial z}$ and ε is a finite order character of W and the above identity is the identity of power series in $\mathcal{O}[\varepsilon][[q]]$. Here we denote by $\mathcal{O}[\varepsilon]$ the subring of $\overline{\mathbf{Q}}_p$ generated over $\mathcal{O}$ by the values of ε. In fact, for each character $\varepsilon : W \to \overline{\mathbf{Q}}_p^\times$ of finite order, regarding ε as a character of $\mathbf{Z}_p^\times$ by $\varepsilon(n) = \varepsilon(\langle n\rangle)$, we have $\kappa(\langle n\rangle)(\varepsilon(u)u^k-1) = n^k\varepsilon\omega^{-k}(n)$ and thus

$$E(\xi,\chi)(u^k-1,\varepsilon(u)u^r-1)(q) = \sum_{n=1}^{\infty} \xi\varepsilon\omega^{-r}(n)n^r\sum_{0<b\mid n} b^{k-1}\chi\omega^{-k}(b)q^n$$
$$= d^r\{\sum_{n=1}^{\infty} \xi\varepsilon\omega^{-r}(n)\sum_{0<b\mid n} b^{k-1}\chi\omega^{-k}(b)q^n\} = d^r(E(\chi\kappa^k)\mid\xi\varepsilon\omega^{-r}).$$

Here abusing the symbols a little, we have written κ_0 for $\omega^{-1}N$. For each character $\varepsilon : W \to \overline{\mathbf{Q}}_p^\times$ of finite order, we consider the form $E(\xi,\chi)(X,\varepsilon(u)-1)$. Then by (E1), we have

$$E(\xi,\chi)(u^k-1,\varepsilon(u)-1) = E(\chi\kappa_0^k)\mid\xi\varepsilon \in \mathcal{M}_k(\Gamma_0(p^\alpha p),\varepsilon^2\xi^2\chi)$$

for sufficiently large α independent of k.

Now we take a finite extension $\mathbf{M}$ of the quotient field $\mathbf{L}$ of $\Lambda = \mathcal{O}[[Y]]$ and write $\mathbf{J}$ for the integral closure of $\Lambda = \mathcal{O}[[Y]]$ in $\mathbf{M}$. Take a $\mathbf{J}$-adic form $G \in \mathbf{S}(\psi,\mathbf{J})$. We define a convolution product

$$G*E(\xi,\psi^{-1}\chi)(X,Z) = GE((1+Y)^{-1}(1+X)(1+Z)^{-2}-1,Z) \in \mathbf{J}[[X,Z]][[q]].$$

Write $\chi_P = \varepsilon'\chi\omega^{-k}$ and $\psi_Q = \varepsilon''\psi\omega^{-l}$ for $Q \in \mathcal{A}(\mathbf{J})$ and $P \in \mathcal{A}(\Lambda)$ when $P \cap \Lambda = P_{k,\varepsilon'}$ and $Q \cap \Lambda = P_{l,\varepsilon''}$. Then, if $0 \le r \le \frac{k-l}{2}$, we have

$$G*E(\xi,\psi^{-1}\chi)(P,Q,\varepsilon(u)u^r-1) = G(Q)d^r(E(\psi_Q^{-1}\chi_P\varepsilon^{-2}\omega^{2r}N^{k-l-2r}) \mid \xi\varepsilon\omega^{-r}),$$

and if $\frac{k-l-1}{2} \le r < k-l$

$$\begin{aligned} G*E(\xi,\psi^{-1}\chi)(P,Q,\varepsilon(u)u^r-1) &= G(Q)d^r(E(\psi_Q^{-1}\chi_P\varepsilon^{-2}\omega^{2r}N^{k-l-2r}) \mid \xi\varepsilon\omega^{-r}) \\ &= G(Q)d^{-r-1+k-l}d^{2r+l-k+1}(E(\psi_Q^{-1}\chi_P\varepsilon^{-2}\omega^{2r}N^{k-l-2r}) \mid \xi\varepsilon\omega^{-r}) \\ &= G(Q)d^{k-l-r-1}(G(\psi_Q^{-1}\chi_P\varepsilon^{-2}\omega^{2r}N^{2r-k+l+2}) \mid \xi\varepsilon\omega^{-r}). \end{aligned}$$

Then viewing $G*E(\xi,\psi^{-1}\chi)(\varepsilon(u)-1)$ as a formal q-expansion with coefficients in $\Lambda\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ for a fixed finite order character $\varepsilon : W \to \overline{\mathbf{Q}}_p^{\times}$, we know that $G*E(\xi,\psi^{-1}\chi)(\varepsilon(u)-1)$ satisfies, if $k > l$,

$$G*E(\xi,\psi^{-1}\chi)(P,Q,\varepsilon(u)-1) = G(Q)(E(\eta) \mid \xi\varepsilon) \in \mathcal{M}_k(\Gamma_0(p^{\alpha}),\xi^2\chi_P),$$

where $\eta = \psi_Q^{-1}\chi_P\varepsilon^{-2}\omega^{2r}N^{k-l}$ and $\alpha = \max(f(P),f(Q))+2f(\varepsilon)$ for the conductors $p^{f(P)}$, $p^{f(Q)}$ and $p^{f(\varepsilon)}$ of χ_P, ψ_Q and ε, respectively. Thus we know from (7.4.5) that

$$G*E(\xi,\psi^{-1}\chi)(P,Q,\varepsilon(u)-1) \in \mathbf{S}((\xi^2\chi)_\alpha;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}.$$

Here the suffix "α" indicates that we regard the character $(\xi^2\chi)_\alpha = \xi^2\chi$ as defined modulo p^α; thus, the character $(\xi^2\chi)_\alpha$ may not be primitive. By the definition of completed tensor products, $\mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ is the completion of $\bigcup_\alpha \mathbf{S}(\chi_\alpha;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ under the m-adic topology for the maximal ideal m of $\Lambda\hat{\otimes}_{\mathcal{O}}\mathbf{J}$.

Lemma 1. *Let* S *be the space of* $H = \sum_{n=1}^{\infty} a(n;H)(Z)q^n$ *with*

$$a(n;H)(Z) \in (\Lambda\hat{\otimes}_{\mathcal{O}}\mathbf{J})[[Z]]$$

satisfying $H(\varepsilon(u)-1) \in \mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[\varepsilon(u)]$ *for all finite order characters* ε *of* W. *Then, for* $H \in S$, *we have* $H \in \mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]$ *and hence* $H(\varepsilon(u)u^r-1) \in \mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}$. *Moreover, we have*

$$H \mid e(\varepsilon(u)u^r-1) = H(\varepsilon(u)u^r-1) \mid e$$

for all finite order characters ε *and* $r \ge 0$.

Proof. By the same argument as the one given below (7.4.5), we may assume that $\mathbf{J} = \mathbf{Z}_p[[Y]]$ and $\Lambda = \mathbf{Z}_p[[X]]$. Then $\Lambda\hat{\otimes}_{\mathcal{O}}\mathbf{J} = \mathbf{Z}_p[[X,Y]]$. Let ζ_n be a primitive p^n-th root of unity. We put $\phi_n = \prod_\sigma(Z+1-\zeta_n^\sigma) \in \mathbf{Z}[Z]$, where ζ_n^σ runs over all conjugates of ζ_n over $\mathbf{Q}$. Then we know that $\omega_n = (Z+1)^{p^n}-1 = \prod_{0\le m\le n}\phi_m$.

Thus $H \mapsto \oplus_{n=0}^{j} H(\zeta_n-1)$ defines a morphism $\varphi_n : S \to \oplus_{n=0}^{j} \mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}\mathbf{J}[\zeta_n]$. If $\varphi_n(H) = 0$, $a(n;H)$ is divisible by $(Z+1-\zeta_m)$ in $\mathbf{Z}_p[\zeta_m][[X,Y,Z]]$ for all $m \le n$. Thus $H \in \omega_n S$. This shows that $\mathrm{Ker}(\varphi_n) = \omega_n S$. Since $\bigcap_n \omega_n S = \{0\}$, we know that S injects into

$$\varprojlim_n \mathrm{Im}(\varphi_n) = \varprojlim_n (S/\omega_n S).$$

The space $\mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]/(\omega_n)$ consists of $H_n = \sum_{n=1}^{\infty} a(n;H_n)q^n$ with $a(n;H_n) \in \mathbf{Z}_p[[X,Y]][Z]/(\omega_n)$ such that $H_n(\zeta_m-1) \in \mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[\zeta_m]$ for all $0 \le m \le n$. Thus $S/\omega_n S$ is a subspace of $\mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]/(\omega_n)$. Thus we have a natural map of S into $\varprojlim_n \mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]/(\omega_n)$, which is equal to $\mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]$. Since $\mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]$ is a subspace of $\mathbf{Z}_p[[X,Y,Z]][[q]]$, the map is injective, and hence we can regard S as a subspace of $\mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]$. Then the projector

$$e : \mathbf{S}(\chi_\infty;\Lambda) \to \mathbf{S}^{\mathrm{ord}}(\chi_\infty;\Lambda) \qquad \text{(Proposition 7.3.1)}$$

extends linearly to

$$e : \mathbf{S}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]] \to \mathbf{S}^{\mathrm{ord}}(\chi_\infty;\Lambda)\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]].$$

By definition, e commutes with the specialization map: $H \mapsto H|_{Z=z}$ for any $z \in \overline{\mathbf{Q}}_p$. In particular, $H(\varepsilon(u)u^r-1)|e = H|e(\varepsilon(u)u^r-1)$ in $\mathbf{Z}_p[\varepsilon][[X,Y]][[q]]$.

Corollary 1. *Suppose that* $G(Q)$ *has* q*-expansion coefficients in* $\overline{\mathbf{Q}}$ *and* $G(Q) \in \mathcal{S}_k(\Gamma_0(p^\beta),\psi_Q;\overline{\mathbf{Q}})$. *Then the two limits*

$$\lim_{n\to\infty} G(Q)d^r(E(\psi_Q^{-1}\chi_p\varepsilon^{-2}\omega^{2r}N^{k-l-2r})\,|\,\xi\varepsilon\omega^{-r})\,|\,T(p)^{n!} \quad \textit{for} \quad 0 \le r \le \tfrac{k-l}{2},$$

$$\lim_{n\to\infty} G(Q)d^{k-l-r-1}(G(\psi_Q^{-1}\chi_p\varepsilon^{-2}\omega^{2r}N^{2r-k+l+2})\,|\,\xi\varepsilon\omega^{-r})\,|\,T(p)^{n!} \quad \textit{for} \quad \tfrac{k-l-1}{2} \le r < k-l,$$

exist in $\mathcal{O}[\varepsilon][[q]]$ *under the* p*-adic topology, where*

$$\sum_{n=0}^{\infty} a_n q^n\,|\,T(p) = \sum_{n=0}^{\infty} a_{np}q^n.$$

Moreover, writing the above limit as h*, we have, in* $\mathcal{O}[\varepsilon][[q]]$,

$$h = (G*E(\xi,\psi^{-1}\chi)\,|\,e)(P,Q,\varepsilon(u)u^r-1),$$

which is an element in $\mathcal{S}_k(\Gamma_0(p^\alpha\mathbf{p}),\chi_p\xi^2;\overline{\mathbf{Q}})$ *for* α *such that* $\chi_p\xi^2(1+p^\alpha\mathbf{p}\mathbf{Z}_p) = 1$.

Proof. We start with a general argument. Let A be a $\mathbf{Q}$-subalgebra of $\mathbf{C}$ and $g \in \mathcal{N}_l^m(\Gamma_0(p^\alpha),\chi\psi^{-1}\varepsilon^{-2};A)$. Write $g = \sum_{j=0}^{m}(4\pi y)^{-j}g_j$ with $g_j \in A[[q]]$. Take $f \in \mathcal{N}_{k'}^{m'}(\Gamma_0(p^\beta),\psi;A)$ and write $f = \sum_{j=0}^{m'}(4\pi y)^{-j}f_j$. We consider

$$g(\delta_{k'}^{r'} f\,|\,\varepsilon\xi) \in \mathcal{N}_{k'+l+2r'}^{m+m'+r'}(\Gamma_0(p^\beta),\chi;A).$$

If $k'+l \ge 2m+2m'$, we can write uniquely

$$(*)\qquad g(\delta_{k'}^{r'} f \mid \varepsilon\xi) = H(g(\delta_{k'}^{r'} f \mid \varepsilon\xi)) + \sum_{j=1}^{m+m'+r'} \delta_{k'+l-2j}^{j} h_j$$

for $h_j \in \mathcal{S}_{k'+l-2j}(\Gamma_0(p^\beta),\chi;A)$ and $H(g(\delta_{k'}^{r'} f \mid \varepsilon\xi)) \in \mathcal{S}_{k'+l}(\Gamma_0(p^\beta),\chi;A)$. Then equating the constant terms of $(*)$ as a polynomial in $(4\pi y)^{-1}$, we see from (1.3) that

$$(1)\qquad g_0 d^{r'}(f_0 \mid \varepsilon\xi) = H(g(\delta_{k'}^{r'} f \mid \varepsilon\xi)) + \sum_{j=1}^{m+m'+r'} d^j h_j.$$

This shows that $H(g(\delta_{k'}^{r'} f \mid \varepsilon\xi)) = g_0 d^{r'}(f_0 \mid \varepsilon\xi) - \sum_{j=1}^{m+m'+r'} d^j h_j$. Now assume that A is a subalgebra of $\overline{\mathbf{Q}} \cap K$. Then we can consider the identity (1) as an identity in $\overline{\mathbf{Q}}_p[[q]]$. Since $H(g(\delta_{k'}^{r'} f \mid \varepsilon\xi)) \in \mathcal{S}_{k'+l}(\Gamma_0(p^\beta),\chi\xi^2;\overline{\mathbf{Q}}_p)$, we see, under the p-adic topology, that

$$H(g(\delta_{k'}^{r'} f \mid \varepsilon\xi)) \mid e = \lim_{n\to\infty} \{g(\delta_{k'}^{r'}(f \mid \varepsilon\xi)) \mid T(p)^{n!}\},$$

where $T(p)$ acts on q-expansions as in the corollary. Note that, for $\phi \in p^{-\gamma}\mathcal{O}[[q]]$ $(0 \le \gamma \in \mathbf{Z})$,

$$d\phi \mid T(p)^{n!} = \sum_{m=1}^{\infty} a(mp^{n!};d\phi)q^n = \sum_{m=1}^{\infty} mp^{n!} a(mp^{n!};\phi)q^n \to 0$$

as $n \to \infty$. Since $h_j \in p^{-\gamma}\mathcal{O}[[q]]$ for sufficiently large γ by Theorem 6.3.2, we conclude that

$$(2)\qquad H(g(\delta_{k'}^{r'} f \mid \varepsilon\xi)) \mid e = \{g_0 d^{r'}(f_0 \mid \varepsilon\xi)\} \mid e.$$

By (2.4a,b), we find that $E(\xi N^j)$ and $G(\xi N^j)$ are modular forms except when $j = 2$ and $\xi = \mathrm{id}$. The forms $E(N^2)$ and $G(N^2)$ show up in the formula when either $k = l+2r+2$ or $k = 2r+l$. In this case, $m = 0$ and $m' = 1$ by (2.4a,b); thus, we can find $f \in \mathcal{N}_2^1(\Gamma_0(p),\mathbf{Q})$ such that $f_0 = E(N^2)$ or $G(N^2)$. Hence the existence of the limit follows from the above argument. When $k'+l \ge 2m$, $H(f(\delta_l^{r'} g \mid \varepsilon\xi)) \mid e$ is always a classical modular form. Thus to finish the proof, we only need to check the identity $h = (G*E(\xi,\eta) \mid e)(P,Q,\varepsilon(u)u^r-1)$ for $\eta = \psi^{-1}\chi$. Taking f as above and writing $g = G(Q)$, we recall (1):

$$G*E(\xi,\psi^{-1}\chi)(P,Q,\varepsilon(u)u^r-1) = g d^{r'}(f_0 \mid \varepsilon\xi) = H(g(\delta_{k'}^{r'} f \mid \varepsilon\xi)) + \sum_{j=1}^{m+m'+r'} d^j h_j.$$

By Lemma 1, $(G*E(\xi,\psi^{-1}\chi)(Z) \mid_{Z=\varepsilon(u)u^r-1}) \mid e = (G*E(\xi,\psi^{-1}\chi) \mid e)(Z) \mid_{Z=\varepsilon(u)u^r-1}$. Thus $(G*E(\xi,\psi^{-1}\chi) \mid e)(Z) \mid_{Z=\varepsilon(u)u^r-1} \mid e = (G*E(\xi,\psi^{-1}\chi) \mid e)(Z) \mid_{Z=\varepsilon(u)u^r-1}$. Note that $G*E(\xi,\psi^{-1}\chi) \mid e \in \mathbf{S}^{\mathrm{ord}}(\chi\xi^2;\Lambda) \hat{\otimes}_{\mathcal{O}} \mathbf{J}[[Z]]$. For $F \in \mathbf{S}((\chi\xi^2)_\infty;\Lambda)$, we have $F \mid e = \lim_{n\to\infty} F \mid T(p)^{n!}$ under the m-adic topology for the maximal ideal of Λ. In fact, assuming $F \in \mathbf{S}((\chi\xi^2)_\alpha;\Lambda)$ for some $\alpha > 0$, we have by definition,

$F\,|\,e(u^k-1) = f(u^k-1)\,|\,e = \lim_{n\to\infty} F(u^k-1)\,|\,T(p)^{n!}$ under the p-adic topology on $\mathcal{S}_k(\Gamma_0(p^\alpha),\chi\xi^2\omega^{-k})$ for $k > a$ with a sufficiently large a. This implies, writing $P_{\alpha,a} = \prod_{b=a}^{\alpha} P_b$, $F\,|\,e = \varprojlim_{\alpha} \lim_{n\to\infty} (F \bmod P_{\alpha,a})\,|\,T(p)^{n!}$, which is equal to the limit under the m-adic topology. Thus we see that

$$G*E(\xi,\psi^{-1}\chi)\,|\,e = \lim_{n\to\infty} (G*E(\xi,\psi^{-1}\chi))\,|\,T(p)^{n!}.$$

This implies

$$(G*E(\xi,\psi^{-1}\chi)\,|\,e)(P,Q,\varepsilon(u)u^r-1) = \lim_{n\to\infty} (G*E(\xi,\psi^{-1}\chi)(P,Q,\varepsilon(u)u^r-1))\,|\,T(p)^{n!},$$

which is equal to h. Here the last limit is taken in $\mathcal{O}[\varepsilon][[q]]$ under the p-adic topology.

§10.4. Three variable p-adic Rankin products

We take two normalized eigenforms $G \in \mathbf{S}(\psi;\mathbf{J})$ and $F \in \mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I})$. Note that $\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I}) = 0$ for p less than 11 (see §7.6). Thus we may assume that $p \geq 5$. We define the Λ-algebra homomorphisms λ: $\mathbf{h}^{\mathrm{ord}}(\chi;\Lambda) \to \mathbf{I}$ and φ: $\mathbf{h}(\psi;\Lambda) \to \mathbf{J}$ by

$$F\,|\,T(n) = \lambda(T(n))F \quad\text{and}\quad G\,|\,T(n) = \varphi(T(n))G.$$

By extending scalars if necessary, we may assume that

(Ir) *the ring $\mathcal{O}$ is integrally closed in $\mathbf{I}$ and $\mathbf{J}$.*

Then $\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]$ is an integral domain finite and flat over $\mathcal{O}[[X,Y,Z]]$. We write $A = \mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]$ and its field of fractions as $M = \mathrm{Frac}(A)$. Then we consider $\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I})\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]] = \mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]])$. As constructed in §7.4, we have an inner product $(\ ,\ )_{\mathbf{I}}$: $\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I})\times\mathbf{S}^{\mathrm{ord}}(\chi;\mathbf{I}) \to \mathbf{K}$ for the quotient field $\mathbf{K}$ of $\mathbf{I}$. We extend this product linearly to an inner product

$$(\ ,\ )_A : \mathbf{S}^{\mathrm{ord}}(\chi;A)\times\mathbf{S}^{\mathrm{ord}}(\chi;A) \to M.$$

Now we define $L_p(\lambda\otimes\varphi^c) = (F,e(G*E(\mathrm{id},\psi^{-1}\chi)))_A \in M$. We study the values $L_p(\lambda\otimes\varphi^c)(P,Q,R)$ for $(P,Q,R) \in \mathcal{A}(\mathbf{I})\times\mathcal{A}(\mathbf{J})\times\mathcal{A}(\Lambda)$. We write $P\cap\Lambda = P_{k,\varepsilon'}$, $Q\cap\Lambda = P_{l,\varepsilon''}$, $R = P_{r,\varepsilon}$ and $\chi_P = \varepsilon'\chi\omega^{-k}$, $\psi_P = \varepsilon''\psi\omega^{-l}$. We further write

$$\lambda_P : \mathbf{h}_k(\Gamma_0(N),\chi_P;\mathbf{Z}[\chi_P]) \to \overline{\mathbf{Q}} \quad\text{and}\quad \varphi_Q : \mathbf{h}_k(\Gamma_0(p^\beta),\psi_Q;\mathbf{Z}[\psi_Q]) \to \overline{\mathbf{Q}}$$

for the algebra homomorphism given by

$$F(P)\,|\,T(n) = \lambda_P(T(n))F(P) \quad (\text{resp. } G(Q)\,|\,T(n) = \varphi_Q(T(n))G(Q))$$

as long as Q is admissible relative to G. By the ordinarity of F, we have

$$\chi_P \textit{ is either trivial with } N = p \textit{ or primitive modulo } N.$$

To compute the value $L_p(\lambda\otimes\varphi^c)(P,Q,R)$, we assume the following condition on ε:

(P) $\quad G(Q)\,|\,\varepsilon\omega^{-r}$ *is a primitive form of exact level* J *for a* p*-power* J.

Although the condition (P) is hard to verify without using representation theory ([Ge] and [C]), let us explain a little bit about this assumption, referring to [H5, II, Lemma 5.2] for details. By the definition of primitive forms given at the beginning of §10.2, we can always find a primitive form g of level J° associated with $G(Q)\,|\,\varepsilon\omega^{-r}$. We know that $g\,|\,T(n) = \varepsilon\omega^{-r}(n)\lambda_P(T(n))g$ for all n prime to p. If $p\,|\,J^\circ$ and $g\,|\,T(p) = 0$, we see that $g = G(Q)\,|\,\varepsilon\omega^{-r}$ because $\varepsilon\omega^{-r}(p)\lambda_P(T(p)) = 0$. For almost all non-trivial ε, J° is divisible by p and $g\,|\,T(p) = 0$. Thus the assumption (P) is known to be true for almost all ε. When G(Q) is ordinary of level J (and thus G is automatically ordinary), the condition P is equivalent to

(P') $\quad \varepsilon\omega^{-r}$ *is neither* ψ_Q^{-1} *nor* ι_p *if* ψ_Q *is non-trivial, and* $\varepsilon\omega^{-r} \neq \iota_p$ *if* ψ_P *is trivial, where* ι_p *is the trivial character modulo* p.

We state our main result in this section:

Theorem 1 (Three variable interpolation). *Let* $\lambda : \mathbf{h}^{\mathrm{ord}}(\chi;\mathbf{I}) \to \mathbf{I}$ *be an* $\mathbf{I}$*-algebra homomorphism associated with a normalized eigenform* $F \in \mathbf{S}^{\mathrm{ord}}(\chi,\mathbf{I})$ *and* G *be a normalized eigenform in* $\mathbf{S}(\psi;\mathbf{J})$. *For each admissible point* Q *of* $\mathcal{A}(\mathbf{J})$, *we write* $\varphi_Q : \mathbf{h}_{k(Q)}(\Gamma_0(p^\beta),\varepsilon_Q\psi\omega^{-k(Q)};\mathcal{O}[\varepsilon]) \to \overline{\mathbf{Q}}_p$ *for the* $\mathcal{O}[\varepsilon]$*-algebra homomorphism associated with* G(Q). *Then we have a unique* p*-adic L-function* $L_p(\lambda\otimes\varphi^c)$ *in the quotient field of* $\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}[[Z]]$ *with the following evaluation property: for* $P \in \mathcal{A}(\mathbf{I})$ *with* $k = k(P)$, *admissible* $Q \in \mathcal{A}(\mathbf{J})$ *with* $l = k(Q)$ *and* $R = P_{r,\varepsilon} \in \mathcal{A}(\Lambda)$ *satisfying the condition (P) and* $0 \le r < k-l$, *we have*

$$\begin{aligned} S(P)L_p(\lambda\otimes\varphi^c)(P,Q,R) &= (-1)^l\lambda_P(T(N_0))\lambda_P(T(J))^{-1}J^{(l/2)+r}N_0^{1-(k/2)}W(\lambda_P)^{-1}W(\varphi_Q\otimes\varepsilon\omega^{-r}) \\ &\quad\times\frac{\Gamma(r+1)\Gamma(l+r)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^r)}{(2\pi i)^{k+l+2r}\pi^{1-k}(F(P)^\circ,F(P)^\circ)}, \end{aligned}$$

where $F(P)^\circ$ *is the primitive form associated with* F(P), N_0 *is the level of* $F(P)^\circ$, J *is the level of the primitive form* $G(Q)\,|\,\varepsilon\omega^{-r}$ *and*

$$S(P) = \begin{cases} 1 & \textit{if either } \chi_P \textit{ is non-trivial or } k = 2, \\ \left(1-\dfrac{p^{k-1}}{\lambda_P(T(p))^2}\right)^{-1}\left(1-\dfrac{p^{k-2}}{\lambda_P(T(p))^2}\right)^{-1} & \textit{otherwise.} \end{cases}$$

Here we understand $W(\lambda_P) = 1$ if χ_P is trivial and $k > 2$. The relation between this three variable p-adic L-function and those obtained already (Theorems 7.4.1 and 7.4.2) will be clarified in the following section. We can even compute the value $L_p(\lambda\otimes\varphi^c)(P,Q,R)$ without assuming (P). However the computation adds additional technical difficulty. Thus here we only present the result under (P). We refer to [H5, II, Th.5.1d] for details in the general case.

We start proving the above theorem. We want to relate the value $L_p(\lambda\otimes\varphi^c)(P,Q,R)$ with the complex L-value $L(s_0,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon)$ for an integer s_0 determined by R. We divide our argument into the following two cases:

$$\text{Case I:}\quad 0 \le r \le \frac{k-l}{2} \text{ and Case II: } \frac{k-l-1}{2} \le r < k-l.$$

By definition, writing A for $\mathbf{Q}_p(\lambda_P{}^c\otimes\varphi_Q\otimes\varepsilon)$, we have by Corollary 3.1

$$(1)\qquad L_p(\lambda\otimes\varphi^c)(P,Q,R)$$
$$= \begin{cases} (F(P),e(G(Q)d^r(E(\psi_Q{}^{-1}\chi_P\varepsilon^{-2}\omega^{2r}N^{k-l-2r})\,|\,\varepsilon\omega^{-r})))_A & \text{in Case I,} \\ (F(P),e(G(Q)d^{k-l-r-1}(G(\psi_Q{}^{-1}\chi_P\varepsilon^{-2}\omega^{2r}N^{2r+l-k+2})\,|\,\varepsilon\omega^{-r})))_A & \text{in Case II.} \end{cases}$$

Now we prove a lemma:

Lemma 1. *Let* $\varepsilon : (\mathbf{Z}/p^\gamma\mathbf{Z})^\times \to \mathcal{O}^\times$ *be a character. Assume that* $\lim_{n\to\infty}(f(g\,|\,\varepsilon))\,|\,T(p)^{n!}$ *converges to a power series* $e(f(g\,|\,\varepsilon))$ *p-adically in* $\mathcal{O}[[q]]$ *for* f *and* $g \in \mathcal{O}[[q]]$, *where* $\sum_{n=1}^{\infty} a_nq^n\,|\,T(p) = \sum_{n=1}^{\infty} a_{pn}q^n$ *and* $\sum_{n=1}^{\infty} a_nq^n\,|\,\varepsilon = \sum_{n=1}^{\infty}\varepsilon(n)a_nq^n$. *Then* $\lim_{n\to\infty}((f\,|\,\varepsilon)g)\,|\,T(p)^{n!}$ *converges to a power series* $e((f\,|\,\varepsilon)g)$ *and satisfies* $e(f(g\,|\,\varepsilon)) = \varepsilon(-1)e((f\,|\,\varepsilon)g)$.

Proof. We define $|\sum_{n=1}^{\infty} a_nq^n|_p = \mathrm{Sup}_n\,|a_n|_p$. Then the p-adic convergence is just the convergence under the norm $|\ |_p$ in $\mathcal{O}[[q]]$. Writing a(n,f) for the coefficient in q^n of f, we first prove that

$$a(np^r,f(g\,|\,\varepsilon)) = \varepsilon(-1)a(np^r,(f\,|\,\varepsilon)g) \text{ if } r \ge \gamma.$$

This is just a computation,

$$a(np^r,f(g\,|\,\varepsilon)) - \varepsilon(-1)a(np^r,(f\,|\,\varepsilon)g)$$
$$= \sum_{j=1}^{np^r}\varepsilon(np^r-j)a(j,f)a(np^r-j,g) - \varepsilon(-1)\sum_{j=1}^{np^r}\varepsilon(j)a(j,f)a(np^r-j,g) = 0,$$

because $\varepsilon(np^r-j) = \varepsilon(-j) = \varepsilon(-1)\varepsilon(j)$ if $r \ge \gamma$. This shows

$$(f(g\,|\,\varepsilon))\,|\,T(p)^r = \varepsilon(-1)((f\,|\,\varepsilon)g)\,|\,T(p)^r.$$

This implies that $\lim_{n\to\infty}((f\,|\,\varepsilon)g)\,|\,T(p)^{n!}$ and $\lim_{n\to\infty}(f(g\,|\,\varepsilon))\,|\,T(p)^{n!}$ converge at the same time and $e(f(g\,|\,\varepsilon)) = \varepsilon(-1)e((f\,|\,\varepsilon)g)$.

Note the fact that $e(G(Q)d^r g) = \lim_{n\to\infty}(G(Q)d^r g)\,|\,T(p)^{n!}$ in $\mathcal{O}[[q]]$ under the p-adic topology. Then, writing simply $E = E(\xi N^{k-l-2r})$ and

$$E' = \delta_{j,1}2^{-1}L_L(0,\xi)-\delta_{j,2}\delta_{\xi,\mathrm{id}}(8\pi\,|\,y\,|_A)^{-1}\varphi(L)L^{-1}+G(\xi N^j)$$

for $\xi = \psi_Q^{-1}\chi_P\varepsilon^{-2}\omega^{2r}$ and $j = 2r+l-k+2$, we know, from (1) and the fact that $\varepsilon\omega^{-r}(-1) = (-1)^r$,

$$\begin{aligned}
&L_p(\lambda\otimes\varphi^c)(P,Q,R)\\
&= (-1)^r\times\begin{cases}(F(P),e(G(Q)\,|\,\varepsilon\omega^{-r}d^rE(\xi N^{k-l-2r})))_A & \text{in Case I,}\\ (F(P),e(G(Q)\,|\,\varepsilon\omega^{-r}d^{k-l-r-1}G(\xi N^{2r+l-k+2})))_A & \text{in Case II,}\end{cases}\\
&= (-1)^r\times\begin{cases}(F(P),e(H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^r_{k-l-2r}E)))_A & \text{in Case I,}\\ (F(P),e(H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')))_A & \text{in Case II,}\end{cases}
\end{aligned}$$

where we have used (3.2) and the fact (2.4a,b) that E and E' are classical modular forms to obtain the last equality. Since e is self-adjoint under the pairing $(\ ,\ )_A$ and $F(P)\,|\,e = F(P)$, we have

$$L_p(\lambda\otimes\varphi^c)(P,Q,R) = (-1)^r\times\begin{cases}(F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^r_{k-l-2r}E))_A & \text{in Case I,}\\ (F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E'))_A & \text{in Case II.}\end{cases}$$

Write L for the least common multiple of $N = p^\alpha$ (the level of $F(P)$) and $J = p^{\beta+2\gamma}$ (the level of $G(Q)\,|\,\varepsilon\omega^{-r}$), and put $p^\delta = L/N$. Then the self-adjointness of $T(p^\delta)$ shows that

$$\begin{aligned}
(2)\qquad &L_p(\lambda\otimes\varphi^c)(P,Q,R)\\
&= (-1)^r\lambda_p(T(p))^{-\delta}\times\begin{cases}(F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^r_{k-l-2r}E)\,|\,T(p^\delta))_A & \text{in Case I,}\\ (F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')\,|\,T(p^\delta))_A & \text{in Case II,}\end{cases}\\
&= (-1)^r\lambda_p(T(p))^{-\delta}\times\begin{cases}(F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^r_{k-l-2r}E)\,|\,T(p^\delta))_C & \text{in Case I,}\\ (F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')\,|\,T(p^\delta))_C & \text{in Case II.}\end{cases}
\end{aligned}$$

When either χ_P is primitive modulo $N = p^\alpha$ or $k = 2$, as we have already seen in (7.4.1a) (and in a remark after Corollary 7.2.1 when $k = 2$) that

$$(F(P),g)_C = \frac{(F(P),g)_\infty}{(F(P),F(P))_\infty} = \frac{(g,F(P)_c\,|\,\tau)}{(F(P),F(P)_c\,|\,\tau)} = \frac{(g,F(P))}{(F(P),F(P))},$$

because $F(P)_c\,|\,\tau = W(\lambda^c)F(P)$. We now compute $(F(P),g)_C$ in terms of the complex Petersson product $(\ ,\ )$ when χ_P is trivial. The above formula is true except for the last term. In fact, the linear form

$$L\colon g \mapsto \frac{(F(P),g)_\infty}{(F(P),F(P))_\infty}$$

satisfies $L\circ T(n) = \lambda_P(T(n))L$ and $L(F(P)) = 1$. Thus by the duality theorem (Theorem 6.3.2), we find that $L(g) = (F(P),g)_C$. Therefore we need to compute $F(P)_c\,|\,\tau$ for $\tau = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$. As shown in Corollary 7.2.1 (or its proof), if $k > 2$, there exists a unique normalized eigenform $F(P)^\circ \in \mathcal{S}_k(SL_2(\mathbf{Z}))$ such that $F(P)^\circ\,|\,T(n) = \lambda_P(T(n))F(P)^\circ$ for n prime to p and $F(P)^\circ\,|\,T(p) = (\alpha+\beta)F(P)^\circ$ for $\alpha = \lambda_P(T(p))$ and $\beta = p^{k-1}\lambda_P(T(p))^{-1}$. We note here that $\beta^c = \alpha$ because $\alpha+\beta$ is a real number (because it is an eigenvalue of the self-adjoint operator $T(p)$). Moreover

$$F(P) = F(P)^\circ - \alpha^{-1}F(P)^\circ\,|_k\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

We call this form $F(P)^\circ$ the primitive form associated with $F(P)$. Either when χ_P is primitive modulo p^α or when $k = 2$, we simply put $F(P)^\circ = F(P)$, i.e., $F(P)$ is already primitive. We put $W(\lambda) = 1$ in this case, $W(\lambda) \in \mathbf{C}$ because $F(P)^\circ\,|\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = F(P)^\circ$. Then we see, noting that $(F(P)^\circ)_c = F(P)^\circ$, that

$$F(P)_c\,|\,\tau = F(P)_c\,|\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = F(P)^\circ\,|_k\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} - \beta^{-1}p^{k-2}F(P)^\circ$$
$$= F(P)^\circ\,|_k\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} - \alpha p^{-1}F(P)^\circ = -\alpha p^{-1}(F(P)^\circ - \alpha^{-1}pF(P)^\circ\,|_k\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}).$$

Writing $(\,,\,)_p$ for the Petersson inner product of level p and $(\,,\,)$ for that of level 1, we now compute, for $\delta = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ and $f = F(P)^\circ$,

$$(F(P),F(P)_c\,|\,\tau)_p = -\beta p^{-1}(f - \alpha^{-1}f\,|\,\delta, f - \alpha^{-1}pf\,|_k\delta)_p.$$

Now we use the fact that

$$(f,f)_p = (SL_2(\mathbf{Z}):\Gamma_0(p))(f,f) = (1+p)(f,f), \quad (f,f\,|_k\delta)_p = (f\,|\,T(p),f) = (\alpha+\beta)(f,f),$$
$$(f\,|_k\delta,f)_p = (\alpha+\beta)(f,f) \quad \text{(see the proof of Lemma 2.1)},$$
$$(f\,|_k\delta,f\,|_k\delta)_p = (f\,|_k\tau,f\,|_k\tau)_p = p^{k-2}(f\|_k\tau,f\|_k\tau)_p = p^{k-2}(1+p)(f,f),$$

where $T_p(p)$ in the last formula indicates the Hecke operator of level p. This shows, if χ_P is trivial and $k > 2$, that

$$(3) \qquad (F(P),F(P)_c\,|\,\tau)_p = \lambda_P(T(p))\Big(1 - \frac{p^{k-1}}{\lambda_P(T(p))^2}\Big)\Big(1 - \frac{p^{k-2}}{\lambda_P(T(p))^2}\Big)(F(P)^\circ,F(P)^\circ).$$

We now compute $(F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^r_{k-l-2r}E)\,|\,T(p^\delta))_C$ in Case I. We suppose either $k = 2$ or χ_P is non-trivial. We recall (2.6a) replacing λ and φ there by $\lambda_P{}^c$ and $\varphi_Q{}^c$:

$$(4) \quad 2(4\pi)^{-l-r}\Gamma(l+r)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^r) = (L/N)^{1-(k/2)}(-4\pi)^r\Gamma(r+1)^{-1}\chi_P(-1)W(\lambda_P)$$
$$\times(\{(G(Q)_c\,|\,\varepsilon^{-1}\omega^r\|_l\tau_L)(\delta^r_{k-l-2r}(E'_{k-l-2r,L}(z,j,\xi^{-1})\|_{k-l-2r}\tau_L))\}\,|\,T(p^\delta),F(P))_N$$

where $j = 1-k+l+2r$, $\xi = \chi_P\psi_Q^{-1}\varepsilon^{-2}\omega^{2r}$ and L is the least common multiple of $N = p^\alpha$ and $J = p^{\beta+2\gamma}$ which is the level of $G(Q)\,|\,\varepsilon\omega^{-r}$. As already seen in the proof of Lemma 2.1, the operator $T_{L/N}$ is nothing but $T(p^\delta)$. We want to relate the value $(F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^r_{k-l-2r}E)\,|\,T(p^\delta))_C$ to that of (4). We have

$$\begin{aligned}(5)\qquad &(F(P)^\circ,F(P)^\circ)(F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^r_{k-l-2r}E)\,|\,T(p^\delta))_C\\ &= (H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^r_{k-l-2r}E)\,|\,T(p^\delta),F(P))\\ &= (\{(G(Q)\,|\,\varepsilon\omega^{-r})\delta^r_{k-l-2r}E\}\,|\,T(p^\delta),F(P))\\ &= (-1)^l(\{(G(Q)\,|\,\varepsilon\omega^{-r})\|_l\tau_L\|_l\tau_L\delta^r_{k-l-2r}E\}\,|\,T(p^\delta),F(P)).\end{aligned}$$

We need to compute $G(Q)\,|\,\varepsilon\omega^{-r}\|_l\tau_L$. Under (P), we have (by (2.2))

$$\begin{aligned}(6)\qquad G(Q)\,|\,\varepsilon\omega^{-r}\|_l\tau_L &= G(Q)\,|\,\varepsilon\omega^{-r}\|_l\tau_J\begin{pmatrix}L/J & 0\\ 0 & 1\end{pmatrix}\\ &= (L/J)^{l/2}W(\varphi_Q\otimes\varepsilon\omega^{-r})(G(Q)_c\,|\,\varepsilon^{-1}\omega^r)(Lz/J),\end{aligned}$$

for a constant $W(\varphi_Q\otimes\varepsilon\omega^{-r})$ with absolute value 1. Then (5) is equal to

$$(-1)^l(L/J)^{l/2}W(\varphi_Q\otimes\varepsilon\omega^{-r})(\{G(Q)_c\,|\,\varepsilon^{-1}\omega^r(Lz/J)\}\|_l\tau_L\delta^r_jE(\xi N^j)\,|\,T(p^\delta),F(P)),$$

where $j = k-l-2r$. Then recalling the formula (2.4b),

$$\begin{aligned}(7)\qquad &(E'_{k-l-2r,L}(z,1-k+l+2r,\xi^{-1})\|_k\tau_L)^*\\ &= 2L^{-(k-l-2r)/2}\xi(-1)G_{k-l-2r,L}(x,1-k+l+2r,\xi)\\ &= i^{k-l-2r}2^{1+k-l-2r}L^{(k-l-2r)/2-1}\pi(-1)^{k+l}E(\xi N^{k-l-2r})\end{aligned}$$

and the fact that

$$\begin{aligned}D(s,F(P),g_c(p^\nu z)) &= \sum_{n=1}^\infty \varepsilon^{-1}\omega^r(n)\varphi_Q{}^c(T(n))\lambda_P(T(np^\nu))(np^\nu)^{-s}\\ &= \lambda_P(T(p))^\nu p^{-\nu s}D(s,F(P),g_c),\end{aligned}$$

we see from (4) that (5) is equal to

$$\begin{aligned}&i^{-k+l}2^{-k-l-2r}\pi^{-1-l-2r}J^{(l/2)+r}N^{1-(k/2)}\lambda_P(T(L/J))W(\lambda_P)^{-1}W(\varphi_Q\otimes\varepsilon\omega^{-r})\\ &\qquad\times\Gamma(r+1)\Gamma(l+r)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^r).\end{aligned}$$

Thus finally we get, if either χ_P is non-trivial or $k = 2$ and if (P) holds,

$$\begin{aligned}(8)\quad &L_p(\lambda\otimes\varphi^c)(P,Q,R)\\ &= (-1)^l\lambda_P(T(N))\lambda_P(T(J))^{-1}J^{(l/2)+r}N^{1-(k/2)}W(\lambda_P)^{-1}W(\varphi_Q\otimes\varepsilon\omega^{-r})\\ &\qquad\times\frac{\Gamma(r+1)\Gamma(l+r)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^r)}{(2\pi i)^{k+l+2r}\pi^{1-k}(F(P)^\circ,F(P)^\circ)}.\end{aligned}$$

We will show that the above formula holds also in Case II if either χ_p is non-trivial or $k = 2$ and if (P) holds.

Now we consider the case where χ_p is trivial and $k > 2$, but we still remain in Case I. We then need to compute

$$\begin{aligned}
&(H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{r}_{k-l-2r}E)\,|\,T(p^{\delta}),F(P)_c\,|\,\tau)_p\\
&= p^{(k/2)-1}(G(Q)\,|\,\varepsilon\omega^{-r}\|_l\tau_L\|_l\tau_L\delta^{r}_{k-l-2r}E)\,|\,T(p^{\delta}),F(P)_c\|_k\tau)_p\\
&= (-1)^l p^{(k/2)-1}(L/J)^{l/2}W(\varphi_Q\otimes\varepsilon\omega^{-r})\\
&\qquad\times(\{(G(Q)_c\,|\,\varepsilon^{-1}\omega^{r})(Lz/J)\|_l\tau_L\delta^{r}_{k-l-2r}E\}\,|\,T(p^{\delta}),F(P)_c\|_k\tau)_p\\
&\overset{(7)}{=} i^{k+l+2r}2^{-1-k+l+2r}L^{-(k-2r)/2+l+1}\pi^{-1}p^{(k/2)-1}J^{-l/2}W(\varphi_Q\otimes\varepsilon\omega^{-r})\\
&\quad\times(\{(G(Q)_c\,|\,\varepsilon^{-1}\omega^{r})(\tfrac{Lz}{J})\|\tau_L\delta^{r}_{k-l-2r}E'_{k-l-2r,L}(z,1-k+l+2r,\xi^{-1})\|\tau_L\}\,|\,T(p^{\delta}),F(P)_c\|\tau)_p.
\end{aligned}$$

By (2.6a), we have, for $g = (G(Q)_c\,|\,\varepsilon^{-1}\omega^{r})(Lz/J)$

$$\begin{aligned}
&2(-1)^r(4\pi)^{-l-2r}\Gamma(l+r)\Gamma(r+1)\lambda(T(L/J))(L/J)^{-l-r}(L/N)^{-1+(k/2)}L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^{r})\\
&\qquad= (\{(g\|_l\tau_L)(\delta^{r}_{k-l-2r}E'_{k-l-2r,L}(z,1-k-l+2m,\chi\psi^{-1})\|\tau_L)\}\,|\,T(p^{\delta}),F(P)_c\|_k\tau)_p.
\end{aligned}$$

We then know, noting that $N = p$ and k is even, that

$$\begin{aligned}
(H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{r}_{k-l-2r}E)\,|\,T(p^{\delta}),F(P)_c\,|\,\tau)_p &= (-1)^{l+r}(2\pi i)^{-k-l-2r}\pi^{k-1}J^{(l/2)+r}\\
&\quad\times W(\varphi_Q\otimes\varepsilon\omega^{-r})\Gamma(l+r)\Gamma(r+1)\lambda(T(L/J))L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^{r}).
\end{aligned}$$

By (2) and (3), this shows, if $k > 2$ and χ_p is trivial, under (P), that

$$\begin{aligned}
(9)\qquad L_p(\lambda\otimes\varphi^c)(P,Q,R) &= (-1)^l J^{(l/2)+r}W(\varphi_Q\otimes\varepsilon\omega^{-r})\lambda(T(J))^{-1}\\
&\times(1-\frac{p^{k-1}}{\lambda_P(T(p))^2})^{-1}(1-\frac{p^{k-2}}{\lambda_P(T(p))^2})^{-1}\frac{\Gamma(l+r)\Gamma(r+1)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^{r})}{(2\pi i)^{k+l+2r}\pi^{1-k}(F(P)^\circ,F(P)^\circ)}.
\end{aligned}$$

In this case, for $\lambda_P{}^\circ : \mathbf{h}_k(SL_2(\mathbf{Z});\mathbf{Z}) \to \overline{\mathbf{Q}}$ given by

$$F(P)^\circ\,|\,T(n) = \lambda_P{}^\circ(T(n))F(P)^\circ,$$

we note that $W(\lambda_P{}^\circ) = 1$. We will see later that (9) also holds without any change in Case II if χ_p is trivial and $k > 2$.

We now deal with Case II. As before, we first assume that either χ_p is trivial or $k = 2$. We compute

$$\begin{aligned}
&(F(P)^\circ,F(P)^\circ)(F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')\,|\,T(p^{\delta}))_C\\
&\qquad= (H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')\,|\,T(p^{\delta}),F(P))_N\\
&\qquad= (-1)^l(L/J)^{l/2}W(\varphi_Q\otimes\varepsilon\omega^{-r})\\
&\qquad\quad\times(\{(G(Q)_c\,|\,\varepsilon^{-1}\omega^{r})(Lz/J)\|_l\tau_L G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E'\}\,|\,T(p^{\delta}),F(P))_N.
\end{aligned}$$

Now by (2.7b), solving $k-1-m = k-l-r-1$ and $2m+2-k-l = 2r+l-k+2$, we have $m = l+r$ and

$$\begin{aligned}\lambda(T(L/J))(L/J)^{-l-r}\Gamma(r+1)\Gamma(l+r)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^r)\\ = 2^{k+l+2r}i^{k+l}\pi^{l+2r+1}L^{-r-(l/2)}N^{(k/2)-1}W(\lambda_P)\\ \times(\{((G(Q)_c\,|\,\varepsilon^{-1}\omega^r)(Lz/J)\|_l\tau_L)(\delta^{k-l-r-1}_{2r+l-k+2}E')\}\,|\,T_{L/N},F(P)^\circ)_N.\end{aligned}$$

Thus we have

$$\begin{aligned}&(F(P)^\circ,F(P)^\circ)(F(P),H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')\,|\,T(p^\delta))_C\\ &= (-1)^{l+r}(2\pi i)^{-k-l-2r}\pi^{k-1}N^{-(k/2)+1}\lambda_P(T(L/J))J^{l/2+r}W(\varphi_Q\otimes\varepsilon\omega^{-r})W(\lambda_P)^{-1}\\ &\qquad\times\Gamma(r+1)\Gamma(l+r)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^r),\end{aligned}$$

which shows that the formula (8) again holds in Case II if χ_P is non-trivial or $k = 2$. We now assume that $k > 2$ and χ_P is trivial. Thus $N = p$. We compute

$$\begin{aligned}&(H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')\,|\,T(p^\delta),F(P)_c\,|\,\tau)_N\\ &\quad= (H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')\,|\,T(p^\delta),F(P)_c\,|\,\tau)_N\\ &\quad= C(\{(G(Q)_c\,|\,\varepsilon^{-1}\omega^r)(Lz/J)\|_l\tau_L\delta^{k-l-r-1}_{2r+l-k+2}E'\}\,|\,T(p^\delta),F(P)_c\|_k\tau)_N,\end{aligned}$$

for $C = (-1)^l(L/J)^{l/2}p^{(k/2)-1}W(\varphi_Q\otimes\varepsilon\omega^{-r})$. By (2.7a), for $g = (G(Q)_c\,|\,\varepsilon^{-1}\omega^r)(Lz/J)$,

$$\begin{aligned}&2(4\pi)^{-l-r}(L/J)^{-l-r}\lambda_P(T(L/J))\Gamma(r+1)\Gamma(l+r)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^r)\\ &= (L/N)^{1-(k/2)}(-4\pi)^{k-1-l-r}\Gamma(l+2r+2-k)\\ &\qquad\times(\{(g\|_l\tau_L)(\delta^{k-l-r-1}_{2r+l-k+2}E'_{2r+2-k+l,L}(z,0,\xi^{-1})\|\tau_L)\}\,|\,T_{L/N},f\|_k\tau_N)_N\\ &= 2^{k-l-1}\pi^{1+r}i^{l-k}N^{-1+(k/2)}L^{-(l+2r)/2}(\{(g\|_l\tau_L)(\delta^{k-l-r-1}_{2r+l-k+2}E')\}\,|\,T_{L/N},f\|_k\tau_N)_N,\end{aligned}$$

where we have used (2.4a) and (2.5a) combined with

$$(E'_{k,L}(z,s,\xi^{-1})\|\tau_L)^* = (-1)^{k+l}\Gamma(l-k+2r+2)^{-1}(2\pi i)^{l-k+2r+2}2L^{-(l-k+2r+2)/2}E'.$$

This shows that

$$\begin{aligned}&(H(G(Q)\,|\,\varepsilon\omega^{-r}\delta^{k-l-r-1}_{2r+l-k+2}E')\,|\,T(p^\delta),F(P)_c\,|\,\tau)_N\\ &\qquad= (-1)^{l+r}(2\pi i)^{-k-l-2r}\pi^{k-1}J^{(l/2)+r}W(\varphi_Q\otimes\varepsilon\omega^{-r})\lambda_P(T(L/J))\\ &\qquad\qquad\times\Gamma(r+1)\Gamma(l+r)L(l+r,\lambda_P\otimes\varphi_Q{}^c\otimes\varepsilon^{-1}\omega^r).\end{aligned}$$

Thus again, in Case II, under (P), we know that (9) remains true if χ_P is trivial and $k > 2$. This finishes the proof.

§10.5. Relation to two variable p-adic Rankin products

In this section, we clarify the relation between three variable p-adic Rankin product and the two variable one constructed in §7.4. To relate two p-adic L-functions, we need to perform a supplementary computation to ease a little bit the condition (P) in §4. For that, we use the notation introduced in §4. We assume that G is ordinary and ψ_Q is non-trivial. Let ι_p be the trivial character modulo p. Then

$$G(Q)\,|\,\iota_p = G(Q)-G(Q)\,|\,T(p)(pz) = G(Q)-\varphi_Q(T(p))p^{1-l}G(Q)\,|\,_l\delta$$

for $\delta = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Then writing the exact level of $G(Q)$ as J_0 and assuming that $G(Q)$ is primitive and J_0 is divisible by p, we see for $J = J_0p$ and $\tau = \begin{pmatrix} 0 & -1 \\ J & 0 \end{pmatrix}$ that

$$\begin{aligned} G(Q)\,|\,\iota_p\|_l\tau &= J^{1-(l/2)}\{G(Q)-\varphi_Q(T(p))p^{1-l}G(Q)\,|\,_l\delta\}\,|\,_l\tau \\ &= p^{(l/2)}W(\varphi_Q)G(Q)_c(pz)-\varphi_Q(T(p))p^{-l/2}W(\varphi_Q)G(Q)_c. \end{aligned}$$

Performing the same computation as in §4 replacing the formula (4.6) by

$$G(Q)\,|\,\iota_p\|_l\tau_L = (L/J)^{l/2}\{p^{1-(l/2)}W(\varphi_Q)G(Q)_c\,|\,_l\delta-p^{k-2}J_0^{(k/2)-1}W(\varphi_Q)G(Q)_c\}(\tfrac{Lz}{J}),$$

we have

$$\begin{aligned} (1)\qquad & L_p(\lambda\otimes\varphi^c)(P,Q,R) \\ &= (-1)^l\lambda_p(T(N))\lambda_P(T(J_0))^{-1}J_0^{(l/2)+r}N^{1-(k/2)}W(\lambda_p)^{-1}W(\varphi_Q) \\ &\qquad \times\frac{\Gamma(r+1)\Gamma(l+r)E(l+r)L(l+r,\lambda_p\otimes\varphi_Q{}^c)}{(2\pi i)^{k+l+2r}\pi^{1-k}(F(P)^\circ,F(P)^\circ)}, \end{aligned}$$

where
$$E(s) = \left(1-\frac{p^{s-1}}{\varphi_Q(T(p))^c\lambda_p(T(p))}\right).$$

Let us prove (1). We only deal with Case I because Case II can be done similarly. We have from (4.5) that

$$\begin{aligned} &(F(P)^\circ,F(P)^\circ)(F(P),H(G(Q)\,|\,\iota_p\delta^r_{k-l-2r}E)\,|\,T(p^\delta))_C \\ &\qquad = (-1)^l(\{(G(Q)\,|\,\iota_p)\|_l\tau_L\|_l\tau_L\delta^r_{k-l-2r}E\}\,|\,T_{L/N},F(P)) \\ &= (-1)^{l+1}p^{-(l/2)}\varphi_Q(T(p))W(\varphi_Q)(L/J)^{l/2} \\ &\qquad \times([\{G(Q)_c(Lz/J)-\varphi_Q(T(p))^{-1}p^lG(Q)_c(Lz/J_0)\}\|_l\tau_L\delta^r_{k-l-2r}E]\,|\,T_{L/N},F(P)), \end{aligned}$$

which is equal to (by (4.4) and (4.7))

$$(-1)^{l+1}(-1)^r\pi^{k-1}(2\pi i)^{-k-l-2r}\varphi_Q(T(p))W(\varphi_Q)W(\lambda_P)^{-1}J_0^{-l/2}N^{1-(k/2)}$$
$$\times\Gamma(l+r)\Gamma(r+1)L(l+r,\lambda_P\otimes\varphi_Q{}^c)$$
$$\times L^{l+r}p^{-l}(\lambda_P(T(L/J))(L/J)^{-l-r}-\varphi_Q(T(p))^c p\lambda_P(T(L/J_0))(L/J_0)^{-l-r})$$
$$=(-1)^l(-1)^r\pi^{k-1}(2\pi i)^{-k-l-2r}W(\varphi_Q)W(\lambda_P)^{-1}J_0^{l/2+r}N^{1-(k/2)}\lambda_P(T(L/J_0))$$
$$\times(1-\varphi_Q(T(p))^{-c}\lambda_P(T(p))^{-1}p^{l+r-1})\Gamma(l+r)\Gamma(r+1)L(l+r,\lambda_P\otimes\varphi_Q{}^c).$$

Then by (4.2), we have the formula (1).

We now assume

(Q1) $\xi=\psi_Q{}^{-1}\chi_P$ *is primitive modulo* L,
(Q2) χ_P *is non-trivial and* $\varepsilon\omega^{-r}$ *is trivial,*
(Q3) ψ_Q *is non-trivial.*

We write the level of the primitive form G(Q) as J_0, which is divisible by p by (Q3). We have defined in §7.4 the two variable Rankin product $L_P(\lambda^c\otimes\varphi)$. We had the following evaluation formula (Theorem 7.4.2):

$$L_P(\lambda^c\otimes\varphi)(P,Q)$$
$$=L^{(k-l)}\lambda_P(T(N/L))\varphi_Q(T(L/N))\frac{\Gamma(k-1)\Gamma(k-l)L(k-1,\lambda_P{}^c\otimes\varphi_Q)}{G(\chi_P{}^{-1}\psi_Q)(-2\pi i)^{k-l}(4\pi)^{k-1}(F(P)^\circ,F(P)^\circ)}.$$

We recall the functional equation (Theorem 9.5.1):

$$(2\pi)^{-2k+1+l}\Gamma(k-l)\Gamma(k-1)L(k-1,\lambda_P{}^c\otimes\varphi_Q)=w(2\pi)^{-l-1}\Gamma(l)L(l,\lambda_P\otimes\varphi_Q{}^c),$$

where

$$w=(-1)^lW(\lambda_P{}^c)W(\varphi_Q)G(\chi_P{}^{-1}\psi_Q)\lambda_P(T(L/J_0))L^{1-k}J_0^{l/2}\varphi_Q(T(L/N))^cN^{l-(k/2)}.$$

This shows that

$$L_P(\lambda^c\otimes\varphi)(P,Q)=(-1)^{k+l}W(\lambda_P{}^c)W(\varphi_Q)\lambda_P(T(L/J_0))L^{l-1}J_0^{l/2}\varphi_Q(T(L/N))^cN^{l-(k/2)}$$
$$\times\lambda_P(T(N/L))\varphi_Q(T(L/N))\frac{\Gamma(l)L(l,\lambda_P\otimes\varphi_Q{}^c)}{(2\pi i)^{k+l}\pi^{1-k}(F(P)^\circ,F(P)^\circ)}.$$

By (1), we know that

$$L_P(\lambda\otimes\varphi^c)(P,Q,P_0)$$
$$=(-1)^l\lambda_P(T(N))\lambda_P(T(J_0))^{-1}J_0^{(l/2)}N^{1-(k/2)}W(\lambda_P)^{-1}W(\varphi_Q)\frac{\Gamma(l)E(l)L(l,\lambda_P\otimes\varphi_Q{}^c)}{(2\pi i)^{k+l}\pi^{1-k}(F(P)^\circ,F(P)^\circ)}$$
$$=E(l)L_P(\lambda^c\otimes\varphi)(P,Q),$$

where $E(l) = (1-\frac{p^{l-1}}{\varphi_Q(T(p))^c\lambda_p(T(p))}) = (1-\frac{\varphi_Q(T(p))}{\lambda_p(T(p))})$. Here we note that $E = (1-\frac{\varphi(T(p))}{\lambda(T(p))}) \in \mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ and $E(P,Q) = (1-\frac{\varphi_Q(T(p))}{\lambda_p(T(p))})$. Thus writing $L_p(\lambda\otimes\varphi^c)_{P_0}$ for the element of the quotient field of $\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ given by evaluating the variable R of $L_p(\lambda\otimes\varphi^c)$ at P_0, we expect to have

$$L_p(\lambda\otimes\varphi^c)_{P_0} = E\cdot L_p(\lambda^c\otimes\varphi) \text{ in } \mathrm{Frac}(\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}).$$

To see this, we note the following fact valid in a more general setting. Let A be an integral domain and $\mathcal{P}$ be a set of prime ideals with the property that $\bigcap_{P\in\mathcal{P}}P = \{0\}$. Then the congruence $\alpha \equiv \beta \bmod P$ for all $P \in \mathcal{P}$ (α, $\beta \in A$) implies the identity $\alpha = \beta$. If $\mathcal{P}$ is a set of infinitely many primes of height 1 in Λ, this $\mathcal{P}$ satisfies the above property $\bigcap_{P\in\mathcal{P}}P = \{0\}$ because for $P_1, \ldots, P_r \in \mathcal{P}$, $P_1\cap\cdots\cap P_r$ is contained in the r-th power of the maximal ideal of Λ. Thus we need to prove

Lemma 1. *Let*

$$\mathcal{P} = \{(P,Q) \in \mathcal{A}(\mathbf{I})\times\mathcal{A}(\mathbf{J}) \mid P \text{ and } Q \text{ satisfy (Q1-3) and } k > l\}.$$

Regard $\mathcal{P}$ as a set of prime ideals of $\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}$. Then the intersection of all ideals in $\mathcal{P}$ is null.

Proof. Since $\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ is a finite extension of $\mathcal{O}[[X,Y]] = \Lambda\hat{\otimes}_{\mathcal{O}}\Lambda$, we may assume that $\mathbf{I} = \mathbf{J} = \Lambda$. Then $\Lambda\hat{\otimes}_{\mathcal{O}}\Lambda$ can be identified as a measure space of $W\times W$. Then, as seen in §3.6, the evaluation of power series Φ at $(P_{k,\varepsilon},P_{l,\varepsilon'})$ corresponds to the integration $\Phi \mapsto \int x^k\varepsilon(x)y^l\varepsilon'(y)d\mu_\Phi(x,y)$. For fixed finite order characters ε and ε', the functions $\{x^k\varepsilon(x)y^l\varepsilon'(y) \mid k \geq l\}$ spans a dense subspace inside the space of continuous functions on $W\times W$. In fact, by the variable change $(x,y) \mapsto (xy^{-1},y) = (s,t)$, this set equals the set of primes with respect to the variables (s,t) given by

$$\{(P_{j,\varepsilon\varepsilon'^{-1}},P_{l,\varepsilon'}) \mid j > 0 \text{ and } l > 0\},$$

which corresponds to the space spanned by $\{s^j\varepsilon\varepsilon'^{-1}(s)y^l\varepsilon'(y) \mid j > 0, l > 0\}$, which is obviously dense. Since the measure is determined by the dense subspace, we get the lemma, because $\mathcal{P}$ contains a set of the above type for a suitable choice of ε and ε'.

The above lemma shows the desired identity $L_p(\lambda\otimes\varphi^c)_{P_0} = E\cdot L_p(\lambda^c\otimes\varphi)$, because $L_p(\lambda\otimes\varphi^c)_{P_0}(P,Q) = (E\cdot L_p(\lambda^c\otimes\varphi))(P,Q)$ implies

$$L_p(\lambda\otimes\varphi^c)_{P_0} \equiv E\cdot L_p(\lambda^c\otimes\varphi) \bmod (P,Q)$$

for all $(P,Q) \in \mathcal{P}$ in the lemma inside the subring of $\mathrm{Frac}(\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J})$ in which the denominators of $L_p(\lambda\otimes\varphi^c)_{P_0}$ and $L_p(\lambda^c\otimes\varphi)$ are inverted. Thus we have

Theorem 1. *We have* $L_p(\lambda\otimes\varphi^c)_{P_0} = E\cdot L_p(\lambda^c\otimes\varphi)$ *in the field of fractions of* $\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}$. *That is, we have as a function of* $\mathcal{X}(\mathbf{I})\times\mathcal{X}(\mathbf{J})$

$$L_p(\lambda\otimes\varphi^c)(P,Q,P_0) = \left(1-\frac{\varphi_Q(T(p))}{\lambda_p(T(p))}\right)L_p(\lambda^c\otimes\varphi)(P,Q),$$

where $L_p(\lambda\otimes\varphi^c)$ *is the function in Theorem 4.1 and* $L_p(\lambda^c\otimes\varphi)$ *is the function given in Theorem 7.4.2.*

Note that $E = \left(1-\frac{\varphi(T(p))}{\lambda(T(p))}\right)$ is contained in $\mathbf{I}\hat{\otimes}_{\mathcal{O}}\mathbf{J}$ and hence holomorphic everywhere. When $\varphi = \lambda$, it has a zero along the diagonal line (i.e. E is divisible by $X-Y$). On the other hand, the two variable L-function $L_p(\lambda^c\otimes\lambda)$ has a simple pole at the diagonal. Thus we know that $L_p(\lambda\otimes\varphi^c)(P,Q,P_0)$ does not have any singularity at the diagonal line. Since we can compute the value $L_p(\lambda\otimes\varphi^c)(P,Q,P_0)$ even for non-primitive λ_P, we can remove the condition (P3) in the evaluation formula in Theorem 7.4.2:

Corollary 1. *Let the notation be as in Theorem 10.4.1. Assume that* $G(Q)$ *is primitive and* $\chi_P^{-1}\psi_Q$ *is primitive. Then for the two variable L-function* $L_p(\lambda^c\otimes\varphi)$ *in Theorem 7.4.2, we have*

$$\begin{aligned} &S(P)L_p(\lambda^c\otimes\varphi)(P,Q) \\ &\quad = \lambda_p(T(N_0/L))\varphi_Q(T(L/N_0))L^{k-l}\frac{\Gamma(k-1)\Gamma(k-l)E'(P,Q)L(k-1,(\lambda_P{}^\circ)^c\otimes\varphi_Q)}{G(\chi_P^{-1}\psi_Q)(-2\pi i)^{k-l}(4\pi)^{k-1}(F(P)^\circ,F(P)^\circ)}, \end{aligned}$$

$$\textit{where}\quad E'(P,Q) = \begin{cases} 1 & \textit{if } \lambda_P \textit{ is primitive,} \\ \left(1-\dfrac{\lambda_P(T(p))^c}{\varphi_Q(T(p))p}\right)\left(1-\dfrac{\varphi_Q(T(p))}{\lambda_P(T(p))}\right) & \textit{otherwise.} \end{cases}$$

Proof. We know the following formula by (1) when λ_P is primitive and by Theorem 4.1 (combined with the same computation which yields (1)) when λ_P is not primitive:

$$\begin{aligned} S(P)L_p(\lambda\otimes\varphi^c)(P,Q,R) = (-1)^l\lambda_p(T(N_0))\lambda_P(T(J_0))^{-1}J_0{}^{(l/2)+r}N_0{}^{1-(k/2)}W(\lambda_p)^{-1}W(\varphi_Q) \\ \times\frac{\Gamma(r+1)\Gamma(l+r)E(l+r)L(l+r,\lambda_p\otimes\varphi_Q{}^c)}{(2\pi i)^{k+l+2r}\pi^{1-k}(F(P)^\circ,F(P)^\circ)}. \end{aligned}$$

Here note that $L(s,\lambda_P\otimes\varphi_Q{}^c) = E_1(s)L(s,\lambda_P{}^\circ\otimes\varphi_Q{}^c)$ for the primitive algebra homomorphism $\lambda_P{}^\circ$ associated with λ_P, where

$$E_1(s) = \begin{cases} 1 & \text{if } \lambda \text{ is primitive,} \\ (1-\lambda_P(T(p))^{-1}\varphi_Q{}^c(T(p))p^{k-1-s}) & \text{otherwise.} \end{cases}$$

We can also write, if λ is primitive,

$$\begin{aligned}(1-\lambda_P(T(p))^{-1}\varphi_Q{}^c(T(p))p^{k-1-s}) &= (1-\lambda_P(T(p))^{-1}p^{k-1}\varphi_Q(T(p))^c p^{1-l}p^{-1+l-s}) \\ &= (1-\lambda_P(T(p))^c\varphi_Q(T(p))^{-1}p^{-1+l-s}).\end{aligned}$$

Then by the functional equation, we see that

$$\begin{aligned}&(2\pi)^{-2k+1+l}\Gamma(k-l)\Gamma(k-1)L(k-1,(\lambda_P{}^\circ)^c\otimes\varphi_Q) \\ &= (-1)^l W(\lambda_P{}^c)W(\varphi_Q)G(\chi_P{}^{-1}\psi_Q)\lambda_P(T(L/J_0))L^{1-k}J_0{}^{l/2}\varphi_Q(T(L/N_0))^c N_0{}^{l-(k/2)} \\ &\qquad\times(2\pi)^{-l-1}\Gamma(l)L(l,\lambda_P{}^\circ\otimes\varphi_Q{}^c).\end{aligned}$$

This shows that

$$\begin{aligned}&S(P)L_p(\lambda\otimes\varphi^c)(P,Q,P_0) \\ &\quad = \lambda_P(T(N_0/L))\varphi_Q(T(L/N_0))L^{k-l}\frac{\Gamma(k-1)\Gamma(k-l)E(l)E_1(l)L(k-1,(\lambda_P{}^\circ)^c\otimes\varphi_Q)}{G(\chi_P{}^{-1}\psi_Q)(-2\pi i)^{k-l}(4\pi)^{k-1}(F(P)^\circ,F(P)^\circ)}.\end{aligned}$$

Then the result follows from Theorem 1.

§10.6. Concluding remarks

In this final section, we try to give some indications for further reading. It is certainly affected by prejudice on the author's part and not at all exhaustive. In this book, we have discussed the theory of the critical values for L-functions of two algebraic groups GL(1) and GL(2) defined over the base field $\mathbf{Q}$. About L-functions for more general algebraic groups and related subjects (especially "the theory of automorphic representations"), the reader may take a look at some articles in [CM] and [CT] and other articles and books quoted there. We have proved many algebraicity results for the critical values of L-functions in the sense of Deligne and Shimura [D]. The reader who is interested in such algebraicity results for L-functions of GL(2) and more general algebraic groups should consult Shimura's papers quoted in the references, especially [Sh11, Sh12]. We should also note a paper of Blasius [B] on this subject, which gives a proof of a conjecture of Deligne about CM periods and the critical values of Hecke L-functions of CM fields. For the philosophical and geometric background of such critical values and their transcendental factors, we refer to [D] and some expository articles in [RSS] and [CT]. There exists a largely conjectural theory (due to Beilinson and others)

for L-values at integers outside the critical range, although we have not touched anything about that in the text. The reader may consult [RSS] and some expository papers in [CT] for these topics. We have also proved the existence of many p-adic L-functions out of the algebraicity results of these L-values. Such theory for GL(1) and GL(2) is now available for a large number of base fields, in particular, totally real fields and fields containing CM fields. As for abelian p-adic L-functions for CM fields, the reader will find every detail in an excellent article of Katz [K5], and for such p-adic L-functions with auxiliary conductor outside p, an exposition is given in [HT2]. As for p-adic L-functions for GL(2), some generalization of the results in Chapters 7 and 10 can be found in my paper [H8] and [Pa]. We have only discussed the automorphic side of the theory of p-adic L-functions in the text. As for the geometric side (i.e., the theory of motivic p-adic L-functions), see the articles of Coates and Greenberg in [CT] and articles quoted there. After having constructed p-adic L-functions, it is natural to ask their meaning. A partial answer to this question is supplied by the so-called "main conjectures" of an appropriate Iwasawa theory. As for the original Iwasawa conjecture proved by Mazur and Wiles ([MW] and [Wi2]), see the books of Washington [Wa] and Lang [L]. For the motivic (or geometric) side of such theory, see [Mz2] and [CT], [RSS]. For the automorphic side, see [MzS], [MTT], [Wi2], [MT] and [HT1-3]. Finally, as for the Λ-adic Galois representation described in §7.5, generalizations of the result in §7.5 to totally real base fields can be found in [Wi1] and [H10]. The existence of such large Galois representations can be understood well from the perspective of deformation theory of Galois representations developed by Mazur [Mz3] (see also [HT3]).

Appendix: Summary of homology and cohomology theory

In this appendix, we give a summary of the theory of cohomology and homology on complex and real manifolds, in particular, Riemann surfaces in order to make the text self contained. However we will not give detailed proofs for all of the material presented here. For sheaf cohomology, we refer to [Bd] and for group cohomology to [Bw] and for singular cohomology to [HiW] for details.

Let X be a compact Riemann surface. We remove from X a set S of finitely many points and write Y for the resulting open Riemann surface. We fix a base point $y \in Y$ and let Γ be the fundamental group $\pi_y(Y)$. Let R be a commutative ring and for any left $R[\Gamma]$-module M, we define the cohomology group $H^i(\Gamma,M)$ $(= \mathrm{Ext}^i_{R[\Gamma]}(R,M))$ as follows. Let

$$F: \cdots \xrightarrow{\partial_3} F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} R \to 0$$

be an exact sequence of $R[\Gamma]$-modules, where on R, Γ acts trivially. When the F_i are all $R[\Gamma]$-free modules, we call F an $R[\Gamma]$-free (acyclic) resolution of R. Then by applying the contravariant functor $\mathrm{Hom}_{R[\Gamma]}(*,M)$, we have a complex

$$0 \to \mathrm{Hom}_{R[\Gamma]}(F_0, M) \xrightarrow{\partial_1^*} \mathrm{Hom}_{R[\Gamma]}(F_1, M) \xrightarrow{\partial_2^*} \mathrm{Hom}_{R[\Gamma]}(F_2, M) \to \cdots.$$

Then we define $H^0(\Gamma, M) = \mathrm{Ker}(\partial_1^*) \cong \mathrm{Hom}_{R[\Gamma]}(R, M) \cong M^\Gamma$ and

$$H^q(\Gamma, M) = \mathrm{Ker}(\partial_{q+1}^*)/\mathrm{Im}(\partial_q^*) \text{ for } q > 0.$$

The independence of the cohomology group of the choice of the free resolution follows from

Lemma A.1. *If we have another resolution (which may not be $R[\Gamma]$-free),*

$$F' : \cdots \xrightarrow{\partial'_3} F'_2 \xrightarrow{\partial'_2} F'_1 \xrightarrow{\partial'_1} F'_0 \xrightarrow{\varepsilon'} R \to 0,$$

then there exists a morphism $\varphi : F \to F'$ of complexes extending the identity on R and φ is unique up to homotopy equivalence.

Proof. We can define inductively an $R[\Gamma]$-homomorphism $\varphi_j : F_j \to F'_j$ as follows. For $j = 0$, taking a basis f_α of F_0 over $R[\Gamma]$ and picking $f'_\alpha \in F'_0$ so that $\varepsilon'(f'_\alpha) = \varepsilon(f_\alpha)$, we define $\varphi_0(f_\alpha) = f'_\alpha$ and extend this map to F_0 by $R[\Gamma]$-linearity. Then by definition, φ_0 satisfies $\varepsilon' \circ \varphi_0 = \varepsilon$. Suppose we have constructed $\varphi_0, \ldots, \varphi_j$ satisfying $\varphi_{i-1} \circ \partial_i = \partial'_i \circ \varphi_i$ for all $0 \le i \le j$. Then we see from $\varphi_{j-1} \circ \partial_j = \partial'_j \circ \varphi_j$ that $0 = \varphi_{j-1} \circ \partial_j \circ \partial_{j+1} = \partial'_j \circ \varphi_j \circ \partial_{j+1}$, and hence $\mathrm{Im}(\varphi_j \circ \partial_{j+1}) \subset \mathrm{Ker}(\partial'_j) = \mathrm{Im}(\partial'_{j+1})$. Choosing a basis x_α of F_{j+1} and picking $y_\alpha \in F'_{j+1}$ so that $\partial'_{j+1}(y_\alpha) = \varphi_j \circ \partial_{j+1}(x_\alpha)$, we define $\varphi_{j+1}(x_\alpha) = y_\alpha$ and extend it to F_{j+1} by $R[\Gamma]$-linearity. Then we see that $\varphi_j \circ \partial_{j+1} = \partial'_{j+1} \circ \varphi_{j+1}$. Now we have a morphism of the complex $\varphi = (\varphi_j)$. If there are two morphisms ψ and $\psi' : F \to F'$ extending the identity map on R, we now show the existence of an

$R[\Gamma]$-morphism $\delta_j : F_{j-1} \to F'_j$ such that $\psi'_j - \psi_j = \delta_j \circ \partial_j + \partial'_{j+1} \circ \delta_{j+1}$. Since $\varepsilon' \circ (\psi'_0 - \psi_0) = \mathrm{id} - \mathrm{id} = 0$,

$$\mathrm{Im}(\partial'_1) = \mathrm{Ker}(\varepsilon') \supset \mathrm{Im}(\psi'_0 - \psi_0).$$

Then picking any y_α such that $\psi'_0(f_\alpha) - \psi_0(f_\alpha) = \partial'_1(y_\alpha)$, we define $\delta_1(f_\alpha) = y_\alpha$ for a basis f_α of F_0 and extend it by $R[\Gamma]$-linearity to F_0. Thus $\psi'_0 - \psi_0 = \partial'_1 \circ \delta_1$. Suppose that we have δ_i for $i = 1, \ldots, j$. Then from $\psi'_{j-1} - \psi_{j-1} = \delta_{j-1} \circ \partial_{j-1} + \partial'_j \circ \delta_j$, we see that

$$\begin{aligned} \partial'_j \circ (\psi'_j - \psi_j - \delta_j \circ \partial_j) &= \partial'_j \circ \psi'_j - \partial'_j \circ \psi_j - \partial'_j \circ \delta_j \circ \partial_j \\ &= \partial'_j \circ \psi'_j - \partial'_j \circ \psi_j - (\psi'_{j-1} - \psi_{j-1} - \delta_{j-1} \circ \partial_{j-1}) \circ \partial_j = 0. \end{aligned}$$

This shows $\mathrm{Im}(\partial'_{j+1}) = \mathrm{Ker}(\partial'_j) \supset \mathrm{Im}(\psi'_j - \psi_j - \delta_j \circ \partial_j)$. Taking a basis x_α of F_j, we can find $y_\alpha \in F'_{j+1}$ such that $\partial'_{j+1}(y_\alpha) = (\psi'_j - \psi_j - \delta_j \circ \partial_j)(x_\alpha)$, and we define $\delta_{j+1}(x_\alpha) = y_\alpha$ and extend it to F_j by $R[\Gamma]$-linearity. Then we have

$$\psi'_j - \psi_j = \delta_j \circ \partial_j + \partial'_{j+1} \circ \delta_{j+1}.$$

Thus ψ' is homotopy equivalent to ψ.

Supposing F' is also $R[\Gamma]$-free and interchanging the role of F and F', we find a morphism $\varphi' : F' \to F$ extending the identity on R. Making $F = F'$ and replacing ψ by the identity map and ψ' by $\varphi \circ \varphi'$, we know that φ induces an isomorphism between the cohomology groups of F and F'. Thus the cohomology group is independent of the choice of the resolution.

We define a standard $R[\Gamma]$-free resolution of R as follows. Let F_q be the tensor product of $q+1$ copies of $R[\Gamma]$ over R and consider it as an $R[\Gamma]$-module via multiplication by $R[\Gamma]$ of the first factor. Then F_q is a free $R[\Gamma]$-module with a basis $\{[\gamma_1, \ldots, \gamma_q] = 1 \otimes \gamma_1 \otimes \cdots \otimes \gamma_q \mid (\gamma_1, \ldots, \gamma_q) \in \Gamma^q\}$. Then we define $\partial_q : F_q \to F_{q-1}$ by $\partial_1[\gamma] = \gamma - 1$ and for $q > 1$

$$\partial[\gamma_1, \ldots, \gamma_q] = \gamma_1[\gamma_2, \ldots, \gamma_q] + \sum_{j=1}^{q} (-1)^j [\gamma_1, \ldots, \gamma_j\gamma_{j+1}, \ldots, \gamma_q] + (-1)^q [\gamma_1, \ldots, \gamma_{q-1}]$$

and extend it $R[\Gamma]$-linearly on F_q. One can compute that $\partial_{q-1} \circ \partial_q = 0$. Defining $\varepsilon : F_0 = R[\Gamma] \to R$ by $\varepsilon(\sum_\gamma a_\gamma \gamma) = \sum_\gamma a_\gamma$, we see also that $\varepsilon \circ \partial_1 = 0$. Noting that $\gamma[\gamma_1, \ldots, \gamma_q]$ for $(\gamma, \gamma_1, \ldots, \gamma_q) \in \Gamma^{q+1}$ gives an R-basis of F_q, we define an R-linear map $D_q : F_q \to F_{q+1}$ by $D_q(\gamma[\gamma_2, \ldots, \gamma_q]) = [\gamma, \gamma_1, \ldots, \gamma_q]$. Then we see easily that

$$\partial_q D_{q-1} + D_q \partial_{q-1} = \mathrm{id} \ (q > 1) \text{ and } \partial_1 D_0 + \varepsilon = \mathrm{id}.$$

This shows that F is an $R[\Gamma]$-free acyclic resolution of R. Let $C^i = C^i(\Gamma, M)$ be the space of functions on Γ^i into M and put $C^0(\Gamma, M) = M$. Note that any $R[\Gamma]$-linear map from F_q to M is determined by its values on the standard basis $[\gamma_1, \ldots, \gamma_q]$ and hence $\mathrm{Hom}_{R[\Gamma]}(F_q, M) \cong C^q(\Gamma, M)$. Then the differential map

$\partial : C^i \to C^{i+1}$ induced by ∂ on F is given by $\partial u(\gamma) = (\gamma-1)u$ for $u \in M$ if $i = 0$, and if $i > 0$,

$$\partial u(\gamma_1, \ldots, \gamma_{i+1})$$
$$= \gamma_1 u(\gamma_2, \ldots, \gamma_{i+1}) + \sum_{j=1}^{i} (-1)^j u(\gamma_1, \ldots, \gamma_j\gamma_{j+1}, \ldots, \gamma_{i+1}) + (-1)^{i+1} u(\gamma_1, \ldots, \gamma_i).$$

Then $H^i(\Gamma,M) = Z^i(\Gamma,M)/B^i(\Gamma,M)$ where $Z^i(\Gamma,M) = \mathrm{Ker}(\partial : C^i \to C^{i+1})$ and $B^i(\Gamma,M) = \mathrm{Im}(\partial : C^{i-1} \to C^i)$. Thus we again get

$$H^0(\Gamma,M) = M^\Gamma = \{x \in M \mid \gamma x = x \text{ for all } \gamma \in \Gamma\}.$$

Any element in $Z^i(\Gamma,M)$ (resp. $B^i(\Gamma,M)$) is called an i-cocycle (resp. an i-coboundary). In particular a 1-cocycle $u : \Gamma \to M$ is a map satisfying $u(\gamma\delta) = u(\gamma) + \gamma u(\delta)$ for all $\gamma,\delta \in \Gamma$ and a 1-coboundary u is a map of the form $u(\gamma) = (\gamma-1)x$ for any $x \in M$ independent of γ. This shows that $u(1) = 0$, $u(\gamma^{-1}) = -\gamma^{-1}u(\gamma)$, $u(\gamma\delta\gamma^{-1}) = u(\gamma) + \gamma u(\delta) - \gamma\delta\gamma^{-1}u(\gamma)$ for cocycle u, and

$$H^1(\Gamma,M) = \mathrm{Hom}(\Gamma,M) = \mathrm{Hom}(\Gamma^{ab},M) \text{ if } \Gamma \text{ acts trivially on } M.$$

Let H be the universal covering space of Y and $\pi : H \to Y$ be the projection. For each $s \in S$, we consider $\pi_s \in \Gamma$ which corresponds to the path starting from y turning around the point s in the counterclockwise direction, and returning to y. Let $\Gamma_s = \{\pi_s^m \in \Gamma \mid m \in \mathbf{Z}\}$. We consider the set of all conjugates of π_s for all $s \in S$ in Γ, which will be denoted by P. We define the parabolic cohomology group by

$$H^1_P(\Gamma,M) = Z^1_P(\Gamma,M)/B^1(\Gamma,M), \quad H^2_P(\Gamma,M) = Z^2(\Gamma,M)/B^2_P(\Gamma,M),$$

where $Z^1_P(\Gamma,M) = \{u \in Z^1(\Gamma,M) \mid u(\pi) \in (\pi-1)M \text{ for all } \pi \in P\}$,

$$B^2_P(\Gamma,M) = \{\partial u \mid u \in C^1(\Gamma,M) \text{ with } u(\pi) \in (\pi-1)M \text{ for all } \pi \in P\}.$$

Now the restriction of each 1-cocycle u from Γ to $\Gamma_\pi = \{\pi^m \mid \pi \in \mathbf{Z}\}$ $(\pi \in P)$ yields a morphism $\mathrm{res}_\pi : H^1(\Gamma,M) \to H^1(\Gamma_\pi,M)$. Therefore if u is a 1-cocycle of Γ_π, then

$$u(\pi^r) = (1+\pi+\pi^2+ \cdots +\pi^{r-1})u(\pi) \text{ and}$$
$$u(\pi^{-r}) = -\pi^{-r}u(\pi^r) = -\pi^{-r}(1+\pi+\pi^2+ \cdots +\pi^{r-1})u(\pi) \text{ for } r > 0.$$

Thus the cocycle u is determined by the value $u(\pi)$ at the generator π. If $u(\pi) = (\pi-1)x$ for some $x \in M$, then

$$u(\pi^r) = (1+\pi+\pi^2+ \cdots +\pi^{r-1})(\pi-1)x = (\pi^r-1)x \text{ and}$$
$$u(\pi^{-r}) = -\pi^{-r}(1+\pi+\pi^2+ \cdots +\pi^{r-1})(\pi-1)x = (\pi^{-r}-1)x.$$

Thus $H^1(\Gamma_s,M) = M/(\pi-1)M$ and we now know the exact sequence

$$0 \to H^1_P(\Gamma,M) \to H^1(\Gamma,M) \to \prod_{\pi\in P} H^1(\Gamma_\pi,M),$$

where the last map is given by $\prod_\pi \mathrm{res}_\pi$. Actually, if $u(\pi) \in (\pi-1)M$, then for any $\gamma \in \Gamma$,

$$u(\gamma\pi\gamma^{-1}) = u(\gamma) + \gamma u(\pi) - \gamma\pi\gamma^{-1}u(\gamma) = u(\gamma) + \gamma(\pi-1)x - \gamma\pi\gamma^{-1}u(\gamma)$$
$$= (1-\gamma\pi\gamma^{-1})u(\gamma) + (\gamma\pi\gamma^{-1}-1)\gamma x \in (\gamma\pi\gamma^{-1}-1)M.$$

Thus, in fact, the conditions defining the parabolic cohomology group are finitely many, and we have

$$0 \to H^1_P(\Gamma,M) \to H^1(\Gamma,M) \to \oplus_{s\in\Gamma\backslash P} H^1(\Gamma_s,M).$$

We now consider another description of $H^1_P(\Gamma,M)$ by using a simplicial complex. Let Y_0 be an open Riemann surface obtained from X by excluding a small disk around each point $s \in S$ without overlaps. Let us take the pull back H_0 of Y_0 to H, which is a simply connected open subset of H. We make a simplicial complex K with the underlying space H_0 such that

(T1) Every element of Γ induces a simplicial map of K onto itself,

(T2) for each cusp $s \in S$, the boundary of the excluded disk is the image of a 1-chain t_s of K,

(T3) there exists a fundamental domain of Φ_0 in $\mathcal{H}_0$ whose closure consists of finitely many simplices in K.

We can construct such a complex by first taking a fundamental domain of Φ_0 and then making a finite simplicial complex $\mathcal{K}$ with the property (T2) of the closure of the fundamental domain and finally shifting this simplex to cover all H_0 by elements of Γ. We consider the chain complex (A_i,∂,a) over R constructed from K; thus, A_i is a free R-module generated by i-chains of K. We have an exact sequence (by the simply-connectedness of H_0)

$$0 \to A_2 \xrightarrow{\partial} A_1 \xrightarrow{\partial} A_0 \xrightarrow{a} R \to 0,$$

where ∂ is the usual boundary map and $a(\sum_z c(z)z) = \sum_z c(z) \in R$. We sometimes identify S with the set of generators $\{\pi_s\}$ of Γ_s for $s \in S$. We define $A_i(M) = \mathrm{Hom}_{R[\Gamma]}(A_i,M)$. Thus we have another complex

$$0 \to \mathrm{Hom}_{R[\Gamma]}(R,M) \xrightarrow{\partial} A_0(M) \xrightarrow{\partial} A_1(M) \xrightarrow{\partial} A_2(M) \to 0,$$

which may not be exact. Define

$$Z^i(K,M) = \mathrm{Ker}(\partial : A_i(M) \to A_{i+1}(M))$$

and

$$B^i(K,M) = \mathrm{im}(\partial : A_{i-1}(M) \to A_i(M)) \text{ and } H^i(K,M) = Z^i(K,M)/B^i(K,M).$$

We further define

$$Z^1_P(K,M) = \{u \in Z^1(K,M) \mid u(t_s) \in (\pi_s-1)M \text{ for all } s \in S\},$$
$$B^2_P(K,M) = \{\partial u \mid u(t_s) \in (\pi_s-1)M \text{ for all } s \in S\},$$
$$H^1_P(K,M) = Z^1_P(K,M)/B^1(K,M),\ H^2_P(K,M) = A_2(M)/B^2_P(K,M).$$

Proposition 1 (Shimura [Sh, Prop.8.1]). *There is a canonical isomorphism*

$$H^i_*(K,M) \cong H^i_*(\Gamma,M),$$

where "$*$" indicates P *or the usual cohomology.*

Proof. We shall give two proofs of this fact. By construction, $A : 0 \to A_2 \xrightarrow{\partial} A_1 \xrightarrow{\partial} A_0 \xrightarrow{a} R \to 0$ gives an $R[\Gamma]$-free resolution of R and thus we can compute $H^i(\Gamma,M)$ by using this resolution, which yields the above isomorphism for H^i. For each $\pi \in P$ with $\pi = \gamma\pi_s\gamma^{-1}$, $\gamma(t_s)$ is a simplex of K. Identify $\mathbf{R}$ with the universal covering space of the image of $\gamma(t_s)$ in Φ_0 and let $\iota_\pi : \mathbf{R} \to H$ be the induced map. Then the closure $\overline{\gamma(t_s)}$ gives a triangulation of a fundamental domain of $\Gamma_\pi\backslash\mathbf{R}$ in $\iota_\pi(\mathbf{R})$. Thus we can define $A_i(\pi)$ to be a free $R[\Gamma_\pi]$-module generated by i-simplices in $\overline{\gamma(t_s)}$ and we have an $R[\Gamma_\pi]$-free resolution:

$$A(\pi) : 0 \to A_1(\pi) \xrightarrow{\partial} A_0(\pi) \xrightarrow{a} R \to 0.$$

We have a natural inclusion $\iota_\pi : A(\pi) \to A$ induced by ι_π. Thus we have $\iota : \oplus_{\pi\in P}A(\pi) \to A$. We have a natural action of Γ on $\oplus_{\pi\in P}A_i(\pi)$ which just permutes its simplices. Writing $F = \{F_q\}$ (resp. $F(\pi) = \{F_q(\pi)\}$) for the standard $R[\Gamma]$-free (resp. $R[\Gamma_\pi]$-free) resolution of R, we have a commutative diagram,

$$\begin{array}{ccc} \oplus_{\pi\in P}A(\pi) & \to & \oplus_{\pi\in P}F(\pi) \\ \downarrow & & \downarrow \\ A & \longrightarrow & F, \end{array}$$

where the vertical maps are the natural inclusions and the horizontal maps are the maps extending the identity on R as constructed in the beginning of this section. Then applying the functor $\mathrm{Hom}_{R[\Gamma]}(*, M)$ to this diagram and computing the cohomology, we have another commutative diagram,

$$\begin{array}{ccc} H^1(\Gamma, M) & \to & \oplus_{s\in S}H^1(\Gamma_{\pi_s},M) \\ \downarrow & & \downarrow \\ H^1(K, M) & \to & \oplus_{s\in S}H^1(K(\pi_s),M), \end{array}$$

where $H^q(K(\pi),M)$ is the cohomology group of $\mathrm{Hom}_{R[\Gamma_\pi]}(A(\pi), M)$. Since the vertical arrows are isomorphisms and the parabolic cohomology group is defined by the kernel of the horizontal maps, we see that $H^1_P(K,M) \cong H^1_P(\Gamma,M)$.

We now give another (more explicit) proof given in [Sh, §8.1]. We compute the cohomology group $H^i(\Gamma,M)$ by the homogeneous chain complex; that is, we define (C_i,∂,a) as follows. For $i \geq 0$, C_i is the R-free module generated by all the ordered sets $(\gamma_0,\gamma_1, \ldots, \gamma_i)$ of i+1 elements of Γ, the differential $\partial : C_i \to C_{i-1}$ is defined by

$$\partial(\gamma_0, \gamma_1, \ldots, \gamma_i) = \sum_{j=0}^{i} (-1)^j(\gamma_0, \ldots, \gamma_{j-1},\gamma_{j+1}, \ldots, \gamma_i),$$

the augmentation a is given by $a(\Sigma_i r_i(\gamma_i)) = \Sigma_i r_i$ and Γ acts on C_i by $\gamma(\gamma_0, \gamma_1, \ldots, \gamma_i) = (\gamma\gamma_0, \gamma\gamma_1, \ldots, \gamma\gamma_i)$. Then

$$\cdots \to C_i \xrightarrow{\partial} C_{i-1} \xrightarrow{\partial} \cdots \xrightarrow{\partial} C_0 \xrightarrow{a} R \to 0$$

gives an $R[\Gamma]$-free resolution of R. In fact, we can easily check that this complex is isomorphic to the standard one F by the $R[\Gamma]$-linear isomorphism i given by $i((\gamma_0, \gamma_1, \ldots, \gamma_q)) = \gamma_0[\gamma_0^{-1}\gamma_1, \gamma_1^{-1}\gamma_2, \ldots, \gamma_{q-1}^{-1}\gamma_q]$. Thus by putting $C_i(M) = \mathrm{Hom}_{R[\Gamma]}(C_i,M)$, the cohomology group of the complex

$$0 \xrightarrow{\partial} C_0(M) \xrightarrow{\partial} C_1(M) \xrightarrow{\partial} \cdots$$

gives the cohomology group $H^i(\Gamma,M)$. As already remarked, we can define an isomorphism of complex $(C^i(M),\partial)$ to $(C_i(M),\partial)$ by defining $u' \in C_i(M)$ out of $u \in C^i(M)$ by

$$u'((\gamma_0, \gamma_1, \ldots, \gamma_i)) = \gamma_0 u(\gamma_0^{-1}\gamma_1, \gamma_1^{-1}\gamma_2, \ldots, (\gamma_{i-1})^{-1}\gamma_i).$$

The isomorphism of $H^i(\Gamma,M)$ onto $H^i(K,M)$ can be constructed as follows. We take a finite set of i-simplices S_i in K so that any simplex in K can be written uniquely as $\gamma(s)$ for $\gamma \in \Gamma$. In particular, we can include t_s in S_1 and q_s in S_0 if $\partial t_s = q_s - \pi_s(q_s)$. Then we define a map $f_0 : A_0 \to C_0$ by $f_0(\gamma(s)) = (\gamma)$ for each 0-simplex s in S_0, and then $a \circ f_0 = a$ on A_0. Thus $a(f_0(\partial s)) = 0$ for all $s \in S_1$. Because of the exactness of $C_1 \to C_0 \to R \to 0$, we can find $f_1(s)$ in A_1 so that $\partial f_1(s) = f_0(\partial s)$. We may assume $f_1(t_s) = (1,\pi_s)$. Then we define for any $\gamma \in \Gamma$, $f_1(\gamma s) = \gamma f_1(s)$ and extend this map R-linearly to the whole of A_1. Since we have defined f_1 so that if $\partial s = 0$ for $s \in K$, then $\partial f_1(s) = 0$ and we have $\partial f_1(\partial s) = 0$ for $s \in S_2$. Now we can find $f_2(s) \in C_2$ so that $\partial f_2(s) = f_1(\partial s)$ by the exactness of $C_2 \to C_1 \to C_0$. Then by the $R[\Gamma]$-linearity, we extend f_2 to an $R[\Gamma]$-linear map of A_2 into C_2. The morphism $f = (f_0,f_1,f_2)$ from (A_i,∂,a) to (C_i,∂,a) we have constructed satisfies

(i) $a \circ f_0 = a$, $f \circ \partial = \partial \circ f$ and $f \circ \gamma = \gamma \circ f$ for $\gamma \in \Gamma$,

(ii) $f_1(t_s) = (1,\pi_s)$ for $s \in S$.

By interchanging the role of (A_i,∂) and (C_i,∂), we can similarly construct $g : (C_i,\partial,a) \to (A_i,\partial,a)$ satisfying

(i') $a \circ g_0 = a$, $g \circ \partial = \partial \circ g$ and $g \circ \gamma = \gamma \circ g$ for $\gamma \in \Gamma$,

(ii') $g_1((1,\pi_s)) = t_s + (\pi_s - 1)b_s$ with 1-chain b_s such that $\partial b_s = q_0 - q_s$ for a fixed 0-simplex q_0 in S_0 independent of $s \in S$.

In fact, first fixing a 0-simplex q_0, we define $g_0((\gamma)) = \gamma(q_0)$. Then, by definition, $a \circ g_0 = a$. Thus we can find $g_1((\gamma,\delta))$ such that

$$\partial g_1((\gamma,\delta)) = g_0(\partial(\gamma,\delta)) = g_0((\delta)-(\gamma)) = \delta(q_0) - \gamma(q_0).$$

Then we can extend g_1 to the whole space C_1 by $R[\Gamma]$-linearity. In particular $\partial g_1((1,\pi_s)) = q_0 - \pi_s(q_0)$. Note that $\partial t_s = q_s - \pi_s(q_s)$. Thus by taking $b_s \in A_1$ so

that $\partial b_s = q_s - q_0$ (this is possible since $a(q_s - q_0) = 0$). Then we have $\partial(t_s + (\pi_s - 1)b_s) = q_0 - \pi_s(q_0)$, and we may define $g_1((1,\pi_s)) = t_s + (\pi_s - 1)b_s$, because $g_1((1,\pi_s))$ can be any element x in A_1 such that $\partial x = g_0(\partial(1,\pi_s))$. The maps f and g induce morphisms

$$f^* : H^i_P(\Gamma,M) \to H^i_P(K,M) \text{ and } g^* : H^i_P(K,M) \to H^i_P(\Gamma,M).$$

In fact, if $u : \Gamma \to M$ is a 1-cocycle, the corresponding homogeneous chain u' is given by $u'((1,\gamma)) = u(\gamma)$. In particular if $u(\pi_s) = (\pi_s - 1)x$, then $f^*u'(t_s) = u' \circ f(t_s) = u'((1,\pi_s)) = (\pi_s - 1)x$, and thus f^* takes parabolic cohomology classes to parabolic cohomology classes. Similarly, if $u \in \mathrm{Hom}_{R[\Gamma]}(A_1,M)$ with $u(t_s) \in (\pi_s - 1)M$, then

$$g^*u((1,\pi_s)) = u(t_s + (\pi_s - 1)b_s) \in (\pi_s - 1)M.$$

Since (C_i,∂) and (A_i,∂) are $R[\Gamma]$-free resolutions, and f and g induce the identity on R, $f \circ g$ and $g \circ f$ are homotopy equivalent to the identity. That is, there are $R[\Gamma]$-linear maps $U : C_i \to C_{i+1}$ and $V : A_i \to A_{i+1}$ such that $f \circ g - \mathrm{id} = \partial U + U\partial$ and $g \circ f - \mathrm{id} = \partial V + V\partial$. The map U can be defined as follows. Since $f(g((\gamma))) = (\gamma)$, we have $f_0 \circ g_0 = \mathrm{id}$, and we simply put $U_0 = U|_{C_0} = 0$. We have

$$\partial(f(g((1,\gamma))) - (1,\gamma)) = f(g(\partial(1,\gamma))) - \partial(1,\gamma) = 0$$

because $f_0 \circ g_0 = \mathrm{id}$. Thus we can find $U((1,\gamma))$ so that

$$\partial U((1,\gamma)) = f(g((1,\gamma))) - (1,\gamma).$$

Then we extend U by $R[\Gamma]$-linearity to C_1. By definition, we have $f_1 \circ g_1 - \mathrm{id} = \partial U + U\partial$. Similarly, we see that

$$\begin{aligned}&\partial(f_2(g_2((1,\gamma,\delta))) - (1,\gamma,\delta) - U(\partial(1,\gamma,\delta)))\\ &= f_1(g_1(\partial(1,\gamma,\delta))) - \partial(1,\gamma,\delta) - \partial U(\partial(1,\gamma,\delta)) = 0\end{aligned}$$

because $\partial U((\delta,\gamma)) = f(g((\delta,\gamma))) - (\delta,\gamma)$ and $\partial(1,\gamma,\delta) = (\gamma,\delta) - (1,\delta) + (1,\gamma)$. Thus we can find $U(1,\gamma,\delta)$ so that

$$\partial U(1,\gamma,\delta) = f_2(g_2((1,\gamma,\delta))) - (1,\gamma,\delta) - U(\partial(1,\gamma,\delta)).$$

Then we have U satisfying $f \circ g - \mathrm{id} = \partial U + U\partial$. In this way, we continue to define U inductively (actually, it is sufficient to have U defined as above because $H^i_P(\Gamma,M) = 0$ if $i > 2$). As for V, we proceed as follows. Since $a(g(f(s)) - s) = 0$ by definition, we can find $V : A_0 \to A_1$ so that

$$\partial V(s) = g(f(s)) - s \text{ for all } s \in A_0.$$

Then we consider $\partial(g_1(f_1(s)) - s - V(\partial s)) = g_0(f_0(\partial s)) - \partial s - \partial V(\partial s) = 0$ by the definition of V. Now we can define $V(s)$ for $s \in A_1$ so that $\partial V(s) = g_1(f_1(s)) - s - V(\partial s)$ and continue to define V inductively. Then for each 1-cocycle $u \in Z_i(M)$, we see that $u \circ f \circ g - u = u\partial U + uU\partial = \partial uU \in B_i(M)$. Thus $g^*f^* = \mathrm{id}$ and similarly $f^*g^* = \mathrm{id}$ on the cohomology groups. As already seen, they preserve parabolic classes and hence induce isomorphisms on parabolic cohomology groups.

Let S_0 be a subset of S and T be the disjoint union of the image of t_s in Y for $s \in S_0$. Let K_T be the subcomplex of K generated by all translations of t_s by Γ. We put $K^T = K/K_T$. Consider the free R-module A_i^T (resp. $A_{T,i}$) generated by the i-simplex of K^T (resp. K_T). Then we write $H^q_{S_0}(\Gamma, M)$ for the cohomology group of $\mathrm{Hom}_{R[\Gamma]}(A_i^T, M)$. When $S = S_0$, we write $H^q_c(\Gamma, M)$ for $H^q_S(\Gamma, M)$.

Proposition 2 (Boundary exact sequence). *We have a long exact sequence*

$$0 \to H^0_{S_0}(\Gamma, M) \to H^0(\Gamma, M) \to \oplus_{s \in S_0} H^0(\Gamma_{\pi_s}, M) \to H^1_{S_0}(\Gamma, M)$$
$$\to H^1(\Gamma, M) \to \oplus_{s \in S_0} H^1(\Gamma_{\pi_s}, M) \to H^2_{S_0}(\Gamma, M) \to H^2(\Gamma, M) \to 0.$$

In particular, $H^0_{S_0}(\Gamma, M) = 0$ *if* $S_0 \neq \emptyset$, *and* $H^2_c(\Gamma, M) \cong H^2_P(\Gamma, M)$.

Proof. We need the following well known fact:

(1) If $0 \to A \to B \to C \to 0$ is an exact sequence of complexes, then we have a long exact sequence

$$\cdots \to H^q(A) \to H^q(B) \to H^q(C) \to H^{q+1}(A) \to H^{q+1}(B) \to \cdots.$$

This is checked by applying the snake lemma to the commutative diagram:

$$\begin{array}{ccccccc} A_p/\partial_{p-1}(A_{p-1}) & \to & B_p/\partial_{p-1}(B_{p-1}) & \to & C_p/\partial_{p-1}(C_{p-1}) & \to 0 & \text{(exact)} \\ \downarrow\partial & & \downarrow\partial & & \downarrow\partial & & \\ 0 \to \mathrm{Ker}(\partial_{p+1}|_{A_{p+1}}) & \to & \mathrm{Ker}(\partial_{p+1}|_{B_{p+1}}) & \to & \mathrm{Ker}(\partial_{p+1}|_{C_{p+1}}) & & \text{(exact).} \end{array}$$

We have an exact sequence $0 \to A_T \to A \to A^T \to 0$. Since A^T is also $R[\Gamma]$-free, this sequence splits as $R[\Gamma]$-module, and we have another exact sequence

$$0 \to \mathrm{Hom}_{R[\Gamma]}(A^T, M) \to \mathrm{Hom}_{R[\Gamma]}(A, M) \to \mathrm{Hom}_{R[\Gamma]}(A_T, M) \to 0.$$

Then applying (1), we get the long exact sequence. The vanishing of $H^0_{S_0}(\Gamma, M)$ (when $S_0 \neq \emptyset$) follows from the injectivity of

$$M^\Gamma = H^0(\Gamma, M) \to \oplus_{s \in S_0} H^0(\Gamma_{\pi_s}, M) = \oplus_{s \in S_0} M^{\Gamma_{\pi s}}.$$

The last assertion follows directly from the definition of $H^2_P(\Gamma, M)$.

We now define the notion of sheaves on a smooth manifold Z of real dimension n. Here the word "smooth" means that Z is of C^∞-class. Let $O(Z)$ be the category of all open subsets of Z; that is, objects of $O(Z)$ are open subsets of Z and $\mathrm{Hom}_{O(Z)}(U,V)$ is either the inclusion map $U \to V$ or empty according as U is contained in V or not. A presheaf F on Z is a contravariant functor on $O(Z)$ having values in the category of abelian groups. Thus for each open set U in Z, $F(U)$ is an abelian group and if $U \supset V$, we have a natural restriction map $\mathrm{res}_{U/V} : F(U) \to F(V)$ satisfying $\mathrm{res}_{U/U} = \mathrm{id}$ and $\mathrm{res}_{V/W} \circ \mathrm{res}_{U/V} = \mathrm{res}_{U/W}$ if $U \supset V \supset W$. A presheaf is called a sheaf if the following axiom is satisfied:

(S) If for a given open covering $U = \bigcup_i V_i$, $s_i \in F(V_i)$ satisfies $\mathrm{res}_{V_i/V_i \cap V_j}(s_i) = \mathrm{res}_{V_j/V_i \cap V_j}(s_j)$ for all i and j with $V_i \cap V_j \neq \emptyset$, we have a unique element $s \in F(U)$ such that $\mathrm{res}_{U/V_i}(s) = s_i$.

If $U = \bigcup_{i=1}^{r} V_i$ is an open covering, adding $V_0 = U$ to this covering, the condition (S) implies that $s \in F(U)$ is uniquely determined by $\mathrm{res}_{U/V_i}(s)$ for all $i = 1, \ldots, r$. A morphism ϕ of a sheaf F into another G is defined to be a morphism of contravariant functors. That is, for each open set U, we have a morphism $\phi(U) : F(U) \to G(U)$, and for every open subset V of U, the following diagram is commutative:

$$\begin{array}{ccc} F(U) & \xrightarrow{\phi(U)} & G(U) \\ \downarrow \mathrm{res}_{U/V} & & \downarrow \mathrm{res}_{U/V} \\ F(V) & \xrightarrow[\phi(V)]{} & G(V). \end{array}$$

If U is an open subset of Z, then $O(U)$ is a subcategory of $O(Z)$. Thus we can restrict the sheaf to $O(U)$. The restriction of F to U will be written as $F|_U$.

If $\pi : T \to Z$ is a surjective morphism of smooth manifolds, we can define a sheaf associated with T by

$$T(U) = \{s : U \to T \mid s \text{ is continuous and } \pi \circ s = \mathrm{id} \text{ on } U\}.$$

It is easy to verify the condition (S) for the usual restriction map $\mathrm{res}_{U/V}(s) = s|_V$ if $U \supset V$. Let A be any abelian group with the discrete topology. We consider $T = Z \times A$ with the product topology. Then if an open set U in Z is connected, any continuous section on U of $\pi : T \to Z$ is a constant function, and hence $T(U) = A$. This sheaf T is called the constant sheaf A. A sheaf on Z is called locally constant if for each point $z \in Z$, we can find an open neighborhood U of z such that $F|_U$ is a constant sheaf. Returning to the situation in Lemma 1, we can give plenty of examples of such locally constant sheaves. For any Γ-module M, we can define $T = \Gamma \backslash H \times M$ letting Γ act on $H \times M$ by $\gamma(z,m) = (\gamma(z), \gamma m)$. We put the discrete topology on M and put the quotient topology on T. Then the projection $\pi : T \to Y = \Gamma \backslash H$ gives a sheaf T, which we write $\underline{M}$. For a small open set U_0 of H such that $\gamma U_0 \cap U_0 \neq \emptyset \Leftrightarrow \gamma = 1$, writing U for the image of U_0 in Y, we see easily that $\pi^{-1}(U) = U \times M$ and hence $\underline{M}|_U$ is a constant sheaf M. For every point $z \in Y$, we can always find such a neighborhood U, and hence $\underline{M}$ is a locally constant sheaf.

Now we introduce the Čech cohomology group of a presheaf F. For an open covering $\mathcal{U} = \{U_\alpha\}_{\alpha \in I}$: $Z = \bigcup_{\alpha \in I} U_\alpha$ and $\alpha = (\alpha_0, \ldots, \alpha_r) \in I^{r+1}$, we write

$U_\alpha = U_{\alpha_0}\cap\cdots\cap U_{\alpha_r}$. Then we define $C^r(\mathcal{U};F)$ to be a module of functions $s : I^{r+1} \to \coprod_{\alpha\in I}F(U_\alpha)$ satisfying $s(\alpha) \in F(U_\alpha)$. Then we define

$$\partial_r : C^r(\mathcal{U};F) \to C^{r+1}(\mathcal{U};F)$$

$$\text{by, for } \alpha = (\alpha_0,\ldots,\alpha_{r+1}) \in I^{r+2},\ (\partial s)(\alpha) = \sum_{j=0}^{r+1} (-1)^j \mathrm{res}_{U_{\alpha(j)}/U_\alpha}(s(\alpha^{(j)})),$$

where $\alpha^{(j)} = \{\alpha_i \in \alpha \mid i \neq j\}$ and we understand $F(\varnothing) = 0$. For example,

$$\partial(s)_{\alpha\beta\gamma} = s_{\beta\gamma}|U_{\alpha\beta\gamma} - s_{\alpha\gamma}|U_{\alpha\beta\gamma} + s_{\alpha\beta}|U_{\alpha\beta\gamma} \quad \text{when } r = 1,$$

and when $\partial(s)_{\alpha\beta} = s_\beta|U_{\alpha\beta} - s_\alpha|U_{\alpha\beta}$,

$$\partial(\partial s)_{\alpha\beta\gamma} = \partial s_{\beta\gamma}|U_{\alpha\beta\gamma} - \partial s_{\alpha\gamma}|U_{\alpha\beta\gamma} + \partial s_{\alpha\beta}|U_{\alpha\beta\gamma}$$

$$= s_\gamma|U_{\alpha\beta\gamma} - s_\beta|U_{\alpha\beta\gamma} - \{s_\gamma|U_{\alpha\beta\gamma} - s_\alpha|U_{\alpha\beta\gamma}\} + s_\beta|U_{\alpha\beta\gamma} - s_\alpha|U_{\alpha\beta\gamma} = 0.$$

This shows $\partial_2\circ\partial_1 = 0$. We can similarly check $\partial_{r+1}\circ\partial_r = 0$ for general r. We write the cohomology group $H^q(C(\mathcal{U};F))$ as $\check{H}^q(Z;\mathcal{U};F)$:

$$\check{H}^q(Z;\mathcal{U};F) = \mathrm{Ker}(\partial_r)/\mathrm{Im}(\partial_{r-1}).$$

Another open covering $\mathcal{V} = \{V_\beta\}_{\beta\in J}$ is called a refinement of $\mathcal{U}$ if there exists a map $\rho : J \to I$ such that $U_{\rho(j)} \supset V_j$ for all j. In this case, we write $\mathcal{U} \geq \mathcal{V}$. We define $\mathcal{U}$ and $\mathcal{V}$ to be equivalent if $\mathcal{U} \geq \mathcal{V}$ and $\mathcal{V} \geq \mathcal{U}$. Let $\mathcal{C}$ be the set of equivalence classes of all coverings of Z ($\mathcal{C}$ is a set because the set of all coverings is a subset of the power set of the power set of Z). The partial ordering "$\geq$" induces a filtered ordering on $\mathcal{C}$. In fact, if $\mathcal{U}$ and $\mathcal{V}$ are two coverings, then $\mathcal{U}\times\mathcal{V} = \{U_i\cap V_j\}_{(i,j)\in I\times J}$ is a common refinement. Suppose $\mathcal{V} = \{V_\beta\}_{\beta\in J}$ is a refinement of $\mathcal{U}$ with the map $\rho : J \to I$. Then ρ induces a map $\rho^{r+1} : J^{r+1} \to I^{r+1}$. For each $s \in C^r(\mathcal{U};F)$, we can define $\rho^*s \in C^r(\mathcal{V};F)$ as follows:

$$\rho^*s(\beta) = \mathrm{res}_{U_{\rho^{r+1}(\beta)}/V_\beta} s(\rho^{r+1}(\beta)).$$

It is obvious that ρ^* commutes with the differentials and therefore induces a morphism of cohomology groups:

$$\rho^* : \check{H}^q(Z;\mathcal{U};F) \to \check{H}^q(Z;\mathcal{V};F).$$

Lemma 2. *The morphism* ρ^* *does not depend on the choice of the map* $\rho: J \to I$.

Sketch of a proof. Let ι be another map from J into I having the same property as ρ. We show that ρ^* and ι^* are homotopy equivalent. Let $\delta : C^q(\mathcal{U};F) \to C^{q+1}(\mathcal{V};F)$ be a map defined by

$$(\delta s)(\beta) = \sum_{j=0}^{q}(-1)^j s(\rho(\beta_0),\rho(\beta_1),\ldots,\rho(\beta_j),\iota(\beta_j),\ldots,\iota(\beta_q))$$

Then by a direct computation, we get $\iota - \rho = \delta\partial + \partial\delta$.

By Lemma 2, if $\mathcal{U} \geq \mathcal{V}$, we have the canonical homomorphism

$$\iota(\mathcal{U},\mathcal{V}) : \check{H}^q(Z;\mathcal{U};F) \to \check{H}^q(Z;\mathcal{V};F).$$

If $\mathcal{U}$ and $\mathcal{V}$ are equivalent, by the uniqueness $\iota(\mathcal{U},\mathcal{V})\circ\iota(\mathcal{V},\mathcal{U})$ and $\iota(\mathcal{V},\mathcal{U})\circ\iota(\mathcal{U},\mathcal{V})$ have to be the identity, because $\iota(\mathcal{U},\mathcal{U})$ is the identity. Thus $\check{H}^q(Z;\mathcal{U};F)$ is determined by the class of $\mathcal{U}$ in $\mathcal{C}$. Similarly, if $\mathcal{U}\geq\mathcal{V}\geq\mathcal{W}$, then $\iota(\mathcal{V},\mathcal{W})\circ\iota(\mathcal{U},\mathcal{V}) = \iota(\mathcal{U},\mathcal{W})$. Since $\mathcal{C}$ is filtered, we have an injective system $\{\check{H}^q(Z;\mathcal{U};F),\iota(\mathcal{U},\mathcal{V})\}_{\mathcal{U},\mathcal{V}\in\mathcal{C}}$. We then define

$$\check{H}^q(Z,F) = \varinjlim_{\mathcal{U}} \check{H}^q(Z;\mathcal{U};F).$$

Giving a 0-cocycle s in $C^0(\mathcal{U};F)$ is tantamount to giving $s_i \in F(U_i)$ for each $i \in I$ such that $\mathrm{res}_{U_i/U_{ij}}(s_i) = \mathrm{res}_{U_j/U_{ij}}(s_j)$. Thus if F is a sheaf, we have a unique $s \in F(Z)$ such that $\mathrm{res}_{Z/U_i}(s) = s_i$. This shows

(2) $$\check{H}^0(Z;\mathcal{U};F) = F(Z) \text{ if } F \text{ is a sheaf.}$$

Proposition 3. *Suppose that* Z *is simply connected and* $\mathcal{U} = \{U_i\}_{i\in I}$ *is a covering of* Z *with a countable* I *such that (*)* U_α *for each* $\alpha \in I^{r+1}$ *is either empty or simply connected for all* $r \in \mathbf{N}$. *If* $\mathrm{res}_{U/V}$ *is surjective for all* $V \subset U$ *with* V *connected (this assumption holds if* F *is constant), then* $\check{H}^q(Z;\mathcal{U};F) = 0$ *if* $q > 0$.

Proof. We fix $\beta \in I$ and write $U = U_\beta$. We consider $F|_U$ and $\mathcal{U}|_U = \{U\cap U_\alpha \mid \alpha\in I\}$. Then we can define, for the fixed $\beta \in I$

$\delta_r : C^{r+1}(\mathcal{U}|_F;F|_U) \to C^r(\mathcal{U}|_U;F|_U)$ by $\delta s(\alpha) = s(\beta\cup\alpha) \in F(U\cap U_\alpha) = F(U_\alpha)$.

Then $\partial\delta s(\alpha) = \sum_{j=0}^r(-1)^j \mathrm{res}_{U_{\alpha(j)}/U_\alpha}\delta s(\alpha^{(j)}) = \sum_{j=0}^r(-1)^j \mathrm{res}_{U_{\alpha(j)}/U_\alpha}(s(\beta\cup\alpha^{(j)}))$ and $\delta\partial s(\alpha) = \partial s(\beta\cup\alpha) = s(\alpha)-\sum_{j=0}^r(-1)^j \mathrm{res}_{U_{\alpha(j)}/U_\alpha}s(\beta\cup\alpha^{(j)}) = s(\alpha)-\partial\delta s(\alpha)$. Thus $\mathrm{id} = \delta\partial+\partial\delta$. So if s is an r-cocycle $(r > 0)$ in $C^{r+1}(\mathcal{U};F)$, we can find t such that $s|_U = \partial t$. The cochain t is uniquely determined by s modulo $\partial C^r(\mathcal{U}|_U;F|_U)$. By the same argument applied to $U' = U_\beta$ with $U\cap U' \neq \emptyset$, we find t' so that $\partial t' = s|_{U'}$ on U'. Modifying t' by an element in $\partial C^r(\mathcal{U}|_U;F|_U)$, we may assume that $\mathrm{res}_{U/U\cap U'}t = \mathrm{res}_{U'/U\cap U'}t'$, because the restriction map $\partial C^r(\mathcal{U}|_U;F|_U) \to \partial C^r(\mathcal{U}|_{U\cap U'};F|_{U\cap U'})$ is surjective. Thus t extends to $U\cup U'$. By continuing this process, by the simple connectedness of Z, we can extend t to $\bigcup_i U_i = Z$. This shows the result.

For a presheaf F, we study the presheaf $F^\# : U \mapsto \check{H}^0(U,F|_U)$. The restriction map $\mathrm{res}_{U/V}$ of F induces that of $F^\#$. By (2), if F is a sheaf, then $F^\# = F$. Let $\mathcal{U} = \{U_i\}_{i\in I}$ be an open covering of U. To each $s \in F(U)$, assigning the 0-cocycle $s(i) = \mathrm{res}_{U/U_i}(s) \in C^0(\mathcal{U};F)$, we have a cohomology class $[s]$ in $F^\#(U)$. Thus we have a natural morphism of presheaves $\iota : F \to F^\#$. If $s \in F^\#(U)$ and if

$\mathrm{res}_{U/U_i}(s) = 0$ for all i, s itself vanishes because the image of s in $\check{H}^0(U;\mathcal{U};F|_U)$ is 0. Thus $s \in F^{\#}(U)$ is determined by its local data. Let s_i for all $i \in I$ be sections in $F^{\#}(U_i)$ satisfying $\mathrm{res}_{U_i/U_{ij}}(s_i) = \mathrm{res}_{U_j/U_{ij}}(s_j)$ for all i and j. Then we take a sufficiently fine open covering $\mathcal{U}_i = \{U^i_k\}_{k\in J}$ of U_i and choose a 0-cocycle $s^i \in C^0(\mathcal{U}_i;F|_{U_i})$ representing s_i. Then writing $\rho : I\times J \to I$ for the projection, we regard $\mathcal{V} = \{U^i_k\}_{(i,k)\in I\times J}$ as a refinement of $\mathcal{U}$. Then the cochain: $(i,k) \mapsto s^i(k)$ is a 0-cocycle in $C^0(\mathcal{V};F|_U)$. Writing s for the cohomology class of this cocycle, we have plainly $s_i = \mathrm{res}_{U/U_i}(s)$ for all $i \in I$. Thus $F^{\#}$ is a sheaf. If $\phi : F \to G$ is a morphism of presheaves and if G is a sheaf, ϕ induces $\phi_* : F^{\#} \to G^{\#} = G$. It is obvious that $\phi = \phi_* \circ \iota$ and ϕ_* is characterized by this property because any $s \in F^{\#}(U)$ can be described by local sections. Thus $F^{\#}$ satisfies the following universal property:

(3) for each morphism ϕ of presheaves from F into a sheaf G, there exists a unique $\phi_* : F^{\#} \to G$ satisfying $\phi = \phi_* \circ \iota$.

By this universality, $F^{\#}$ is uniquely determined by F (up to isomorphisms). We call $F^{\#}$ the sheaf generated by F.

We say a sheaf (resp. a presheaf) is a sheaf (resp. a presheaf) of *R-modules* for a commutative ring R if $F(U)$ is an R-module for every open set U and $\mathrm{res}_{U/V} : F(U) \to F(V)$ is an R-linear map if $U \supset V$. For any presheaf F of R-modules, the sheaf $F^{\#}$ generated by F is naturally a sheaf of R-modules. If F and G are two sheaves of R-modules, then we write $F\otimes_R G$ for the sheaf generated by the presheaf: $U \mapsto F(U)\otimes_R G(U)$. The map $(x,y) \mapsto x\otimes y$ composed with the canonical map ι is again denoted by the same symbol: $(x,y) \mapsto x\otimes y$ for $(x,y) \in F(U)\times G(U)$. It is easy to verify the following universal property (see the description after Corollary 1.1.1):

(4) If there is a morphism of sheaves of R-modules $\phi : F\times G \to H$ such that $\phi(U)$ is R-bilinear and $\phi(U)(x,\lambda y) = \phi(U)(\lambda x,y)$ for all $\lambda \in R$, then there exists a unique morphism of sheaves of R-modules $\phi_* : F\otimes_R G \to H$ such that $\phi_*(U)(x\otimes y) = \phi(x,y)$.

If F is a subsheaf of a sheaf G, we can define a presheaf $U \mapsto F(U)\backslash G(U)$. We write $F\backslash G$ for the sheaf generated by the above presheaf. We have a natural morphism $G \to G/H$. On the other hand, it is plain from the sheaf axiom (S) that, if $\varphi : F \to G$ is a morphism of sheaves,

$$\mathrm{Ker}(\varphi) : U \to \mathrm{Ker}(\varphi(U)) \text{ is again a sheaf.}$$

A sequence of morphisms of sheaves $F \xrightarrow{\alpha} G \xrightarrow{\beta} H$ is called *exact* if $\mathrm{Im}(\alpha)^{\#} = \mathrm{Ker}(\beta)$, where $\mathrm{Im}(\alpha)^{\#}$ is the sheaf generated by the presheaf $U \mapsto \mathrm{Im}(\alpha(U))$. For any presheaf F and $x \in Z$, we define the stalk F_x at x by $F_x = \varinjlim_{x \in U} F(U)$, where the transition map is given by $\mathrm{res}_{U/V}$, and the order on the set of open sets containing x is given by the inclusion relation. Then it is easy to check from the definition that

(5a) $F^{\#}{}_x = F_x$ for all $x \in Z$, and $F \to G \to H$ is exact as sheaves if and only if $\prod_{x \in Z} F_x \to \prod_{x \in Z} G_x \to \prod_{x \in Z} H_x$ is exact as abelian groups.

In other words,

(5b) if $\alpha : F \to G$ is a surjective morphism of sheaves, then for each $g \in G(Z)$, there exists an open covering $\{U_i\}_{i \in I}$ with $f_i \in F(U_i)$ such that $\alpha(f_i) = \mathrm{res}_{Z/U_i}(g)$ for all i.

For each section $f \in F(U)$, we define $\mathrm{Supp}(f)$ to be the closed set in U defined by $\{x \in U \mid f_x \neq 0\}$, where f_x is the natural image of f in F_x.

Now we return to the original situation: X is a compact Riemann surface, $Y = X\text{-}S$ and Γ is the fundamental group of Y. Let M be a Γ-module and $\underline{M}$ denote the locally constant sheaf on Y associated to M.

Theorem 1. *Let* $\mathcal{U} = \{U_i\}_{i \in I}$ *be a covering of* Y *with a countable index set* I *such that (i) for each* U_i, *there exists a simply connected open subset* U_i^* *in* H *such that the projection* $\pi : H \to \Gamma \backslash H$ *induces an isomorphism* $U_i^* \cong U_i$, *and (ii) for all* r, $U_\alpha^* = U_{\alpha_0}^* \cap \cdots \cap U_{\alpha_r}^*$ *is either simply connected or empty for all* $\alpha \in I^{r+1}$. *Then there is a canonical isomorphism* $H^q(\Gamma, M) \cong \check{H}^q(Y; \mathcal{U}; \underline{M})$.

Proof. We consider the open covering $\mathcal{U}^* = \{\gamma(U_i^*)\}_{\gamma \in \Gamma, i \in I}$ of H. By (i) and (ii), if $U_\alpha \neq \varnothing$ for $\alpha = (\alpha_0, \ldots, \alpha_{r+1}) \in I^{r+1}$, then there exists a unique $(\gamma_0, \ldots, \gamma_r) \in \Gamma^{r+1}$ so that $U_\alpha^* = \gamma_0 U_{\alpha_0}^* \cap \cdots \cap \gamma_r U_{\alpha_r}^* \neq \varnothing$. We put $U_\alpha^* = \varnothing$ if $U_\alpha = \varnothing$. Then γU_α^* for $\gamma \in \Gamma$ is either empty or simply connected. Thus if $\gamma U_\alpha^* \neq \varnothing$, then $F(\gamma U_\alpha^*) = M$. We consider the subset I_r in I^{r+1} consisting of α with non-empty U_α. Let $R[\Gamma][I_r]$ be the formal free module generated over $R[\Gamma]$ by elements of I_r, and write $[\gamma, \alpha]$ for the element (γ, α) ($\gamma \in \Gamma$ and $\alpha \in I_r$) in $R[\Gamma][I_r]$. Then we see that $\{[\gamma, \alpha]\}_{\gamma \in \Gamma, \alpha \in I_r}$ is a basis of $R[\Gamma][I_r]$ over R, and we have

$$\mathrm{Hom}_R(R[\Gamma][I_r], M) \cong C^r(\mathcal{U}^*; M) \text{ by } \phi \mapsto s$$

where $s(\gamma, \alpha) = \phi([\gamma, \alpha]) \in F(\gamma U_\alpha^*) = M$. By this isomorphism, $C^r(\mathcal{U}^*; \underline{M})$ has a natural structure as $R[\Gamma]$-module. We define an R-linear map

$$\partial_r : R[\Gamma][I_r] \to R[\Gamma][I_{r-1}] \text{ by } \partial[\gamma,\alpha] = \sum_{j=0}^{r} (-1)^j[\gamma,\alpha^{(j)}],$$

where $\alpha^{(j)} = (\alpha_0,\ldots,\alpha_{j-1},\alpha_{j+1},\ldots,\alpha_r)$. Obviously ∂_r is $R[\Gamma]$-linear. Thus we have a complex

$$R[\Gamma][I] : \cdots \xrightarrow{\partial_3} R[\Gamma][I_2] \xrightarrow{\partial_2} R[\Gamma][I_1] \xrightarrow{\partial_1} R[\Gamma][I_0] \xrightarrow{\varepsilon} R \to 0,$$

where

$$\varepsilon(\sum_{(\gamma,\alpha)} a_{(\gamma,\alpha)}[\gamma,\alpha]) = \sum_{[\gamma,\alpha]} a_{[\gamma,\alpha]}.$$

Then $C(\mathcal{U}^*;\underline{M}) = \mathrm{Hom}_R(R[\Gamma][I], M)$ as complexes. Since H is simply connected, by Proposition 3, $C(\mathcal{U}^*;\underline{M})$ is exact and thus $R[\Gamma][I]$ is an $R[\Gamma]$-free resolution of R. It is obvious that

$$\mathrm{Hom}_{R[\Gamma]}(R[\Gamma][U], M) \cong C(\mathcal{U};\underline{M}) \text{ as complexes.}$$

Thus by Lemma 1, we get the desired isomorphism.

Since we can take a simply connected polygon as the fundamental domain of Y, for any covering $\mathcal{V}$ of Y, we can find a refinement $\mathcal{U}$ satisfying the assumption of Theorem 1. Thus we see the following

Corollary 1. *Under the same notation as in Theorem 1, we have a canonical isomorphism* $H^q(\Gamma,M) \cong \breve{H}^q(Y,\underline{M})$.

Exercise 1. (i) Let U be an open subset in Z and suppose $U = \bigcup_{i=1}^{h} U_i$ is a disjoint union of connected open sets U_i. Show that $\breve{H}^0(U,\mathbf{C}) \cong \mathbf{C}^h$.
(ii) Show $\breve{H}^r(\mathbf{R},\mathbf{C}) = 0$ if $r > 0$.
(iii) Show $\breve{H}^r(\mathbf{R}/\mathbf{Z},\mathbf{C}) = \begin{cases} \mathbf{C} & \text{if } r = 0 \text{ and } 1, \\ 0 & \text{otherwise.} \end{cases}$

Let F be a locally constant sheaf on Z having values in the category of finite dimensional vector spaces over $\mathbf{C}$. We consider the sheaf $\mathcal{A}_F{}^r$ (on Z) of smooth differential forms of degree r with values in F. Thus $\mathcal{A}_F{}^r(U)$ is the space of C^∞-r-forms defined on the open set U with values in $F(U)$; so, $\mathcal{A}_F{}^r = \mathcal{A}_C{}^r \otimes_C F$ in the sense of the tensor product of sheaves (4). Since the exterior derivation d is defined locally on $\mathcal{A}_C{}^r$ and locally $\mathcal{A}_F{}^r(U) = \mathcal{A}_C{}^r \otimes F(U)$, d is well defined on $\mathcal{A}_F{}^r$ and we have a resolution of the sheaf F:

$$\mathcal{A}_F : 0 \to F \to \mathcal{A}_F{}^0 \xrightarrow{d} \mathcal{A}_F{}^1 \xrightarrow{d} \mathcal{A}_F{}^2 \xrightarrow{d} \cdots.$$

The above sequence is exact in the sense of sheaves (5a,b) by Poincaré's lemma, which tells us the validity of (5b) for $d_q : \mathcal{A}_F{}^q \to Z_{q+1} = \mathrm{Ker}(d_{q+1})$ on every simply connected open set. Let $\mathcal{U} = \{U_i\}_{i\in I}$ be an open covering of Z. Let $\{\phi_j\}_{j\in J}$ be a partition of unity subordinate to the covering $\mathcal{U}$ Thus there is a map $\sigma : J \to I$ such that ϕ_j is a smooth function on Z with $U_{\sigma(j)} \supset \mathrm{Supp}(\phi_j)$, all but a finite number of ϕ_j vanish at each point $x \in Z$ and $\sum_j \phi_j(x) = 1$ for all

$x \in Z$. Such a partition of unity is known to exist. Then we put for all cocycles $s \in C^r(\mathcal{U};\mathcal{A}_F{}^p)$, $s'(\beta) = \sum_j \phi_j s(\sigma(j)\cup\beta)$ for $\beta \in \Gamma^r$. Then

$$\partial s'(\alpha) = \sum_{k=0}^{r} (-1)^k \sum_j \phi_j s(\sigma(j)\cup\alpha^{(k)}) = \sum_j \phi_j \sum_{k=0}^{r} (-1)^k s(\sigma(j)\cup\alpha^{(k)}).$$

Since $\partial s(\sigma(j)\cup\alpha) = s(\alpha)-\sum_{k=0}^{r}(-1)^k s(\sigma(j)\cup\alpha^{(k)}) = 0$, we see that

$$\partial s'(\alpha) = \{\sum_j \phi_j\} s(\alpha) = s(\alpha).$$

This shows that

$$\check{H}^q(Z;\mathcal{U};\mathcal{A}_F{}^p) = 0 \text{ for every } \mathcal{U}. \tag{6}$$

Let $H^q_{DR}(Z, F)$ be the cohomology group of the complex

$$\mathcal{A}_F(Z) : 0 \to \mathcal{A}_F{}^0(Z) \xrightarrow{d} \mathcal{A}_F{}^1(Z) \xrightarrow{d} \mathcal{A}_F{}^2(Z) \xrightarrow{d} \cdots.$$

The group $H^q_{DR}(Z, F)$ is called the de Rham cohomology group. Then we have

Theorem 2. *If the covering $\mathcal{U}$ of Z satisfies the condition of Proposition 3, then there is a natural isomorphism* $H^q_{DR}(Z, F) \cong \check{H}^q(Z;\mathcal{U};\mathcal{A}_F{}^p)$.

Proof. For any sheaf, it is easy to see that the presheaf:

$$U \mapsto C(\mathcal{U}|_U;F|_U) = \oplus_q C^q(\mathcal{U}|_U;F|_U)$$

is actually a sheaf of complexes, where $\mathcal{U}|_U = \{U_i \cap U \mid i \in I\}$. We still write this sheaf of complexes as $C(\mathcal{U};F)$. From the exact sequence:

$$0 \to Z_q \to \mathcal{A}_F{}^q \to Z_{q+1} \to 0 \quad (Z_q = \mathrm{Ker}(d_q : \mathcal{A}_F{}^q \to \mathcal{A}_F{}^{q+1})),$$

we get another exact sequence of sheaves of complexes:

$$0 \to C(\mathcal{U};Z_q) \to C(\mathcal{U};\mathcal{A}_F{}^q) \to C(\mathcal{U};Z_{q+1}) \to 0. \tag{$*$}$$

In fact, for each simply connected open set U, Poincaré's lemma tells us the surjectivity of $d : \mathcal{A}_F{}^q(U) \to Z_{q+1}(U)$. Since every non-empty U_α $(\alpha \in \Gamma^{r+1})$ is simply connected, $(*)$ is not only exact as sheaves but also exact as complex of $\mathbf{C}$-vector-spaces. Then we have the long exact sequence (1) attached to $(*)$:

$$0 \to Z_q(Z) \to \mathcal{A}_F{}^q(Z) \to Z_{q+1}(Z) \to \check{H}^1(Z;\mathcal{U};Z_q) \to \check{H}^{p-1}(Z;\mathcal{U};\mathcal{A}_F{}^q) \to$$
$$\cdots \to \check{H}^{p-1}(Z;\mathcal{U};Z_{q+1}) \to \check{H}^p(Z;\mathcal{U};Z_q) \to \check{H}^p(Z;\mathcal{U};\mathcal{A}_F{}^q) \to \cdots.$$

Since the restriction map of $\mathcal{A}_F{}^q(U)$ to $\mathcal{A}_F{}^q(V)$ for $V \subset U$ is surjective, we can apply Proposition 3 and know that $\check{H}^p(Z;\mathcal{U};\mathcal{A}_F{}^q) = 0$ for all $p > 0$. This shows

$$\check{H}^q(Z;\mathcal{U};F) = \check{H}^q(Z;\mathcal{U};Z_0) \cong \check{H}^{q-1}(Z;\mathcal{U};Z_1) \cong \cdots \cong \check{H}^1(Z;\mathcal{U};Z_{q-1})$$
$$\cong Z_q(Z)/d\mathcal{A}_F{}^{q-1}(Z) = H^q_{DR}(Z, F).$$

A sheaf F is called *flabby* if for every inclusion of open sets $V \subset U$, $\mathrm{res}_{U/V} : F(U) \to F(V)$ is surjective. We define abelian groups $\Gamma(F)$ and $\Gamma_c(F)$ by $\Gamma(F) = F(Z)$ and $\Gamma_c(F) = \{f \in \Gamma(F) \mid \mathrm{Supp}(f) \text{ is compact}\}$.

Lemma 3. *If* $0 \to F \to G \to H \to 0$ *is an exact sequence of sheaves on* Z. *Suppose that* F *is flabby. Then* $0 \to \Gamma(F) \to \Gamma(G) \to \Gamma(H) \to 0$ *and* $0 \to \Gamma_c(F) \to \Gamma_c(G) \to \Gamma_c(H) \to 0$ *are exact sequences of abelian groups. In particular, if* F *and* G *are flabby, then* H *is flabby.*

Proof. We only need to check surjectivity of $\alpha : \Gamma_c(G) \to \Gamma_c(H)$ and $\Gamma(G) \to \Gamma(H)$. Let $s \in \Gamma(H)$. Let C be the collection of all pairs (t,U) $(t \in G(U))$ such that $\alpha(U)(t) = \mathrm{res}_{Z/U}(s)$. We give an order on C so that $(t,U) \geq (t',U')$ if $U \supset U'$ and $\mathrm{res}_{U/U'}(t) = t'$. Evidently C is inductively ordered. Thus there is a maximal element (U,t) in C by Zorn's lemma. Suppose $U \neq Z$. Let $x \in Z\text{-}U$ and take a small neighborhood V in Z of x. If V is sufficiently small, we can find $v \in G(V)$ so that $(V,v) \in C$ by the surjectivity (see (5b)). Then $\mathrm{res}_{U/U\cap V}(t)\text{-}\mathrm{res}_{V/V\cap U}(v) \in \mathrm{Ker}(\alpha)(U\cap V)$. Thus by flabbiness of F, we can find $f \in F(U\cup V)$ such that

$$\mathrm{res}_{U\cup V/U\cap V}(f) = \mathrm{res}_{U/U\cap V}(t)\text{-}\mathrm{res}_{V/V\cap U}(v).$$

This implies that t and $f+v$ coincide on $U\cap V$. Then by the sheaf axiom, we can find $t' \in G(U\cup V)$ such that

$$\mathrm{res}_{U\cup V/V}(t') = f+v \text{ and } \mathrm{res}_{U\cup V/U}(t') = t.$$

Then $(U\cup V, t')$ is larger than (U,t) contradicting the maximality of (U,t). Thus $U = Z$ and $\alpha(t) = s$. This shows the assertion for Γ. When $s \in \Gamma_c(H)$, then $V = Z\text{-}\mathrm{Supp}(s)$ is an open set and $\mathrm{res}_{Z/V}(s) = \mathrm{res}_{Z/V}(\alpha(t)) = 0$. Thus we can find $t' \in \Gamma(F)$ such that $\mathrm{Supp}(t\text{-}t') \subset \mathrm{Supp}(s)$. Then $t\text{-}t' \in \Gamma_c(G)$ and $\alpha(t\text{-}t') = s$. This shows the assertion for Γ_c.

Let F be an arbitrary sheaf. Let

$$Fl : 0 \to F \to Fl_0 \to Fl_1 \to Fl_2 \to \cdots$$

be an exact sequence of sheaves where the Fl_i are all flabby. Such a complex is called a flabby (acyclic) resolution. There is a standard flabby resolution $Fl(F)$ of F: We define $Fl^0(F)(U) = \prod_{x\in U} F_x$. Then $Fl^0(F)$ is plainly a flabby sheaf. Then the diagonal map: $f \mapsto \prod_{x\in U} f_x$ takes injectively F into $Fl^0(F)$ by (S). After defining $Fl^k(F)$ and $\partial_{k-1} : Fl^{k-1}(F) \to Fl^k(F)$, we just define

$$Fl^{k+1}(F) = Fl^0(\mathrm{Coker}(\partial_{k-1})) \text{ and } \partial_k : Fl^k(F) \to \mathrm{Coker}(\partial_{k-1}) \to Fl^{k+1}(F),$$

where the last arrow is the natural diagonal map. We define the sheaf cohomology group $H^q(Z,F)$ (resp. the compactly supported sheaf cohomology group

$H^q_c(Z,F))$ to be the cohomology group of the complex $\Gamma(Fl(F))$ (resp. $\Gamma_c(Fl(F))$).

Proposition 4. *There exists a canonical isomorphism* $H^q(Z,F) \cong \check{H}^q(Z;F)$.

Proof. By Lemma 3, $H^q(Z,F) = H^q_c(Z,F) = 0$ if F is flabby. First suppose that F is flabby. Then the sheaf $C^q(\mathcal{U};F)$ is flabby. Consider the exact sequence of sheaves $0 \to \mathcal{Z}_q \to C^q(\mathcal{U};F) \to \mathcal{Z}_{q+1} \to 0$ for $\mathcal{Z}_q = \mathrm{Ker}(\partial_q)$. This induces an exact sequences of complexes

$$0 \to Fl(\mathcal{Z}_q) \to Fl(C(\mathcal{U};F)) \to Fl(\mathcal{Z}_{q+1}) \to 0.$$

Note that $Fl(C^q(\mathcal{U};F))$ is flabby. Applying (1), we have a long exact sequence:

$$H^p(Z,C^q(\mathcal{U};F)) \to H^p(Z,\mathcal{Z}_{q+1}) \to H^{p+1}(Z,\mathcal{Z}_q) \to H^{p+1}(Z,C^q(\mathcal{U};F)).$$

Since both ends of the above sequence vanish because of flabbiness of $C(\mathcal{U};F)$, we have

$$H^p(Z,\mathcal{Z}_{q+1}) \cong H^{p+1}(Z,\mathcal{Z}_q).$$

This shows

$$0 = H^q(Z,\mathcal{Z}_0) \cong H^{q-1}(Z,\mathcal{Z}_1) \cong \cdots \cong H^1(Z,\mathcal{Z}_{q-1}) = \check{H}^q(Z;\mathcal{U};F).$$

Thus we see that

(7) If F is flabby, then $\check{H}^q(Z;\mathcal{U};F) = 0$ for all covering $\mathcal{U}$.

Now we treat the general case. Consider the exact sequence of sheaves:

$$0 \to \mathcal{Z}'_q \to Fl_q(F) \to \mathcal{Z}'_{q+1} \to 0 \quad \text{for } \mathcal{Z}'_q = \mathrm{Ker}(\partial_q).$$

Note that $Fl_q(F)$ is flabby. From the long exact sequence of Čech cohomology, we have an exact sequence

$$0 = \check{H}^q(Z,Fl_q(F)) \to \check{H}^q(Z,\mathcal{Z}'_{q+1}) \to \check{H}^{q+1}(Z,\mathcal{Z}'_q) \to \check{H}^{q+1}(Z,Fl_q(F)) = 0.$$

Since both ends of the above sequence vanish because of flabbiness of $C(\mathcal{U};F)$, we have $\check{H}^q(Z,\mathcal{Z}'_{q+1}) \cong \check{H}^{q+1}(Z,\mathcal{Z}'_q)$. This shows

$$\check{H}^q(Z,F) = \check{H}^q(Z,\mathcal{Z}'_0) \cong \check{H}^{q-1}(Z,\mathcal{Z}'_1) \cong \cdots \cong \check{H}^1(Z,\mathcal{Z}'_{q-1}) = H^q(Z,F).$$

In fact, we can compute the sheaf cohomology group $H^q(Z,F)$ of F using *any* flabby resolution $0 \to F \to Fl$ of F. Out of the sheaf exact sequence

$$0 \to \mathcal{Z}_q \to Fl_q \to \mathcal{Z}_{q+1} \to 0$$

for $\mathcal{Z}_q = \mathrm{Ker}(\partial_q)$, we have another exact sequence of complexes

$$0 \to Fl(\mathcal{Z}_q) \to Fl(Fl_q) \to Fl(\mathcal{Z}_{q+1}) \to 0.$$

Applying (1) to this, we have, for H^q_* denoting any one of H^q and H^q_c,

$$H^q_*(Z,F) = H^q_*(Z,\mathcal{Z}_0) \cong H^{q-1}_*(Z,\mathcal{Z}_1) \cong \cdots \cong H^0_*(Z,\mathcal{Z}_q) = H^q_*(Fl).$$

Thus we have

(8) For any flabby resolution $0 \to F \to Fl$,

$$H^q(Fl) \cong H^q(Z,F) \cong \check{H}^q(Z,F) \text{ and } H^q_c(Fl) \cong H^q_c(Z,F).$$

Suppose F is a presheaf with surjective $\mathrm{res}_{U/V}$ for every inclusion $V \subset U$ and F satisfies a part of (S):

(S') If for each covering $\{U_i\}$, a given set of elements $s_i \in F(U_i)$ satisfies $\mathrm{res}_{Z/U_i \cup U_j} s_i = \mathrm{res}_{Z/U_i \cup U_j} s_j$, *there exists* $s \in F(U)$ *such that* $\mathrm{res}_{Z/U_i}(s) = s_i$ *for all* i;

then we see easily that $F^{\#}$ is flabby.

Now assume that Z has a triangulation K. We now introduce the subdivision process of complexes. Let $\Delta^2 = (a,b,c)$ be an r-simplex. We define a subdivision $\mathrm{Sd}(\Delta^2)$ of Δ^2 by all the simplices in Figure (ii):

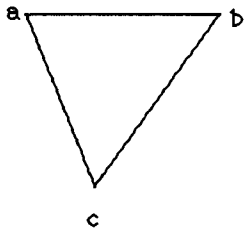


Figure (i)

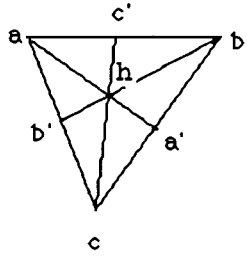


Figure (ii)

Here h is the barycenter of Δ. Thus writing $h*(x_1,\ldots,x_r) = (h,x_1,\ldots,x_r)$, we see that $\mathrm{Sd}(a) = a$, $\mathrm{Sd}(b,c) = (b,a')+(a',c)$ for the barycenter a' of the line segment (b,c) and $\mathrm{Sd}(\Delta) = h*\mathrm{Sd}(\partial\Delta)$. By the last formula, we can inductively define the subdivision operator Sd for all r-simplices. We apply this process of subdivision to each simplex of the complex $K = K_0$. We write the resulting simplex as $K_1 = \mathrm{Sd}(K_0)$. We continue this process n times and write the n-th subdivision obtained by $K_n = \mathrm{Sd}^n(K) = \mathrm{Sd}(K_{n-1})$. Finally we define $K_\infty = \varinjlim_{\alpha} K_\alpha$. Let R be a commutative algebra with identity. For any open set U on Z, we can consider a module $A_q(U)$ of formal linear combinations $\sum_{a_\Delta \in R} a_\Delta \Delta$ for $a_\Delta \in R$ for i-simplices Δ in $K_\infty \cap U$. Then we have a covariant functor $A_q : U \mapsto A_q(U)$ with natural inclusion map $\mathrm{Inc}_{U/V} : A_q(V) \to A_q(U)$ if $U \supset V$. Thus we have a presheaf $\mathrm{Hom}_R(A_q,F) : U \mapsto \mathrm{Hom}_R(A_q(U), F(U))$. If F is locally constant, $\mathrm{Hom}_R(A_q,F)$ satisfies (S) and hence it is a sheaf and $\mathrm{Hom}_R(A_q,F)$ gives a flabby resolution of F. We can thus compute $H^q(Z,F)$ and $H^q_c(Z,F)$ using $\mathrm{Hom}_R(A_q,F)$.

We now return to the situation in Proposition 1: $Z = H_0$ and $F = M$. Let $A_{q,\alpha}$ be the R-free module generated by q-simplices in K_α and put

$$S^q(K_\alpha;M) = \mathrm{Hom}_R(A_{i,\alpha};M) \text{ with } \Gamma\text{-action } (\phi|\gamma)(\Delta) = \gamma^{1}\phi(\gamma\Delta).$$

Then we define $H^q(K_\alpha,M)$ by the cohomology group of the complex

$$0 \to S^0(K_\alpha;M)^\Gamma \to S^1(K_\alpha;M)^\Gamma \to S^2(K_\alpha;M)^\Gamma \to 0.$$

We want to show that Sd induces an isomorphism $H^q(K_\alpha,M) \cong H^q(K_{\alpha+1},M)$. Let $\mathcal{K}_\alpha$ be the triangulation of Y_0 induced by K_α. Each vertex $x \in \mathcal{K}_{\alpha+1}$ is a barycenter of a unique simplex Δ of $\mathcal{K}_\alpha$ by the definition of the subdivision. Choose one vertex y of Δ and define $\varphi(x) = y$. We know that if (x,y) is a 1-simplex of $\mathcal{K}_{\alpha+1}$, then either x or y, say x, is the barycenter of itself. Hence y is the barycenter of (x,z). Then $\varphi(x) = x$ and either $\varphi(y) = x$ or $\varphi(y) = z$. In either case $(\varphi(x),\varphi(y))$ is a simplex of $\mathcal{K}_{\alpha+1}$. Here we allow repetition of vertices: (x,x) implies the 0-simplex x. Similarly, if (x,y,z) is a 2-simplex of $\mathcal{K}_{\alpha+1}$, then looking at figure (ii), we may assume that x is the barycenter of x itself, y is the barycenter of $(x,a) \in \mathcal{K}_\alpha$ and z is the barycenter of $(x,a,b) \in \mathcal{K}_\alpha$. Thus we define $\varphi(x) = x$, $\varphi(y) = x$ or z and $\varphi(z) = x$, a or b. In any choice, $(\varphi(x),\varphi(y),\varphi(z))$ is a simplex of $\mathcal{K}_\alpha$. Thus φ induces a simplicial map and hence a continuous map on Y_0 into itself, which we denote by the same letter φ. We want to show that φ is homotopically equivalent to the identity. For each $x \in Y_0$, by definition, both $\varphi(x)$ and x belong to the closure of a 2-simplex $t(x)$. Moving Y_0 into $\mathbf{R}^2$ by the homeomorphism given by the triangulation $\mathcal{K}$, we may assume that Y_0 is embedded in $\mathbf{R}^2$. Then we define $F : [0,1]\times Y_0 \to Y_0$ by $F(u,x) = (1-u)(x-a)+u(\varphi(x)-a)+a$ if $t(x) = (a,b,c)$ for three vectors a, b and c in $\mathbf{R}^2$. Obviously F is continuous and hence gives the homotopy equivalence between φ and the identity. Extending the simplicial map φ to $\varphi : A_{q,\alpha+1} \to A_{q,\alpha}$ by $R[\Gamma]$-linearity, we have an $R[\Gamma]$-morphism φ which induces an isomorphism

$$\varphi_* : H^q(K_{\alpha+1},M) \cong H^q(K_\alpha,M) \quad \text{satisfying } \varphi_* \circ Sd = Sd \circ \varphi_* = \mathrm{id}.$$

We now identify $H^q(K_\alpha, M)$ with $H^q(K, M)$ by Sd^α. Since Y_0 is isomorphic to Y as a smooth manifold, we can compactify Y identifying Y with the closure of Y_0 in X. We write Y^S for this compactification. Note that Y^S and X are different; that is, X has one point at the cusp but the boundary of Y^S at the cusp is a circle S^1 isomorphic to a small circle around the cusp in X. We can think of something in between Y and Y^S depending on S_0 for a given subset S_0 of S. We remove the boundary at $s \in S_0$ from Y^S and write it as Y^{S-S_0}. Note here that $Y^\varnothing = Y$. Since $S^q(K_\infty;M)^\Gamma$ are the global sections of the sheaf $\mathrm{Hom}_R(A_q,\underline{M})$ on Y_0, we have

Proposition 5. *Let the notation be as in Propositions 1 and 2 and Theorem 1. Then we have canonical isomorphisms*

$$H^q_c(Y^{S-S_0},\underline{M}) \cong H^q_{S_0}(\Gamma,M) \textit{ for all subsets } S_0 \textit{ in } S \textit{ and } H^q(Y,\underline{M}) \cong H^q(K,M).$$

Then by the boundary exact sequence in Proposition 2, we have

Corollary 2. *Let the notation be as in Proposition 2. We have a long exact sequence*

$$0 \to H^0_c(Y^{S-S_0},\underline{M}) \to H^0(Y,\underline{M}) \to \oplus_{s\in S_0}H^0(\partial_s Y^*,\underline{M}) \to H^1_c(Y^{S-S_0},\underline{M})$$
$$\to H^1(Y,\underline{M}) \to \oplus_{s\in S_0}H^1(\partial_s Y^*,\underline{M}) \to H^2_c(Y^{S-S_0},\underline{M}) \to H^2(Y,\underline{M}) \to 0,$$

where $\partial_s Y^*$ *is the boundary around* s.

We now briefly recall the Poincaré duality for Y. Our proof of the duality is merely a sketch, and the reader should consult standard texts (for example [HiW, 4.4.13]) for details. Suppose that R is a field and M is a finite dimensional vector space over R. Let $\phi \in \mathrm{Hom}_R(A_{0,\alpha},M^*)$ be a cocycle for $M^* = \mathrm{Hom}_R(M,R)$, where α is a fixed integer (which we make large if necessary). We suppose that ϕ is compactly supported on Y. Then we can find a small open neighborhood of ∂Y^S which does not meet the support of ϕ. We take a cocycle $\omega \in \mathrm{Hom}_R(A_{2,\alpha},M)$. Then we define for each i-simplex Δ of $\mathcal{K}_\alpha$,

$$\langle\phi,\omega\rangle(\Delta) = \langle\phi(\Delta),\omega(\Delta)\rangle \text{ for the dual pairing } \langle\ ,\ \rangle : M^*\times M \to R.$$

Since Δ is simply connected, ϕ is a constant function on Δ. Here we write $\phi(\Delta)$ for this value of ϕ on Δ. It is obvious that $\langle\phi,\omega\rangle \in \mathrm{Hom}_R(A_{2,\alpha},R)$ and $\mathrm{Supp}\langle\phi,\omega\rangle$ is compact in Y. We see easily that $\langle\phi,\partial\omega\rangle = \partial\langle\phi,\omega\rangle$ and hence $\langle\phi,\omega\rangle$ is a 2-cocycle. It is well known (see Proposition 6.1.1 for a proof) that $H^2_c(Y,R) \cong R$. That is, we have a pairing

$$\langle\ ,\ \rangle : H^0(Y,\underline{M}^*)\times H^2_c(Y,\underline{M}) \to R.$$

Suppose $\langle\phi,\omega\rangle = \partial\eta_\phi$ for all ϕ with compactly supported $\eta_\phi \in \mathrm{Hom}_R(A_1,R)$ depending on ϕ. We fix a basis $\{e_1, \ldots, e_r\}$ of M and take its dual basis $\{e_1^*,\ldots, e_r^*\}$ of M^*. We write $\phi = \sum_i\phi_i e_i^*$ and $\omega = \sum_i\omega_i e_i$. Then we can define a 1-chain $\xi_i \in \mathrm{Hom}_R(A_1,M)$ by $\xi_i(\Delta_1) = \eta_{\phi_i e_i^*}(\Delta_1)e_i^*$ on each 1-simplex Δ_1 in the Δ. Put $\xi = \sum_i\xi_i$. Then we see from construction that $\partial\xi = \omega$ on Δ. We extend this process of defining ξ to 2-simplices adjacent to Δ. Then inductively, we get ξ such that $\partial\xi = \omega$. Thus the pairing is non-degenerate on $H^2_c(Y,\underline{M})$. Similarly, we can show that the pairing is non-degenerate on $H^0(Y,\underline{M}^*)$ much more easily because there is no-restriction for ω to be a 2-cocycle (i.e. Y is two dimensional). Thus we have

Proposition 6. *Suppose that* R *is a field and* M *is finite dimensional. Then the pairing* $\langle\ ,\ \rangle : H^0(Y,\underline{M}^*)\times H^2_c(Y,\underline{M}) \to R$ *is a perfect duality.*

References

Books

[BGR] S. Bosch, U. Güntzer and R. Remmert, *Non-Archimedean analysis,* Springer, 1984

[Bour1] N. Bourbaki, *Algèbre commutative,* Hermann, Paris, 1961, 1964, 1965 and 1983

[Bour2] N. Bourbaki, *Topologie générale,* Hermann, Paris, 1960, 1965

[Bour3] N. Bourbaki, *Algèbre,* Hermann, Paris, 1958-

[Bd] Bredon, *Sheaf theory,* McGraw-Hill, 1967

[Bw] K. S. Brown, *Cohomology of groups,* Graduate Texts in Math. 87, Springer, 1982

[CM] L. Clozel and J. S. Milne, *Automorphic forms, Shimura varieties and L-functions,* Perspectives in Math. 10, 11 (1990), Academic Press

[CT] J. Coates and M. J. Taylor, *L-functions and arithmetic,* LMS Lecture notes series 153 (1991), Cambridge Univ. Press

[dS] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication,* Perspectives in Math. 3 (1987), Academic Press

[FT] A. Fröhlich and M. J. Taylor, *Algebraic number theory,* Cambridge studies in advanced mathematics 27, Cambridge University Press, 1991

[G] R. Godement, *Notes on Jacquet-Langlands theory,*

[Gv] F. Q. Gouvêa, *Arithmetic of p-adic modular forms,* Lecture Notes in Math. 1304 (1988), Springer

[Ge] S. S. Gelbart, *Automorphic forms on adele groups,* Ann. of Math. Studies 83, Princeton University Press, 1975

[Ha] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. 52, Springer, 1877

[HiW] P. J. Hilton and S. Wylie, *Homology Theory,* Cambridge University Press, 1960

[HiSt] P. J. Hilton and U. Stammbach, *A course in homological algebra,* Graduate Texts in Math. 4, Springer, 1971

[Hör] L. Hörmander, *An introduction to complex analysis in several variables,* North-Holland, 1973

[Iw1] K. Iwasawa, *Lectures on p-adic L-functions,* Ann. of Math. Studies 74, Princeton Univ. Press, 1972

[J] H. Jacquet, *Automorphic forms on GL(2), II,* Lecture notes in Math. 278, 1972, Springer

[JL] H. Jacquet and R. P. Langlands, *Automorphic forms on GL(2),* Lecture notes in Math. 114, Springer

[Kb] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta functions,* Graduate Texts in Math. 58, Springer, 1977

[Ko] K. Kodaira, *Complex manifolds and deformation of complex structure,* Springer, 1986

[L] S. Lang, *Cyclotomic fields*, Graduate Texts in Math. 59, Springer, 1978

[M] T. Miyake, *Modular forms,* Springer, 1989

[Mm1] D. Mumford, *Abelian varieties,* Oxford Univ. Press, 1974

[N] J. Neukirch, *Class field theory*, Springer, 1986

[NZ] I. Niven and H.S. Zuckerman, *An introduction to the theory of numbers,* John Wiley & Sons, 1980 (4th Edition)

[P] L. S. Pontryagin, *Theory of continuous groups* (Russian), Moscow, 1954

[Pa] A.A. Panchishkin, *Non-Archimedean L-functions of Siegel and Hilbert modular forms,* Lecture notes in Math. 1471, 1991, Springer

[RSS] M. Rapoport, N. Schappacher and P. Schneider (ed.), *Beilinson's conjectures on special values of L-functions,* Perspectives in Math. 4, Academic Press, 1988

[Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic functions,* Princeton Univ. Press, 1971

[Wa] L. C. Washington, *Introduction to cyclotomic fields,* Graduate Texts in Math. 83, Springer, 1980

[W1] A. Weil, *Basic number theory,* Springer, 1974

[W2] A. Weil, *Elliptic functions according to Eisenstein and Kronecker,* Springer, 1976

[W3] A. Weil, *Dirichlet series and automorphic forms,* Lecture notes in Math. 189, Springer, 1971

Articles

[Ba] D. Barsky, Fonctions zêta p-adiques d'une classe de rayon des corps totalement réels, *Groupe d'étude d'analyse ultrametrique* 1977-78; errata, 1978-79

[B] D. Blasius, On the critical values of Hecke L-series, *Ann. of Math.* **124** (1986), 23-63

[Cl] H. Carayol, Sur les représentations l-adiques associées aux formes modulaires, *Ann. Scient. Ec. Norm. Sup. 4e série*, **19** (1986), 409-468

[C] W. Casselman, On some results of Atkin and Lehner, *Math. Ann.* **201** (1973), 301-314

[CN] P. Cassou-Nogués, Valeurs aux entiers négatifs des fonctions zêta p-adiques, *Inventiones Math.* **51** (1979), 29-59

[Co] P. Colmez, Résidu en $s = 1$ des fonctions zêta p-adiques, *Inventiones Math.* **91** (1988), 371-389

[D] P. Deligne, Formes modulaires et représentations l-adiques, *Sém. Bourbaki*, exp.355, 1969

[D1] P. Deligne, Valeurs de fonctions L et périodes d'intégrales, *Proc. Symp. Pure Math.* **33** (1979), Part 2, 313-346

[DR] P. Deligne and K. A. Ribet, Values of abelian L-functions at negative integers over totally real fields, *Inventiones Math.* **59** (1980), 227-286

[DS] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, *Ann. Scient. Ec. Norm. Sup.* **7** (1974), 507-530.

[DuS] G. F. D. Duff and D. C. Spencer, Harmonic tensors on Riemannian manifolds with boundary, *Ann. of Math.* **56** (1952), 128-156

[GJ] S. Gelbart and H. Jacquet, A relation between automorphic representations of GL(2) and GL(3), *Ann. Scient. Ec. Norm. Sup.* 4e série **11** (1978), 471-542

[GS] R. Greenberg and G. Stevens, p-adic L-functions and p-adic periods of modular forms, preprint

[Ha] G. Harder, Eisenstein cohomology of arithmetic groups. The case GL_2, Inventiones Math. **89** (1987), 37-118

[H1] H. Hida, On congruence divisors of cusp forms as factors of the special values of their zeta functions, Inventiones Math. **64** (1981), 221-262

[H2] H. Hida, Congruences of cusp forms and Hecke algebras, Sém. de Théorie des Nombres, Paris 1983-84, Progress in Math. **59** (1985), 133-146

[H3] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Scient. Ec. Norm. Sup. 4e série **19** (1986), 213-273

[H4] H. Hida, Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms, Inv. Math. 85 (1986), 546-613

[H5] H. Hida, A p-adic measure attached to the zeta functions associated with two elliptic modular forms, I, II. I: Inventiones Math. **79** (1985), 159-195; II: Ann. Institut Fourier **38** No.3 (1988), 1-83

[H6] H. Hida, p-adic L-functions for base change lifts of GL_2 to GL_3, In: *Automorphic forms, Shimura varieties, and L-functions, II*, Perspectives in Mathematics **11** (1990), Academic Press, pp.93-142

[H7] H. Hida, Le produit de Petersson et de Rankin p-adique, Sem. Théorie des Nombres, Paris 1988-89, Progress in Math. **91** (1990), 87-102

[H8] H. Hida, On p-adic L-functions of $GL(2)\times GL(2)$ over totally real fields, Ann. Institut Fourier 41, 2 (1991), 311-391

[H9] H. Hida, On the critical values of L-functions of GL(2) and $GL(2)\times GL(2)$, in preparation

[H10] H. Hida, Nearly ordinary Hecke algebras and Galois representations of several variables, in supplement to the Amer. J. Math. with the title: *Algebraic analysis, geometry and number theory*, Johns Hopkins Univ. Press, 1989, pp.115-134

[HT1] H. Hida and J. Tilouine, Katz p-adic L-functions, congruence modules and deformation of Galois representations, Proc. LMS Symposium on "L-functions and arithmetic", Durham, England, July 1989, LMS Lecture notes series **153** (1991), Cambridge Univ. Press, pp.271-293

[HT2] H. Hida and J. Tilouine, Anti-cyclotomic Katz p-adic L-functions and congruence modules, Ann. Ec. Norm. Sup., 4e série, **25** (1992)

[HT3] H. Hida and J. Tilouine, On the anticyclotomic main conjecture for CM fileds, preprint

[K1] N. M. Katz, p-adic properties of modular schemes and modular forms, in *Modular functions of one variable*, Lecture Notes in Math. **350** (1973), Springer, pp.69-190

[K2] N. M. Katz, p-adic L-functions via moduli of elliptic curves, Proc. Symp. Pure. Math. **29** (1975), 479-506

[K3] N. M. Katz, p-adic interpolation of real analytic Eisenstein series, Ann. of Math. **104** (1976), 459-571

[K4] N. M. Katz, Formal groups and p-adic interpolation, Astérisque **41-42** (1977), 55-65

[K5] N. M. Katz, p-adic L-functions of CM fields, Inventiones Math. **49** (1978), 199-297

[K6] N. M. Katz, Another look at p-adic L-functions for totally real fields, Math. Ann. **255** (1981), 33-43

[Ki] K. Kitagawa, On standard p-adic L-functions of families of elliptic cusp forms, preprint

[KL] T. Kubota and H. W. Leopoldt, Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-funktionen, J. reine angew. Math. **214/215** (1964), 328-339

[La] R. P. Langlands, Modular forms and l-adic representations, In *Modular functions of one variable II*, Lecture Notes in Math. **349**, 1973, Springer, pp.361-500

[Md] Y. Maeda, Generalized Bernoulli numbers and congruence of modular forms, Duke Math J. **57** (1988), 673-696

[Ma] K. Mahler, An interpolation series for continuous functions of a p-adic variable, J. reine angew. Math. **199** (1958), 23-34

[Mn1] Y. I. Manin, Periods of cusp forms, and p-adic Hecke series, Math. USSR-Sb.**21** (1973), 371-393

[Mn2] Y. I. Manin, The values of p-adic Hecke series at integer points of the critical strips, Math. USSR-Sb. **22** (1974), 631-637

[MM] Y. Matsushima and S. Murakami, On vector bundle valued harmonic forms and automorphic forms on symmetric Riemannian manifolds, Ann. of Math. **78** (1963), 365-416

[MSh] Y. Matsushima and G. Shimura, On the cohomology groups attached to certain vector valued differential forms on the product of upper half planes, Ann. of Math. **78** (1963), 417-449

[Mz1] B. Mazur, Courbes elliptiques et symboles modulaires, Sém. Bourbaki, exposé 414 (1972, juin)

[Mz2] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Inventiones Math. **18** (1972), 183-266

[Mz3] B. Mazur, Deforming Galois representations, Proc. of workshop on Galois groups over $\mathbf{Q}$, Springer, 1989, pp.385-437

[MzS] B. Mazur and H.P.F. Swinnerton-Dyer, Arithmetic of Weil curves, Inventiones Math. **25** (1974), 1-61

[MT] B. Mazur and J. Tilouine, Représentations galoisiennes, différentielles de Kähler et "conjectures principales", Publ. I.H.E.S. **71** (1990), 65-103

[MTT] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Inventiones Math. **84** (1986), 1-48

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbf{Q}$, Inventiones Math. **76** (1984), 179-330

[Ri] K. A. Ribet, A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$, Inventiones Math. **34** (1976), 151-162

[R] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Inventiones Math. **103** (1991), 25-68

[Sch] C.-G. Schmidt, p-adic measures attached to automorphic representations of GL(3), Invent. Math. **92** (1988), 597-631

[Se] J.-P. Serre, Formes modulaires et fonctions zêta p-adiques, In *Modular functions of one variable III*, Lecture Notes in Math. **350** (1973), Springer, pp.191-268.

[Sh1] G. Shimura, Sur les intégrales attachés aux formes automorphes, J. Math. Soc. Japan **11** (1959),291-311

[Sh2] G. Shimura, On the holomorphy of certain Dirichlet series, Proc. London Math. Soc. **31** (1975), 79-98

[Sh3] G. Shimura, The special values of the zeta functions associated with cusp forms, Comm. Pure Appl. Math. **29** (1976), 783-804

[Sh4] G. Shimura, On the periods of modular forms, Math. Ann. **229** (1977), 211-221

[Sh5] G. Shimura, The special values of the zeta functions associated with Hilbert modular forms, Duke Math. J. **45** (1978), 637-679

[Sh6] G. Shimura, On certain zeta functions attached to two Hilbert modular forms: I. The case of Hecke characters, Ann. of Math.**114** (1981), 127-164; II. The case of automorphic forms on a quaternion algebra, ibid. 569-607

[Sh7] G. Shimura, Confluent hypergeometric functions on tube domains, Math. Ann. **260** (1982), 269-302

[Sh8] G. Shimura, Algebraic relations between critical values of zeta functions and inner products, Amer. J. Math. **104** (1983), 253-285

[Sh9] G. Shimura, On Eisenstein series, Duke Math. J. **50** (1983), 417-476

[Sh10] G. Shimura, On a class of nearly holomorphic automorphic forms, Ann. of Math. **123** (1986), 347-406

[Sh11] G. Shimura, On the critical values of certain Dirichlet series and the periods of automorphic forms, Inventiones Math. **94** (1988), 245-305

[Sh12] G. Shimura, On the fundamental periods of automorphic forms of arithmetic type, Inventiones Math. **102** (1990), 399-428

[St1] T. Shintani, On evaluation of zeta functions of totally real algebraic number fields at non-positive integers, J. Fac. Sci. Univ. Tokyo, Sec.IA **23** (1976), 393-417

[St2] T. Shintani, On a Kronecker limit formula for real quadratic fields, J. Fac. Sci. Univ. Tokyo, Sec.IA **24** (1977), 167-199

[St3] T. Shintani, On values at $s = 1$ of certain L-functions of totally real algebraic number fields, In *Algebraic number theory*, Proc. Int. Symp. Kyoto, 1976, pp. 201-212

[St4] T. Shintani, On certain ray class invariants of real quadratic fields, J. Math. Soc. Japan, **30** (1977), 139-167

[St5] T. Shintani, A remark on zeta functions of algebraic number fields, In *Automorphic forms, representation theory and arithmetic*, Tata Institute of Fundamental Research, Bombay, 1979, pp.255-260

[St6] T. Shintani, A proof of the classical Kronecker limit formula, Tokyo J. Math. **3** (1980), 191-199

[Si] C. L. Siegel, Berechnung von Zeta-funktionen an ganzzahligen Stellen, Nachr. Akad. Wiss. Göttingen 1969, 87-102

[Wi1] A. Wiles, On ordinary λ-adic representations associated to modular forms, Inventiones Math. **94** (1988), 529-573

[Wi2] A. Wiles, The Iwasawa conjecture for totally real fields, Ann. of Math. **131** (1990), 493-540

Answers to selected exercises

§1.2.

1. We only need to show that $(\mathcal{P}\cap I(m):\mathcal{P}_+(m))$ is finite, because $I(m)/\mathcal{P}\cap I(m)$ injects into $I/\mathcal{P}$. We see by definition that the natural map $\mathcal{O}-\{0\} \to \mathcal{P}$, which takes each integer $\alpha \in \mathcal{O}$ to the principal ideal generated by α, induces a surjection from the finite group $(\mathcal{O}/m)^\times$ onto $\mathcal{P}\cap I(m)/\mathcal{P}(m)$. Hence $(\mathcal{P}\cap I(m):\mathcal{P}(m))$ is finite. The map $F \to \mathbf{R}^r\times\mathbf{C}^t$ given by $F \ni \alpha \mapsto (\alpha^{(i)})$ induces an injection of $\mathcal{P}(m)/\mathcal{P}_+(m) \to (\mathbf{R}^\times)^r/(\mathbf{R}_{>0})^r$, where $\mathbf{R}_{>0} = \{x \in \mathbf{R} \mid x > 0\}$. Thus $(\mathcal{P}(m):\mathcal{P}_+(m)) \le 2^r$. This shows the desired assertion.

2. (b) What we need to show is that the integer ring $\mathcal{O}$ is not a unique factorization domain. Note that $\mathcal{O} = \{x+y\sqrt{-5} \mid x,y \in \mathbf{Z}\}$. We have a decomposition $3\cdot 7 = 21 = (1+2\sqrt{-5})(1-2\sqrt{-5})$. All these factors cannot be factored into a product of two non-units. For example, if $3 = \alpha\beta$ with non-unit α and β, then $9 = N(\alpha)N(\beta)$ and hence $N(\alpha) = 3$ because otherwise β becomes a unit. This is impossible because $5 \bmod 3$ is not a square. Similarly, one can show that 7, $(1+2\sqrt{-5})$ and $(1-2\sqrt{-5})$ are all primes. Obviously, $(1\pm2\sqrt{-5})/3$ and $(1\pm2\sqrt{-5})/7$ are not integers, and hence the prime factorization in $\mathcal{O}$ is not unique.

3. By the Minkowski estimate, there is $0 \ne \alpha \in \mathcal{O}$ such that $1 \le |N(\alpha)| \le |\sqrt{D_F}|\dfrac{2^t d!}{\pi^t d^d}$. Thus $1 < \dfrac{\pi^t d^d}{2^t d!} \le |\sqrt{D_F}|$. There is another way to prove this only using an argument similar to the proof of Lemma 1.2.4: In fact, by the lemma, if $\kappa_1\cdot\cdots\cdot\kappa_d = |\sqrt{D_F}|$, then the set

$$Y(\kappa_1,\ldots,\kappa_d) = \{0 \ne \alpha \in \mathcal{O} \mid |\alpha^{(i)}| \le \kappa_i \text{ for all } i\}$$

is not empty. In particular, for any $\delta > 1$, choosing a small $\varepsilon > 0$ so that $\delta\kappa_1\cdot(\kappa_2-\varepsilon)\cdot\cdots\cdot(\kappa_d-\varepsilon) = |\sqrt{D_F}|$, then $Y(\delta\kappa_1,(\kappa_2-\varepsilon),\ldots,(\kappa_d-\varepsilon)) \ne \varnothing$. By putting

$$X(\kappa_1,\ldots,\kappa_d) = \{0 \ne \alpha \in \mathcal{O} \mid |\alpha^{(i)}| < \kappa_i \text{ for all } i > 1 \text{ and } |\alpha^{(i)}| \le \kappa_i\},$$

we have $X(\delta\kappa_1,\ldots,\kappa_d) \supset Y(\delta\kappa_1,(\kappa_2-\varepsilon),\ldots,(\kappa_d-\varepsilon)) \ne \varnothing$. Then making $\delta \to 1$ and keeping in mind the fact that $X(\kappa_1,\ldots,\kappa_d)$ is a finite discrete set, we conclude that $X(\kappa_1,\ldots,\kappa_d) \ne \varnothing$. Thus for $\alpha \in X(\kappa_1,\ldots,\kappa_d)$, we see that $1 \le |N(\alpha)| < |\sqrt{D_F}|$.

5. For any proper subset S of $\{1,2,\ldots,r+t\}$, interchanging the order of infinite places, we may assume that $\{1,\ldots,r+t-1\} \supset S$. Consider the map $l : \mathcal{O}^\times \to \mathbf{R}^{r+t-1}$ given by $l(\varepsilon) = (\log|\varepsilon^{(i)}|^\delta)$, where $\delta = 1$ or 2 according as (i) is real or complex. Then as shown by Dirichlet's theorem and its proof, $l(\mathcal{O}^\times)$ is a discrete submodule of $\mathbf{R}^{r+t-1}$ and $\mathbf{R}^{r+t-1}/l(\mathcal{O}^\times)$ is compact. Thus for a sufficiently large M, any vector $v \in \mathbf{R}^{r+t-1}$ can be brought into the domain

$$D = \{(x_i) \in \mathbf{R}^{r+t-1} \mid |x_i| < M \text{ for all } i\}$$

by translation by an element of $l(\mathcal{O}^\times)$. We take $v \in \mathbf{R}^{r+t-1}$ so that $v_i = N$ for some $N > 0$ and for $i \in S$ and $v_i = -M$ for $i \in S_0\text{-}S$. Then we pick $\varepsilon \in \mathcal{O}^\times$ so that $v\text{-}l(\varepsilon) \in D$. Then $-M < N\text{-}\log|\varepsilon^{(i)}|^\delta < M$ for $i \in S$ and $-M < -M\text{-}\log|\varepsilon^{(i)}|^\delta < M$, so $\log|\varepsilon^{(i)}|^\delta > N\text{-}M$ for all $i \in S$ and $-2M < \log|\varepsilon^{(i)}|^\delta < 0$ for $i \in S_0\text{-}S$. Thus by making N sufficiently large, we see that $\log|\varepsilon^{(i)}|^\delta > 0$ for all $i \in S$ and $\log|\varepsilon^{(i)}|^\delta < 0$ for $i \in S_0\text{-}S$ and $\sum_{i=1}^{r+t-1}\log|\varepsilon^{(i)}|^\delta > 0$. Thus $|\varepsilon^{(i)}| > 1$ for all $i \in S$ and $|\varepsilon^{(i)}| < 1$ for all $i \notin S \cap S_0$ and $\prod_{i=1}^{r+t-1}|\varepsilon^{(i)}|^\delta > 1$. Since $\prod_{i=1}^{r+t}|\varepsilon^{(i)}|^\delta = |N(\varepsilon)| = 1$, we see that $|\varepsilon^{(r+t)}| < 1$. This shows the desired assertion.

§2.1.

3. (a) Note that if z stays in a compact set inside $\mathbf{C}\text{-}\mathbf{Z}$, we can find a positive integer M such that $\left|\frac{1}{z+n}+\frac{1}{z-n}\right| \le Mn^{-2}$ for all $n > 0$, and hence $\sum_{n=1}^{\infty}\left|\frac{1}{z+n}+\frac{1}{z-n}\right| \le M\zeta(2)$. Thus $\sum_{n=1}^{\infty}\left\{\frac{1}{z+n}+\frac{1}{z-n}\right\}$ converges absolutely and locally uniformly on $\mathbf{C}\text{-}\mathbf{Z}$. Similarly, if z stays in a compact set in $\mathbf{C}\text{-}\mathbf{Z}$, we can find $\varepsilon > 0$ such that $\left|\frac{1}{z+n}\right| > \varepsilon n^{-1}$. Thus $\sum_{n=1}^{m}\left|\frac{1}{z+n}\right| > \varepsilon\sum_{n=1}^{m} n^{-1}$. Since $\sum_{n=1}^{m} n^{-1} > \int_1^{m+1}\frac{1}{x+1}dx \to +\infty$ as $m \to +\infty$, we know the divergence of $\sum_{n=-\infty}^{\infty}\frac{1}{z+n}$ because in an absolutely convergent series, any partial series is also absolutely convergent.

(b) We shall first show the absolute convergence of $\sum_{k=1}^{\infty}\sum_{n=1}^{\infty} n^{-2k}z^{2k-1}$ when $|z| < 1$. We see that $\sum_{k=1}^{\infty}\sum_{n=1}^{\infty}|n^{-2k}z^{2k-1}| \le \sum_{k=1}^{\infty}|\zeta(2k)||z|^{2k-1}$. Note that

$$|\zeta(2k)| \le 1+\int_1^{\infty}x^{-2k}dx = 1+\left[\frac{x^{1-2k}}{1-2k}\right]_1^{\infty} = 1+(2k-1)^{-1} \le 2.$$

Thus

$$\sum_{k=1}^{\infty}\sum_{n=1}^{\infty}|n^{-2k}z^{2k-1}| \le \sum_{k=1}^{\infty}|\zeta(2k)||z|^{2k-1} \le 2\sum_{k=1}^{\infty}|z|^k \le 2\frac{|z|}{1-|z|}.$$

This shows the absolute convergence of $\sum_{k=1}^{\infty}\sum_{n=1}^{\infty} n^{-2k}z^{2k-1}$. Since the limit value of the absolute convergent series does not depend on the order of summation, we know that

$$\sum_{k=1}^{\infty}\sum_{n=1}^{\infty} n^{-2k}z^{2k-1} = \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} n^{-2k}z^{2k-1},$$

which was to be shown.

4. Write $F(x)$ for $\frac{e^x}{1+e^x}$. Then $F(-x) = \frac{e^{-x}}{1+e^{-x}} = \frac{1}{1+e^x} = 1-F(x)$, and we see that $(-1)^m\left(\frac{d}{dx}\right)^m F(x)\big|_{x=0} = \left(\frac{d}{dx}\right)^m F(-x)\big|_{x=0} = -\left(\frac{d}{dx}\right)^m F(x)\big|_{x=0}$ for $m > 0$. Thus if m is even and positive, we see that $\left(\frac{d}{dx}\right)^m F(x)\big|_{x=0} = 0$. Writing $m = 2n$, we know formally, by the functional equation, that

$$\zeta(2n+1) = \frac{(2\pi)^{2n+1}\zeta(-2n)}{2\Gamma(2n+1)\cos(n\pi+(\pi/2))}.$$

Note that $\zeta(s)$ is finite at $s = 2n+1$ but $\cos(n\pi+(\pi/2)) = 0$. Thus $\zeta(-2n)$ has to be 0 for the validity of the above equation. Thus we know that $\zeta(-m) = \left(\frac{d}{dx}\right)^m F(x)\big|_{x=0} = 0$ for even positive integer m.

5. Looking at the expression

$$\Psi(t) = \frac{-\sum_{b=1}^{a}\chi(b)(1+t+t^2+\cdots+t^{b-1})}{1+t+t^2+\cdots+t^{a-1}},$$

we know that $\left(t\frac{d}{dt}\right)^m\Psi(t)$ has the expression

$$\left(t\frac{d}{dt}\right)^m\Psi(t) = \frac{P_m(t)}{(1+t+t^2+\cdots+t^{a-1})^{m+1}}$$

for a polynomial $P_m(t)$ with integer coefficients. This can be proven by induction. Then of course, we have

$$\frac{P_m(t)}{(1+t+t^2+\cdots+t^{a-1})^{m+1}}\Big|_{t=1} \in a^{-m-1}\mathbf{Z}.$$

This shows the result.

6. (b) Suppose p appears in the denominator of $\zeta(1-k)$. Then by Exercise 5, for any integer $a > 1$, $a^k(a^k-1)\zeta(1-k) \in \mathbf{Z}$. Thus if a is prime to p, a^k-1 must be divisible by p, that is, $a^k \equiv 1 \bmod p$. We choose a so that $a \bmod p$ gives the generator of the cyclic group $(\mathbf{Z}/p\mathbf{Z})^\times$. Then $a^k \equiv 1 \bmod p$ if and only if $k \equiv 0 \bmod p-1$.

§2.2.

3. (b) First of all, when $s = 1$,

$$\int_{P(\varepsilon)} G(y)dy = \int_{\partial D(\varepsilon)} G(y)dy = (2\pi i)\mathrm{Res}_{y=0}(G(y)) = 2\pi i.$$

On the other hand, we know that

$$\mathrm{Res}_{s=1}(e^{2\pi is}-1)^{-1} = (2\pi i)^{-1}.$$

Thus by $(e^{2\pi is}-1)\Gamma(s)\zeta(s) = \int_{P(\varepsilon)} G(y)y^{s-1}dy$, we have

$$\mathrm{Res}_{s=1}\zeta(s) = 1.$$

4. (a) By the functional equation, we get

$$\zeta(2n) = \frac{(2\pi)^{2n}B_{2n}}{2(2n)!(-1)^{n+1}}.$$

Since $\zeta(2n) > 0$, we know the signature of B_n.

6. We give the argument for the integral over $Q_l(m)$ since we can treat $Q_r(m)$ in the same way. For z on $Q_l(m)$, $z = -(2m+1)+yi$. Thus $|e^{-z}| = e^{2m+1}$ and $|1-e^{-z}| \geq |e^{-z}|-1 = e^{2m+1}-1$. Therefore

$$|G(z)| \leq \frac{e^{2m+1}}{e^{2m+1}-1} \leq 2 \text{ on } Q_l(m) \text{ if } m > 0.$$

This gives an estimate:

$$\left|\int_{Q_l(m)} G(z)z^{s-1}dz\right| = \left|\int_{-(2m+1)\pi}^{(2m+1)\pi} G(-(2m+1)+yi)(-(2m+1)+yi)^{s-1}dy\right|$$

$$\leq 2\int_{-(2m+1)\pi}^{(2m+1)\pi} |-(2m+1)+yi|^{\sigma-1}dy \leq 2\int_{-(2m+1)\pi}^{(2m+1)\pi} ((2m+1)^2+y^2)^{(\sigma-1)/2}dy$$

$$\leq 2(2m+1)^{\sigma-1}\int_{-(2m+1)\pi}^{(2m+1)\pi} dy$$

$$\leq 4\pi(2m+1)^{\sigma} \to 0 \text{ as } m \to +\infty \text{ (if } \sigma = \mathrm{Re}(s) < 0).$$

§2.3.

4. By Corollary 2, $L(1-n,\chi^{-1}) = 0$ if $\chi(-1) = 1$ and $L(1-n,\chi^{-1})$ is finite otherwise. Then by the functional equation

$$L(s,\chi) = \begin{cases} \dfrac{G(\chi)(2\pi/N)^s L(1-s,\chi^{-1})}{2\Gamma(s)\cos(\pi s/2)} & \text{if } \chi(-1) = 1, \\[2ex] \dfrac{G(\chi)(2\pi/N)^s L(1-s,\chi^{-1})}{2\sqrt{-1}\Gamma(s)\sin(\pi s/2)} & \text{if } \chi(-1) = -1, \end{cases}$$

if $\chi(-1) = -1$, $\Gamma(s)\sin(\pi s/2)$ is finite at $s = 1$ and hence $L(s,\chi)$ is finite at $s = 1$ and if $\chi(-1) = 1$, the simple zero of $\Gamma(s)\cos(\pi s/2)$ is canceled out by the zero of $L(1-s,\chi^{-1})$ at $s = 1$ and hence $L(s,\chi)$ is finite at $s = 1$.

5. Since the argument is essentially the same in the two cases where $\chi(-1) = \pm 1$, we only treat the case of $\chi(-1) = 1$. Then by the functional equation, we see that

$$G(\chi) = \frac{2\Gamma(s)\cos(\pi s/2)L(s,\chi)}{(2\pi/N)^s L(1-s,\chi^{-1})}.$$

Expanding $L(s,\chi) = \sum_{n\geq m} a_m(s-\frac{1}{2})^n$ with $a_m \neq 0$, we see that

$$L(s,\chi^{-1}) = \overline{L(\bar{s},\chi)} = \Sigma_{n\geq m}\,\bar{a}_m(s-\tfrac{1}{2})^n \quad \text{and} \quad G(\chi)G(\chi^{-1}) = \frac{2\Gamma(\frac{1}{2})^2|a_m|^2}{(2\pi/N)(-1)^{2m}|a_m|^2}.$$

Applying the functional equation for the Riemann zeta function (i.e. replacing $G(\chi)$ by 1 and χ by the trivial character in the above formula), we know that $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ because $\Gamma(\frac{1}{2}) > 0$ and hence $G(\chi)G(\chi^{-1}) = N = \chi(-1)N$. When χ is real valued, $\chi^{-1} = \chi$, $a_m \in \mathbf{R}$ and by the above formula, we see that $G(\chi) = (-1)^m\sqrt{N}$. Thus if the order of zero at $\frac{1}{2}$ is even (in particular if $L(\frac{1}{2},\chi) \neq 0$), we know that $G(\chi) = \sqrt{N} = \sqrt{\chi(-1)N}$.

§2.4.

1. (a) For $a = |a|e^{i\theta} \in H'$ ($|\theta| < \frac{\pi}{2}$) and $s = \sigma+i\tau$ ($\sigma,\tau \in \mathbf{R}$), we see that $|a^{-s}|^2 = a^{-s}(\bar{a})^{-\bar{s}} = |a|^{-2\sigma}e^{2\theta\tau}$. Thus if s stays in a compact subset of $\mathbf{C}$, then $|a^{-s}| \leq M|a|^{-2\mathrm{Re}(s)}$ for a positive constant M independent of a. When A is not real, then

$$\begin{aligned}
&|L^*(n+x)^{-s}| \\
&\quad\leq M\Pi_{i=1}^m |\mathrm{Re}(a_{1i}(n_1+x_1)+\cdots+a_{ri}(n_r+x_r))+\mathrm{Im}(a_{1i}(n_1+x_1)+\cdots+a_{ri}(n_r+x_r))|^{-\sigma_i} \\
&\qquad\leq M\Pi_{i=1}^m |\mathrm{Re}(a_{1i}(n_1+x_1)+\cdots+a_{ri}(n_r+x_r)))|^{-\sigma_i} \text{ if } \sigma_i > 0.
\end{aligned}$$

Thus we may assume that A is real by replacing A by $\mathrm{Re}(A)$. When A is a real matrix, let $M > 0$ be the minimum of all entries of A. Then

$$\begin{aligned}
|L^*(n+x)^{-s}| &= \Pi_{i=1}^m(a_{1i}(n_1+x_1)+\cdots+a_{ri}(n_r+x_r))^{-\sigma_i} \\
&\leq \Pi_{i=1}^m(M(n_1+x_1)+\cdots+M(n_r+x_r))^{-\sigma_i} \leq M^{-\mathrm{Tr}(\sigma)}\Pi_{i=1}^m(n_1+\cdots+n_r))^{-\sigma_i}
\end{aligned}$$

if $\sigma_i > 0$ and not all n_i are zero (if σ_i is negative, then replacing M by the maximum of the entries of A, we can deduce a similar inequality). Thus we may assume that all the entries of A are equal to 1, $x_i = 1$ for all i and $\chi_i = 1$ for all i. Then

$$|\zeta(s,A,x,\chi)| \leq \Sigma_{n\in \mathbf{Z}_+^r}(n_1+\cdots+n_r)^{-\mathrm{Tr}(\sigma)}.$$

We see easily that $\#\{(n_1,\ldots, n_r) \in \mathbf{Z}_+^r \mid n_1+\cdots+n_r = k\} \leq Ck^{r-1}$ for a positive constant C and hence

$$\Sigma_{n\in \mathbf{Z}_+^r}(n_1+\cdots+n_r)^{-\mathrm{Tr}(\sigma)} \leq C\Sigma_{k=1}^\infty k^{r-1-\mathrm{Tr}(\sigma)} = C\zeta(\mathrm{Tr}(\sigma)-r+1).$$

Since the Riemann zeta function $\zeta(s)$ converges if $\mathrm{Re}(s) > 1$, $\zeta(s,A,x,\chi)$ converges if $\mathrm{Re}(\mathrm{Tr}(s)) > r$ and $\mathrm{Re}(s_i) > 0$ for all i.

(b) It is sufficient to show that

$$B(r,k) = \#\{(n_1,\dots, n_r) \in \mathbf{Z}_+^{\,r} \mid n_1+\cdots+n_r = k\} \geq ck^{r-1}$$

for a positive constant c, because then

$$c\zeta(\mathrm{Tr}(\sigma)-r+1) \leq \textstyle\sum_{n\in \mathbf{Z}_+^{\,r}}(n_1+\cdots+n_r)^{-\mathrm{Tr}(\sigma)}.$$

We see easily that $B(2,k) = k+1$ and hence we can take 1 as c in this case. Supposing that $B(r-1,k) \geq ck^{r-2}$ for some $c > 0$, we prove the assertion for r. We see easily that

$$B(r,k) = \textstyle\sum_{j=0}^{k}B(r-1,j) > c\sum_{j=0}^{k}j^{r-2} \geq c\int_0^k x^{r-2}dx = \dfrac{ck^{r-1}}{r-1},$$

which shows the desired assertion.

3. We have

$$(e^{4\pi is}-1)(e^{2\pi is}-1)\Gamma(s)^2\zeta((s,s),A,x,(1,1))$$
$$= \int_{P(\varepsilon)}\int_{P(\varepsilon,1)}G_1(u,t)u^{2s-1}t^{s-1}dudt + \int_{P(\varepsilon)}\int_{P(\varepsilon,1)}G_2(u,t)u^{2s-1}t^{s-1}dudt,$$

where

$$G_1(u,t) = \frac{\exp(-x_1u(a+bt))}{1-\exp(-u(a+bt))} \times \frac{\exp(-x_2u(c+dt))}{1-\exp(-u(c+dt))},$$
$$G_2(u,t) = \frac{\exp(-x_1u(at+b))}{1-\exp(-u(at+b))} \times \frac{\exp(-x_2u(ct+d))}{1-\exp(-u(ct+d))}.$$

Since $\dfrac{e^{-xz}}{1-e^{-z}} = \sum_{m=0}^{\infty}(-1)^mB_m(x)\dfrac{z^{m-1}}{m!}$ and

$$\lim_{s\to 1-n}(e^{4\pi is}-1)(e^{2\pi is}-1)\Gamma(s)^2 = \frac{2\cdot(2\pi i)^2}{((n-1)!)^2},$$

we see that

$\dfrac{2\cdot(2\pi i)^2}{((n-1)!)^2}\zeta((1-n,1-n))$ = the coefficient of $u^{2(n-1)}t^{n-1}$ of

$$(2\pi i)^2\{\textstyle\sum_{k=0}^{\infty}(-1)^kB_k(x_1)\dfrac{(u(a+bt))^{k-1}}{k!} \times \sum_{j=0}^{\infty}(-1)^jB_j(x_2)\dfrac{(u(c+dt))^{j-1}}{j!}$$
$$+ \textstyle\sum_{k=0}^{\infty}(-1)^kB_k(x_1)\dfrac{(u(at+b))^{k-1}}{k!} \times \sum_{j=0}^{\infty}(-1)^jB_j(x_2)\dfrac{(u(ct+d))^{j-1}}{j!}\}$$

= the coefficient of t^{n-1} of

$$(2\pi i)^2\textstyle\sum_{k+j=2n,\ k\geq 0,\ j\geq 0}(-1)^{k+j}\dfrac{B_k(x_1)B_j(x_2)}{k!j!}\{(a+bt)^{k-1}(c+dt)^{j-1}+(at+b)^{k-1}(ct+d)^{j-1}\}$$

$$= (2\pi i)^2\textstyle\sum_{k+j=2n,\ k\geq 0,\ j\geq 0}(-1)^{k+j}\dfrac{B_k(x_1)B_j(x_2)}{k!j!}$$

$$\times\{\textstyle\sum_{\alpha+\beta=n-1,\ \alpha\geq 0,\ \beta\geq 0}\binom{k-1}{\alpha}\binom{j-1}{\beta}(b^\alpha d^\beta a^{k-1-\alpha}c^{j-1-\beta}+a^\alpha c^\beta b^{k-1-\alpha}d^{j-1-\beta})\},$$

where we have used the binomial formula

$$(X+Y)^s = \textstyle\sum_{n=0}^{\infty}\binom{s}{n}Y^nX^{s-n}$$

for $\binom{s}{n} = \begin{cases} 1 & \text{if } n = 0, \\ \dfrac{s(s-1)\cdot\cdots\cdot(s-n+1)}{n!} & \text{if } n > 0 \end{cases}$ (in particular, $\binom{-1}{n} = (-1)^n$).

Therefore, the final formula is

$$\zeta((1\text{-}n,1\text{-}n),x,\begin{pmatrix} a & b \\ c & d \end{pmatrix},(1,1)) = 2^{-1}(n-1)!^2\Sigma_{k+j=2n,\ k\geq 0,\ j\geq 0}(-1)^{k+j}\frac{B_k(x_1)B_j(x_2)}{k!j!}$$
$$\times\{\Sigma_{\alpha+\beta=n-1,\ \alpha\geq 0,\ \beta\geq 0}\binom{k-1}{\alpha}\binom{j-1}{\beta}(b^\alpha d^\beta a^{k-1-\alpha}c^{j-1-\beta}+a^\alpha c^\beta b^{k-1-\alpha}d^{j-1-\beta})\}$$

§2.5.

2. Let a and m be two ideals in O, and first show that there is $\alpha \in O$ such that $\alpha O = ab$ and b is prime to m. Write $m = p_1^{e_1}\cdot\cdots\cdot p_r^{e_r}$ ($e_i > 0$). Put $c = ap_1p_2\cdot\cdots\cdot p_r$ and $c_i = c/p_i$. Then $c_i \supset c$, and the two ideals are distinct. Thus we can find $\alpha_i \in c_i\text{-}c$. Then α_i is in ap_j for $j \neq i$ but is not contained in ap_i. If α is in ap_i, then α_i belongs to ap_i because all other α_j ($j \neq i$) are inside ap_i, a contradiction. Thus $\alpha = \alpha_1+\cdots+\alpha_r$ is not contained in ap_i for all i. Since $\alpha \in a$, we can write $\alpha O = ab$ and b is prime to m. Now, fixing a class C of ideals, we show that there exists an ideal $d \in$ C such that d is prime to a given ideal m. In fact, d can be taken inside O. First take an integral ideal c in the class C and write $c = c_0c'$ so that the prime factors of c_0 consists of those of m and c' is prime to m. Take arbitrary $0 \neq \gamma \in c_0$ and decompose $\gamma O = ac_0$. By the above argument, we can find $\alpha \in O$ such that $\alpha O = ab$ and b is prime to m. Then

$$\frac{\alpha}{\gamma}c = \frac{abc}{ac_0} = bc'$$

and the integral ideal $d = bc'$ is prime to m and in the same class C as c.

3. Let C be the class of m^{-1} and take an integral ideal b in C prime to m (We have used Exercise 2). Then $bm = \gamma O$, because bm is in the principal class.

4. (b) Consider the module $\mathbf{Z}^2$ which we consider to be made of row integer vectors. Then, for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$,

$$(m,n) \mapsto (m,n)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ma+nc,\ mb+nd)$$

induces an automorphism of $\mathbf{Z}^2$ whose inverse is given by α^{-1} (α^{-1} again has integer entries). In particular, if $\alpha \in \Gamma(N)$, α obviously induces an automorphism of the set $(a,b)+N\mathbf{Z}^2$. On the other hand, we see that

$$(m\alpha(z)+n) = m\frac{az+b}{cz+d} + n = (cz+d)^{-1}((ma+nc)z+(mb+nd)).$$

Thus $E_{k,N}(\alpha(z),s;a,b) = \Sigma_{(m,n)\in(a,b)+\mathbf{Z}^2}(m\alpha(z)+n)^{-k}\,|(m\alpha(z)+n)|^{-2s}$

$$= \sum_{(m,n)\in((a,b)+Z^2)\alpha} (mz+n)^{-k}\,|(mz+n)|^{-2s}(cz+d)^k\,|cz+d|^{2s}$$
$$= \sum_{(m,n)\in((a,b)+Z^2)} (mz+n)^{-k}\,|(mz+n)|^{-2s}(cz+d)^k\,|cz+d|^{2s}$$
$$= E_{k,N}(z,s;a,b)(cz+d)^k\,|cz+d|^{2s} \text{ for } \alpha\in\Gamma(N).$$

Thus $E_{k,N}(z,s;a,b)$ is a modular form on $\Gamma(N)$ of weight (k,s).

§2.6.

1. We have a non-trivial unit ε such that $0<\varepsilon<1<\varepsilon^\sigma$. Then if $\chi : I(m)\to \mathbf{C}^\times$ is an ideal character such that $\chi((\alpha)) = \alpha^k\alpha^{\sigma m}$, then

$$\alpha^k\alpha^{\sigma m} = \chi((\alpha)) = \chi((\varepsilon\alpha)) = (\varepsilon\alpha)^k(\varepsilon\alpha)^{\sigma m}.$$

Thus $\varepsilon^k\varepsilon^{\sigma m} = 1$. By taking logarithms of both sides, we see that $k\log(\varepsilon) + m\log(\varepsilon^\sigma) = 0$, which yields $k\log(\varepsilon) = m\log(\varepsilon)$ because $\varepsilon\varepsilon^\sigma = 1$. Since $\log(\varepsilon)\neq 0$, we know that $k = m$.

3. Writing h for the class number of $\mathbf{Q}(\sqrt{-p})$ and $\chi(a) = \left(\frac{a}{p}\right)$, we have $\sum_{a=1}^{p-1}\chi(a)a = -hp$. Since $p\equiv 3 \bmod 4$, $\chi(-1) = -1$, $\chi(p-a) = -\chi(a)$ and

$$\sum_{a=1}^{p-1}\chi(a)a = \sum_{a=1}^{(p-1)/2}\{\chi(a)a+\chi(p-a)(p-a)\} = 2\sum_{a=1}^{(p-1)/2}\chi(a)a - p\sum_{a=1}^{(p-1)/2}\chi(a) = -hp.$$

Similarly

$$\sum_{a=1}^{p-1}\chi(a)a = \sum_{a=1}^{(p-1)/2}\chi(2a)2a + \sum_{a=1}^{(p-1)/2}\chi(p-2a)(p-2a)$$
$$= 4\sum_{a=1}^{(p-1)/2}\chi(2a)a - p\sum_{a=1}^{(p-1)/2}\chi(2a)$$
$$= 4\chi(2)\{\sum_{a=1}^{(p-1)/2}\chi(a)a - p\sum_{a=1}^{(p-1)/2}\chi(a)\} = -hp.$$

Thus combining the above two formula, we have

$$0 < h = \frac{1}{2-\chi(2)}\sum_{a=1}^{(p-1)/2}\chi(a) = \frac{1}{2-\chi(2)}(A-B),$$

where A (resp. B) is the number of quadratic residues (resp. non-residues) modulo p between 1 and $\frac{p}{2}$. By the quadratic reciprocity law, $\chi(2) = 1$ or -1 according as $p\equiv 7$ or $3 \bmod 8$. This shows (1) and (2).

§3.5.

1. We know from (1a) that $\int\binom{x}{n}d\mu_\varphi = (\partial_n\Phi_\varphi)\,|_{T=0}$. We write $x^m = \sum_{j=0}^m c_j\binom{x}{j}$ with $c_j\in\mathbf{Z}$. Then $\left(t\frac{d}{dt}\right)^m = \sum_{j=0}^m c_j\partial_j$ since $\partial_n = \binom{t\frac{d}{dt}}{n}$. This shows

$$\int x^m d\mu_\varphi = \sum_{j=0}^m c_j\int\binom{x}{j}d\mu_\varphi = \sum_{j=0}^m c_j\partial_j\Phi_\varphi\,|_{T=0} = (\left(t\tfrac{d}{dt}\right)^m\Phi_\varphi)(0).$$

2. By (2b), we see that

$$\Phi_{\varphi*\psi}(t-1) = \int t^x d(\varphi*\psi)(x) = \iint t^{x+y} d\varphi(x)d\psi(y)$$
$$= \iint t^{x+y} d\varphi(x)d\psi(y) = \int t^x d\varphi(x) \int t^y d\psi(y) = \Phi_\varphi(t-1)\Phi_\psi(t-1).$$

3. We know that $\mathbf{Z}_p[T]]$ is the completion of R under the m-adic topology for $m = (p,T)$ $(T = t-1)$. Thus $R = \mathbf{Z}_p[[T]] \cap \mathbf{Q}_p(t)$, where the intersection is taken in the quotient field of $\mathbf{Z}_p[[T]]$. Since $\mathbf{Z}_p[[T]] \cong \mathcal{M}eas(\mathbf{Z}_p;\mathbf{Z}_p)$, the operator $[\phi]$ preserves $\mathbf{Z}_p[[T]]$ for any locally constant function ϕ on $\mathbf{Z}_p$ having values in $\mathbf{Z}_p$, because the operation $[\phi] : d\mu \mapsto \phi d\mu$ preserves the measure space. On the other hand, by definition $[\phi]$ preserves $\mathbf{Q}_p(t)$. Thus $[\phi]$ preserves the intersection R.

§3.6.

1.(ii). By definition, $R_\varphi = R/\varphi(\mathrm{Ker}(e'))R$. Thus we have a sequence of groups:

$$\begin{array}{ccccccc} 0 \to & \mathrm{Hom}_{A\text{-alg}}(R_\varphi,S) & \xrightarrow{\pi^*} & \mathrm{Hom}_{A\text{-alg}}(R,S) & \xrightarrow{\varphi^*} & \mathrm{Hom}_{A\text{-alg}}(R',S) \\ & \| & & \| & & \| \\ 0 \longrightarrow & \mathrm{Ker}(\varphi^*)(S) & \xrightarrow{\pi^*} & G(S) & \xrightarrow{\varphi^*} & G(S), \end{array}$$

where $\pi : R \to R_\varphi$ is the projection map. The injectivity of π^* follows from the surjectivity of π. An algebra homomorphism $\phi : R \to S$ is in $\mathrm{Ker}(\varphi^*)$ if and only if the following diagram is commutative:

$$\begin{array}{ccc} R' & \xrightarrow{\varphi} & R \\ \downarrow e' & & \downarrow \phi \\ A & \to & S. \end{array}$$

Thus $\phi \in \mathrm{Ker}(\varphi^*) \Leftrightarrow \varphi(\mathrm{Ker}(e')) \subset \mathrm{Ker}(\phi) \Leftrightarrow \phi$ induces $\phi' : R_\varphi \to S$ such that $\pi^*\phi' = \phi$. This shows the exactness at G(S).

§8.1.

1. Since the adele ring F_A is the restricted direct product with respect to $\mathcal{O}_v$, for v outside m, we can consider an adele a in $\hat{\mathcal{O}}(m)$ whose v component is 1 for almost all v and is ϖ_v-1 for some finite number of places v outside m, where ϖ_v is a prime element of $\mathcal{O}_v$. Then 1+a in $1+\hat{\mathcal{O}}(m)$ has ϖ_v for some finite number of places. On the other hand, the v-component of any idele in $\hat{\mathcal{O}}(m)^\times$ is a unit in $\mathcal{O}_v$ for all finite places. Thus $1+a \notin \hat{\mathcal{O}}(m)^\times$.

§8.2.

1. If $x_n \in F_A{}^\times$ converges to x, then for sufficiently large n, $(x_n x^{-1})_f$ falls in the neighborhood $U(m)$. Thus $\lambda((x_n)_f) = \lambda(x_f)$. On the other hand, $\lambda((x_n)_\infty) = (x_n)_\infty{}^\xi$ is a polynomial function on the vector space

$$F_\infty = \prod_{v \text{ real}} \mathbf{R} \times \prod_{v \text{ complex}} \mathbf{C} \quad (1.1.5b),$$

which is obviously continuous. Thus $\lim_{n\to\infty}\lambda((x_n)_\infty) = \lambda(x_\infty)$ and hence $\lim_{n\to\infty}\lambda(x_n) = \lambda(x)$. That is, λ is continuous.

3. (i) Since $\mathrm{Cl}(m)$ is a finite group, if one writes h for its order, for any ideal a prime to m, $a^h = \alpha O$ for $\alpha \in P(m)$. Thus $\lambda^*(a)^h = \lambda^*(\alpha O) = \alpha^\xi$, which is contained in the Galois closure Φ of F over $\mathbf{Q}$. Thus $\lambda(a)$ is always algebraic. If $\{a_i\}_{i=1,\dots,h}$ is a representative of classes modulo m, then any a can be written as αa_i for one of the a_i's. In particular,

$$\lambda(a) = \alpha^\xi\lambda(a_i) \in K = \Phi(\lambda(a_i) \mid i=1,\dots, h).$$

The field K is generated over Φ by finitely many algebraic numbers and hence is a number field. Since $\lambda(x) = \lambda^*(xO)$ for $x \in F_A(m)$, we know that $\lambda(x)$ is contained in a number field K independent of $x \in F_A(m)$.

(ii) This follows from (1.3.4b).

(iii) (A. Weil) Writing $x = \alpha u a x_\infty \in F_A^\times$ for $\alpha \in F^\times$, $u \in U(m)$, $a \in F_A(mp)$ and $x_\infty \in F_{\infty+}$, we define $\lambda_p(x) = \lambda^*(aO)u_p^{-\xi}$, where u_p is the projection of u to $\prod_{v|p}F_v^\times$. If there are two expressions $\alpha u a x_\infty = \alpha' u' a' x'_\infty$, then $\alpha_p u_p = \alpha'_p u'_p$ because $(ax_\infty)_p = (a'x'_\infty)_p = 1$. On the other hand,

$$\alpha'^{-1}\alpha = u'u^{-1}a'a^{-1}x'_\infty x_\infty^{-1} \in U(mp)F_A(mp)F_{\infty+}\cap F^\times = P(mp).$$

Thus $a'O = \alpha'^{-1}\alpha a O$ and we see that

$$\begin{aligned}\lambda^*(a'O)u'^{-\xi}_p &= \lambda^*(\alpha'^{-1}\alpha a O)u'^{-\xi}_p = \lambda^*(aO)\alpha'^{-\xi}\alpha^\xi u'^{-\xi}_p \\ &= \lambda^*(aO)\alpha'^{-\xi}\alpha^\xi\alpha'^{\xi}_p\alpha_p^{-\xi}u_p^{-\xi} = \lambda^*(aO)u_p^{-\xi}.\end{aligned}$$

Thus the character λ_p is well defined. The continuity can be verified as in Exercise 1 replacing F_∞ by F_p in the argument there.

§8.3.

1. Suppose that $\alpha_n : K \to T$ is a sequence of continuous homomorphisms with $\alpha_n(x) = \psi(y_n x)$ for $y_n \in K$ and that α_n converges locally uniformly to α. We want to show that y_n converges to $y \in K$ given by $\alpha(x) = \psi(yx)$ for all $x \in K$. Since α_n converges to α, for any given $m > 0$, α_n-α has values in I_1 on $\pi^{-m}O_v$ for sufficiently large n and hence by Lemma 1, $\alpha_n = \alpha$ on $\pi^{-m}O_v$. If $\pi^r O_v$ is the different of ψ, then $\alpha_n = \alpha$ on $\pi^{-m}O_v$ means that $y_n - y \in \pi^{m-r}O_v$ and hence making m large, we know that y_n converges to y in K. Conversely, if y_n converges to y in K, then reversing the above argument, we know that α_n converges to α. Thus the isomorphism of Proposition 1 is also the topological isomorphism.

§8.5.

1. (ii) Note that $a+p_v^i = a(1+a^{-1}\varpi^i O_v)$ and thus by definition,

$$\mu_v^\times(a+p_v^i) = \left|\frac{\varpi^i}{a}\right|_v (1-\frac{1}{N(p_v)})^{-1} = (1-\frac{1}{N(p_v)})^{-1}|a|_v^{-1}\mu_v(a+p_v^i) \text{ if } |a|_v \geq |\varpi^i|_v.$$

Therefore, for any locally constant function ϕ factoring through $(\mathcal{O}_v/p_v^i)^\times$,

$$\int_{\mathcal{O}_v}\phi d\mu^\times = \sum_{a\in(O_v/p_v^i)^\times}\phi(a)|a|_v^{-1}\mu_v(a+p_v^i) = (1-N(p_v)^{-1})^{-1}\int_{\mathcal{O}_v}\phi(x)|x|_v^{-1}d\mu(x).$$

Any locally constant function on $\mathcal{O}_v^\times$ is of the above form for sufficiently large i and therefore the above formula is true for any locally constant functions on $\mathcal{O}_v^\times$. The formula holds even on $F_v^\times$ because $F_v^\times = \bigcup_i \varpi^i\mathcal{O}_v^\times$.

(iii). By the above formula, $|x|_v^{-1}d\mu(x)$ gives a multiplicative Haar measure. Therefore $\int_{F_v}\phi(ax)|x|_v^{-1}d\mu(x) = \int_{F_v}\phi(x)|x|_v^{-1}d\mu(x)$ for any locally constant function ϕ. Any locally constant function ϕ can be written $\phi(x) = f(x)|x|_v$ for another locally constant function f, and the correspondence $\phi \mapsto f$ is bijective on the space of locally constant functions. Replacing ϕ by $f(x)|x|_v$ in the above formula, we see that

$$|a|_v\int_{F_v}f(ax)d\mu(x) = \int_{F_v}f(ax)|a|_v d\mu(x) = \int_{F_v}f(x)d\mu(x),$$

which proves the assertion.

§8.6.

1. Using the fact that $F_A^\times/F^\times = F_A^{(1)}/F^\times\times\mathbf{R}_{>0}$ via $x \mapsto (x_f(\frac{x_\infty}{|x|_A^{1/[F:Q]}}), |x|_A)$ (where $\mathbf{R}_{>0} = \{x \in \mathbf{R} \mid x > 0\}$), we can write $\lambda(x) = \lambda_1(x)\lambda_2(x)$ for characters λ_1 of $F_A^{(1)}/F^\times$ and λ_2 of $\mathbf{R}_{>0}$. Since $F_A^{(1)}/F^\times$ is compact (Theorem 1.1), λ_1 must have values in $\mathbf{T}$, which is the unique maximal compact subgroup of $\mathbf{C}^\times$ (in fact $\mathbf{C}^\times = \mathbf{T}\times\mathbf{R}_{>0}$). Any continuous linear map of $\mathbf{R}$ into $\mathbf{C}$ is given by $t \mapsto \alpha t$ with $\alpha \in \mathbf{C}$. By identifying $\mathbf{R}$ with $\mathbf{R}_{>0}$ via "exp", any continuous multiplicative map of $\mathbf{R}_{>0}$ into $\mathbf{C}^\times$ is given by $x \mapsto x^s$ with $s \in \mathbf{C}$. Thus $|\lambda(x)| = |\lambda_2(x)| = |x|_A^s$ for some $s \in \mathbf{C}$.

2. Let χ be as in the exercise. We see in the same manner as above that $|\chi(x)| = |x|^s$ for some $s \in \mathbf{C}$. Thus by taking $\chi/|\chi|$ instead of χ, we may assume that χ has values in $\mathbf{T}$. We already know that $\mathrm{Hom}_{\mathrm{cont}}(\mathbf{R}_{>0},\mathbf{T}) \cong \mathbf{R}$ (assigning $\alpha \in \mathbf{R}$ to the character $x \mapsto x^{i\alpha}$) and $\mathrm{Hom}_{\mathrm{cont}}(\mathbf{T},\mathbf{T}) \cong \mathbf{Z}$ (assigning $n \in \mathbf{Z}$ to the character $x \mapsto x^n$). Since $\mathbf{C}^\times = \mathbf{T}\times\mathbf{R}_{>0}$ via $x \mapsto (x/|x|, |x|)$, we thus see from this that χ has the desired form.

3. For any standard function Φ_f on F_{A_f}, we can find a rational number $N \neq 0$ and real number M such that $|\Phi_f(x)| \leq M|\Psi_f(Nx)|$ for the characteristic function Ψ_f of $\mathbf{Z}_f$. Thus we may assume that $\Phi = \Phi_f\Phi_\infty$ and that Φ_f is the characteristic function of $\mathbf{Z}_f$. We may also assume that $\Phi_\infty(x) = x^k\exp(-\pi x^2)$ for $0 \leq k \in \mathbf{Z}$. Then for $\xi \in \mathbf{Q}$, $\Phi(\xi) \neq 0$ if and only if $\xi \in \mathbf{Z}$. This shows that $\sum_{\xi\in\mathbf{Q}} \Phi(\xi) = \sum_{n\in\mathbf{Z}} n^k\exp(-\pi n^2)$, whose convergence is obvious from the convergence of geometric series $\sum_{n=1}^{\infty}\exp(-\pi n)$ and its derivatives $\sum_{n=1}^{\infty} n^k\exp(-\pi n)$.

§9.1.

2. Since $\chi : \mathrm{Cl}(m) = \mathbf{A}_F^\times/F^\times U(m)F_{\infty+} \to \mathbf{T}$, $\chi_v(\mathcal{O}_v^\times) = 1$ if v is outside m and $\chi(F^\times) = 1$. If $\varepsilon \in \mathcal{O}^\times$, then $\varepsilon \in \mathcal{O}_v^\times$ for all finite v. Thus

$$1 = \chi(\varepsilon) = (\textstyle\prod_{v\,|\,m}\chi_v(\varepsilon))\chi_\infty(\varepsilon) = (\prod_{v\,|\,m}\chi_v(\varepsilon))(N(\varepsilon)/|N(\varepsilon)|)^k.$$

Therefore $\prod_{v\,|\,m}\chi_v(\varepsilon) = \left(\dfrac{N(\varepsilon)}{|N(\varepsilon)|}\right)^k$ for all $\varepsilon \in \mathcal{O}^\times$. In particular, if $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B_\infty$, then $d \in \mathcal{O}^\times$. Thus $\chi^*\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = \left(\dfrac{N(d)}{|N(d)|}\right)^k$. On the other hand, $j(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}x_\infty, \mathbf{i})^k = \left(\dfrac{N(d)}{|N(d)|}\right)^k$. Hence we have

$$\chi^*\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}x\right)j(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}x_\infty, \mathbf{i})^k = \chi^*(x)j(x_\infty, \mathbf{i})^k \text{ for } \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B_\infty.$$

Index