Graduate Texts in Mathematics

听雨尘心@含藏识

GTM 系列电子书下载

Springer 版权所有

仅供学习，请支持正版书籍

http://realking1980.bokee.com

Lawrence C. Washington

Introduction to Cyclotomic Fields

Springer-Verlag
New York Heidelberg Berlin

Lawrence C. Washington

Department of Mathematics
University of Maryland
College Park, MD 20742
U.S.A.

Editorial Board

P. R. Halmos
Managing Editor
Indiana University
Department of
Mathematics
Bloomington, IN 47401
U.S.A.

F. W. Gehring
University of Michigan
Department of
Mathematics
Ann Arbor, MI 48104
U.S.A.

C. C. Moore
University of California
at Berkeley
Department of
Mathematics
Berkeley, CA 94720
U.S.A.

AMS Subject Classifications (1980): 12-01

Library of Congress Cataloging in Publication Data

Washington, Lawrence C.
Introduction to cyclotomic fields.

(Graduate texts in mathematics; 83)
Bibliography: p.
Includes index.
1. Fields, Algebraic. 2. Cyclotomy. I. Title.
II. Series.
QA247.W35 512′.3 82-755
AACR2

© 1982 by Springer-Verlag New York Inc.
All rights reserved. No part of this book may be translated or reproduced in any form without written permission from Springer-Verlag, 175 Fifth Avenue, New York, New York 10010, U.S.A.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-90622-3 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90622-3 Springer-Verlag Berlin Heidelberg New York

To My Parents

Preface

This book grew out of lectures given at the University of Maryland in 1979/1980. The purpose was to give a treatment of p-adic L-functions and cyclotomic fields, including Iwasawa's theory of $\mathbb{Z}_p$-extensions, which was accessible to mathematicians of varying backgrounds.

The reader is assumed to have had at least one semester of algebraic number theory (though one of my students took such a course concurrently). In particular, the following terms should be familiar: Dedekind domain, class number, discriminant, units, ramification, local field. Occasionally one needs the fact that ramification can be computed locally. However, one who has a good background in algebra should be able to survive by talking to the local algebraic number theorist. I have not assumed class field theory; the basic facts are summarized in an appendix. For most of the book, one only needs the fact that the Galois group of the maximal unramified abelian extension is isomorphic to the ideal class group, and variants of this statement.

The chapters are intended to be read consecutively, but it should be possible to vary the order considerably. The first four chapters are basic. After that, the reader willing to believe occasional facts could probably read the remaining chapters randomly. For example, the reader might skip directly to Chapter 13 to learn about $\mathbb{Z}_p$-extensions. The last chapter, on the Kronecker–Weber theorem, can be read after Chapter 2.

The notations used in the book are fairly standard; $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, and $\mathbb{Q}_p$ denote the integers, the rationals, the p-adic integers, and the p-adic rationals, respectively. If A is a ring (commutative with identity), then $A^\times$ denotes its group of units. At Serge Lang's urging I have let the first Bernoulli number be $B_1 = -\frac{1}{2}$ rather than $+\frac{1}{2}$. This disagrees with Iwasawa [23] and several of my papers, but conforms to what is becoming standard usage.

Throughout the preparation of this book I have found Serge Lang's two volumes on cyclotomic fields very helpful. The reader is urged to look at them for different viewpoints on several of the topics discussed in the present volume and for a different selection of topics. The second half of his second volume gives a nice self-contained (independent of the remaining one and a half volumes) proof of the Gross–Koblitz relation between Gauss sums and the p-adic gamma function, and the related formula of Ferrero and Greenberg for the derivative of the p-adic L-function at 0, neither of which I have included here. I have also omitted a discussion of explicit reciprocity laws. For these the reader can consult Lang [4], Hasse [2], Henniart, Ireland–Rosen, Tate [3], or Wiles [1].

Perhaps it is worthwhile to give a very brief history of cyclotomic fields. The subject got its real start in the 1840s and 1850s with Kummer's work on Fermat's Last Theorem and reciprocity laws. The basic foundations laid by Kummer remained the main part of the theory for around a century. Then in 1958, Iwasawa introduced his theory of $\mathbb{Z}_p$-extensions, and a few years later Kubota and Leopoldt invented p-adic L-functions. In a major paper (Iwasawa [18]), Iwasawa interpreted these p-adic L-functions in terms of $\mathbb{Z}_p$-extensions. In 1979, Mazur and Wiles proved the Main Conjecture, showing that p-adic L-functions are essentially the characteristic power series of certain Galois actions arising in the theory of $\mathbb{Z}_p$-extensions.

What remains? Most of the universally accepted conjectures, in particular those derived from analogy with function fields, have been proved, at least for abelian extensions of $\mathbb{Q}$. Many of the conjectures that remain are probably better classified as "open questions," since the evidence for them is not very overwhelming, and there do not seem to be any compelling reasons to believe or not to believe them. The most notable are Vandiver's conjecture, the weaker statement that the p-Sylow subgroup of the ideal class group of the pth cyclotomic field is cyclic over the group ring of the Galois group, and the question of whether or not $\lambda = 0$ for totally real fields. In other words, we know a lot about imaginary things, but it is not clear what to expect in the real case. Whether or not there exists a fruitful theory remains to be seen.

Other possible directions for future developments could be a theory of $\hat{\mathbb{Z}}$-extensions ($\hat{\mathbb{Z}} = \prod \mathbb{Z}_p$; some progress has recently been made by Friedman [1]), and the analogues of Iwasawa's theory in the elliptic case (Coates–Wiles [4]).

I would like to thank Gary Cornell for much help and many excellent suggestions during the writing of this book. I would also like to thank John Coates for many helpful conversations concerning Chapter 13. This chapter also profited greatly from the beautiful courses of my teacher, Kenkichi Iwasawa, at Princeton University. Finally, I would like to thank N.S.F. and the Sloan Foundation for their financial support and I.H.E.S. and the University of Maryland for their academic support during the writing of this book.

Contents

CHAPTER 1
Fermat's Last Theorem 1

CHAPTER 2
Basic Results 9

CHAPTER 3
Dirichlet Characters 19

CHAPTER 4
Dirichlet L-series and Class Number Formulas 29

CHAPTER 5
p-adic L-functions and Bernoulli Numbers 47

5.1. p-adic functions 47
5.2. p-adic L-functions 54
5.3. Congruences 59
5.4. The value at $s = 1$ 63
5.5. The p-adic regulator 70
5.6. Applications of the class number formula 77

CHAPTER 6
Stickelberger's Theorem 87

6.1. Gauss sums 87
6.2. Stickelberger's theorem 93
6.3. Herbrand's theorem 100
6.4. The index of the Stickelberger ideal 102
6.5. Fermat's Last Theorem 107

CHAPTER 7
Iwasawa's Construction of p-adic L-functions 113

7.1. Group rings and power series 113
7.2. p-adic L-functions 117
7.3. Applications 125
7.4. Function fields 128
7.5. $\mu = 0$ 130

CHAPTER 8
Cyclotomic Units 143

8.1. Cyclotomic units 143
8.2. Proof of the p-adic class number formula 151
8.3. Units of $\mathbb{Q}(\zeta_p)$ and Vandiver's conjecture 153
8.4. p-adic expansions 160

CHAPTER 9
The Second Case of Fermat's Last Theorem 167

9.1. The basic argument 167
9.2. The theorems 173

CHAPTER 10
Galois Groups Acting on Ideal Class Groups 184

10.1. Some theorems on class groups 184
10.2. Reflection theorems 187
10.3. Consequences of Vandiver's conjecture 195

CHAPTER 11
Cyclotomic Fields of Class Number One 204

11.1. The estimate for even characters 205
11.2. The estimate for all characters 210
11.3. The estimate for h_m^- 217
11.4. Odlyzko's bounds on discriminants 221
11.5. Calculation of h_m^+ 228

CHAPTER 12
Measures and Distributions 231

12.1. Distributions 231
12.2. Measures 236
12.3. Universal distributions 251

CHAPTER 13
Iwasawa's Theory of $\mathbb{Z}_p$-extensions 263

13.1. Basic facts 264
13.2. The structure of Λ-modules 268
13.3. Iwasawa's theorem 276
13.4. Consequences 284
13.5. The maximal abelian p-extension unramified outside p 290
13.6. The main conjecture 295
13.7. Logarithmic derivatives 299
13.8. Local units modulo cyclotomic units 310

CHAPTER 14
The Kronecker–Weber Theorem 319

Appendix 331

1. Inverse limits 331
2. Infinite Galois theory and ramification theory 332
3. Class field theory 336

Tables 347

1. Bernoulli numbers 347
2. Irregular primes 350
3. Class numbers 352

Bibliography 361

List of Symbols 386

Index 388

Chapter 1

Fermat's Last Theorem

We start with a special case of Fermat's Last Theorem, since not only was it the motivation for much work on cyclotomic fields but also it provides a sampling of the various topics we shall discuss later.

Theorem 1.1. *Suppose p is an odd prime and p does not divide the class number of the field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive* pth *root of unity. Then*

$$x^p + y^p = z^p, \qquad (xyz, p) = 1$$

has no solutions in rational integers.

Remark. The case where p does not divide x, y, and z is called the first case of Fermat's Last Theorem, and is in general easier to treat than the second case, where p divides one of x, y, z. We shall prove the above theorem in the second case later, again with the assumption on the class number.

Factoring the above equation as

$$\prod_{i=0}^{p-1} (x + \zeta_p^i y) = z^p,$$

we find we are naturally led to consider the ring $\mathbb{Z}[\zeta_p]$. We first need some basic results on this ring. Throughout the remainder of this chapter, we let $\zeta = \zeta_p$.

Proposition 1.2. *$\mathbb{Z}[\zeta]$ is the ring of algebraic integers in the field $\mathbb{Q}(\zeta)$. Therefore $\mathbb{Z}[\zeta]$ is a Dedekind domain (so we have unique factorization into prime ideals, etc.).*

Proof. Let $\mathcal{O}$ denote the algebraic integers of $\mathbb{Q}(\zeta)$. Clearly $\mathbb{Z}[\zeta] \subseteq \mathcal{O}$. We must show the reverse inclusion.

Lemma 1.3. *Suppose r and s are integers with $(p, rs) = 1$. Then $(\zeta^r - 1)/(\zeta^s - 1)$ is a unit of $\mathbb{Z}[\zeta]$.*

Proof. Writing $r \equiv st \pmod{p}$ for some t, we have

$$\frac{\zeta^r - 1}{\zeta^s - 1} = \frac{\zeta^{st} - 1}{\zeta^s - 1} = 1 + \zeta^s + \cdots + \zeta^{s(t-1)} \in \mathbb{Z}[\zeta].$$

Similarly, $(\zeta^s - 1)/(\zeta^r - 1) \in \mathbb{Z}[\zeta]$. This completes the proof of the lemma. □

Remark. The units of Lemma 1.3 are called cyclotomic units and will be of great importance in later chapters.

Lemma 1.4. *The ideal $(1 - \zeta)$ is a prime ideal of $\mathcal{O}$ and $(1 - \zeta)^{p-1} = (p)$. Therefore p is totally ramified in $\mathbb{Q}(\zeta)$.*

Proof. Since $X^{p-1} + X^{p-2} + \cdots + X + 1 = \prod_{i=1}^{p-1} (X - \zeta^i)$, we let $X = 1$ to obtain $p = \prod (1 - \zeta^i)$. From Lemma 1.3, we have the equality of ideals $(1 - \zeta) = (1 - \zeta^i)$. Therefore $(p) = (1 - \zeta)^{p-1}$. Since (p) can have at most $p - 1 = \deg(\mathbb{Q}(\zeta)/\mathbb{Q})$ prime factors in $\mathbb{Q}(\zeta)$, it follows that $(1 - \zeta)$ must be a prime ideal of $\mathcal{O}$. Alternatively, if $(1 - \zeta) = A \cdot B$, then $p = N(1 - \zeta) = NA \cdot NB$ so either $NA = 1$ or $NB = 1$. Therefore the ideal $(1 - \zeta)$ does not factor in $\mathcal{O}$. □

We now return to the proof of Proposition 1.2. Let v denote the valuation corresponding to the ideal $(1 - \zeta)$, so $v(1 - \zeta) = 1$ and $v(p) = p - 1$, for example. Since $\mathbb{Q}(\zeta) = \mathbb{Q}(1 - \zeta)$, we have that $\{1, 1 - \zeta, (1 - \zeta)^2, \ldots, (1 - \zeta)^{p-2}\}$ is a basis for $\mathbb{Q}(\zeta)$ as a vector space over $\mathbb{Q}$. Let $\alpha \in \mathcal{O}$. Then

$$\alpha = a_0 + a_1(1 - \zeta) + \cdots + a_{p-2}(1 - \zeta)^{p-2}$$

with $a_i \in \mathbb{Q}$. We want to show $a_i \in \mathbb{Z}$. Since $v(a) \equiv 0 \pmod{p - 1}$ for $a \in \mathbb{Q}$, the numbers $v(a_i(1 - \zeta)^i)$, $0 \leq i \leq p - 2$, are distinct (mod $p - 1$), hence are distinct. Therefore, by standard facts on non-archimedean valuations, $v(\alpha) = \min(v(a_i(1 - \zeta)^i))$. Since $v(\alpha) \geq 0$ and $v((1 - \zeta)^i) < p - 1$, we must have $v(a_i) \geq 0$. Therefore p is not in the denominator of any a_i. Rearrange the expression for α to obtain

$$\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2},$$

with $b_i \in \mathbb{Q}$, but no b_i has p in the denominator.

The proof may now be completed by observing that the discriminant of the basis $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a power of p. More explicitly, we have

$$\alpha^\sigma = b_0 + b_1\zeta^\sigma + \cdots + b_{p-2}(\zeta^\sigma)^{p-2}$$

where σ runs through $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Let $\alpha_i = \alpha^\sigma$, where $\sigma: \zeta \mapsto \zeta^i$. Then we have

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{p-1} \end{pmatrix} = \begin{pmatrix} 1 & \zeta & \zeta^2 & \cdots \\ 1 & \zeta^2 & \zeta^4 & \cdots \\ 1 & \zeta^3 & \zeta^6 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix} \begin{pmatrix} b_0 \\ \vdots \\ b_{p-2} \end{pmatrix}$$

But the determinant of the matrix is a Vandermonde determinant, so it is equal to

$$\prod_{1 \le j < k \le p-1} (\zeta^k - \zeta^j) = (\text{unit})(\text{power of } 1 - \zeta).$$

Therefore $b_i = (\text{algebraic integer})/(\text{power of } 1 - \zeta)$. Since b_i has no p in the denominator, we must have b_i = algebraic integer; therefore $b_i \in \mathbb{Z}$, so we are done.

Alternatively, we could finish the proof as follows. Since $\zeta^{-i}\alpha$ is an algebraic integer, its trace from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$ is a rational integer: $\mathrm{Tr}(\zeta^{-i}\alpha) \in \mathbb{Z}$. Now the minimal polynomial for ζ^j, $(j, p) = 1$, is $X^{p-1} + X^{p-2} + \cdots + X + 1$, so $\mathrm{Tr}(\zeta^j) = -1$. We obtain

$$pb_i - \sum_{j=0}^{p-2} b_j = (p-1)b_i - \sum_{j \ne i} b_j = \mathrm{Tr}(\zeta^{-i}\alpha) \in \mathbb{Z}.$$

Using this equation for $i = 0$ and $i = i$ and subtracting, we obtain $p(b_0 - b_i) \in \mathbb{Z}$, therefore $b_0 - b_i \in \mathbb{Z}$. It remains to show $b_0 \in \mathbb{Z}$. Write

$$\alpha = b_0(1 + \zeta + \cdots + \zeta^{p-2}) + [(b_1 - b_0)\zeta + \cdots + (b_{p-2} - b_0)\zeta^{p-2}].$$

By the above, the expression in brackets is an algebraic integer. Therefore

$$-\zeta^{p-1}b_0 = b_0(1 + \zeta + \cdots + \zeta^{p-2}) \in \mathcal{O},$$

so $b_0 \in \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. Therefore $b_i \in \mathbb{Z}$ for all i, so again we are done. This finishes the proof of Proposition 1.2. □

Before proceeding to the proof of Theorem 1.1, we need the following result, which will be discussed in more detail later.

Proposition 1.5. *Let ε be a unit of $\mathbb{Z}[\zeta_p]$. Then there exist $\varepsilon_1 \in \mathbb{Q}(\zeta + \zeta^{-1})$ and $r \in \mathbb{Z}$ such that $\varepsilon = \zeta^r\varepsilon_1$.*

Remark. Take any embedding of $\mathbb{Q}(\zeta)$ into the complex numbers. Complex conjugation acts as an automorphism sending ζ to ζ^{-1}. The fixed field is $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos(2\pi/p))$ and is called the maximal real subfield of $\mathbb{Q}(\zeta)$. The proposition says that any unit of $\mathbb{Z}[\zeta]$ may be written as a root of unity times a real unit. This result is plausible since the field $\mathbb{Q}(\zeta + \zeta^{-1})$ has $(p-1)/2$ real embeddings and no complex embeddings into $\mathbb{C}$, while $\mathbb{Q}(\zeta)$

has no real embeddings and $(p-1)/2$ pairs of complex embeddings. Therefore the $\mathbb{Z}$-rank of the unit groups of each field is $(p-3)/2$, so the units of $\mathbb{Q}(\zeta+\zeta^{-1})$ are of finite index in those of $\mathbb{Q}(\zeta)$. However, it does not appear that Dirichlet's unit theorem can be used to prove the proposition.

Proof of Proposition 1.5. Let $\alpha = \varepsilon/\bar{\varepsilon}$. Then α is an algebraic integer since $\bar{\varepsilon}$ is a unit. Also, all conjugates of α have absolute value 1 (this follows easily from the fact that complex conjugation commutes with the other elements of the Galois group).

We now need a lemma.

Lemma 1.6. *If α is an algebraic integer all of whose conjugates have absolute value* 1, *then α is a root of unity.*

Proof. The coefficients of the irreducible polynomials for all powers of α are rational integers which can be given bounds depending only on the degree of α over $\mathbb{Q}$. It follows that there are only finitely many irreducible polynomials which can have a power of α as a root. Therefore there are only finitely many distinct powers of α. The lemma follows. □

Remark. The assumption that α is an algebraic integer is essential, as the example $\alpha = \frac{3}{5} + \frac{4}{5}i$ shows. Also we note that it is actually possible for an algebraic integer to have absolute value 1 while some of its conjugates do not. An example is $\alpha = \sqrt{2-\sqrt{2}} + i\sqrt{\sqrt{2}-1}$. One conjugate may be obtained by mapping $\sqrt{2}$ to $-\sqrt{2}$, which yields $\sqrt{2+\sqrt{2}} \pm \sqrt{\sqrt{2}+1}$, neither of which have absolute value 1. However, if $\mathbb{Q}(\alpha)$ is abelian over $\mathbb{Q}$ then all automorphisms commute with complex conjugation; so if $\alpha\bar{\alpha} = 1$ then $\alpha^\sigma\overline{\alpha^\sigma} = 1$ for all σ.

Returning to the proof of Proposition 1.5, we find that $\varepsilon/\bar{\varepsilon}$ is a root of unity, therefore $\varepsilon/\bar{\varepsilon} = \pm\zeta^a$ for some a (the only roots of unity in $\mathbb{Q}(\zeta)$ are of this form. This will follow from results in the next chapter).

Suppose first that $\varepsilon/\bar{\varepsilon} = -\zeta^a$. Write $\varepsilon = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$. Then $\varepsilon \equiv b_0 + b_1 + \cdots + b_{p-2} \pmod{1-\zeta}$. Also $\bar{\varepsilon} = b_0 + b_1\zeta^{-1} + \cdots \equiv b_0 + b_1 + \cdots + b_{p-2} \equiv \varepsilon = -\zeta^a\bar{\varepsilon} \equiv -\bar{\varepsilon}$. Therefore $2\bar{\varepsilon} \equiv 0 \pmod{1-\zeta}$. But $2 \notin (1-\zeta)$. Since $(1-\zeta)$ is a prime ideal, $\bar{\varepsilon} \in (1-\zeta)$, which is impossible since $\bar{\varepsilon}$ is a unit.

Therefore $\varepsilon/\bar{\varepsilon} = +\zeta^a$. Let $2r \equiv a \pmod{p}$, and let $\varepsilon_1 = \zeta^{-r}\varepsilon$. Then $\varepsilon = \zeta^r\varepsilon_1$, and $\bar{\varepsilon}_1 = \varepsilon_1$. This proves Proposition 1.5. □

Proof of Theorem 1.1. We first treat the case $p = 3$. If $3 \nmid x$ then $x^3 \equiv \pm 1 \pmod 9$ and similarly for y and z. Therefore $x^3 + y^3 \equiv -2, 0$, or $+2 \pmod 9$ but $z^3 \equiv \pm 1$. Therefore $x^3 + y^3 \neq z^3$. Similarly, we may treat the case $p = 5$ by considering congruences mod 25. However, we must stop at

$p = 7$ since $1^7 + 30^7 \equiv 31^7 \pmod{49}$. In fact there are still solutions if we consider congruences to higher powers of 7 (see the Exercises). So we need a new method.

Assume $p \geq 5$ and suppose $x^p + y^p = z^p$, $p \nmid xyz$. Suppose $x \equiv y \equiv -z \pmod{p}$. Then $-2z^p \equiv z^p$, which is impossible since $p \nmid 3z$. Therefore we may rewrite the equation if necessary (as $x^p + (-z)^p = (-y)^p$) to obtain $x \not\equiv y \pmod{p}$. We shall need this assumption later on. Also we may assume x, y, and z are relatively prime, otherwise divide by the greatest common divisor.

Lemma 1.7. *The ideals $(x + \zeta^i y)$, $i = 0, 1, \ldots, p - 1$, are pairwise relatively prime.*

Proof. Suppose $\mathscr{P}$ is a prime ideal with $\mathscr{P} \mid (x + \zeta^i y)$ and $\mathscr{P} \mid (x + \zeta^j y)$, where $i \neq j$. Then $\mathscr{P} \mid (\zeta^i y - \zeta^j y) = (\text{unit})(1 - \zeta)y$. Therefore $\mathscr{P} = (1 - \zeta)$ or $\mathscr{P} \mid y$. Similarly, $\mathscr{P}$ divides $\zeta^j(x + \zeta^i y) - \zeta^i(x + \zeta^j y) = (\text{unit})(1 - \zeta)x$, so $\mathscr{P} = (1 - \zeta)$ or $\mathscr{P} \mid x$. If $\mathscr{P} \neq (1 - \zeta)$ then $\mathscr{P} \mid x$ and $\mathscr{P} \mid y$, which is impossible since $(x, y) = 1$. Therefore $\mathscr{P} = (1 - \zeta)$. But then $x + y \equiv x + \zeta^i y \equiv 0 \bmod \mathscr{P}$, the second congruence being by the choice of $\mathscr{P}$. Since $x + y \in \mathbb{Z}$, we have $x + y \equiv 0 \pmod{p}$. But $z^p = x^p + y^p \equiv x + y \equiv 0 \pmod{p}$, so $p \mid z$, contradiction. The lemma is proved. □

Lemma 1.8. *Let $\alpha \in \mathbb{Z}[\zeta]$. Then α^p is congruent mod p to a rational integer (note this congruence is mod p, so it is much stronger than a congruence mod $1 - \zeta$).*

Proof. Let $\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$. Then $\alpha^p \equiv b_0^p + (b_1\zeta)^p + \cdots + (b_{p-2}\zeta^{p-2})^p = b_0^p + b_1^p + \cdots + b_{p-2}^p \pmod{p}$, which proves the lemma. □

Lemma 1.9. *Suppose $\alpha = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ with $a_i \in \mathbb{Z}$ and at least one $a_i = 0$. If $n \in \mathbb{Z}$ and n divides α then n divides each a_j.*

Proof. Since $1 + \zeta + \cdots + \zeta^{p-1} = 0$, we may use any subset of $\{1, \zeta, \ldots, \zeta^{p-1}\}$ with $p - 2$ elements as a basis of the $\mathbb{Z}$-module $\mathbb{Z}[\zeta]$. Since at least one $a_i = 0$, the other a_j's give the coefficients with respect to a basis. The result follows. □

We may now finish the proof of Theorem 1.1. Consider the equation

$$\prod_{i=0}^{p-1} (x + \zeta^i y) = (z)^p$$

as an equality of ideals. Since the ideals $(x + \zeta^i y)$, $0 \leq i \leq p - 1$, are pairwise relatively prime by Lemma 1.7, each one must be the pth power of an ideal:

$$(x + \zeta^i y) = A_i^p.$$

Note that A_i^p is principal.

Now comes the big step: since the class number of $\mathbb{Q}(\zeta)$ is assumed to be not divisible by p, the ideal A_i must be principal, say $A_i = (\alpha_i)$. Consequently $(x + \zeta^i y) = (\alpha_i^p)$, so $x + \zeta^i y = (\text{unit}) \cdot \alpha_i^p$. We note that this is exactly the same as we could have obtained under the stronger assumption that $\mathbb{Z}[\zeta]$ has unique factorization, rather than just class number prime to p.

Let $i = 1$ and omit the subscripts, so $x + \zeta y = \varepsilon\alpha^p$ for some unit ε. Proposition 1.5 says that $\varepsilon = \zeta^r \varepsilon_1$ for some integer r and where $\bar{\varepsilon}_1 = \varepsilon_1$. Lemma 1.8 says that there is a rational integer a such that $\alpha^p \equiv a \pmod{p}$. Therefore $x + \zeta y = \zeta^r \varepsilon_1 \alpha^p \equiv \zeta^r \varepsilon_1 a \pmod{p}$. Also $x + \zeta^{-1} y = \zeta^{-r}\varepsilon_1 \bar{\alpha}^p \equiv \zeta^{-r}\varepsilon_1 \bar{a} \pmod{\bar{p}} = \zeta^{-r}\varepsilon_1 a \pmod{p}$ since $\bar{a} = a$ and $p = \bar{p}$. We obtain

$$\zeta^{-r}(x + \zeta y) \equiv \zeta^r(x + \zeta^{-1} y) \pmod{p}$$

or

$$x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \pmod{p}. \qquad (*)$$

If $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are distinct, then (since $p \geq 5$) Lemma 1.9 says that p divides x and y, which is contrary to our original assumptions. Therefore, they are not distinct. Since $1 \neq \zeta$ and $\zeta^{2r} \neq \zeta^{2r-1}$, we have three cases:

(1) $1 = \zeta^{2r}$. We have from $(*)$ that $x + \zeta y - x - \zeta^{-1} y \equiv 0 \pmod{p}$, so, $\zeta y - \zeta^{p-1} y \equiv 0 \pmod{p}$. Lemma 1.9 implies that $y \equiv 0 \pmod{p}$, contradiction.

(2) $1 = \zeta^{2r-1}$ or, equivalently, $\zeta = \zeta^{2r}$. Equation $(*)$ becomes

$$(x - y) - (x - y)\zeta \equiv 0 \pmod{p}.$$

Lemma 1.9 implies $x - y \equiv 0 \pmod{p}$, which contradicts the choice of x and y made at the beginning of the proof.

(3) $\zeta = \zeta^{2r-1}$. Equation $(*)$ becomes

$$x - \zeta^2 x \equiv 0 \pmod{p},$$

so $x \equiv 0 \pmod{p}$, contradiction. The proof of Theorem 1.1 is now complete. □

Remarks. (Proofs for the following statements will appear in later chapters). The obvious question now arises: How can one determine whether or not p divides the class number of $\mathbb{Q}(\zeta)$? Kummer answered this question quite nicely. Define the Bernoulli numbers B_n by the formula

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

(for example, $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$ and in fact $B_{2k+1} = 0$ for $k \geq 1$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = -\frac{691}{2730}$). Then p divides the class number of $\mathbb{Q}(\zeta)$ if and only if p divides the numerator of some B_k, $k = 2, 4, 6, \ldots, p - 3$. For example, 691 divides the numerator of B_{12} so 691 divides the class number of $\mathbb{Q}(\zeta_{691})$.

If p does not divide the class number of $\mathbb{Q}(\zeta)$ then p is called regular, otherwise p is called irregular. The first few irregular primes are 37, 59, 67, 101, 103, 131, 149, and 157 (which in fact divides two different Bernoulli numbers). The irregular primes up to 125000 have been calculated by Wagstaff. Approximately $1 - e^{-1/2} \simeq 39\%$ of primes are irregular and $e^{-1/2} \simeq 61\%$ are regular. There are probability arguments which make these empirical results plausible. It is known there are infinitely many irregular primes, but it is an open problem to show there are infinitely many regular primes. Moreover, it is not even known whether or not Fermat's Last Theorem, even in the first case, holds for infinitely many p.

One may also ask how often $\mathbb{Z}[\zeta]$ has unique factorization, or equivalently when the class number is equal to one. It turns out that the class number grows quite rapidly as p increases, so there can only be finitely many p for which there is unique factorization. In fact, Montgomery and Uchida proved (independently) that the class number is one exactly when $p \leq 19$.

To finish this chapter we shall show that $\mathbb{Q}(\zeta_{23})$ does not have class number one. It is known that $\mathbb{Q}(\sqrt{-23}) \subseteq \mathbb{Q}(\zeta_{23})$. For a proof, see the Exercises for the next chapter, or use Lemma 4.7 plus Lemma 4.8. The prime 2 splits in $\mathbb{Q}(\sqrt{-23})$ as $\mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p} = (2, (1 + \sqrt{-23})/2)$ (see the Exercises). Let $\mathscr{P}$ be a prime of $\mathbb{Q}(\zeta_{23})$ lying above $\mathfrak{p}$. We claim that $\mathscr{P}$ is nonprincipal. The norm of $\mathscr{P}$ from $\mathbb{Q}(\zeta_{23})$ to $\mathbb{Q}(\sqrt{-23})$ is $\mathfrak{p}^f$, where f is the degree of the residue class field extension. In particular, f divides $\deg(\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})) = 11$, so $f = 1$ or 11 (actually, $f = 1$). Since $\mathfrak{p}$ is nonprincipal and $\mathfrak{p}^3$ is principal, $\mathfrak{p}^{11}$ is nonprincipal. Therefore $\mathfrak{p}^f$ cannot be principal. But if $\mathscr{P}$ is principal, so is its norm. Therefore $\mathscr{P}$ is nonprincipal, so $\mathbb{Z}[\zeta_{23}]$ cannot have unique factorization.

Notes

The proof of Theorem 1.1 is due to Kummer [2]. At present, the first case has been proved for $p < 6 \times 10^9$ (Lehmer [4]) using the Wieferich criterion: if $2^{p-1} \not\equiv 1 \bmod p^2$ then the first case is true. For more on Fermat's Last Theorem, see Vandiver [1] and Ribenboim [1].

Exercises

1.1. (a) Show that the irreducible polynomial for ζ_{p^n} is $X^{(p-1)p^{n-1}} + X^{(p-2)p^{n-1}} + \cdots + X^{p^{n-1}} + 1$ (one way to prove irreducibility: evaluate the polynomial as geometric series to get a rational function, change X to $X + 1$, rewrite as a polynomial reduced mod p, then use Eisenstein).

(b) Show the ring of integers of $\mathbb{Q}(\zeta_{p^n})$ is $\mathbb{Z}[\zeta_{p^n}]$.

1.2. Suppose $p \equiv 1 \pmod 3$. Using the fact that $\mathbb{Z}_p$ contains the cube roots of unity, show that $x^p + y^p \equiv z^p \pmod{p^n}$, $p \nmid xyz$, has solutions for each $n \geq 1$.

1.3. Using the fact that $\mathbb{Z}[\sqrt{-5}]$ has class number 2, show that $x^2 + 5 = y^3$ has no solutions in rational integers.

1.4. Show that the ideal $\mathfrak{p} = (2, (1 + \sqrt{-23})/2)$ is nonprincipal in $\mathbb{Z}[(1 + \sqrt{-23})/2]$, but that its third power is principal. Also show that $\mathfrak{p}\bar{\mathfrak{p}} = (2)$.

1.5. Show that the class number of $\mathbb{Q}(\zeta_{23})$ is divisible by 3 (in fact, it is exactly 3, but do not show this).

Chapter 2

Basic Results

In this chapter we prove some basic results on cyclotomic fields which will lay the groundwork for later chapters. We let ζ_n denote a primitive nth root of unity. First we determine the ring of integers and discriminant of $\mathbb{Q}(\zeta_n)$. We start with the prime power case.

Proposition 2.1. *The discriminant of* $\mathbb{Q}(\zeta_{p^n})$ *is*

$$\pm p^{p^{n-1}(pn-n-1)},$$

where we have $-$ *if* $p^n = 4$ *or if* $p \equiv 3 \pmod 4$, *and we have* $+$ *otherwise.*

Proof. From Exercise 1.1, the ring of integers is $\mathbb{Z}[\zeta_{p^n}]$, so an integral basis is $\{1, \zeta_{p^n}, \ldots, \zeta_{p^n}^{\phi(p^n)-1}\}$. The square of the determinant of $(\zeta_{p^n}^{ij})_{\substack{0\le i<(p-1)p^{n-1}\\ 0<j<p^n,\, p\nmid j}}$ gives the discriminant. But this determinant is Vandermonde, so it equals

$$\prod_{\substack{0<k<j<p^n\\ p\nmid jk}} (\zeta_{p^n}^j - \zeta_{p^n}^k) = (\text{root of unity})\cdot \prod_{\substack{k<j\\ p\nmid jk}} (1 - \zeta_{p^n}^{k-j}).$$

Since $(1 - \zeta_{p^n}^{-a}) = -\zeta_{p^n}^{-a}(1 - \zeta_{p^n}^{a})$, we may include all pairs j, k with $j \neq k$ to get the discriminant

$$\det(\zeta_{p^n}^{ij})^2 = (\text{root of unity})\cdot \prod_{\substack{0<j,k<p^n\\ j\neq k\\ p\nmid jk}} (1 - \zeta_{p^n}^{k-j}).$$

We immediately see that the discriminant, up to sign, must be a power of p. Let v denote the valuation corresponding to the prime ideal $(1 - \zeta_{p^n})$ of $\mathbb{Z}[\zeta_{p^n}]$. As in the first chapter for the case $n = 1$, we have $(1 - \zeta_{p^n})^{(p-1)p^{n-1}} = (p)$. It follows that $v(p) = (p-1)p^{n-1}$ and $v(1 - \zeta_{p^m}) = p^{n-m}$ for $1 \le m \le n$.

Consequently, if $k \equiv j \pmod{p^m}$ but $k \not\equiv j \pmod{p^{m+1}}$, we have $v(1 - \zeta_{p^n}^{k-j}) = p^m$ since $\zeta_{p^n}^{k-j}$ is a p^{n-m}th root of unity. Fix j with $p \nmid j$. It is easy to see that there are $(p-2)p^{n-1}$ values of k with $j \not\equiv k \pmod p$, and $(p-1)p^{n-1-i}$ values of k such that $j \equiv k \pmod{p^i}$ but $j \not\equiv k \pmod{p^{i+1}}$. Also, there are $(p-1)p^{n-1}$ possibilities for j. Therefore, the valuation of the discriminant is

$$(p-1)p^{n-1}\left[(p-2)p^{n-1} + \sum_{i=1}^{n-1}(p-1)p^{n-1-i}\cdot p^i\right]$$
$$= (p-1)p^{n-1}[p^{n-1}(pn - n - 1)].$$

Since $v(p) = (p-1)p^{n-1}$, we must have the discriminant $=$

$$\pm p^{p^{n-1}(pn-n-1)}.$$

To determine the sign, we use the following lemma.

Lemma 2.2. *Let k be a number field with r_2 pairs of complex embeddings. Then $d(k)$ = discriminant of k has sign $(-1)^{r_2}$.*

Proof. Let $\{\alpha_1, \ldots, \alpha_m\}$ be a $\mathbb{Z}$-module basis for the ring of integers of k. Then

$$d(k) = (\det(\alpha_i^\sigma)_{\sigma,i})^2,$$

where σ runs through all embeddings of k into $\mathbb{C}$. If σ is a complex embedding, then $\bar\sigma$ is another embedding, where the bar refers to complex conjugation. Therefore

$$\overline{\det(\alpha_i^\sigma)} = (-1)^{r_2}\det(\alpha_i^\sigma),$$

since r_2 pairs of rows are interchanged. If r_2 is even then $\det(\alpha_i^\sigma)$ is real, so $d(k) > 0$. If r_2 is odd, then $\det(\alpha_i^\sigma)$ is purely imaginary, so $d(k) < 0$. This proves the lemma. □

Returning to the proof of Proposition 2.1, we note that $r_2 = \frac{1}{2}(p-1)p^{n-1}$, which is even unless $p^n = 4$ or $p \equiv 3 \pmod 4$. This completes the proof. □

Now let $m = \prod p_i^{n_i}$ be a positive integer. We shall always assume that $m \not\equiv 2 \pmod 4$, since if m is odd then $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$. Clearly $\mathbb{Q}(\zeta_m)$ is the compositum of the fields $\mathbb{Q}(\zeta_{p_i^{n_i}})$.

Proposition 2.3. *p ramifies in $\mathbb{Q}(\zeta_m) \Leftrightarrow p$ divides m.*

Proof. If p divides m then $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_m)$. Since p ramifies in $\mathbb{Q}(\zeta_p)$, it ramifies in $\mathbb{Q}(\zeta_m)$. Conversely, suppose p does not divide $m = \prod p_i^{n_i}$. Then p is unramified in each $\mathbb{Q}(\zeta_{p_i^{n_i}})$ since p does not divide the discriminant. Therefore p does not ramify in the compositum, which is $\mathbb{Q}(\zeta_m)$. This completes the proof. □

Note that the proposition implies that p divides the discriminant if and only if p divides m.

Proposition 2.4. *If $(m, n) = 1$ then $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$.*

Proof. Let $K = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. If $K \neq \mathbb{Q}$ then there is some prime, call it p, which ramifies in K (this follows from the fact that $|d(K)| > 1$. See Lemma 14.3). By the previous proposition, $p \mid m$ and $p \mid n$, which is impossible. Therefore $K = \mathbb{Q}$. □

Theorem 2.5. $\deg(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n)$ *and* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, *with* $a \bmod n$ *corresponding to the map* $\zeta_n \mapsto \zeta_n^a$.

Proof. Since $\mathbb{Q}(\zeta_m)$ is normal over $\mathbb{Q}$, Proposition 2.4 implies that if $(m, n) = 1$ then $\deg(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}) = \deg(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cdot \deg(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. It therefore suffices to evaluate the degree for prime powers, which we have already done (Exercise 1.1). Since $\phi(p^n) = (p - 1)p^{n-1}$ and $\phi(mn) = \phi(m)\phi(n)$ for $(m, n) = 1$, we obtain $\deg(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n)$.

It is a standard exercise in Galois theory to show that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Since they are of the same order, they must be equal. This completes the proof. □

Theorem 2.6. $\mathbb{Z}[\zeta_n]$ *is the ring of algebraic integers of* $\mathbb{Q}(\zeta_n)$.

Proof. We need the following result (for a proof see Lang [1], p. 68):

Suppose K and E are two number fields which are linearly disjoint ($\Leftrightarrow \deg(KE/\mathbb{Q}) = \deg(K/\mathbb{Q}) \cdot \deg(E/\mathbb{Q})$) and whose discriminants are relatively prime. Then $\mathcal{O}_{KE} = \mathcal{O}_K \mathcal{O}_E$, where $\mathcal{O}_F$ denotes the ring of algebraic integers in a field F. Also

$$d(KE) = d(K)^{\deg(E/\mathbb{Q})}\, d(E)^{\deg(K/\mathbb{Q})}.$$

Applying this result to cyclotomic fields, using the fact that Theorem 2.6 is true in the prime power case, we obtain the theorem for all n. □

We now compute the discriminant of $\mathbb{Q}(\zeta_n)$. The above-mentioned result may be written as

$$\frac{\log|d(KE)|}{\deg(KE/\mathbb{Q})} = \frac{\log|d(K)|}{\deg(K/\mathbb{Q})} + \frac{\log|d(E)|}{\deg(E/\mathbb{Q})}.$$

Therefore if $n = \prod p_i^{a_i}$ we have

$$\frac{\log|d(\mathbb{Q}(\zeta_n))|}{\phi(n)} = \sum_i p_i^{a_i - 1}(p_i a_i - a_i - 1)(\log p_i)/\phi(p_i^{a_i})$$

$$= \sum_i \left(a_i - \frac{1}{p_i - 1}\right)(\log p_i) = \log n - \sum_{p \mid n} (\log p)/(p - 1).$$

We obtain the following (the sign is determined from Lemma 2.2).

Proposition 2.7.

$$d(\mathbb{Q}(\zeta_n)) = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}. \qquad \square$$

One difference between the prime-power case and the case of general n is given in the following.

Proposition 2.8. *Suppose n has at least two distinct prime factors. Then $1 - \zeta_n$ is a unit of $\mathbb{Z}[\zeta_n]$ and $\prod_{\substack{0<j<n \\ (j,n)=1}} (1 - \zeta_n^j) = 1$.*

PROOF. Since $X^{n-1} + X^{n-2} + \cdots + X + 1 = \prod_{j=0}^{n-1} (X - \zeta_n^i)$, we may let $X = 1$ to obtain $n = \prod_{j=0}^{n-1} (1 - \zeta_n^j)$. If p^a is the exact power of p dividing n then, letting j run through multiples of n/p^a, we find that this product contains $\prod_{j=0}^{p^a-1} (1 - \zeta_{p^a}^j) = p^a$. If we remove these factors for each prime dividing n, we obtain $1 = \prod (1 - \zeta_n^j)$, where the product is over those j such that ζ_n^j is not of prime power order. Since n is not a prime power, $1 - \zeta_n$ appears as a factor in this product, hence is a unit. But $\prod_{(j,n)=1} (1 - \zeta_n^j)$ is the norm of $(1 - \zeta_n)$ from $\mathbb{Q}(\zeta_n)$ to $\mathbb{Q}$, therefore equals a unit of $\mathbb{Z}$, namely ± 1. Since complex conjugation is in the Galois group, the norm of any element may be written in the form $\alpha\bar{\alpha}$, which is positive. It follows that $\prod_{(j,n)=1} (1 - \zeta_n^j) = +1$, which completes the proof. We remark that the proof works even if $n \equiv 2 \pmod 4$. □

One might ask what the irreducible polynomial for ζ_n looks like. We define the nth cyclotomic polynomial

$$\Phi_n(X) = \prod_{(j,n)=1} (X - \zeta_n^j).$$

Since $\deg(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n) = \deg \Phi_n(X)$, it follows that $\Phi_n(X)$ is the irreducible polynomial for ζ_n. Also, $\Phi_n(X) \in \mathbb{Z}[X]$ since the coefficients are rational and also are algebraic integers. In addition, it is easy to see that

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

The first few cyclotomic polynomials are

$$\Phi_1(X) = X - 1, \qquad \Phi_2(X) = X + 1, \qquad \Phi_3(X) = X^2 + X + 1,$$
$$\Phi_4(X) = X^2 + 1.$$

All these have coefficients ± 1 and 0; however, this is not true in general. By choosing n with many prime factors one can obtain arbitrarily large coefficients.

One use of cyclotomic polynomials is to give an elementary proof of a special case of Dirichlet's theorem on primes in arithmetic progressions (Corollary 2.11).

Lemma 2.9. *Suppose $p \nmid n$ and $a \in \mathbb{Z}$. Then $p \mid \Phi_n(a) \Leftrightarrow$ the multiplicative order of a mod p is n (i.e., $a^n \equiv 1 \pmod p$ and n is minimal).*

Proof. Suppose $p \mid \Phi_n(a)$. Since $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$, we have $a^n \equiv 1 \pmod p$. Let k be the order of $a \pmod p$. Then $k \mid n$. Suppose $k < n$. As above, we have $0 \equiv a^k - 1 \equiv \prod_{d \mid k} \Phi_d(a) \pmod p$. Consequently $\Phi_{d_0}(a) \equiv 0 \pmod p$ for some d_0. Therefore $a^n - 1 = \Phi_n(a)\Phi_{d_0}(a) \cdot (\text{other factors}) \equiv 0 \pmod{p^2}$. Since $\Phi_n(a + p) \equiv \Phi_n(a) \equiv 0 \pmod p$, and similarly for Φ_{d_0}, we also have $(a + p)^n - 1 \equiv 0 \pmod{p^2}$. Therefore $0 \equiv (a + p)^n - 1 \equiv a^n + npa^{n-1} - 1 \equiv npa^{n-1} \pmod{p^2}$. Since $p \nmid na$, this is impossible. Therefore $k = n$.

Conversely, suppose $a^n - 1 \equiv 0 \pmod p$. Then $\Phi_d(a) \equiv 0 \pmod p$ for some $d \mid n$. But if $d < n$ then the order of a would be less than n since we would have $a^d - 1 \equiv 0 \pmod p$. Therefore $\Phi_n(a) \equiv 0 \pmod p$, and the proof is complete. □

Proposition 2.10. *Suppose $p \nmid n$. Then p divides $\Phi_n(a)$ for some $a \in \mathbb{Z} \Leftrightarrow p \equiv 1 \pmod n$.*

Proof. If $p \mid \Phi_n(a)$ then $a \pmod p$ has order n. Since the order of an element divides the order of the group, n divides $p - 1$. Conversely, if $p \equiv 1 \pmod n$, then there is an element $a \pmod p$ of order n, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Therefore $p \mid \Phi_n(a)$. □

Corollary 2.11. *For any $n \geq 1$ there are infinitely many primes $p \equiv 1 \pmod n$.*

Proof. Suppose there are only finitely many, say $p_1, \ldots, p_r$. Let $M = np_1 \cdots p_r$ and let $N \in \mathbb{Z}$. Then $\Phi_n(NM) \equiv \Phi_n(0) \equiv \pm 1 \pmod M$, therefore mod p_i and mod n ($\Phi_n(0) = \pm 1$ since it is a root of unity by the definition of $\Phi_n(X)$). In particular $\Phi_n(NM)$ is not divisible by p_i and none of its prime factors divides n. As $N \to \infty$, $\Phi_n(NM) \to \infty$, so for large N we have $\Phi_n(NM) \neq \pm 1$. Therefore there is a prime p dividing $\Phi_n(NM)$. By the proposition, $p \equiv 1 \pmod n$. From the above, $p \neq p_i$, $1 \leq i \leq r$. Therefore we have obtained a new prime. This completes the proof. □

We remark that Euclid's classical proof is just the above proof using $\Phi_2(X)$. Similarly, $\Phi_4(X)$ is used to obtain primes of the form $4n + 1$.

Now we turn our attention to the splitting of primes in cyclotomic fields. First we need the following useful result.

Lemma 2.12. *Suppose $p \nmid n$ and let $\mathscr{P}$ be a prime of $\mathbb{Q}(\zeta_n)$ lying above p. Then the nth roots of unity are distinct mod $\mathscr{P}$.*

Proof. The result follows immediately from the equation

$$n = \prod_{j=0}^{n-1} (1 - \zeta_n^j). \qquad □$$

Note that this result is not true for $p|n$. In $\mathbb{Q}(\zeta_p)$ we have $\zeta_p \equiv 1 \bmod (1 - \zeta_p)$.

Assume $p \nmid n$ and let $\mathscr{P}$ lie above p in $\mathbb{Q}(\zeta_n)$. The Frobenius automorphism of $\mathbb{Q}(\zeta_n)$ is defined by

$$\sigma_p x \equiv x^p \pmod{\mathscr{P}} \quad \text{for all} \quad x \in \mathbb{Z}[\zeta_n].$$

Since $\sigma_p \zeta_n$ is an nth root of unity, Lemma 2.12 implies that $\sigma_p \zeta_n = \zeta_n^p$. The order of σ_p is the degree of the residue class extension $\mathbb{Z}[\zeta_n] \pmod{\mathscr{P}}/\mathbb{Z} \pmod{p}$. Now $\sigma_p^f = 1 \Leftrightarrow \sigma_p^f(\zeta_n) = \zeta_n \Leftrightarrow \zeta_n^{p^f} = \zeta_n \Leftrightarrow p^f \equiv 1 \pmod{n}$. Since p is unramified in $\mathbb{Q}(\zeta_n)$, it is a standard fact from algebraic number theory that the degree of the residue class extension multiplied by the number of primes above p equals the degree of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. We have therefore proved the following.

Theorem 2.13. *Suppose $p \nmid n$ and let f be the smallest positive integer such that $p^f \equiv 1 \pmod{n}$. Then p splits into $g = \phi(n)/f$ distinct primes in $\mathbb{Q}(\zeta_n)$, each of which has residue class degree f. In particular, p splits completely $\Leftrightarrow p \equiv 1 \pmod{n}$.* □

Remarks. The fact that p splits completely if and only if $p \equiv 1 \pmod{n}$ means that $\mathbb{Q}(\zeta_n)$ is the ray class field modulo $n\infty$ in the sense of class field theory. Since every abelian extension of the rationals is contained in some ray class field, this proves the celebrated Kronecker–Weber theorem: Every abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$. Later we shall give a proof of this result without assuming class field theory.

We also note that the splitting type of p depends only on its congruence class modulo n. This is a characteristic of abelian extensions which can be proved using class field theory.

Theorem 2.13 is sometimes called the cyclotomic reciprocity law. One purpose of a reciprocity law is to give nice conditions for when a prime splits. For example, the quadratic reciprocity law (see Exercises) allows one to change a statement about q splitting in $\mathbb{Q}(\sqrt{p})$, which depends on whether or not p is a square mod q, into a question of whether or not q is a square mod p. If one wished to make a list of the primes which split in $\mathbb{Q}(\sqrt{p})$, then checking whether or not p is a square mod q for each q would be rather laborious. However, after making an initial list of squares mod p. one would find checking each q mod p to be rather easy. The cyclotomic reciprocity law has the same advantages.

As an example for the theorem, let $p = 2$ and $n = 23$. Then $2^{11} \equiv 1 \pmod{23}$, so $f = 11$. Therefore 2 splits into two factors in $\mathbb{Q}(\zeta_{23})$. But we already know that 2 splits as $\mathscr{P}\bar{\mathscr{P}}$ in $\mathbb{Q}(\sqrt{-23})$, where $\mathscr{P} = (2, (1 + \sqrt{-23})/2)$ (see Exercise 1.4). Going from $\mathbb{Q}(\sqrt{-23})$ to $\mathbb{Q}(\zeta_{23})$, $\mathscr{P}$ and $\bar{\mathscr{P}}$ must remain prime. Therefore $(2) = (2, (1 + \sqrt{-23})/2)(2, (1 - \sqrt{-23})/2)$ is the explicit factorization of (2) in $\mathbb{Q}(\zeta_{23})$. As shown at the end of Chapter 1, neither of these ideals can be principal.

We can also use Theorem 2.13 to treat the case $p|n$, since $\mathbb{Q}(\zeta_n)$ is the compositum of the linearly disjoint fields $\mathbb{Q}(\zeta_{n/p^a})$ and $\mathbb{Q}(\zeta_n)$, where p^a is the exact power of p dividing n. We determine f and g for $\mathbb{Q}(\zeta_{n/p^a})$ by Theorem 2.13 and then note that p is totally ramified in $\mathbb{Q}(\zeta_{p^a})$, with ramification index $e = (p - 1)p^{a-1}$. Therefore, the ramification index, residue class degree, and number of primes above p in $\mathbb{Q}(\zeta_n)$ must be at least e, f, and g, respectively. Since $efg = \deg(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, these e, f, g must give the correct answers for the full extension. It is now easy to see that $\mathbb{Q}(\zeta_{n/p^a})$ is the inertia field and that if we identify $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p^a\mathbb{Z})^\times \oplus (\mathbb{Z}/(n/p^a)\mathbb{Z})^\times$, then the inertia group for p is $(\mathbb{Z}/p^a\mathbb{Z})^\times$ and the decomposition group is generated by $(\mathbb{Z}/p^a\mathbb{Z})^\times$ and $p \pmod{(n/p^a)\mathbb{Z}}$.

It is possible, in theory, to give explicit generators for the prime ideals lying above a rational prime. We need the following result (for a proof, see Lang [1], p. 27).

Proposition 2.14. *Let A be a Dedekind domain with quotient field K, let E/K be a finite separable extension, and let B be the integral closure of A in E. Suppose $B = A[\alpha]$ for some $\alpha \in E$ and let $f(X)$ be the irreducible polynomial for α over K. Let $\mathscr{P}$ be a prime ideal of A. Let $\overline{f(X)}$ denote reduction modulo $\mathscr{P}$. Suppose*

$$\overline{f(X)} = \overline{P_1(X)}^{e_1} \cdots \overline{P_g(X)}^{e_g}$$

is the factorization of $f(X)$ mod *$\mathscr{P}$ into powers of distinct monic irreducible polynomials over $(A/\mathscr{P})[X]$. Let $P_i(X) \in A[X]$ be a monic polynomial which reduces* mod *$\mathscr{P}$ to $\overline{P_i(X)}$. Let $\tilde{P}_i$ be the ideal of B generated by $\mathscr{P}$ and $P_i(\alpha)$. Then $\tilde{P}_i$ is a prime ideal of B lying over $\mathscr{P}$, e_i is the ramification index, the $\tilde{P}_i$'s are distinct, and*

$$\mathscr{P}B = \tilde{P}_1^{e_1} \cdots \tilde{P}_g^{e_g}$$

is the factorization of $\mathscr{P}$ in B. □

Applying the proposition to our case, we factor the cyclotomic polynomial mod p as

$$\overline{\Phi_n(X)} = \overline{P_1(X)}^{e_1} \cdots \overline{P_g(X)}^{e_g}$$

(actually, $e_1 = e_2 = \cdots = e_g$ since we are working with a Galois extension). Then $\tilde{P}_i = (p, P_i(\zeta_n))$. In the special case $p \equiv 1 \pmod{n}$, the ideals lying above p are of the form $(p, a - \zeta_n)$, where $a \pmod{p}$ is of order n.

When g is small, in particular $g = 2$, and p is unramified, then perhaps it is easier to determine the generators for the primes in the splitting field. Since these primes are then inert the rest of the way up to the full cyclotomic field, these generators work for $\mathbb{Q}(\zeta_n)$ also. This is the method we used for $p = 2$ in $\mathbb{Q}(\zeta_{23})$ previously.

Finally, we discuss subfields of $\mathbb{Q}(\zeta_n)$. The most important for our purposes is the maximal real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, denoted $\mathbb{Q}(\zeta_n)^+$. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is of degree 2 since the lower field is the fixed field of complex conjugation. Alternatively, ζ_n is a root of $X^2 - (\zeta_n + \zeta_n^{-1})X + 1$. One interesting fact is the following.

Proposition 2.15. (*a*) *If* $n = p^m$ *then* $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ *is ramified at the prime above* p *and at the archimedean primes, and unramified at the other primes.*

(*b*) *If* n *is not a prime power,* $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ *is unramified except at the archimedean primes.*

Proof. In both cases, the archimedean primes ramify since $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is totally real and $\mathbb{Q}(\zeta_n)$ is totally complex. Part (a) is true since p is totally ramified in $\mathbb{Q}(\zeta_{p^m})$ and is the only ramified finite prime. Part (b) may be proved as follows. Let p and q be two different prime divisors of n (if p or q is 2, then use 4 instead of 2). Then ζ_p and ζ_q are in $\mathbb{Q}(\zeta_n)$, but not in $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, since the latter field is real. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is of degree 2, we must have $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \zeta_p) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \zeta_q)$. Adjoining ζ_p allows ramification only at primes above p and the archimedean primes (if L/K is unramified at a prime $\mathscr{P}$, then LF/KF is unramified at primes above $\mathscr{P}$. Here $F = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $L = \mathbb{Q}(\zeta_p)$, $K = \mathbb{Q}$). Similarly, adjoining ζ_q allows ramification only above q and at the infinite primes. Therefore there is no ramification at finite primes, so the proof is complete. □

We now look at subfields of $\mathbb{Q}(\zeta_p)$ in more detail. Let g be a primitive root mod p, let e be a fixed divisor of $p - 1$, and let $f = (p - 1)/e$ (there is no relationship with ramification indices, etc.). Define

$$\eta_i = \sum_{j=0}^{f-1} \zeta_p^{g^{ej+i}}, \qquad i = 0, 1, \ldots, e - 1.$$

These numbers are called periods and their significance is as follows. Let σ be the automorphism of $\mathbb{Q}(\zeta_p)$ which maps ζ_p to ζ_p^g. Since g is a primitive root, σ generates the Galois group. The subgroup of order f is

$$H = \{1, \sigma^e, \ldots, \sigma^{e(f-1)}\},$$

which corresponds to $\{1, g^e, \ldots, g^{e(f-1)}\} \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$. Consequently, $\{g^{ej+i} | 0 \le j \le f - 1\}$ is a coset of this subgroup. It is easy to see that H fixes η_i. Also $\sigma(\eta_i) = \eta_{i+1}$ for $0 \le i \le e - 2$, and $\sigma(\eta_{e-1}) = \eta_0$. So η_i has exactly e conjugates under $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. It follows that η_i, for any i, generates the subfield of $\mathbb{Q}(\zeta_p)$ of degree e over $\mathbb{Q}$. For example, if $e = (p - 1)/2, f = 2$, then $\eta_i = \zeta_p^{g^i} + \zeta_p^{-g^i}$, which in the case $i = 0$ gives us $\zeta_p + \zeta_p^{-1}$.

One may ask whether or not $\mathbb{Z}[\eta_i]$ is the ring of integers of $\mathbb{Q}(\eta_i)$. In general, the answer is no (see below), but for $f = 2$ the answer is yes. In fact, we have the following.

Proposition 2.16. $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ is the ring of integers of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Proof. Suppose $\alpha = a_0 + a_1(\zeta_n + \zeta_n^{-1}) + \cdots + a_N(\zeta_n + \zeta_n^{-1})^N$ is an algebraic integer, with $N \le \frac{1}{2}\phi(n) - 1$ and with $a_i \in \mathbb{Q}$. By removing those terms with $a_i \in \mathbb{Z}$, we may assume $a_N \notin \mathbb{Z}$. Multiplying by ζ_n^N and expanding the result as a polynomial in ζ_n, we find that $\zeta_n^N\alpha = a_N + \cdots + a_N\zeta_n^{2N}$ is an algebraic integer in $\mathbb{Q}(\zeta_n)$, therefore in $\mathbb{Z}[\zeta_n]$. Since $2N \leq \phi(n) - 2 \leq \phi(n) - 1$, $\{1, \zeta_n, \ldots, \zeta_n^{2N}\}$ forms a subset of a $\mathbb{Z}$-basis for the ring $\mathbb{Z}[\zeta_n]$. Therefore $a_N \in \mathbb{Z}$. This completes the proof. □

For the case of η_i, $i \neq 0$, we may take Galois conjugates of everything to find that $\mathbb{Z}[\eta_i]$ is the ring of integers of $\mathbb{Q}(\eta_i)\,(=\mathbb{Q}(\eta_0))$ for $f = 2$.

There are many counterexamples for $f > 2$. Several may be obtained in a way similar to the following. Let $p = 31$, $f = 5$. Since $2^5 \equiv 1 \pmod{31}$, 2 splits completely in the extension over $\mathbb{Q}$ of degree 6, which is $\mathbb{Q}(\eta_i)$. Suppose the ring of integers of $\mathbb{Q}(\eta_i)$ has the form $\mathbb{Z}[\alpha]$ for some α. Let $f(X)$ be the irreducible polynomial for α over $\mathbb{Q}$. By Proposition 2.14, $f(X)$ must factor as a product of 6 distinct linear factors over $\mathbb{Z}/2\mathbb{Z}$. But X and $X + 1$ are the only linear polynomials mod 2, so this is impossible. Therefore the ring of integers cannot be $\mathbb{Z}[\alpha]$; in particular, it cannot be $\mathbb{Z}[\eta_i]$.

Notes

Most of the results in this chapter are due to Kummer. For an application of the cyclotomic splitting laws to primality testing, see Adleman–Pomerance–Rumely [1] and Lenstra [7].

Exercises

2.1. Show $\mathbb{Q}(\zeta_p)$ contains a quadratic subfield (p is an odd prime). Using the fact that only p can ramify, show that this field must be $\mathbb{Q}(\sqrt{\pm p})$, where we have + if $p \equiv 1 \pmod 4$ and − if $p \equiv 3 \pmod 4$.

2.2. Show that $\mathbb{Q}(\zeta_8)$ contains 3 quadratic subfields. Determine which ones they are.

2.3. Show that the only roots of unity in $\mathbb{Q}(\zeta_n)$ are of the form $\pm\zeta_n^j$.

2.4. Let p be an odd prime. Show that there is a unique subfield K of $\mathbb{Q}(\zeta_{p^2})$ of degree p over $\mathbb{Q}$. Show that $2^{p-1} \equiv 1 \pmod{p^2}$ if and only if 2 splits completely in K (the primes 1093 and 3511 are the only primes known which satisfy this relation. It can be shown that if $2^{p-1} \not\equiv 1 \pmod{p^2}$ then the first case of Fermat's Last Theorem holds.).

2.5 (a) Determine explicitly the factorizations of 2, 3, 5, 7, and 11 in $\mathbb{Q}(\zeta_{20})$, and show that all the prime ideals lying above these primes are principal (*Hints*: The quadratic subfields of $\mathbb{Q}(\zeta_{20})$ are $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{5})$. The prime 2 may be treated via $\mathbb{Q}(i)$. For 3 and 7, observe that $\omega_1^2 + \omega_2^2 = 3$ and $\omega_1^4 + \omega_2^4 = 7$, where $\omega_1 = (1 + \sqrt{5})/2$ and $\omega_2 = (1 - \sqrt{5})/2$. For 5, show that the norm from $\mathbb{Q}(\zeta_{20})$ to $\mathbb{Q}(\zeta_5)$ of $(\zeta_5 + \zeta_5^{-1}) + \zeta_5^2 \cdot i$ is $1 - \zeta_5$. For 11, first determine its prime factors in $\mathbb{Q}(\zeta_5)$).

(b) A theorem of Minkowski states that in every ideal class of a number field K, there exists an integral ideal A satisfying

$$NA \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d(K)|},$$

where NA is the norm of A, n is the degree of K over $\mathbb{Q}$, $d(K)$ is the discriminant, and r_2 is the number of pairs of complex embeddings (see Lang [1] p. 119). Show that all ideals A satisfying this inequality are principal, so $\mathbb{Q}(\zeta_{20})$ has class number 1 (note however that it has a subfield $\mathbb{Q}(\sqrt{-5})$ of class number 2).

2.6. Let p and q be distinct odd primes. Let $(p/q) = +1$ if $x^2 \equiv p \pmod{q}$ has a solution, and $(p/q) = -1$ otherwise. The quadratic reciprocity law states that

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{if either } p \equiv 1 \pmod{4} \quad \text{or} \quad q \equiv 1 \pmod{4}$$

and

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \quad \text{if both } p \equiv 3 \pmod{4} \quad \text{and} \quad q \equiv 3 \pmod{4}.$$

Justify the steps in the following proof.

(a) Assume $p \equiv 1 \pmod{4}$, q arbitrary. Then

$$\left(\frac{p}{q}\right) = 1 \Leftrightarrow x^2 - x + \frac{1-p}{4} \equiv 0 \pmod{q} \text{ is solvable}$$

$$\Leftrightarrow q \text{ splits in } \mathbb{Q}(\sqrt{p}) = \mathbb{Q}\left(\frac{1+\sqrt{p}}{2}\right)$$

$$\Leftrightarrow \sigma_q \; (= \text{Frobenius for } q \text{ in } \mathbb{Q}(\zeta_p)) \text{ fixes } \mathbb{Q}(\sqrt{p})$$

$$\Leftrightarrow q \equiv a^2 \pmod{p} \text{ is solvable} \Leftrightarrow \left(\frac{q}{p}\right) = 1.$$

The same argument works if $q \equiv 1 \pmod{4}$ and p is arbitrary.

(b) Assume both $p \equiv 3 \pmod{4}$ and $q \equiv 3 \pmod{4}$. Imitate part (a) to show $(p/q) = -(q/p)$. (Since -1 is not a square modulo a prime congruent to 3 mod 4, we have $x^2 \equiv p \pmod{q}$ has a solution $\Leftrightarrow$ $x^2 \equiv -p \pmod{q}$ does not have a solution).

2.7. Using the techniques of the previous exercise, show that $x^2 \equiv 2 \pmod{p}$ has a solution if $p \equiv \pm 1 \pmod{8}$ and does not have a solution if $p \equiv \pm 3 \pmod{8}$.

2.8. (Lenstra). This exercise gives another proof of Proposition 2.7.

(a) Let $\Phi_n(X)$ be the nth cyclotomic polynomial. Show that

$$\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)},$$

where $\mu(d)$ is the Möbius function: $\mu(d) = 0$ if d is not square-free; if d is square-free then $\mu(d) = (-1)^{\pi}$ where π is the number of prime factors of d. A useful fact: $\sum_{d|n} \mu(d) = 1$ if $n = 1$, $=0$ if $n > 1$.

(b) Let $X^n - 1 = \Phi_n(X) \cdot \Psi_n(X)$. Show that $\Phi_n'(\zeta_n) = n\zeta_n^{n-1}/\Psi_n(\zeta_n)$. Since ζ_n generates the ring of integers of $\mathbb{Q}(\zeta_n)$, $\Phi_n'(\zeta_n)$ generates the different, and its norm to $\mathbb{Q}$ gives the discriminant.

(c) Show that $\Psi_n(\zeta_n) = (\text{unit}) \cdot \prod_{p|n} (\zeta_n^{n/p} - 1)$.

(d) Show that $\text{Norm}(\zeta_p - 1) = p^{\phi(n)/(p-1)}$.

(e) Deduce Proposition 2.7.

Chapter 3

Dirichlet Characters

In this chapter we introduce the basic facts about Dirichlet characters. We then show how they may be used to obtain information about the arithmetic of number fields. As a result, we show how to obtain ideal class groups containing prescribed subgroups.

A Dirichlet character is basically a multiplicative homomorphism $\chi: (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$. If $n|m$ then χ induces a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ by composition with the natural map $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore, we could regard χ as being defined mod m or mod n, since both are essentially the same map. It is convenient to choose n minimal and call it the conductor of χ, denoted f or f_χ.

Examples. (1) Let $\chi: (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times$ be defined by $\chi(1) = 1$, $\chi(3) = -1$, $\chi(5) = 1$, $\chi(7) = -1$. Since $\chi(a + 4) = \chi(a)$, it is clear χ may be defined mod 4 by $\chi(1) = 1$, $\chi(-3) = -1$. Since 4 is minimal, $f_\chi = 4$.

(2) Let $\chi: (\mathbb{Z}/6\mathbb{Z})^\times \to \mathbb{C}^\times$ be defined by $\chi(1) = 1$, $\chi(5) = -1$. Then χ is induced by the map $(\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$ which sends 1 to 1 and 2 to -1. Therefore $f_\chi = 3$.

It is convenient to classify characters into two types: if $\chi(-1) = 1$ then χ is called even; if $\chi(-1) = -1$ then χ is called odd. Both of the above examples are odd characters.

Many times we regard χ as a map $\mathbb{Z} \to \mathbb{C}$ by letting $\chi(a) = 0$ if $(a, f_\chi) \neq 1$. It is therefore important to make a convention regarding the modulus of definition of χ. We shall always regard χ as being defined modulo its conductor. Such characters are called primitive. Essentially, this choice makes $\chi(a) = 0$ happen as little as possible. Also χ is then periodic of period f_χ.

In Example 2, the fact that χ defined mod 6 did not have period 3 can be explained by the fact that 6 contains the extraneous prime 2, so all even a had $\chi(a) = 0$.

In the following, when we talk of the characters of $(\mathbb{Z}/n\mathbb{Z})^\times$, or of the characters mod n, we shall be including characters of conductor dividing n, for example the trivial character of conductor 1.

The convention that all characters are primitive plays a part in the multiplication of characters. Let χ and ψ be Dirichlet characters of conductors f_χ and f_ψ. We define $\chi\psi$ as follows. Consider the homomorphism

$$\gamma: (\mathbb{Z}/lcm(f_\chi, f_\psi)\mathbb{Z})^\times \to \mathbb{C}^\times$$

defined by $\gamma(a) = \chi(a)\psi(a)$. Then $\chi\psi$ is the primitive character associated to γ.

Examples. (3) Define χ mod 12 by $\chi(1) = 1, \chi(5) = -1, \chi(7) = -1, \chi(11) = 1$ and define ψ mod 3 by $\psi(1) = 1$, $\psi(2) = -1$. Then $\chi\psi$ on $(\mathbb{Z}/12\mathbb{Z})^\times$ has the values $\chi\psi(1) = 1$, $\chi\psi(5) = \chi(5)\psi(2) = 1$, $\chi\psi(7) = -1$, $\chi\psi(11) = -1$. It is easy to see that $\chi\psi$ has conductor 4 and satisfies $\chi\psi(1) = 1$, $\chi\psi(3) = -1$. Note that $\chi\psi(3) = -1 \neq \chi(3)\psi(3)$.

(4) Let χ be any character and let $\psi = \bar{\chi}$ (complex conjugate). Then $\psi(a) = \chi(a)^{-1}$ if $(a, f_\chi) = 1$. It follows that $\chi\bar{\chi}$ is the trivial character: $\chi\bar{\chi}(a) = 1$ for all a (including $a = 0$).

(5) If $(f_\chi, f_\psi) = 1$ then $f_{\chi\psi} = f_\chi f_\psi$ (see Exercises).

The advantage of using primitive characters become evident when one takes a product of several characters of various conductors, since otherwise the modulus of definition could grow quite rapidly. Also, with our convention, there is only one trivial character, rather than one for each modulus.

It is sometimes advantageous to think of Dirichlet characters as being characters of Galois groups of cyclotomic fields. If we identify $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^\times$ then a Dirichlet character mod n is a Galois character. The Examples 1 and 2 above may be interpreted as follows:

(1) The kernel is 1 (mod 8) and 5 (mod 8). In the Galois group these form $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4))$, so χ is a character of the quotient of $(\mathbb{Z}/8\mathbb{Z})^\times$ by this subgroup. Consequently χ is a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq (\mathbb{Z}/4\mathbb{Z})^\times$.

(2) In this case $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$ so a character mod 6 and a character mod 3 are characters of the same Galois group.

In general, let χ be a character mod n, hence a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let K be the fixed field of the kernel of χ. Then $K \subseteq \mathbb{Q}(\zeta_n)$, and if n is minimal then $n = f_\chi$. The field K depends only on χ and is called the field belonging to χ. More generally, let X be a finite group of Dirichlet characters. Let n be the least common multiple of the conductors of the characters in X, so X is a subgroup of the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let H be the intersection of the kernels of these characters and let K be the fixed field of H. Then X is precisely the set of homomorphisms $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$ (see below). The field K is called the field belonging to X, and we have $\deg(K/\mathbb{Q}) =$ order of X; in fact, $X \simeq \mathrm{Gal}(K/\mathbb{Q})$ (see below). If X is cyclic, generated by χ, then K is precisely the same as the field belonging to χ mentioned above.

Examples. (6) If X is the group of characters of $(\mathbb{Z}/n\mathbb{Z})^\times$ satisfying $\chi(-1) = +1$, then complex conjugation $(\zeta_n \mapsto \zeta_n^{-1})$ is in the kernel of each $\chi \in X$. The field associated to X is $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, which is the maximal real subfield of $\mathbb{Q}(\zeta_n)$. Similarly, if χ is any character then the field belonging to χ is real if and only if $\chi(-1) = +1$.

(7) The character χ of example (3) must correspond to a quadratic subextension of $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\zeta_3)\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-3})\mathbb{Q}(i)$. The three quadratic subfields are $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{3})$. The first two choices would force χ to have conductor 3 and 4, respectively, which is not the case. Therefore, $\mathbb{Q}(\sqrt{3})$ is the field belonging to χ. Alternatively, since $\chi(-1) = +1$, the field belonging to χ must be real. The fact that the discriminant of $\mathbb{Q}(\sqrt{3})$ is 12 can be used to explain the fact that χ has conductor 12 (see Theorem 3.11).

The preceding notions can be put in the setting of characters of finite abelian groups, which we now review. Let G be a finite abelian group and let $\hat{G}$ denote the group of multiplicative homomorphisms from G to $\mathbb{C}^\times$.

Lemma 3.1. *If G is a finite abelian group, then $G \simeq \hat{G}$ (noncanonically).*

Proof. G may be written a direct sum of groups of the form $\mathbb{Z}/m\mathbb{Z}$. Therefore $\hat{G}$ is the product of groups of the form $(\mathbb{Z}/m\mathbb{Z})^\wedge$. But if $\chi \in (\mathbb{Z}/m\mathbb{Z})^\wedge$, then $\chi(1)$ determines χ (remember $\mathbb{Z}/m\mathbb{Z}$ is additive). Since $\chi(1)$ can be any mth root of unity, the lemma is true for $\mathbb{Z}/m\mathbb{Z}$, hence for G. □

Corollary 3.2. $\hat{\hat{G}} \simeq G$ (canonically).

Proof. Let $g \in G$. Then $g\colon \hat{G} \to \mathbb{C}^\times$ by $g\colon \chi \to \chi(g)$. Suppose $\chi(g) = 1$ for all $\chi \in \hat{G}$. Let H be the subgroup of G generated by g. Then $\hat{G}$ acts as a set of distinct characters of G/H. But there are at most $\#(G/H)$ of these by the lemma. Therefore, $H = 1$, so $g = 1$. Consequently G injects into $\hat{\hat{G}}$. Since $\#(G) = \#(\hat{G}) = \#(\hat{\hat{G}})$, we are done. □

Many times it is convenient to identify $\hat{\hat{G}} = G$. We have a natural pairing

$$G \times \hat{G} \to \mathbb{C}^\times$$
$$(g, \chi) \mapsto \chi(g).$$

This pairing is nondegenerate: if $\chi(g) = 1$ for all $\chi \in \hat{G}$ then $g = 1$ by the above argument. If $\chi(g) = 1$ for all $g \in G$ then, of course, $\chi = 1$.

Now let H be a subgroup of G. Let

$$H^{\perp} = \{\chi \in \hat{G} \mid \chi(h) = 1, \forall h \in H\}.$$

We clearly have a natural isomorphism $H^{\perp} \simeq (\widehat{G/H})$.

Proposition 3.3. $\hat{H} \simeq \hat{G}/H^{\perp}$.

Proof. By restriction we have a map $\hat{G} \to \hat{H}$. The kernel is $H^{\perp}$. It remains to show surjectivity. But $\#(H^{\perp}) = \#(\widehat{G/H}) = \#(G/H) = \#(G)/\#(H)$. Therefore $\#(\hat{H}) = \#(H) = \#(G)/\#(H^{\perp}) = \#(\hat{G})/\#(H^{\perp})$. The proposition follows. □

Proposition 3.4. $(H^{\perp})^{\perp} = H$ (*we equate* $\hat{\hat{G}} = G$).

Proof. As in the preceding proof, a straightforward calculation shows both groups have the same order. If $h \in H$ then $h\colon \chi \to \chi(h)$ maps $H^{\perp} \to 1$. Therefore $H \subseteq H^{\perp\perp}$. Therefore they are equal. □

Remarks. Since $\hat{\hat{G}} = G$, we may reverse the roles of G and $\hat{G}$ in all the above. The above results, with the exception of Lemma 3.1, hold for locally compact abelian groups. However, the proofs are more difficult since counting arguments cannot be used.

We now return to Dirichlet characters. Let X be the group of Dirichlet characters associated to a field K. Then we have a pairing

$$\mathrm{Gal}(K/\mathbb{Q}) \times X \to \mathbb{C}^{\times}.$$

Let L be a subfield of K and let

$$Y = \{\chi \in X \mid \chi(g) = 1, \forall\, g \in \mathrm{Gal}(K/L)\}.$$

Then

$$\begin{aligned} Y = \mathrm{Gal}(K/L)^{\perp} &= (\mathrm{Gal}(K/\mathbb{Q})/\mathrm{Gal}(K/L))^{\wedge} \\ &= \mathrm{Gal}(L/\mathbb{Q})^{\wedge}. \end{aligned}$$

Conversely, if we start with a subgroup $Y \subseteq X$ and let L be the fixed field of

$$Y^{\perp} = \{g \in \mathrm{Gal}(K/\mathbb{Q}) \mid \chi(g) = 1, \forall \chi \in Y\},$$

then $Y^{\perp} = \mathrm{Gal}(K/L)$, by Galois theory. Therefore $Y = Y^{\perp\perp} = \mathrm{Gal}(K/L)^{\perp} = \mathrm{Gal}(L/\mathbb{Q})^{\wedge}$. It follows that we have a one-one correspondence between subgroups of X and subfields of K given by

$$\begin{aligned} \mathrm{Gal}(K/L)^{\perp} &\leftrightarrow L \\ Y &\leftrightarrow \text{fixed field of } Y^{\perp}. \end{aligned}$$

This gives us a one–one correspondence between all groups of Dirichlet characters and subfields of cyclotomic fields, since any two groups may be regarded as subgroups of some larger group.

Since $\mathrm{Gal}(L/\mathbb{Q})$ is a finite abelian group we have $Y = \mathrm{Gal}(L/\mathbb{Q})\hat{} \simeq \mathrm{Gal}(L/\mathbb{Q})$. This isomorphism, though useful, is noncanonical and is better expressed by the natural nondegenerate pairing

$$\mathrm{Gal}(L/\mathbb{Q}) \times Y \to \mathbb{C}^\times.$$

We leave the following statements as exercises: Let X_i correspond to K_i. Then

(1) $X_1 \subseteq X_2 \Leftrightarrow K_1 \subseteq K_2$.
(2) The group generated by X_1 and X_2 corresponds to the compositum K_1K_2.

We now show how ramification indices may be computed in terms of characters.

Let $n = \prod p^a$. Corresponding to the decomposition

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod (\mathbb{Z}/p^a\mathbb{Z})^\times$$

we may write any character χ defined mod n as

$$\chi = \prod \chi_p$$

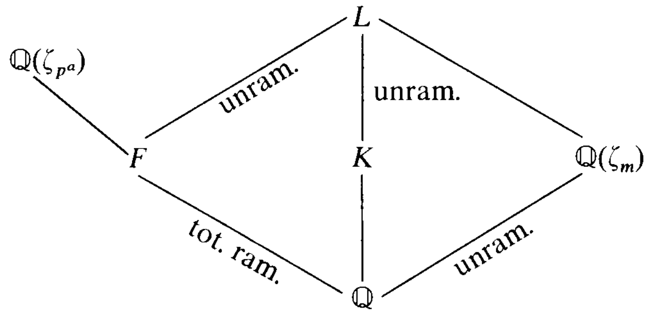
where χ_p is a character defined mod p^a. If X is a group of Dirichlet characters, then we let

$$X_p = \{\chi_p | \chi \in X\}.$$

In Example (3), χ may be written as $\chi = \chi_2 \cdot \chi_3$ where χ_2 is the character $\chi\psi$ of conductor 4 from that example and $\chi_3 = \psi^{-1} = \psi$.

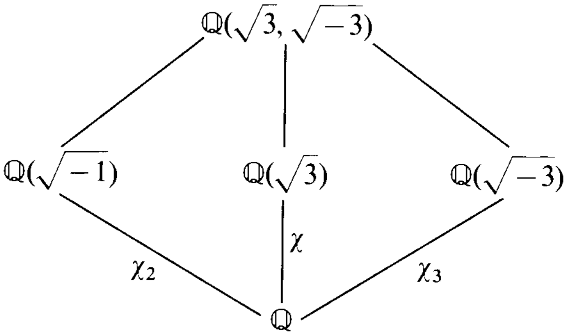
Theorem 3.5. *Let X be a group of Dirichlet characters and K the associated field. Let p be a prime number with ramification index e in K. Then $e = \#(X_p)$.*

Proof. Let n be the least common multiple of the conductors of the characters of X, so $K \subseteq \mathbb{Q}(\zeta_n)$. Let $n = p^a \cdot m$ with $p \nmid m$. Form the field $L = K(\zeta_m) = K \cdot \mathbb{Q}(\zeta_m)$. (See diagram on p. 24). Then the group of characters of L is generated by X and the characters of $(\mathbb{Z}/n\mathbb{Z})^\times$ of conductor prime to p (i.e., the characters mod m). Therefore it is the direct product of X_p with the characters of $\mathbb{Q}(\zeta_m)$. Consequently L is the compositum of $\mathbb{Q}(\zeta_m)$ with the field $F \subseteq \mathbb{Q}(\zeta_{p^a})$ belonging to X_p. Since p is unramified in $\mathbb{Q}(\zeta_m)$, the ramification index for p in K is the same as for p in L. Since L/F is unramified for p, this ramification index is the same as that for F, which is $\deg(F/\mathbb{Q}) = \#(X_p)$. This completes the proof.



□

What happens in the proof is maybe best explained by an example. Consider the quadratic character χ mod 12 corresponding to the field $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{12})$. Then $\chi = \chi_2\chi_3$ as above. The ramifications at 2 and 3 are occurring simultaneously, but we want to isolate, say, the prime 2. So we adjoin the character χ_3 and obtain the group generated by $\chi_2\chi_3$ and χ_3, which is also generated by χ_2 and χ_3. We now have the picture



So we have "split" the field $\mathbb{Q}(\sqrt{3})$ so as to isolate the ramification at 2.

Corollary 3.6. *Let χ be a Dirichlet character and K the associated field. Then p ramifies in $K \Leftrightarrow \chi(p) = 0$ (equivalently $p \mid f$).*

More generally, let L be the field associated with a group X of Dirichlet characters. Then p is unramified in $L/\mathbb{Q} \Leftrightarrow \chi(p) \neq 0$ for all $\chi \in X$.

Proof. p ramifies in $L/\mathbb{Q} \Leftrightarrow X_p \neq 1 \Leftrightarrow \exists \chi \in X$ with $\chi_p \neq 1 \Leftrightarrow \exists \chi \in X$ with $p \mid f_\chi \Leftrightarrow \exists \chi \in X$ with $\chi(p) = 0$. □

Theorem 3.7. *Let X be a group of Dirichlet characters, K the associated field. Let*

$$Y = \{\chi \in X \mid \chi(p) \neq 0\}, \qquad Z = \{\chi \in X \mid \chi(p) = 1\}.$$

Then

$$e = [X : Y], \qquad f = [Y : Z], \quad \text{and} \quad g = [Z : 1]$$

are the ramification index for p in K, the residue class degree, and the number of primes lying above p, respectively. In fact

$$X/Y \simeq \text{the inertia group}, \qquad X/Z \simeq \text{the decomposition group},$$

$$Y/Z \text{ is cyclic of order } f.$$

Proof. Let L be the subfield of K corresponding to Y. By Corollary 3.6, L is the maximal subfield of K in which p is unramified. It is a standard fact from algebraic number theory that L is then the fixed field of the inertia group, so the inertia group is $\mathrm{Gal}(K/L)$. Under the pairing

$$\mathrm{Gal}(K/\mathbb{Q}) \times X \to \mathbb{C}^\times$$

we have $Y = \mathrm{Gal}(K/L)^\perp$ by the correspondence between subgroups and subfields, so

$$\begin{aligned} X/Y &= \mathrm{Gal}(K/\mathbb{Q})\hat{}/\mathrm{Gal}(K/L)^\perp = \mathrm{Gal}(K/L)\hat{} \\ &\simeq \mathrm{Gal}(K/L). \end{aligned}$$

Since the ramification index equals the order of the inertia group, we have $e = [X : Y]$.

We now restrict our attention to the extension $L/\mathbb{Q}$, which is unramified at p and has Y as its group of characters. Let $n = lcm\ f_\chi\ (\chi \in Y)$. Then $p \nmid n$ and $L \subseteq \mathbb{Q}(\zeta_n)$. The Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$ and the Frobenius for p is $p \pmod n$, which corresponds to the map $\zeta_n \mapsto \zeta_n^p$. The Galois group of $L/\mathbb{Q}$ is a quotient group of $(\mathbb{Z}/n\mathbb{Z})^\times$ by $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)$. The Frobenius σ_p for $L/\mathbb{Q}$ is just the coset of p in this quotient. But if $\chi \in Y$ then χ kills $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)$. Therefore $\chi(\sigma_p) = \chi(p)$, so $\chi(\sigma_p) = 1 \Leftrightarrow \chi(p) = 1$. Therefore $Z = \langle\sigma_p\rangle^\perp$ under the pairing

$$\mathrm{Gal}(L/\mathbb{Q}) \times Y \to \mathbb{C}^\times,$$

where $\langle\sigma_p\rangle$ denotes the cyclic group (of order f) generated by σ_p. Consequently

$$Y/Z \simeq \widehat{\langle\sigma_p\rangle} \simeq \langle\sigma_p\rangle,$$

so $f = [Y : Z]$. Since the fixed field of the Frobenius is the splitting field for p, it also follows that Z is the group of characters corresponding to the splitting field, which is of degree g; so $g = [Z : 1]$.

Returning to the extension $K/\mathbb{Q}$, we note that the splitting field is the fixed field of the decomposition group (which is generated by the inertia group and an extension of σ_p to K). Therefore, as above, we obtain $X/Z \simeq$ the decomposition group. This completes the proof. □

We now show how Theorem 3.5 may be used to construct unramified extensions.

Proposition 3.8. *Let G be any finite abelian group. Then there exist fields L and K such that*

(*a*) $\mathrm{Gal}(L/K) \simeq G$, *and*
(*b*) *L/K is unramified at all primes (including the archimedean primes).*

We may also make $L/\mathbb{Q}$ abelian and $K/\mathbb{Q}$ cyclic.

Proof. By the structure theorem for finite abelian groups, we may write

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z}$$

for some integers $n_1, \ldots, n_r$. Let $p_1, \ldots, p_r$ be distinct primes satisfying $p_i \equiv 1 \pmod{2n_i}$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q})$ is cyclic of order $p_i - 1$, there exists a character ψ_i of conductor p_i and order $p_i - 1$. Let $\chi_i = \psi_i^{(p_i-1)/n_i}$. Since $(p_i - 1)/n_i$ is even, $\chi_i(-1) = +1$. Let p_{r+1} be another odd prime and let χ_{r+1} be an odd character of conductor p_{r+1} (for example, ψ_{r+1}). Define

$$\chi = \chi_1 \cdots \chi_{r+1},$$

and let K be the corresponding field. Since

$$\chi(-1) = \chi_1(-1) \cdots \chi_r(-1)\chi_{r+1}(-1) = -1,$$

K is complex, so every extension of K is unramified at the archimedean primes.

Let X be the group generated by $\{\chi_1, \ldots, \chi_{r+1}\}$ and let L be the corresponding field. Clearly X_{p_i} is generated by χ_i for $1 \leq i \leq r + 1$ and X_p is trivial for all other primes p. It follows from Theorem 3.5 that both L and K have the same ramification indices at each finite prime. Therefore L/K is unramified at all primes.

Observing that X is also generated by $\{\chi_1, \ldots, \chi_r, \chi\}$, we easily see that

$$\begin{aligned}\mathrm{Gal}(L/K) &\simeq X/\langle\chi\rangle = \langle\chi_1, \ldots, \chi_r\rangle \\ &\simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z} \simeq G.\end{aligned}$$

This completes the proof. □

Corollary 3.9. *Given any finite abelian group G, there exists a cyclic extension K of $\mathbb{Q}$ such that the ideal class group of K contains a subgroup isomorphic to G.*

Proof. We shall use one of the main results of class field theory:

Let K be a number field and let H be the maximal unramified (at all primes, finite and infinite) abelian extension of K. Then $\mathrm{Gal}(H/K)$ is isomorphic to the ideal class group of K (the field H is called the Hilbert class field of K).

By Proposition 3.8 there exists K, and a subextension of H/K with Galois group G. Therefore the ideal class group has a quotient group isomorphic to G. The corollary follows from the next lemma.

Lemma 3.10. *If A is a finite abelian group and B is a subgroup, then A contains a subgroup isomorphic to A/B.*

Proof. This result could be proved via the structure theory of finite abelian groups. Another proof is the following:

$$A/B \simeq (A/B)\hat{} \simeq B^{\perp} \subseteq \hat{A} \simeq A. \qquad \square\square$$

It is unknown whether or not every finite abelian group occurs as the class group of some number field.

We finish this chapter with a useful result which relates to the material of this chapter but which will be proved in the next chapter.

Theorem 3.11 (Conductor–Discriminant Formula). *Let K be the number field associated to the group X of Dirichlet characters. Then the discriminant of K is given by*

$$d(K) = (-1)^{r_2} \prod_{\chi \in X} f_\chi.$$

This theorem can be very useful for computing discriminants of abelian number fields. For example, consider the real subfield of $\mathbb{Q}(\zeta_p)$. The group of characters consists of the trivial character of conductor 1 and $(p-3)/2$ other characters, all of conductor p. Since $r_2 = 0$ we have $d(\mathbb{Q}(\zeta_p + \zeta_p^{-1})) = p^{(p-3)/2}$.

Notes

The use Dirichlet characters to describe the arithmetic of an abelian field can be found in Leopoldt [9]. The above proofs of Proposition 3.8 and Corollary 3.9 are from Hasse [3]. For a generalization of Proposition 3.8 to non-abelian groups, see Fröhlich [1]. It can be shown that any finite abelian group occurs as a subgroup of the class group of some cyclotomic field $\mathbb{Q}(\zeta_n)$. See Cornell [1]. The techniques of Corollary 3.9 do not suffice for this, since the unramified extension constructed there is contained in a cyclotomic field; hence it collapses when it is lifted (Proposition 4.11 fails). It is not known whether or not every finite abelian group occurs as the class group of some number field. However, every finite abelian ℓ-group is the ℓ-Sylow subgroup of the class group for some number field (Yahagi [1]). The corresponding result for divisor classes of degree 0 is false for function fields over finite fields (Stichtenoth [1]).

The techniques of Proposition 3.8 are part of what is known as genus theory. For more on this useful subject, see Ishida [1].

For more on the conductor–discriminant formula, see Hasse [2].

Exercises

3.1. Show that if $(f_\chi, f_\psi) = 1$ then $f_{\chi\psi} = f_\chi f_\psi$.

3.2. Suppose X_i is a group of Dirichlet characters corresponding to the field K_i, $i = 1, 2$. Show that (a) $X_1 \subseteq X_2 \Leftrightarrow K_1 \subseteq K_2$, and (b) the group generated by X_1 and X_2 corresponds to the composition $K_1 K_2$.

3.3. Let K be the field corresponding to the group X. Describe, in terms of X, the maximal abelian extension L of K which is abelian over $\mathbb{Q}$ and is unramified (over K)

at all primes. Do this for both the case where there is no ramification at the infinite primes and the case where ramification at infinity is allowed. You may assume the Kronecker–Weber theorem, which says that all abelian extensions of $\mathbb{Q}$ lie inside cyclotomic fields.

3.4. Using the notation of Exercise 3.3, let K be a quadratic field. Give the field L explicitly in the form $\mathbb{Q}(\alpha, \beta, \gamma, \ldots)$. Conclude that if the discriminant of K has s distinct prime factors then (a) 2^{s-1} divides the class number if K is imaginary, (b) 2^{s-2} divides the class number if K is real. (This relates to the theory of genera. L is called the genus field.)

3.5. (a) Show that there are two quadratic characters of conductor exactly 8, one of which is even, the other odd.
(b) Show that if $f = 4$ or an odd prime, then there is a quadratic character of conductor exactly f.
(c) Let D be the discriminant of a quadratic field. Show there is a quadratic character of conductor $|D|$ and show this character is unique unless $8 \mid D$, in which case there are two such characters, one even and one odd.
(d) Show that for any integer D there is at most one quadratic field whose discriminant is $\pm D$, unless $8 \mid D$, in which case there are can be two such fields, one real and the other imaginary.
(e) Show that every quadratic field is contained in a cyclotomic field. If the discriminant is D, we may use $\mathbb{Q}(\zeta_{|D|})$; show that $\mathbb{Q}(\zeta_n)$ with $n < |D|$ does not contain the quadratic field.

3.6. (a) Let χ be a nontrivial character. Show that

$$\sum_{a=1}^{f} \chi(a) = 0.$$

(*Hint*: multiply by $\chi(b)$, with $\chi(b) \neq 1$.)
(b) Suppose n is a positive integer and suppose $a \not\equiv 1 \pmod{n}$ and $(a, n) = 1$. Show that there is a character χ defined modulo n (possibly of smaller conductor) such that $\chi(a) \neq 1$. Use this fact to show

$$\sum_{\chi \bmod n} \chi(a) = 0.$$

If we do not assume $(a, n) = 1$ then this is not necessarily true. Show

$$\sum_{\chi \bmod 12} \chi(4) = 2.$$

(This is one disadvantage of using primitive characters.)

3.7. Let $\chi = \prod \chi_p$ be the decomposition of a character χ as in the discussion preceding Theorem 3.5.
(a) Show that $(\chi\psi)_p = \chi_p\psi_p$.
(b) Show that if $(f_\chi, f_\psi) = 1$ then $\chi(a)\psi(a) = \chi\psi(a)$ for all a.
(c) Show that $\chi(a)\psi(a) = \chi\psi(a)$ unless $\chi(a) = \psi(a) = 0$ (χ and ψ arbitrary).

Chapter 4

Dirichlet L-series and Class Number Formulas

In this chapter we review some of the basic facts about L-series. Then their values at negative integers are given in terms of generalized Bernoulli numbers. Finally, we discuss the values at 1 and relations with class numbers.

Let χ be a Dirichlet character of conductor f. The L-series attached to χ is defined by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad \operatorname{Re}(s) > 1.$$

For $\chi = 1$, this is the usual Riemann zeta function. It is well known that $L(s, \chi)$ may be continued analytically to the whole complex place, except for a simple pole at $s = 1$ when $\chi = 1$.

Let $\Gamma(s)$ be the gamma function, $\tau(\chi) = \sum_{a=1}^{f} \chi(a) e^{2\pi i a/f}$ be a Gauss sum, and $\delta = 0$ if $\chi(-1) = 1$, $\delta = 1$ if $\chi(-1) = -1$. Then

$$\left(\frac{f}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s, \chi) = W_\chi \left(\frac{f}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s, \bar{\chi}),$$

where

$$W_\chi = \frac{\tau(\chi)}{\sqrt{f} i^\delta}.$$

It will follow from Lemma 4.8 that $|W_\chi| = 1$. The functional equation may be rewritten as

$$\Gamma(s) \cos\left(\frac{\pi(s-\delta)}{2}\right) L(s, \chi) = \frac{\tau(\chi)}{2 i^\delta} \left(\frac{2\pi}{f}\right)^s L(1-s, \bar{\chi}).$$

Also $L(s, \chi)$ has the convergent Euler product expansion

$$L(s, \chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}, \qquad \mathrm{Re}(s) > 1.$$

It follows that $L(s, \chi) \neq 0$ for $\mathrm{Re}(s) > 1$. It is also true that $L(1, \chi) \neq 0$, but this is a deeper fact which will be proved later. From the functional equation we find that for $n \in \mathbb{Z}$, $n \geq 1$, we have

$$L(1 - n, \chi) \neq 0 \quad \text{if } n \equiv \delta \ (\mathrm{mod}\ 2)$$

and

$$L(1 - n, \chi) = 0 \quad \text{if } n \not\equiv \delta \ (\mathrm{mod}\ 2),$$

except for the case $\chi = 1$, $n = 1$, where we have $L(0, 1) = \zeta(0) = -\frac{1}{2}$. This exception is easily seen to result from the fact that the only pole for L-series occurs for $\chi = 1$ at $s = 1$.

More generally, we may define the Hurwitz zeta function

$$\zeta(s, b) = \sum_{n=0}^{\infty} \frac{1}{(b + n)^s}, \qquad \mathrm{Re}(s) > 1, \qquad 0 < b \leq 1.$$

Then

$$L(s, \chi) = \sum_{a=1}^{f} \chi(a) f^{-s} \zeta\left(s, \frac{a}{f}\right).$$

The functions $f^{-s}\zeta(s, a/f) = \sum_{m \equiv a(f)} m^{-s}$ are sometimes called partial zeta functions. They do not usually have Euler product expansions or nice functional equations, but they may be analytically continued to the whole complex plane, except for a pole at $s = 1$.

We wish to give the numbers $L(1 - n, \chi)$ explicitly. For this we need the generalized Bernoulli numbers. The ordinary Bernoulli numbers B_n are defined by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

The generalized Bernoulli numbers $B_{n,\chi}$ are defined by

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

Note that when $\chi = 1$ we have

$$\sum_{n=0}^{\infty} B_{n,1} \frac{t^n}{n!} = \frac{te^t}{e^t - 1} = \frac{t}{e^t - 1} + t,$$

so $B_{n,1} = B_n$ except for $n = 1$, when we have $B_{1,1} = \frac{1}{2}$, $B_1 = -\frac{1}{2}$. Also observe that if $\chi \neq 1$ then $B_{0,\chi} = 0$, since $\sum_{a=1}^{f} \chi(a) = 0$.

We shall also need the Bernoulli polynomials $B_n(X)$ defined by

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=1}^{\infty} B_n(X)\frac{t^n}{n!}.$$

An easy calculation shows that

$$B_n(1 - X) = (-1)^n B_n(X).$$

Since the generating function is the product of

$$\frac{t}{e^t - 1} = \sum B_n \frac{t^n}{n!} \quad \text{and} \quad e^{Xt} = \sum X^n \frac{t^n}{n!},$$

it follows easily that

$$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}.$$

Proposition 4.1. *Let F be any multiple of f. Then*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

PROOF.

$$\sum_{n=0}^{\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) \frac{t^n}{n!} = \sum_{a=1}^{F} \chi(a) \frac{te^{(a/F)Ft}}{e^{Ft} - 1}.$$

Let $g = F/f$ and $a = b + cf$. Then we have

$$\sum_{b=1}^{f} \sum_{c=0}^{g-1} \chi(b) \frac{te^{(b+cf)t}}{e^{fgt} - 1} = \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

The result follows. □

In particular, since $B_1(X) = X - \frac{1}{2}$, we have

$$B_{1,\chi} = \frac{1}{f} \sum_{a=1}^{f} \chi(a) a, \qquad \chi \neq 1.$$

It is easy to see that the defining relation for the $B_{n,\chi}$ is an even function of t when χ is even and odd when χ is odd. Therefore

$$B_{n,\chi} = 0 \quad \text{if } n \not\equiv \delta \pmod 2,$$

with the usual exception $B_{1,1} = \frac{1}{2}$ (or $B_1 = -\frac{1}{2}$).

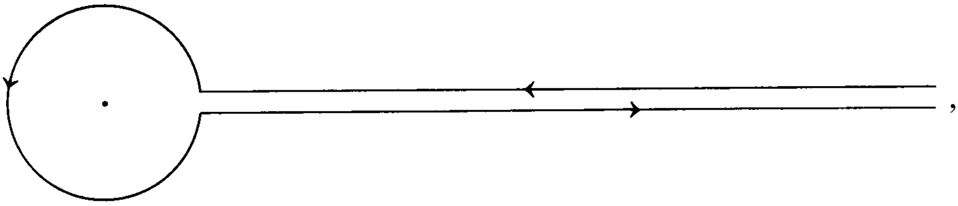
At this point the reader has probably conjectured that there is a relationship between $L(1 - n, \chi)$ and $B_{n,\chi}$; so we prove the following result.

Theorem 4.2. $L(1 - n, \chi) = -B_{n,\chi}/n$, $n \geq 1$. *More generally*, $\zeta(1 - n, b) = -B_n(b)/n$, $0 < b \leq 1$.

Proof. Let

$$F(t) = \frac{te^{(1-b)t}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(1-b)\frac{t^n}{n!}.$$

Define $H(s) = \int F(z)z^{s-2}\,dz$, where the integral is over the following path



which consists of the positive real axis (top side), a circle C_ε around 0 of radius ε, and the positive real axis (bottom side). We interpret z^s to mean $\exp(s \log z)$, where we take log to be defined by $\log t$ on the top side of the real axis and $\log t + 2\pi i$ on the bottom side. It is easy to see that $H(s)$ is defined and analytic for all s. We may write

$$H(s) = (e^{2\pi i s} - 1)\int_\varepsilon^\infty F(t)t^{s-2}\,dt + \int_{C_\varepsilon} F(z)z^{s-2}\,dz.$$

Assume first that $\mathrm{Re}(s) > 1$. Then $\int_{C_\varepsilon} \to 0$ as $\varepsilon \to \infty$, so

$$\begin{aligned} H(s) &= (e^{2\pi i s} - 1)\int_0^\infty F(t)t^{s-2}\,dt \\ &= (e^{2\pi i s} - 1)\int_0^\infty t^{s-1}\sum_{m=0}^{\infty} e^{-(b+m)t}\,dt \\ &= (e^{2\pi i s} - 1)\sum_{m=0}^{\infty}\int_0^\infty t^{s-1}e^{-(b+m)t}\,dt \\ &= (e^{2\pi i s} - 1)\sum_{m=0}^{\infty}\frac{1}{(m+b)^s}\Gamma(s) \\ &= (e^{2\pi i s} - 1)\Gamma(s)\zeta(s, b). \end{aligned}$$

Therefore $\zeta(s, b) = H(s)/(e^{2\pi i s} - 1)\Gamma(s)$, which by analytic continuation holds for all $s \neq 1$. Incidentally, this gives the analytic continuation of $\zeta(s, b)$.

We now assume that $s = 1 - n$, where $n \geq 1$ is an integer. Then $e^{2\pi i s} = 1$, so

$$H(1-n) = \int_{C_\varepsilon} F(z)z^{-n-1}\,dz = (2\pi i)\frac{B_n(1-b)}{n!}.$$

It is easy to show that

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

Therefore

$$\zeta(1-n, b) = (-1)^{n-1}\frac{B_n(1-b)}{n} = -\frac{B_n(b)}{n}.$$

Consequently

$$\begin{aligned} L(1-n, \chi) &= \sum_{a=1}^{f} \chi(a) f^{n-1} \zeta\left(1-n, \frac{a}{f}\right) \\ &= -\frac{1}{n}\sum_{a=1}^{f} \chi(a) f^{n-1} B_n\left(\frac{a}{f}\right) \\ &= -\frac{B_{n,\chi}}{n}. \end{aligned}$$

This completes the proof. □

We now turn our attention to the value of $L(1, \chi)$. It is well known that $L(1, \chi) \neq 0$. One proof uses the following.

Theorem 4.3. *Let X be a group of Dirichlet characters, K the associated field, and $\zeta_K(s)$ the Dedekind zeta function of K. Then*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).$$

Proof. It suffices to consider the Euler factors corresponding to each prime p. Suppose

$$(p) = (\mathscr{P}_1 \dots \mathscr{P}_g)^e$$

is the prime factorization of p in K, and each $\mathscr{P}$ has residue class degree f, $N\mathscr{P} = p^f$. Then $\zeta_K(s)$ contains the factor

$$\prod_{\mathscr{P} \mid p} (1 - (N\mathscr{P})^{-s})^{-1} = (1 - p^{-fs})^{-g}.$$

The L-series gives us $\prod_\chi (1 - \chi(p)p^{-s})^{-1}$. Those χ with $\chi(p) = 0$ do not contribute so we ignore them. By Theorem 3.7, Y/Z is cyclic of order f, where Y is the group of those $\chi \in X$ with $\chi(p) \neq 0$ and Z consists of those with $\chi(p) = 1$. As χ runs through a set of coset representatives for Y/Z, $\chi(p)$ runs through all fth roots of unity. Each coset has g elements. Since

$$\prod_{a=0}^{f-1} (1 - \zeta_f^a p^{-s}) = (1 - p^{-fs}),$$

the result follows. □

Corollary 4.4. $L(1, \chi) \neq 0$.

Proof. Let K be the field belonging to χ. It is well known that the zeta function of K has a (simple) pole at $s = 1$. Let b be the order of χ. Then

$$\zeta_K(s) = \prod_{a=0}^{b-1} L(s, \chi^a) = \zeta(s) \cdot \prod_{a=1}^{b-1} L(s, \chi^a).$$

Since $\zeta(s)$ has only a simple pole at $s = 1$, none of the factors $L(s, \chi^a)$ can vanish at $s = 1$. This completes the proof. □

The classical application of Corollary 4.4 is the following.

Theorem 4.5 (Dirichlet). *Let $(a, n) = 1$. Then there are infinitely many primes $p \equiv a$ (mod n).*

Proof. Let χ be a Dirichlet character. Then for $\mathrm{Re}(s) > 1$ we have

$$\begin{aligned}\log L(s, \chi) &= -\sum_p \log(1 - \chi(p)p^{-s}) \\ &= \sum_p \sum_{m=1}^{\infty} \frac{\chi(p)^m p^{-sm}}{m} \\ &= \sum_p \frac{\chi(p)}{p^s} + g_\chi(s),\end{aligned}$$

where trivial estimates show that $g_\chi(s)$ is holomorphic for $\mathrm{Re}(s) > \frac{1}{2}$. Therefore, summing over all characters χ mod n, we have

$$\sum_{\chi \bmod n} \chi(a^{-1}) \log L(s, \chi) = \sum_{p \equiv a(n)} \frac{\phi(n)}{p^s} + g(s)$$

with $g(s)$ holomorphic for $\mathrm{Re}(s) > \frac{1}{2}$ (we have used Exercise 3.6).

Now let $s \to 1$. Since $L(s, 1) = \zeta(s)$ has a pole at $s = 1$, $\log L(s, 1) \sim -\log(s - 1) \to \infty$. Since $L(1, \chi) \neq 0, \infty$ for $\chi \neq 1$, $\log L(s, \chi)$ remains bounded. Therefore the left-hand side $\to \infty$, so the same is true for the right-hand side. Since $g(s)$ is holomorphic at $s = 1$, we must have

$$\lim_{s \to 1} \sum_{p \equiv a(n)} \frac{\phi(n)}{p^s} = \infty.$$

Therefore the sum cannot have finitely many terms. This completes the proof. □

We now use Theorem 4.3 to give a proof of Theorem 3.6, the Conductor–Discriminant Formula. Recall that X is a group of Dirichlet characters associated to a field K, so Theorem 4.3 applies. It is known (see, for example, Lang [1], p. 254) that $\zeta_K(s)$ satisfies the functional equation

$$A^s \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta_K(s) = A^{1-s} \Gamma\left(\frac{1-s}{2}\right)^{r_1} \Gamma(1-s)^{r_2} \zeta_K(1-s),$$

where

$$A = 2^{-r_2}\pi^{-N/2}\sqrt{|d(K)|}.$$

Here $N = \deg(K/\mathbb{Q})$ and r_1 and r_2 have their usual meanings. Since $K/\mathbb{Q}$ is Galois, either $r_1 = 0$ or $r_2 = 0$. Suppose first that $r_2 = 0$, so K is totally real and $\chi(-1) = 1$ for all χ. The functional equations for the L-series read

$$\left(\frac{f}{\pi}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)L(s, \chi) = W_\chi\left(\frac{f}{\pi}\right)^{(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)L(1-s, \bar{\chi}).$$

Taking the product over all χ and comparing with the equation for $\zeta_K(s)$, we find that we must have

$$A^2 = \prod_\chi\left(\frac{f_\chi}{\pi}\right) \quad \text{and} \quad \prod_\chi W_\chi = 1.$$

Consequently $|d(K)| = \prod_\chi f_\chi$, as desired.

If $r_1 = 0$ then $r_2 = N/2$. In this case, half the characters are even and half are odd. Using the identity

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) = 2^{1-s}\sqrt{\pi}\,\Gamma(s)$$

(see, for example, Whittaker and Watson [1] p. 240), we again obtain the desired result. The sign of the discriminant is determined, as usual, by Lemma 2.2. This completes the proof of Theorem 3.6. □

Corollary 4.6.

$$\prod_{\chi\in X}\tau(\chi) = \begin{cases}\sqrt{|d(K)|}, & \textit{if } K \textit{ is totally real}\\ i^{\deg(K/\mathbb{Q})/2}\sqrt{|d(K)|}, & \textit{if } K \textit{ is complex.}\end{cases}$$

Proof. It follows from the above proof that $\prod_{\chi\in X} W_\chi = 1$. The result follows immediately. □

Note that this corollary contains the famous theorem on the sign of the Gaussian sum: if χ is the unique quadratic character mod p then $\tau(\chi) = \sqrt{p}$ if $p \equiv 1 \pmod 4$ and $\tau(\chi) = i\sqrt{p}$ if $p \equiv 3 \pmod 4$.

We now evaluate $L(1, \chi)$. For odd χ this is easily accomplished via the functional equation:

$$\begin{aligned}L(1, \chi) &= \frac{\tau(\chi)}{2i}\frac{2\pi}{f}L(0, \bar{\chi})\\ &= \frac{\pi i\tau(\chi)}{f}B_{1,\bar{\chi}}.\end{aligned}$$

For even characters the argument is somewhat more difficult. We first need some lemmas.

Lemma 4.7. *For every integer b,*

$$\sum_{a=1}^{f} \bar{\chi}(a)e^{2\pi iab/f} = \chi(b)\tau(\bar{\chi}).$$

In particular,

$$\overline{\tau(\chi)} = \chi(-1)\tau(\bar{\chi}).$$

PROOF. If $(b, f) = 1$, then change variables: $c \equiv ab \pmod{f}$. Since everything depends only on residue classes mod f, the result follows in this case. If $(b, f) = d > 1$ then the result is still true, since both sides vanish. The right-hand side is obviously 0. For the left, observe that if $\chi(y) = 1$ for all $y \equiv 1 \pmod{f/d}$, $(y, f) = 1$, then χ would be defined mod f/d (note that $(\mathbb{Z}/f\mathbb{Z})^\times$ maps onto $(\mathbb{Z}/(f/d)\mathbb{Z})^\times$), hence could not have conductor f. Therefore there exists $y \equiv 1 \pmod{f/d}$, $(y, f) = 1$, such that $\chi(y) \neq 1$. Since $dy \equiv d \pmod{f}$, so $by \equiv b \pmod{f}$, we have

$$\begin{aligned}\sum_{a=1}^{f} \bar{\chi}(a)e^{2\pi iab/f} &= \sum_{a=1}^{f} \bar{\chi}(a)e^{2\pi iaby/f}\\ &= \chi(y)\sum_{a=1}^{f} \bar{\chi}(a)e^{2\pi iab/f}.\end{aligned}$$

Since $\chi(y) \neq 1$, the sum is 0.

For the second statement, use the first statement with $b = -1$. □

Lemma 4.8. $|\tau(\chi)| = \sqrt{f_\chi}$

PROOF.

$$\begin{aligned}\phi(f)|\tau(\chi)|^2 &= \sum_{b=1}^{f} |\chi(b)\tau(\chi)|^2 \quad \text{(note only } \phi(f) \text{ terms are non-zero)}\\ &= \sum_{b=1}^{f}\sum_{a=1}^{f} \chi(a)e^{2\pi iab/f}\sum_{c=1}^{f}\bar{\chi}(c)e^{-2\pi ibc/f} \quad \text{(by Lemma 4.7)}\\ &= \sum_a\sum_c \chi(a)\bar{\chi}(c)\sum_b e^{2\pi ib(a-c)/f}\\ &= \sum_a \chi(a)\bar{\chi}(a)f \quad \text{(the sum over } b \text{ is 0 unless } a = c)\\ &= f\phi(f),\end{aligned}$$

since $\chi(a)\bar{\chi}(a) = 1$ if $(a, f) = 1$, and is 0 otherwise. This completes the proof. □

We now evaluate $L(1, \chi)$. We ignore questions of convergence, most of which may be treated by partial summation techniques.

$$\begin{aligned} L(1, \chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{1}{n} \frac{1}{\tau(\bar{\chi})} \sum_{a=1}^{f} \bar{\chi}(a) e^{2\pi i a n/f} \\ &= \frac{1}{\tau(\bar{\chi})} \sum_{a=1}^{f} \bar{\chi}(a) \sum_{n=1}^{\infty} \frac{1}{n} e^{2\pi i a n/f} \\ &= \frac{-1}{\tau(\bar{\chi})} \sum_{a=1}^{f} \bar{\chi}(a) \log(1 - \zeta_f^a), \qquad \zeta_f = e^{2\pi i/f}. \end{aligned}$$

Since $\tau(\bar{\chi}) = \chi(-1)\overline{\tau(\chi)} = \chi(-1)f/\tau(\chi)$, we obtain

$$L(1, \chi) = -\frac{\chi(-1)\tau(\chi)}{f} \sum_{a=1}^{f} \bar{\chi}(a) \log(1 - \zeta_f^a).$$

Now $\log(1 - \zeta_f^a) + \log(1 - \zeta_f^{-a}) = 2\log|1 - \zeta_f^a|$. Consequently, if χ is even, so $\chi(a) = \chi(-a)$, we have

$$L(1, \chi) = \frac{-\tau(\chi)}{f} \sum_{a=1}^{f} \bar{\chi}(a) \log|1 - \zeta_f^a|.$$

We have proved the following (odd characters were treated before Lemma 4.7).

Theorem 4.9.

$$L(1, \chi) = \pi i \frac{\tau(\chi)}{f} B_{1,\bar{\chi}} = \pi i \frac{\tau(\chi)}{f} \frac{1}{f} \sum_{a=1}^{f} \bar{\chi}(a) a \quad \text{if } \chi(-1) = -1.$$

$$L(1, \chi) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \bar{\chi}(a) \log|1 - \zeta_f^a| \quad \text{if } \chi(-1) = 1, \chi \neq 1. \qquad \square$$

Note that the theorem implies that $B_{1,\chi} \neq 0$ if χ is odd. There is no elementary proof known for this fact.

Later we shall give algebraic interpretations of these formulas.

We now discuss class number formulas. The zeta function of a field K has a simple pole at $s = 1$ with residue

$$\frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|d|}},$$

where r_1, r_2 are as usual, h is the class number of K, R is the regulator (see below), w is the number of roots of unity in K, and d is the discriminant. Suppose K belongs to a group X of Dirichlet characters. Using the relation $\zeta_K(s) = \prod L(s, \chi)$, and the fact that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1, we obtain

$$\frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|d|}} = \prod_{\substack{\chi \in X \\ \chi \neq 1}} L(1, \chi).$$

Using Theorem 4.9, we now have in theory a method for calculating the class number of an abelian number field, as long as we can calculate the regulator, which involves finding a basis for the group of units. Usually this computation becomes too lengthy to be practical. So we need another method of obtaining information about the class number. For this, we shall factor the class number into two factors, one of which is relatively easy to work with.

The next few results hold not only for abelian fields, but also for a wider class, namely CM-fields (also called J-fields). A field is called totally real if all its embeddings into $\mathbb{C}$ lie in $\mathbb{R}$ and totally imaginary if none of its embeddings lie in $\mathbb{R}$. A CM-field is a totally imaginary quadratic extension of a totally real number field. Such a field may be obtained by starting with a totally real field and adjoining the square root of a number all of whose conjugates are negative. All of the fields $\mathbb{Q}(\zeta_n)$ are CM-fields. Their maximal real subfields are $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, and we obtain $\mathbb{Q}(\zeta_n)$ by adjoining the square root of $\zeta_n^2 + \zeta_n^{-2} - 2$ (the discriminant of $X^2 - (\zeta_n + \zeta_n^{-1})X + 1$), which is totally negative.

One feature of a CM-field is that complex conjugation on $\mathbb{C}$ induces an automorphism on the field which is independent of the embedding into $\mathbb{C}$. Namely, let K be CM, K^+ the real subfield. Let $\phi, \psi\colon K \to \mathbb{C}$ be two embeddings. We claim that $\phi^{-1}(\overline{\phi(\alpha)}) = \psi^{-1}(\overline{\psi(\alpha)})$ for all $\alpha \in K$. First note that $\phi(K)/\phi(K^+)$ is quadratic, hence normal, and complex conjugation fixes $\phi(K^+)$. Therefore $\bar{\phi}(K) = \phi(K)$. In particular, $\phi^{-1}(\bar{\phi})$ is defined. Clearly both $\phi^{-1}(\bar{\phi})$ and $\psi^{-1}(\bar{\psi})$ are automorphisms of K and both fix K^+ since it is totally real. Since K is totally imaginary, neither automorphism can be the identity. Therefore they must be equal since $\mathrm{Gal}(K/K^+)$ has order 2. Consequently, when working with CM-fields we may talk about $\bar{\alpha}$, which is well-defined. Also, $|\alpha|^2 = \alpha\bar{\alpha}$ is independent of the embedding. This is useful when applying Lemma 1.6. For example, if ε is a unit then $\varepsilon/\bar{\varepsilon}$ is an algebraic integer of absolute value 1, hence a root of unity.

Theorem 4.10. *Let K be a CM-field, K^+ its maximal real subfield, and let h and h^+ be the respective class numbers. Then h^+ divides h.*

The quotient h^- is called the relative class number (some authors call h^- the first factor; a few call it the second factor).

Proof. We need the following result from class field theory.

Proposition 4.11. *Let K/L be an extension of number fields such that there is no nontrivial unramified (at all primes, including archimedean ones) subextension F/L with* $\mathrm{Gal}(F/L)$ *abelian. Then the class number of L divides the class number of K. (Note: this proposition is usually used in the case that K/L is totally ramified at some prime. However it could also be used if K/L is normal with a non-abelian simple group as Galois group).*

PROOF. Let H be the maximal unramified (at all primes) abelian extension of L. By class field theory, $\mathrm{Gal}(H/L)$ is isomorphic to the ideal class group of L. The assumptions on K/L imply that $H \cap K = L$. Therefore $[KH:K] = [H:L]$. But KH/K is unramified abelian, so is contained in the maximal unramified abelian extension of K. Therefore the class number of $L = [H:L] = [KH:K]$ divides the class number of K. This proves the proposition. We remark that H is called the Hilbert class field of L. □

Returning to the proof of the theorem, we observe that K/K^+ is totally ramified at the archimedean primes, so the proposition applies. This completes the proof of the theorem. □

We now prove a result which generalizes Proposition 1.5.

Theorem 4.12. *Let K be a CM-field and let E be its unit group. Let E^+ be the unit group of K^+ and let W be the group of roots of unity in K. Then*

$$Q \overset{\text{def}}{=} [E:WE^+] = 1 \text{ or } 2.$$

PROOF. Define $\phi: E \to W$ by $\phi(\varepsilon) = \varepsilon/\bar{\varepsilon}$. Since $\overline{\varepsilon^\sigma} = (\bar{\varepsilon})^\sigma$ for all embeddings $\sigma(K$ is $CM)$, we have $|\phi(\varepsilon)^\sigma| = 1$ for all σ. By Lemma 1.6, $\phi(\varepsilon) \in W$. Let $\psi: E \to W/W^2$ be the map induced by ϕ. Suppose $\varepsilon = \zeta\varepsilon_1$, where $\zeta \in W$ and $\varepsilon_1 \in E^+$. Then $\phi(\varepsilon) = \zeta^2 \in W^2$, so $\varepsilon \in \mathrm{Ker}(\psi)$. Conversely, suppose $\phi(\varepsilon) = \zeta^2 \in W^2$. Then it is easy to see that $\varepsilon_1 = \zeta^{-1}\varepsilon$ is real. It follows that $\mathrm{Ker}(\psi) = WE^+$. Since $|W/W^2| = 2$, we are done. Note that if $\phi(E) = W$ then $Q = 2$; if $\phi(E) = W^2$ then $Q = 1$. □

Corollary 4.13. *Let $K = \mathbb{Q}(\zeta_n)$. Then $Q = 1$ if n is a prime power and $Q = 2$ if n is not a prime power.*

PROOF. The proof when n is an odd prime power is exactly the same as that given in Proposition 1.5. For $p = 2$ we must argue a little differently. Suppose ε is a unit in $Q(\zeta_{2^m})$ such that $\varepsilon/\bar{\varepsilon} \notin W^2$. Then $\varepsilon/\bar{\varepsilon} = \zeta =$ a primitive 2^mth root of unity. Let N denote the norm from $\mathbb{Q}(\zeta_{2^m})$ to $\mathbb{Q}(i)$. Then $N(\zeta) = \zeta^a$, where

$$a = \sum_{\substack{0<b<2^m \\ b\equiv 1(4)}} b = \sum_{j=0}^{2^{m-2}-1} (1+4j) = 2^{m-2} + 2^{m-1}(2^{m-2}+1)$$

$$\equiv 2^{m-2} \pmod{2^{m-1}}.$$

Therefore ζ^a is a primitive 4th root of 1: $\zeta^a = \pm i$. It follows that $N(\varepsilon)/\overline{N(\varepsilon)} = \pm i$. But $N(\varepsilon)$ is a unit of $\mathbb{Q}(i)$, therefore ± 1 or $\pm i$. None of these possibilities works, so we have a contradiction. So $Q = 1$ for $\mathbb{Q}(\zeta_{2^m})$.

Now assume n is not a prime power. By Proposition 2.8, $1 - \zeta_n$ is a unit. But $(1 - \zeta_n)/(1 - \bar{\zeta}_n) = -\zeta_n$. Suppose $-\zeta_n \in W^2$. Then $-\zeta_n = (\pm\zeta_n^r)^2 = \zeta_n^{2r}$, so $-1 = \zeta_n^{2r-1}$. Clearly n must be even, so $n \equiv 0 \pmod 4$. Since $-1 = \zeta_n^{n/2}$, we have $n/2 \equiv 2r - 1 \pmod n$, therefore $n/2 \equiv -1 \pmod 2$, which is impossible. It follows that $-\zeta_n \notin W^2$, so $Q = 2$. This completes the proof. □

When $K = \mathbb{Q}(\zeta_n)$, we may prove a result which is stronger than Theorem 4.10.

Theorem 4.14. *Let C be the ideal class group of $\mathbb{Q}(\zeta_n)$ and C^+ the ideal class group of the real subfield $\mathbb{Q}(\zeta_n)^+$. Then the natural map $C^+ \to C$ is an injection.*

Proof. Suppose I is an ideal of $\mathbb{Q}(\zeta_n)^+$ which becomes principal when lifted to $\mathbb{Q}(\zeta_n)$. We must show I was principal to begin with. Let $I = (\alpha)$ with $\alpha \in \mathbb{Q}(\zeta_n)$. Then $(\bar{\alpha}/\alpha) = \bar{I}/I = (1)$, since I is real. Therefore $\bar{\alpha}/\alpha$ is a unit and has absolute value 1. By Lemma 1.6, $\bar{\alpha}/\alpha$ is a root of unity. If n is not a prime power, $Q = 2$; the proof of Theorem 4.12 shows that there is a unit ε such that $\varepsilon/\bar{\varepsilon} = \bar{\alpha}/\alpha$. Then $\alpha\varepsilon$ is real and $I = (\alpha) = (\alpha\varepsilon)$. It follows from unique factorization of ideals that $I = (\alpha\varepsilon)$ in $\mathbb{Q}(\zeta_n)^+$, so I was originally principal. Now suppose $n = p^m$. Let $\pi = \zeta_{p^m} - 1$. We have $\pi/\bar{\pi} = -\zeta_{p^m}$, which generates the roots of unity in $\mathbb{Q}(\zeta_{p^m})$. Therefore $\bar{\alpha}/\alpha = (\pi/\bar{\pi})^d$ for some d. Since the π-adic valuation takes on only even values on $\mathbb{Q}(\zeta_{p^m})^+$ and since $\alpha\pi^d$ and I are real, $d = v_\pi(\alpha\pi^d) - v_\pi(\alpha) = v_\pi(\alpha\pi^d) - v_\pi(I)$ is even. Hence $\alpha/\alpha = (-\zeta_{p^m})^d \in W^2$. In particular, $\bar{\alpha}/\alpha = \zeta/\bar{\zeta}$ for some root of unity ζ, and $\alpha\zeta$ is real. As before, $I = (\alpha\zeta)$, so I was originally principal. This completes the proof. □

This theorem is not true for arbitrary CM-fields: Since $(2, \sqrt{10})^2 = (-2)$ in $\mathbb{Q}(\sqrt{10})$, the nonprincipal ideal $(2, \sqrt{-10})$ becomes principal in $\mathbb{Q}(\sqrt{10}, \sqrt{-2})$. In general, at most one nonprincipal class becomes principal (see Theorem 10.3).

Theorem 4.12 may be used to give a relation between the regulator of K and that of K^+. Recall that the regulator of a number field L is defined as follows. Let $r = r_1 + r_2 - 1$ and let $\varepsilon_1, \dots, \varepsilon_r$ be a set of independent units of L. Write the embeddings of L into $\mathbb{C}$ as $\sigma_1, \dots, \sigma_{r_1}$, $\sigma_{r_1+1}, \dots, \sigma_{r+1}$, $\bar{\sigma}_{r_1+1}, \dots, \bar{\sigma}_{r+1}$, where σ_j, $1 \le j \le r_1$, is real, and σ_j, $\bar{\sigma}_j$, $r_1 + 1 \le j \le r + 1$, is a pair of complex embeddings. Finally let $\delta_j = 1$ if σ_j is real and $\delta_j = 2$ is σ_j is complex. The regulator is defined to be

$$R_L(\varepsilon_1, \dots, \varepsilon_r) = \text{absolute value of } \det(\delta_i \log|\varepsilon_j^{\sigma_i}|)_{1 \le i, j \le r}.$$

Note that we omit one σ_j. Since the norm of each ε is ± 1, the sum over all σ_i, $1 \le i \le r + 1$, of $\delta_i \log|\varepsilon_j^{\sigma_i}|$ is 0. Since we take the absolute value of the determinant, the possible sign change from omitting a different σ does not happen.

If $\varepsilon_1, \ldots, \varepsilon_r$ is a basis for the group of units of L modulo roots of unity, then $R_L(\varepsilon_1, \ldots, \varepsilon_r) = R_L$ is called the regulator of L. Again, the fact that we took the absolute value of the determinant makes R_L independent of the choice of basis and ordering of the σ's.

Now let $\varepsilon_1, \ldots, \varepsilon_r$ be a basis for the units of K^+ modulo $\{\pm 1\}$. Then $\varepsilon_1, \ldots, \varepsilon_r$ forms a basis for a subgroup of index Q ($=1$ or 2) in the units of K modulo roots of unity. However each $\delta_i = 1$ for K^+ and each $\delta_i = 2$ for K. Therefore

$$R_K(\varepsilon_1, \ldots, \varepsilon_r) = 2^r R_{K^+}(\varepsilon_1, \ldots, \varepsilon_r) = 2^r R_{K^+}.$$

We now need the following result.

Lemma 4.15. *Let $\varepsilon_1, \ldots, \varepsilon_r$ be independent units of a number field K which generate a subgroup A of the units of K modulo roots of unity, and let $\eta_1, \ldots, \eta_r$ generate a subgroup B. If $A \subseteq B$ is of finite index then*

$$[B:A] = \frac{R_K(\varepsilon_1, \ldots, \varepsilon_r)}{R_K(\eta_1, \ldots, \eta_r)}.$$

Proof. We may write

$$\varepsilon_i = \left(\prod_l \eta_l^{a_{il}}\right) \cdot (\text{root of unity}), \quad \text{with } a_{il} \in \mathbb{Z}.$$

Therefore

$$\delta_j \log|\varepsilon_i^{\sigma_j}| = \sum_l a_{il}\delta_j \log|\eta_l^{\sigma_j}|.$$

Consequently

$$\frac{R_K(\varepsilon_1, \ldots, \varepsilon_r)}{R_K(\eta_1, \ldots, \eta_r)} = |\det(a_{il})|.$$

By the theory of elementary divisors, there exist integer matrices M and N of determinant ± 1 such that $M(a_{il})N = \operatorname{diag}(d_1, \ldots, d_r)$; so $\det(a_{il}) = \pm \prod d_i$. But M and N correspond to changing bases of A and B, so we have bases $x_1, \ldots, x_r$ of A and $y_1, \ldots, y_r$ of B with $x_i = d_i y_i$. Therefore $B/A \simeq \bigoplus_i \mathbb{Z}/d_i\mathbb{Z}$ and $[B:A] = |\prod_i d_i|$. This completes the proof of the lemma. □

From the lemma, we see that $R_K(\varepsilon_1, \ldots, \varepsilon_r) = QR_K$, in the above notation. We have proved the following.

Proposition 4.16. *Let K be a CM-field and K^+ its maximal real subfield. Then*

$$\frac{R_K}{R_{K^+}} = \frac{1}{Q}2^r, \quad \textit{where } r = \tfrac{1}{2}\deg(K/\mathbb{Q}) - 1. \qquad \square$$

We may now return to the class number formulas. Let X be a group of Dirichlet characters and K the associated field. We assume K is totally complex, so half of the characters in X are odd and half are even. Let $n = \deg(K/\mathbb{Q})$. Then

$$\frac{2^{n/2}h(K^+)R_{K^+}}{2\sqrt{|d(K^+)|}} = \prod_{\substack{\chi \in X \\ \chi \text{ even} \\ \chi \neq 1}} L(1, \chi),$$

and

$$\frac{(2\pi)^{n/2}h(K)R_K}{w\sqrt{|d(K)|}} = \prod_{\substack{\chi \in X \\ \chi \neq 1}} L(1, \chi).$$

Dividing, we obtain

$$\frac{\pi^{n/2}h^-(K)2^{n/2}}{Qw\sqrt{|d(K)/d(K^+)|}} = \prod_{\chi \text{ odd}} L(1, \chi).$$

Now $L(1, \chi) = (\pi i \tau(\chi)/f_\chi)B_{1,\bar{\chi}}$ for χ odd, and by the conductor-discriminant formula $\sqrt{|d(K)/d(K^+)|} = (\prod_{\chi \text{ odd}} f_\chi)^{1/2}$. Also, by Corollary 4.6,

$$\prod_{\chi \text{ odd}} \tau(\chi) = i^{n/2}\sqrt{|d(K)/d(K^+)|}.$$

Putting everything together, we obtain the following.

Theorem 4.17.

$$h^-(K) = Qw \prod_{\chi \text{ odd}} (-\tfrac{1}{2}B_{1,\chi}). \qquad \square$$

Observe that this formula, as opposed to that obtained earlier, involves no transcendental quantities. It is therefore possible to use it to obtain divisibility properties of $h^-(K)$. Sometimes it is possible to obtain results about the full class number $h(K)$ from those about $h^-(K)$. Later we shall show that p divides $h(\mathbb{Q}(\zeta_p)) \Leftrightarrow p$ divides $h^-(\mathbb{Q}(\zeta_p))$. The above formula will allow us to translate the statement about p dividing h^- into one about p dividing certain Bernoulli numbers.

We close this chapter by showing that the class number of $\mathbb{Q}(\zeta_n)$ grows quite rapidly with n. For this we need the Brauer–Siegel theorem (see Lang [1]):

Suppose K runs through a sequence of number fields normal over $\mathbb{Q}$ such that

$$\frac{[K:\mathbb{Q}]}{\log|d(K)|} \to 0.$$

Then

$$\frac{\log(h(K)R_K)}{\log\sqrt{|d(K)|}} \to 1.$$

Unfortunately this result involves the regulator, so we do not immediately obtain any information about h by itself. However we may apply the result to both $\mathbb{Q}(\zeta_n)$ and its maximal real subfield, and then compare.

For convenience, let $d_n = |d(\mathbb{Q}(\zeta_n))|$, $h_n = h(\mathbb{Q}(\zeta_n))$, $R_n = R_{\mathbb{Q}(\zeta_n)}$, and let d_n^+, h_n^+, R_n^+ denote the corresponding objects for $\mathbb{Q}(\zeta_n)^+$. We first estimate d_n.

Lemma 4.18. $\log d_n = \phi(n)\log n + o(\phi(n)\log n)$.

Proof. From Proposition 2.7, we have

$$\log d_n = \phi(n)\log n - \phi(n)\sum_{p|n}\frac{\log p}{p-1}.$$

Let $m = \log n/\log 2$. Since $2^m = n$, it follows that n has at most m prime factors. Clearly

$$\sum_{p|n}\frac{\log p}{p-1} \le \sum_{i=1}^{m}\frac{\log p_i}{p_i - 1} \le 2\sum_{i=1}^{m}\frac{\log p_i}{p_i}$$

where the last two summations are over the first m primes. From the prime number theorem, it follows easily that there exists a constant C such that the mth prime is less than $x = Cm\log m$, and the number of primes less than x is less than $Dx/\log x$ for some D. Therefore

$$\sum_{p|n}\frac{\log p}{p-1} \le 2\sum_{p<x}\frac{\log p}{p} \le 2\sum_{p\le\sqrt{x}}1 + 2\sum_{\sqrt{x}<p\le x}\frac{\log x}{\sqrt{x}}$$

$$\le 2\sqrt{x} + 2\frac{\log x}{\sqrt{x}}\frac{Dx}{\log x} = 0(\sqrt{x})$$

$$= 0(\sqrt{m\log m}) = 0(\sqrt{\log n\log\log n}) = o(\log n).$$

This estimate gives the result. □

Lemma 4.19. *If n is not a prime power then $d_n = (d_n^+)^2$. If $n = p^a$ then $d_n = p(d_n^+)^2$ if $p \ne 2$, $d_n = 4(d_n^+)^2$ if $p = 2$. In all cases we have*

$$\log d_n^+ = \tfrac{1}{2}\phi(n)\log n + o(\phi(n)\log n).$$

Proof. Recall the formula (see Lang [1], pp. 60, 66, or Long [1] p. 82)

$$|d(L)| = (N\mathcal{D}_{L/K})|d(K)|^{\deg(L/K)},$$

where L/K is any extension of number fields, $\mathcal{D}_{L/K}$ is the relative different, and N is the norm from L to $\mathbb{Q}$. If the ring of integers $\mathcal{O}_L$ of L can be written in the form $\mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$, then $\mathcal{D}_{L/K}$ is the ideal of $\mathcal{O}_L$ generated by $f'(\alpha)$, where $f(X)$ is the irreducible polynomial for α over K. In the present case, we have

$$\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_n + \zeta_n^{-1}][\zeta_n]$$

and $f(X) = X^2 - (\zeta_n + \zeta_n^{-1})X + 1$, so $f'(\zeta_n) = \zeta_n - \zeta_n^{-1} = \zeta_n^{-1}(\zeta_n^2 - 1)$.

If n is not a prime power then $\zeta_n^2 - 1$ is a unit, so $\mathscr{D}_{L/K} = 1$. Therefore $d_n = (d_n^+)^2$.

If $n = p^a$, $p \neq 2$, then $N\mathscr{D} = N(\zeta_n^2 - 1) = p$, so $d_n = p(d_n^+)^2$.

If $n = 2^a$, then ζ_n^2 is a 2^{a-1}st root of 1; so $N\mathscr{D} = N(\zeta_n^2 - 1) = 4$. Therefore $d_n = 4(d_n^+)^2$.

The final statement follows from Lemma 4.18 and the fact that $\log p = 0(\log n)$. This completes the proof. □

From Lemmas 4.18 and 4.19, we have

$$\frac{\phi(n)}{\log d_n} \to 0 \quad \text{and} \quad \frac{\frac{1}{2}\phi(n)}{\log d_n^+} \to 0,$$

so the Brauer–Siegel theorem applies. Therefore

$$\log h_n R_n = \tfrac{1}{2}\log d_n + o(\log d_n)$$

and

$$\log h_n^+ R_n^+ = \tfrac{1}{2}\log d_n^+ + o(\log d_n).$$

By Proposition 4.16,

$$\log\left(\frac{R_n}{R_n^+}\right) = 0(\phi(n)).$$

Therefore

$$\begin{aligned}\log h_n^- &= \log(h_n R_n) - \log(h_n^+ R_n^+) - \log\left(\frac{R_n}{R_n^+}\right)\\ &= \tfrac{1}{2}\log d_n - \tfrac{1}{2}\log d_n^+ + 0(\phi(n)) + o(\log d_n)\\ &= \tfrac{1}{4}\phi(n)\log n + o(\phi(n)\log n).\end{aligned}$$

We have proved the following result.

Theorem 4.20. *Let h_n^- denote the relative class number for $\mathbb{Q}(\zeta_n)$. Then*

$$\log h_n^- \sim \tfrac{1}{4}\phi(n)\log n \quad \text{as } n \to \infty.$$

Therefore $h_n \to \infty$ as $n \to \infty$, so there are only finitely many n such that $\mathbb{Z}[\zeta_n]$ has unique factorization. □

(*Note*: $a \sim b$ means $a/b \to 1$).

Unfortunately the above result is not effective, in the sense that it does not allow us to compute a constant n_0 such that $h_n^- > 1$ if $n \geq n_0$. To do that we need other techniques. See Chapter 11.

Notes

For more on ordinary Bernoulli numbers, see Nielsen [1]. The generalized Bernoulli numbers were defined by Berger [1], by Ankeny–Artin–Chowla [1], and by Leopoldt [3], who used them extensively.

The standard reference for class number formulas is Hasse [1]. See also Borevich–Shafarevich [1]. The book of Hasse also contains a detailed study of the unit index Q (*warning*: Satz 29 is incorrect).

Another good reference for some of the topics of this chapter is Iwasawa [23].

Exercises

4.1. Show that for $n, k \geq 0$, $\sum_{a=0}^{k-1} a^n = [1/(n+1)](B_{n+1}(k) - B_{n+1}(0))$.

4.2. (a) Show that if $\chi \neq 1$ and $\chi(-1) = 1$ then $B_{2,\chi} = (1/f)\sum_{a=1}^{f}\chi(a)a^2$.
(b) Show that if $\chi(-1) = -1$ then

$$B_{3,\chi} = \frac{1}{f}\sum_{a=1}^{f}\chi(a)a^3 - f\sum_{a=1}^{f}\chi(a)a;$$

therefore

$$B_{3,\chi} \neq \frac{1}{f}\sum_{a=1}^{f}\chi(a)a^3.$$

4.3. (a) Use the definition of $B_{n,\chi}$ to show that

$$\limsup_{n\to\infty}\left(\frac{|B_{n,\chi}|}{n!}\right)^{1/n} = \frac{f}{2\pi}.$$

(b) Use the functional equation for $L(s, \chi)$ to show that

$$\lim_{\substack{n\to\infty \\ n\equiv\delta(2)}} \frac{\sqrt{f}}{2}\left(\frac{2\pi}{f}\right)^n \frac{|B_{n,\chi}|}{n!} = 1.$$

4.4. Show that if $m|n$ then $h(\mathbb{Q}(\zeta_m))$ divides $h(\mathbb{Q}(\zeta_n))$.

4.5. Let $p > 3$ and $p = 3 \pmod 4$, and let h be the class number of $\mathbb{Q}(\sqrt{-p})$. Let χ be the quadratic character mod p.
(a) Show that $hp = -2\sum_{0<a<p/2}\chi(a)a + p\sum_{0<a<p/2}\chi(a)$.
(b) Show that $hp = -4\sum_{0<a<p/2}\chi(2a)a + p\sum_{0<a<p/2}\chi(2a)$
(*Hint*: $\chi(2a) = -\chi(p - 2a)$).
(c) Show that $h = [1/(2 - \chi(2))]\sum_{0<a<p/2}\chi(a)$.
(d) Show that for $p \equiv 3 \pmod 4$ there are more quadratic residues than nonresidues in the interval $(0, p/2)$.

4.6. (a) Show that for $p \equiv 1 \pmod 4$ the number of quadratic residues in the interval $(0, p/2)$ equals the number of nonresidues.

(b) Let $p \equiv 1 \pmod 4$, and let h and χ be the class number and character for the field $\mathbb{Q}(\sqrt{p})$. Let $\varepsilon > 1$ be the fundamental unit and let $\zeta_p = e^{2\pi i/p}$. Show that

$$\varepsilon^{2h} = \prod_{a=1}^{p-1} (1 - \zeta_p^a)^{-\chi(a)}$$

and

$$\varepsilon^h = \prod_b \left(\sin \frac{\pi b}{p}\right) \Big/ \prod_c \left(\sin \frac{\pi c}{p}\right),$$

where b runs through the quadratic nonresidues in the interval $(0, p/2)$ and c runs through the residues in $(0, p/2)$. Since $\sin x$ is monotone increasing in $(0, \pi/2)$, this shows that the residues tend to cluster near the beginning and the nonresidues near the end of the interval $(0, p/2)$.

Chapter 5

p-adic L-functions and Bernoulli Numbers

In this chapter we shall construct p-adic analogues of Dirichlet L-functions. Since the usual series for these functions do not converge p-adically, we must resort to another procedure. The values of $L(s, \chi)$ at negative integers are algebraic, hence may be regarded as lying in an extension of $\mathbb{Q}_p$. We therefore look for a p-adic function which agrees with $L(s, \chi)$ at the negative integers. With a few minor modifications, this is possible.

The resulting p-adic L-functions will be used to prove congruences for generalized Bernoulli numbers, from which we deduce Kummer's criterion for irregularity of primes. We shall also show there are infinitely many irregular primes.

Finally we evaluate the p-adic L-functions at $s = 1$ and find a formula remarkably similar to the classical one. This yields a p-adic class number formula, from which we deduce Kummer's result "$p \mid h_p^+ \Rightarrow p \mid h_p^-$," and also a congruence for class numbers of real quadratic fields due to Ankeny–Artin–Chowla. Along the way, we define the p-adic regulator and prove that it does not vanish (Leopoldt's conjecture) for abelian number fields.

There are several ways to construct p-adic L-functions. We have taken the quickest approach here. Later, we shall give other methods which give additional insights into relationships with cyclotomic fields.

§5.1 p-adic Functions

First, we need some basic results on p-adic analysis. We start with the p-adic rationals $\mathbb{Q}_p$. Since we shall need to consider algebraic extensions (e.g., generated by values of Dirichlet characters) we extend to $\overline{\mathbb{Q}}_p$, the algebraic closure. The absolute value on $\mathbb{Q}_p$ extends uniquely to $\overline{\mathbb{Q}}_p$; we normalize by $|p| = 1/p$ (throughout this chapter, $|x|$ will be the p-adic absolute value; so we write $|x|_p$ only for emphasis).

Proposition 5.1. *$\overline{\mathbb{Q}}_p$ is not complete.*

PROOF. Let

$$\alpha = \sum_{n=1}^{\infty} \zeta_{n'} p^n,$$

where $n' = n$ if $(n, p) = 1$ and $n' = 1$ otherwise. If $\overline{\mathbb{Q}}_p$ were complete, then the series would converge to $\alpha \in \overline{\mathbb{Q}}_p$. Therefore α would lie in a finite extension K of $\mathbb{Q}_p$. Suppose $\zeta_{n'} \in K$ for all $n < m$. We may assume $p \nmid m$. Then

$$\beta = p^{-m}\left(\alpha - \sum_{n=0}^{m-1} \zeta_{n'} p^n\right) \in K$$

and $\beta \equiv \zeta_m \pmod p$. Therefore $X^m - 1 \equiv 0 \pmod p$ has a solution in K. By Hensel's Lemma (since $p \nmid m$), K contains a solution of $X^m - 1 = 0$ which is congruent to β mod p, hence to ζ_m mod p. Since the mth roots of unity are distinct mod p (recall

$$m = \prod_{\substack{\zeta^m = 1 \\ \zeta \neq 1}} (1 - \zeta))$$

it follows that $\zeta_m \in K$. By induction, $\zeta_m \in K$ for all m with $p \nmid m$. Since, as above, the roots of unity of order prime to p are distinct mod p, we have infinitely many residue classes mod p in the ring of integers of K. Since $K/\mathbb{Q}_p$ is a finite extension, this is a contradiction. Therefore $\alpha \notin \overline{\mathbb{Q}}_p$ and $\overline{\mathbb{Q}}_p$ is not complete. □

Since it is more convenient to do analysis in a complete field, we let $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}}_p$ with respect to the p-adic absolute value. The p-adic absolute value naturally extends to $\mathbb{C}_p$ and $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$.

Proposition 5.2. *$\mathbb{C}_p$ is algebraically closed.*

PROOF. We need the following lemma, due to Krasner.

Lemma 5.3. *Suppose K is a complete field with respect to a non-archimedean valuation. Let $\alpha, \beta \in \overline{K}$, the algebraic closure of K, with α separable over $K(\beta)$. Finally, suppose that for all conjugates $\alpha_i \neq \alpha$ of α we have*

$$|\beta - \alpha| < |\alpha_i - \alpha|.$$

Then $K(\alpha) \subseteq K(\beta)$ ($|x|$ denotes the unique extension of the absolute value on K).

In other words, if β is sufficiently close to α then $\alpha \in K(\beta)$.

PROOF. Consider the extension $K(\alpha, \beta)/K(\beta)$ and let $L/K(\beta)$ be the Galois closure. Let $\sigma \in \mathrm{Gal}(L/K(\beta))$. Then $\sigma(\beta - \alpha) = \beta - \sigma(\alpha)$. Since $|\sigma x| = |x|$ for all x (by the uniqueness of the extension of the absolute value), we have

$$|\beta - \sigma(\alpha)| = |\beta - \alpha| < |\alpha_i - \alpha|$$

for all $\alpha_i \neq \alpha$. Therefore

$$|\alpha - \sigma(\alpha)| \leq \mathrm{Max}(|\alpha - \beta|, |\beta - \sigma(\alpha)|) < |\alpha_i - \alpha|.$$

It follows that $\sigma(\alpha) = \alpha$, so $\alpha \in K(\beta)$, as desired. □

Returning to the proof of the proposition, we let $K = \mathbb{C}_p$. Suppose α is algebraic over $\mathbb{C}_p$ and let $f(X)$ be its irreducible polynomial in $\mathbb{C}_p[X]$. Since $\bar{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$, we may choose a polynomial $g(X) \in \bar{\mathbb{Q}}_p[X]$ whose coefficients are close to those of $f(X)$. Then $g(\alpha) = g(\alpha) - f(\alpha)$ is very small. Writing $g(X) = \prod (X - \beta_j)$, we see that $|\alpha - \beta|$ is small for some root β of $g(X)$. In particular, we can choose $g(X)$ and then β so that $|\beta - \alpha| < |\alpha_i - \alpha|$ for all conjugates $\alpha_i \neq \alpha$. Therefore $\alpha \in \mathbb{C}_p(\beta) = \mathbb{C}_p$, since $\beta \in \bar{\mathbb{Q}}_p \subset \mathbb{C}_p$. The proof is complete. □

Sometimes, for technical reasons, it is convenient to embed $\mathbb{C}_p$ in $\mathbb{C}$, or vice versa. In fact, the two fields are algebraically, but not topologically, isomorphic: Both fields have the same uncountable transcendence degree over $\mathbb{Q}$, and both are obtained by starting with $\mathbb{Q}$, adjoining a transcendence basis, and then taking the algebraic closure.

From now on, unless otherwise stated, we shall be working in $\mathbb{C}_p$, which may be regarded as the p-adic analogue of the complex numbers. We next introduce the p-adic exponential and logarithm functions. Define

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

Since there are $[n/p^i]$ multiples of p^i less than or equal to n, it is easy to see that the exponent of p in $n!$ is

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots < \frac{n}{p-1}.$$

If $p^a \leq n < p^{a+1}$ then the sum is greater than

$$\frac{n}{p} + \cdots + \frac{n}{p^a} - a = \frac{n}{p-1} - a - \frac{np^{-a}}{p-1} > \frac{n-p}{p-1} - \frac{\log n}{\log p}.$$

Therefore

$$\frac{n-p}{p-1} - \frac{\log n}{\log p} < v_p(n!) < \frac{n}{p-1}.$$

It follows that $|X^n/n!| \to 0$ as $n \to \infty$ if $|X| < p^{-1/(p-1)}$ and $|X^n/n!| \to \infty$ if $|X| > p^{-1/(p-1)}$. Therefore $\exp(X)$ has radius of convergence $p^{-1/(p-1)} < 1$ (recall that a non-archimedean series converges $\Leftrightarrow$ its nth term $\to 0$). Note that $e = \exp(1)$ is undefined, but e^p (e^4 if $p = 2$) is defined. We could of course let $e = (\exp(p))^{1/p}$ but this would not be unique.

We now define

$$\log_p(1 + X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}X^n}{n}.$$

Since the exponent of p in n is at most $\log n/\log p$, we find that the series has radius of convergence 1. However in this case we can extend the function. Note that since $\log_p(XY) = \log_p(X) + \log_p(Y)$ is an identity for formal power series, it is true whenever the series converge.

Proposition 5.4. *There exists a unique extension of* $\log_p$ *to all of* $\mathbb{C}_p^\times$ *such that* $\log_p(p) = 0$ *and* $\log_p(xy) = \log_p x + \log_p y$ *for all* $x, y \in \mathbb{C}_p^\times$.

Proof. We need to investigate the multiplicative structure of $\mathbb{C}_p^\times$. For each rational number r choose a power p^r of p in such a way that $p^r p^s = p^{r+s}$ (one way: let p^r be the positive real rth power of p in $\bar{\mathbb{Q}}$, then embed $\bar{\mathbb{Q}}$ in $\mathbb{C}_p$). Denote by $p^{\mathbb{Q}}$ this set of p^r, $r \in \mathbb{Q}$.

Let $\alpha \in \mathbb{C}_p^\times$. If $\alpha_1 \in \bar{\mathbb{Q}}_p$ is sufficiently close to α then $|\alpha| = |\alpha_1|$. But $|\alpha_1| = (p^{1/e})^n$ for some n where e is the ramification index of $\mathbb{Q}_p(\alpha_1)/\mathbb{Q}_p$. Therefore $|\alpha| = p^{-r}$ for some $r \in \mathbb{Q}$, so $|\alpha p^{-r}| = 1$.

Now suppose $\beta \in \mathbb{C}_p^\times$, $|\beta| = 1$. Choose $\beta_1 \in \bar{\mathbb{Q}}_p$ close to β. Every unit of the finite extension $\mathbb{Q}_p(\beta_1)/\mathbb{Q}_p$ is congruent modulo $\mathfrak{p}$ (the prime above p) to a root of unity of order prime to p (lift from $(\mathcal{O}/\mathfrak{p})^\times$ via Hensel's lemma). It follows that $|\beta_1 - \omega| < 1$, hence $|\beta - \omega| < 1$ and $|\beta\omega^{-1} - 1| < 1$, for some root of unity ω of order prime to p. Since such roots of unity are distinct modulo $\mathfrak{p}$, ω is unique. Let W denote the group of all roots of unity of order prime to p in $\mathbb{C}_p^\times$. We have proved that

$$\mathbb{C}_p^\times = p^{\mathbb{Q}} \times W \times U_1$$

where

$$U_1 = \{x \in \mathbb{C}_p \,|\, |x - 1| < 1\}.$$

Now let $\alpha = p^r\omega x \in \mathbb{C}_p^\times$. Define $\log_p \alpha = \log_p x$. Since $x \in U_1$, $\log_p x$ is defined by the power series. Clearly this extension satisfies the desired properties.

Suppose $f(\alpha)$ gives another extension. If $\omega^N = 1$ then

$$\begin{aligned} f(\alpha) = \frac{1}{N} f(\alpha^N) &= \frac{1}{N} f(p^{rN}) + \frac{1}{N} f(1) + \frac{1}{N} f(x^N) \\ &= 0 + 0 + \frac{1}{N} \log_p(x^N) = \log_p(x). \end{aligned}$$

Therefore the extension is unique. This completes the proof of the proposition. □

If $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ then since $|\sigma x| = |x|$ for all $x \in \bar{\mathbb{Q}}_p$ we may extend σ to a continuous automorphism of $\mathbb{C}_p$. By continuity,

$$\log_p(1 + \sigma x) = \sum (-1)^{n+1}(\sigma x)^n/n = \sigma \sum (-1)^{n+1}x^n/n = \sigma \log_p(1 + x).$$

By the uniqueness of $\log_p$, we therefore have $\sigma^{-1}\log_p(\sigma\alpha) = \log_p\alpha$ for $\alpha \in \mathbb{C}_p^\times$, i.e., $\log_p(\sigma\alpha) = \sigma(\log_p\alpha)$. It follows that for $\alpha \in \overline{\mathbb{Q}}_p$, $\log_p(\alpha) \in \mathbb{Q}_p(\alpha)$; this fact also follows from the power series expansion.

For $\mathbb{Q}_p$ we may carry out the construction of the proposition more explicitly. For convenience we introduce the notation

$$q = \begin{cases} p, & \text{if } p \neq 2 \\ 4, & \text{if } p = 2. \end{cases}$$

Given $a \in \mathbb{Z}_p$, $p \nmid a$, there exists a unique $\phi(q)$th (i.e., $(p-1)$st if $p \neq 2$) root of unity $\omega(a) \in \mathbb{Z}_p$ such that

$$a \equiv \omega(a) \pmod{q}.$$

Let

$$\langle a \rangle = \omega(a)^{-1}a,$$

so $\langle a \rangle \equiv 1 \pmod{q}$. Then $\log_p a = \log_p\langle a \rangle$. Alternatively, $a^{p-1} \equiv 1 \pmod{p}$, so $\log_p a = \log_p(a^{p-1})/(p-1)$.

Lemma 5.5. *If* $|x| < p^{-1/(p-1)}$ *then* $|\log_p(1+x)| = |x|$ *and if* $|x| \leq p^{-1/(p-1)}$ *then* $|\log_p(1+x)| \leq |x|$.

Proof. If $n < p$ then $|n| = 1$, and in general $|n| \geq 1/n$. Therefore, if $|x| < p^{-1/(p-1)}$ we have

$$\left|\frac{x^n}{n}\right| = |x|^{n-1} \cdot |x| < |x| \quad \text{if } 2 \leq n < p$$

and

$$\left|\frac{x^n}{n}\right| < np^{(1-n)/(p-1)}|x| \leq |x| \quad \text{if } n \geq p,$$

since $n \cdot p^{(1-n)/(p-1)}$ is decreasing for $n \geq p$. Therefore $|x - x^2/2 + \cdots| = |x|$, as desired. The second part follows similarly. This completes the proof. □

Proposition 5.6. $\log_p x = 0 \Leftrightarrow x$ *is a rational power of p times a root of unity* (*of arbtirary order*).

Proof. Clearly such x satisfy $\log_p x = 0$. Conversely, suppose $\log_p x = 0$. Since $\mathbb{C}_p^\times = p^{\mathbb{Q}} \times W \times U_1$, we may assume $x = 1 + y$ with $|y| < 1$. Let N be large enough that $|y^{p^N}| < p^{-1/(p-1)}$. Then

$$x^{p^N} = (1+y)^{p^N} = 1 + p^N y + \cdots + \binom{p^N}{j} y^j + \cdots + y^{p^N}.$$

All the middle terms have absolute value at most $|py| < |p| \leq p^{-1/(p-1)}$, and by the choice of N we have $|y^{p^N}| < p^{-1/(p-1)}$. Therefore $|x^{p^N} - 1| < p^{-1/(p-1)}$ and by Lemma 5.5

$$0 = |\log_p(x^{p^N})| = |x^{p^N} - 1|.$$

Therefore x is a p^Nth root of unity. This completes the proof. □

Proposition 5.7. *If* $|x| < p^{-1/(p-1)}$ *then*

$$\log_p \exp(x) = x$$

and

$$\exp \log_p(1 + x) = 1 + x.$$

Proof. Both are formal power series identities, so we need only check convergence. Since $|x^n/n!| < 1$ for $n \geq 1$ (because $v_p(n!) < n/(p-1)$), we have $|\exp(x) - 1| < 1$ for all x with $|x| < p^{-1/(p-1)}$, so $\exp(x)$ and $\log_p \exp(x)$ converge. Similarly, Lemma 5.5 may be used to treat the second identity. □

Note that the first identity is true whenever $\exp(x)$ converges. But the second is not true for all x. Let $x = \zeta_p - 1$. Then $0 = \log_p(\zeta_p)$, so $\exp(\log_p(\zeta_p)) = 1 \neq \zeta_p$. This is true even though $\log_p(\zeta_p)$ converges ($|\zeta_p - 1| < 1$). The point is that $|\log_p x|$ is not less than $p^{-1/(p-1)}$ for *all* x with $|x| \leq |\zeta_p - 1| = p^{-1/(p-1)}$, so the formal rearrangement of the power series to get

$$\exp \log_p(1 + x) = 1 + x$$

does not work.

Finally, let $a \in \mathbb{Z}_p$, $p \nmid a$. We may define

$$\langle a \rangle^x = \exp(x \log_p \langle a \rangle) = \exp(x \log_p a).$$

Since $|\log_p \langle a \rangle| \leq |q| = 1/q$, this converges if $|x| < qp^{-1/(p-1)} > 1$. If $x = 1$ then $\langle a \rangle^1 = \langle a \rangle$ by Proposition 5.7. Similarly, if $n \in \mathbb{Z}$ then $\langle a \rangle^n$ agrees with the usual definition. In particular, if $n \equiv 0 \pmod{p-1}$, or $0 \pmod 2$ if $p = 2$, then $\langle a \rangle^n = a^n$.

We now turn our attention to more general functions. Let

$$\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}.$$

Then $\binom{X}{n}$ is a polynomial of degree n in X and if X is an integer we obtain a binomial coefficient. If $X \in \mathbb{Z}_p$ then X is close to a rational integer, so $\binom{X}{n}$ is close to an integer. It follows that $\binom{X}{n} \in \mathbb{Z}_p$ if $X \in \mathbb{Z}_p$. However this is not true for extensions of $\mathbb{Q}_p$. For example,

$$\binom{\sqrt{2}}{p} \in \mathbb{Z}_p[\sqrt{2}] \Leftrightarrow \sqrt{2} \quad \text{is congruent mod } p \text{ to a rational integer}$$

$$\Leftrightarrow \sqrt{2} \in \mathbb{Q}_p \Leftrightarrow p \equiv \pm 1 \pmod 8.$$

A classical theorem of Mahler states that any continuous function $f(X)$ from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ may be written uniquely in the form

$$f(X) = \sum_{n=0}^{\infty} a_n \binom{X}{n} \quad \text{with } a_n \to 0 \text{ as } n \to \infty.$$

Clearly any such function is continuous since it is a uniform limit of continuous functions. Since $f(m) = \sum_{n=0}^{m} a_n\binom{m}{n}$, we may use the identity

$$\binom{m}{i}\binom{i}{j} = \binom{m}{j}\binom{m-j}{i-j}$$

to obtain

$$\begin{aligned}\sum_{i=0}^{m}(-1)^{m-i}\binom{m}{i}f(i) &= \sum_{i=0}^{m}\sum_{j=0}^{i}(-1)^{m-i}a_j\binom{m}{i}\binom{i}{j}\\ &= \sum_{j=0}^{m}\binom{m}{j}a_j\sum_{j=i}^{m}\binom{m-j}{i-j}(-1)^{m-i}\\ &= \sum_{j=0}^{m}\binom{m}{j}a_j(1-1)^{m-j} = a_m\end{aligned}$$

(note that $0^0 = 1$ since it comes from $\binom{m-m}{m-m}(-1)^0 = 1$). Therefore $f(X)$ determines a_m. The hard part is showing $a_m \to 0$. We shall not prove this here because we do not need it. See Lang [4], p. 99.

If $a_n \to 0$ sufficiently rapidly, then $f(X)$ is analytic; that is, $f(X)$ may be expanded in a power series.

Proposition 5.8. *Suppose $r < p^{-1/(p-1)} < 1$ and*

$$f(X) = \sum_{n=0}^{\infty} a_n\binom{X}{n}$$

with $|a_n| \leq Mr^n$ for some M. Then $f(X)$ may be expressed as a power series with radius of convergence at least $R = (rp^{1/(p-1)})^{-1} > 1$.

Lemma. *Let $P_i(X) = \sum_{n=0}^{\infty} a_{n,i}X^n$, $i = 0, 1, 2, \ldots$ be a sequence of power series which converge in a fixed subset D of $\mathbb{C}_p$ and suppose*

(1) *$a_{n,i} \to a_{n,0}$ as $i \to \infty$ for each n, and*

(2) *for each $X \in D$ and every $\varepsilon > 0$ these exists an $n_0 = n_0(X, \varepsilon)$ such that $|\sum_{n\geq n_0} a_{n,i}X^n| < \varepsilon$ uniformly in i $(=0, 1, 2, \ldots)$.*

Then $\lim_{i\to\infty} P_i(X) = P_0(X)$ *for all $X \in D$.*

Proof of Lemma. Given ε and X, choose n_0 as above. Then

$$|P_0(X) - P_i(X)| \leq \underset{n\leq n_0}{\mathrm{Max}}\{\varepsilon, |a_{n,0} - a_{n,i}|\cdot|X^n|\} = \varepsilon$$

for i sufficiently large. □

Proof of Proposition 5.8. Let

$$P_i(X) = \sum_{n\leq i} a_n\binom{X}{n} = \sum_{n\leq i} a_{n,i}X^n, \qquad i = 1, 2, 3, \ldots.$$

Then

$$a_{n,i} = a_n \frac{\text{integer}}{n!} + a_{n+1} \frac{\text{integer}}{(n+1)!} + \cdots,$$

so

$$|a_{n,i}| \leq \operatorname*{Max}_{j \geq n} \left| \frac{a_j}{j!} \right| \leq MR^{-n}.$$

Also,

$$|a_{n,i} - a_{n,i+k}| = \left| a_{i+1} \frac{\text{integer}}{(i+1)!} + \cdots + a_{i+k} \frac{\text{integer}}{(i+k)!} \right|$$
$$\leq MR^{-(i+1)} \to 0 \quad \text{as } i \to \infty.$$

Therefore $\{a_{n,i}\}_{i=1}^{\infty}$ is a Cauchy sequence. Let $a_{n,0} = \lim_{i\to\infty} a_{n,i}$. Then $|a_{n,0}| \leq MR^{-n}$. Let $P_0(X) = \sum_{n=0}^{\infty} a_{n,0} X^n$, so P_0 converges in $D = \{x \in C_p \,|\, |x| < R\}$. The polynomials $P_1, P_2, \ldots$ of course also converge in D. Finally, if $X \in D$ then

$$\left| \sum_{n \geq n_0} a_{n,i} X^n \right| \leq \operatorname*{Max}_{n \geq n_0}\{MR^{-n}|X|^n\} \to 0 \quad \text{as } n_0 \to \infty,$$

uniformly in i. Therefore $\lim_{i\to\infty} P_i(X) = P_0(X)$, so $f(X)$ is analytic in D, as desired. □

As an application, let us reconsider the function $\langle a \rangle^s$. We may expand it as a binomial series

$$(1 + \langle a \rangle - 1)^s = \sum_{n=0}^{\infty} \binom{s}{n} (\langle a \rangle - 1)^n.$$

Since $|\langle a \rangle - 1| \leq q^{-1}$, we may let $r = q^{-1}$. We find that the series represents an analytic function with radius of convergence at least $qp^{-1/(p-1)}$, just as before. In fact

$$\exp(s \log_p \langle a \rangle) = \sum_{n=0}^{\infty} \binom{s}{n} (\langle a \rangle - 1)^n$$

since the functions are analytic in s and are equal when s is a positive integer. Since the positive integers have 0 as a (p-adic) accumulation point, the functions must be identically equal.

§5.2 p-adic L-functions

We are now able to consider the main subject of this chapter. Let

$$H(s, a, F) = \sum_{\substack{m \equiv a(F) \\ m > 0}} m^{-s} = \sum_{n=0}^{\infty} \frac{1}{(a + nF)^s} = F^{-s} \zeta\left(s, \frac{a}{F}\right),$$

where s is a complex variable, a and F are integers with $0 < a < F$, and $\zeta(s, b)$ is the Hurwitz zeta function. Then

$$H(1 - n, a, F) = -\frac{F^{n-1}B_n(a/F)}{n} \in \mathbb{Q}, \qquad n \geq 1,$$

and H has a simple pole at $s = 1$ with residue $1/F$.

Theorem 5.9. *Suppose $q | F$ and $p \nmid a$. Then there exists a p-adic meromorphic function $H_p(s, a, F)$ on*

$$\{s \in \mathbb{C}_p | |s| < qp^{-1/(p-1)} > 1\}$$

such that

$$H_p(1 - n, a, F) = \omega^{-n}(a)H(1 - n, a, F), \qquad n \geq 1.$$

In particular, when $n \equiv 0 \pmod{p - 1}$, or (mod 2) *if $p = 2$, then*

$$H_p(1 - n, a, F) = H(1 - n, a, F).$$

The function H_p is analytic except for a simple pole at $s = 1$ with residue $1/F$.

Proof. Let

$$H_p(s, a, F) = \frac{1}{s - 1}\frac{1}{F}\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1 - s}{j}(B_j)\left(\frac{F}{a}\right)^j.$$

Assume convergence for the moment. Then

$$\begin{aligned} H_p(1 - n, a, F) &= \frac{-1}{nF}\langle a\rangle^n\sum_{j=0}^{n}\binom{n}{j}(B_j)\left(\frac{F}{a}\right)^j \\ &= -\frac{F^{n-1}\omega^{-n}(a)}{n}B_n\left(\frac{a}{F}\right) \\ &= \omega^{-n}(a)H(1 - n, a, F), \quad \text{as desired.} \end{aligned}$$

At $s = 1$, we have residue

$$\frac{1}{F}\langle a\rangle^0\sum_{j=0}^{\infty}\binom{0}{j}(B_j)\left(\frac{F}{a}\right)^j = \frac{1}{F}.$$

It remains to prove convergence. We need the following well-known result.

Theorem 5.10 (von Staudt–Clausen). *Let n be even and positive. Then*

$$B_n + \sum_{(p-1)|n}\frac{1}{p} \in \mathbb{Z},$$

where the sum is over those primes p such that $p - 1$ divides n (in particular, 2 and 3 appear in the denominator of each Bernoulli number). Consequently, pB_n is p-integral for all n and all p.

PROOF. We shall show that for each prime p we have $B_n \equiv -1/p$ or $0 \bmod \mathbb{Z}_p$, depending on whether $p - 1$ does or does not divide n. Assume by induction that this is true for $m < n$. In particular, $pB_m \in \mathbb{Z}_p$ for $m < n$. Since the cases $m = 0, 1$ are easily treated, we assume also that $n \geq 2$ is even. From Proposition 4.1 we have

$$\begin{aligned} B_n = B_{n,1} &= p^{n-1} \sum_{a=1}^{p} B_n\left(\frac{a}{p}\right) \\ &= p^{n-1} \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} (B_j) \left(\frac{a}{p}\right)^{n-j} \\ &= \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} (pB_j) a^{n-j} p^{j-2} \\ &\equiv \sum_{a=1}^{p} (pB_0 a^n p^{-2} + npB_1 a^{n-1} p^{-1} + pB_n p^{n-2}) \pmod{\mathbb{Z}_p}. \end{aligned}$$

Since $B_1 = -\frac{1}{2}$, $B_1 \in \mathbb{Z}_p$ if $p \neq 2$. Since n is even, $nB_1 \in \mathbb{Z}_2$. Therefore we may omit the term with B_1. We obtain

$$(1 - p^{n-1})B_n \equiv \frac{1}{p} \sum_{a=1}^{p} a^n \equiv \begin{cases} \dfrac{p-1}{p}, & \text{if } (p-1) \mid n \\ 0, & \text{if } (p-1) \nmid n. \end{cases}$$

Since $1 - p^{n-1} \equiv 1 \pmod{p}$, we have $B_n \equiv -1/p$ or $0 \bmod \mathbb{Z}_p$.

Now consider $B_n + \sum_{(p-1)|n} 1/p$. By the above, this is in $\mathbb{Z}_p$ for every p, so there are no primes in the denominator. Therefore it must be an integer. This completes the proof of Theorem 5.10. □

Returning to the proof of Theorem 5.9, we note that $|(B_j)(F/a)^j| \leq p|q|^j$. Therefore, by Proposition 5.8 with $r = |q| = 1/q$, we find that

$$\sum_{j=0}^{\infty} \binom{s}{j} (B_j) \left(\frac{F}{a}\right)^j$$

is analytic on $D = \{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$. Since $qp^{-1/(p-1)} > 1$, this is the same set as $\{s \in \mathbb{C}_p \mid |1 - s| < qp^{-1/(p-1)}\}$, so

$$\sum \binom{1-s}{j} (B_j) \left(\frac{F}{a}\right)^j$$

is analytic in D. Similarly $\langle a \rangle^s$, hence $\langle a \rangle^{1-s}$, is analytic in D. Therefore $(s - 1)H_p(s, a, F)$ is analytic in D. This completes the proof of Theorem 5.9. □

We are now ready to construct p-adic L-functions. Let χ be a Dirichlet character. If we fix, once and for all, an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$, we may regard the values of χ as lying in $\mathbb{C}_p$. Also, observe that $\omega(a)$ is a p-adic Dirichlet character of conductor q and order $\phi(q)$ $(=2$ or $p-1)$. It may be regarded as coming from a complex character if desired, but the choice is noncanonical and depends on an embedding of $\mathbb{Q}(\zeta_{p-1})$ into $\mathbb{Q}_p$. It is better to regard ω as a p-adic object. Note that it generates the group of Dirichlet characters defined mod q.

Theorem 5.11. *Let χ be a Dirichlet character of conductor f and let F be any multiple of q and f. Then there exists a p-adic meromorphic (analytic if $\chi \neq 1$) function $L_p(s, \chi)$ on $\{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$ such that*

$$L_p(1-n, \chi) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \qquad n \geq 1.$$

If $\chi = 1$ then $L_p(s, 1)$ is analytic except for a pole at $s = 1$ with residue $(1 - 1/p)$.

In fact, we have the formula

$$L_p(s, \chi) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j.$$

Remarks. The factor $(1 - \chi\omega^{-n}(p)p^{n-1})$ is the Euler factor at p for $L(s, \chi\omega^{-n})$. It is a general principle that to obtain p-adic analogues of complex functions, the p-part must be removed (intuitively, $\sum 1/n^s$ has p-adically arbitrarily large terms if p is allowed to divide n, while at least the terms are bounded if $p\nmid n$). The expression $\chi\omega^{-n}(p)$ is taken in the sense of multiplication of characters given in Chapter 3. In general, $\chi\omega^{-n}(p) \neq \chi(p)\omega^{-n}(p)$. For example, if $\chi = \omega^n \neq 1$, then $\chi\omega^{-n}(p) = 1$, while $\chi(p) = \omega^n(p) = 0$.

Note that

$$L_p(1-n, \chi) = (1 - \chi(p)p^{n-1})L(1-n, \chi) \quad \text{if } n \equiv 0 \pmod{p-1}$$

(mod 2 if $p = 2$). In general, $L_p(s, \chi)$ is an intertwining of the functions $L(s, \chi\omega^j)$, $j = 0, 1, \ldots, p-2$. If χ is an odd character then n and $\chi\omega^{-n}$ have different parities so $B_{n,\chi\omega^{-n}} = 0$. Therefore $L_p(s, \chi)$ is identically zero for odd χ. If χ is even then $B_{n,\chi\omega^{-n}} \neq 0$ so $L_p(s, \chi)$ is not the zero function. The nature of its zeros is not yet understood.

Proof of Theorem 5.11. We show that the formula gives the desired function. Since

$$L_p(s, \chi) = \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)H_p(s, a, F),$$

the analyticity properties follow at once. At $s = 1$, $L_p(s, \chi)$ has residue $\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)(1/F)$. If $\chi = 1$ then this sum equals $1 - 1/p$. If $\chi \neq 1$ then the sum is

$$\frac{1}{F}\sum_{a=1}^{F}\chi(a) - \frac{1}{F}\sum_{b=1}^{F/p}\chi(pb).$$

The first sum is 0. If $p \mid f$ then $\chi(pb) = 0$ for all b. If $p \nmid f$ then $f \mid (F/p)$, so again the second sum is 0. Therefore $L_p(s, \chi)$ has no pole at $s = 1$ if $\chi \neq 1$.

If $n \geq 1$ then

$$\begin{aligned} L_p(1-n, \chi) &= \sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a) H_p(1-n, a, F) \\ &= -\frac{1}{n} F^{n-1} \sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi\omega^{-n}(a) B_n\left(\frac{a}{F}\right) \qquad \text{(cf. Exercise 3.7(c))} \\ &= -\frac{1}{n} F^{n-1} \sum_{a=1}^{F} \chi\omega^{-n}(a) B_n\left(\frac{a}{F}\right) \\ &\quad + \frac{1}{n} p^{n-1} \left(\frac{F}{p}\right)^{n-1} \sum_{b=1}^{F/p} \chi\omega^{-n}(pb) B_n\left(\frac{b}{F/p}\right). \end{aligned}$$

If $p \mid f_{\chi\omega^{-n}}$ then $\chi\omega^{-n}(pb) = 0$. Otherwise $f_{\chi\omega^{-n}} \mid (F/p)$. By Proposition 4.1 we have

$$\begin{aligned} L_p(1-n, \chi) &= -\frac{1}{n}(B_{n, \chi\omega^{-n}} - \chi\omega^{-n}(p) p^{n-1} B_{n, \chi\omega^{-n}}) \\ &= -\frac{1}{n}(1 - \chi\omega^{-n}(p) p^{n-1}) B_{n, \chi\omega^{-n}}. \end{aligned}$$

This completes the proof of Theorem 5.11. □

What happens at the positive integers? We shall treat the case $s = 1$ shortly. Let $n \geq 1$. It is classical that

$$\frac{(-1)^{n+1}}{n!} \frac{d^{n+1}}{(dz)^{n+1}} \log \Gamma(z) = \sum_{m=0}^{\infty} \frac{1}{(z+m)^{n+1}} = \zeta(1+n, z).$$

Recall Stirling's asymptotic series (see Whittaker and Watson, [1], p. 241)

$$\log \frac{\Gamma(z)}{\sqrt{2\pi}} \sim (z - \tfrac{1}{2}) \log z - z + \sum_{j=1}^{\infty} \frac{B_{j+1}}{j(j+1)} z^{-j}.$$

The series does not converge for complex z, but $\log(\Gamma(z)/\sqrt{2\pi})$ equals the mth partial sum $+ 0(|z|^{-m-1})$ as $z \to \infty$. If we differentiate $(n+1)$-times (this can be justified) we obtain

$$\frac{(-1)^{n+1}}{n!} \frac{d^{n+1}}{(dz)^{n+1}} \log \Gamma(z) \sim \frac{1}{n} \sum_{j=0}^{\infty} \binom{-n}{j} (B_j) z^{-(n+j)}.$$

Note that the right-hand side converges p-adically if $|z|_p > 1$. We therefore regard

$$\frac{z^{-n}}{n} \sum_{j=0}^{\infty} \binom{-n}{j} (B_j) z^{-j}$$

as the p-adic analogue of

$$\sum_{m=0}^{\infty} \frac{1}{(z+m)^{n+1}} = \zeta(1+n, z).$$

Letting $z = a/F$, we see that for $n \geq 1$

$$H_p(1+n, a, F)$$

is the analogue of

$$\omega^{-n}(a)F^{n+1}\zeta\left(1+n, \frac{a}{F}\right) = \omega^n(a)H(1+n, a, F).$$

An easy calculation shows that $L_p(1+n, \chi)$ is the analogue of

$$(1 - \chi\omega^n(p)p^{-(n+1)})L(1+n, \chi\omega^n).$$

Note that $L(1+n, \chi\omega^n)$ gives the values for even characters at odd integers and for odd characters at even integers. Very little is known about these numbers, either in the complex case or the p-adic case.

§5.3 Congruences

Theorem 5.12. *Suppose $\chi \neq 1$ and $pq \nmid f_\chi$. Then*

$$L_p(s, \chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \cdots$$

with $|a_0| \leq 1$ and with $p \mid a_i$ for all $i \geq 1$ (note that since $L_p(s, \chi)$ has radius of convergence greater than 1, $a_i \to 0$ as $i \to \infty$; so we a priori have $p \mid a_i$ for large i).

Proof. We may choose F as in Theorem 5.11 so that $q \mid F$ but $pq \nmid F$. Also we may assume χ is even since everything is 0 otherwise.

If $j \geq 6$ then

$$\left|\frac{B_j}{j!}\frac{F^{j-1}}{a^j}\right| \leq p^{j/(p-1)} \cdot p \cdot \frac{1}{q^{j-1}} \leq \frac{1}{q}.$$

A check of the cases $j = 3, 4, 5$ shows that the inequality holds for $j \geq 3$. Therefore all coefficients in the power series expansion of

$$\frac{1}{F}\sum_{j \geq 3}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j$$

are divisible by p. Also, the terms for $j \leq 2$ have possibly q, but not pq, in the denominator.

Similarly,

$$\langle a \rangle^{1-s} = \exp((1-s)\log_p\langle a \rangle) = \sum_{j=0}^{\infty} \frac{1}{j!}(1-s)^j(\log_p\langle a \rangle)^j$$

has all coefficients in $\mathbb{Z}_p$, and they are divisible by pq for $j \geq 2$, since $q \mid \log_p\langle a\rangle$.

Therefore we need only consider

$$\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)(1+(1-s)\log_p\langle a\rangle)\left(\frac{1}{F}-\frac{1-s}{2a}+\frac{(1-s)(1-s-1)F}{12a^2}\right).$$

We find that

$$a_0 \equiv -\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(\frac{1}{F}\log_p\langle a\rangle-\frac{1}{2a}-\frac{F}{12a^2}\right)\pmod{p}.$$

Clearly $(1/F)\log_p\langle a\rangle$ and $F/12$ are in $\mathbb{Z}_p$. Since $a \equiv \omega(a) \pmod{q}$,

$$\tfrac{1}{2}\sum\chi(a)\frac{1}{a} \equiv \tfrac{1}{2}\sum\chi\omega^{-1}(a) \equiv 0 \pmod{\tfrac{1}{2}q}$$

(we need the same reasoning as was used in the proof of Theorem 5.11 to handle the fact that the sum only includes a with $p\nmid a$). This shows that $|a_0| \leq 1$.

Next, we have

$$a_1 \equiv \sum_{p\nmid a}\chi(a)\left(\frac{F}{12a^2}-\frac{\log_p\langle a\rangle}{2a}-\frac{F\log_p\langle a\rangle}{12a^2}\right)\pmod{p}.$$

Clearly $F\log_p\langle a\rangle/12a^2$ and $\log_p\langle a\rangle/2a$ are divisible by p. If $p \geq 5$ then $F/12 \in p\mathbb{Z}_p$, so $p \mid a_1$. If $p = 2$ or 3 then $F/12 \in \mathbb{Z}_p^\times$. But $a^2 \equiv 1 \pmod{p}$ if $p \nmid a$, so $\sum_{p\nmid a}\chi(a)a^{-2} \equiv \sum_{p\nmid a}\chi(a) \equiv 0$. Again we have $p \mid a_1$.

Finally, we have

$$a_2 \equiv -\sum_{p\nmid a}\chi(a)(\log_p\langle a\rangle)\frac{F}{12a^2} \equiv 0 \pmod{p}.$$

Since all the higher coefficients are already divisible by p, from the above, the theorem is proved. □

Most of the congruences for Bernoulli numbers and generalized Bernoulli numbers follow from this theorem. We give a few examples. For another approach, see the Exercises for Chapter VII.

Corollary 5.13. *Suppose $\chi \neq 1$, $pq \nmid f$. Let $m, n \in \mathbb{Z}$. Then*

$$L_p(m,\chi) \equiv L_p(n,\chi) \pmod{p},$$

and both numbers are p-integral.

Proof. Both sides are congruent to a_0 in the notation of the theorem. □

Corollary 5.14 (Kummer's Congruences). *Suppose $m \equiv n \not\equiv 0 \pmod{p-1}$ are positive even integers. Then*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

More generally, if m and n are positive even integers with $m \equiv n \pmod{(p-1)p^a}$ and $n \not\equiv 0 \pmod{p-1}$, then

$$(1 - p^{m-1})\frac{B_m}{m} \equiv (1 - p^{n-1})\frac{B_n}{n} \pmod{p^{a+1}}.$$

Proof. Consider $L_p(s, \omega^m) = L_p(s, \omega^n)$. Then

$$L_p(1 - m, \omega^m) = -(1 - p^{m-1})(B_m/m)$$

and similarly for n. Also

$$\begin{aligned} L_p(1 - m, \omega^m) &= a_0 + a_1(-m) + a_2(-m)^2 + \cdots \\ &\equiv a_0 + a_1(-n) + a_2(-n)^2 + \cdots \pmod{p^{a+1}} \\ &\quad (\text{since } p \mid a_i,\ i \geq 1) \\ &= L_p(1 - n, \omega^n). \end{aligned}$$

The result follows. □

Corollary 5.15. *Suppose n is odd, $n \not\equiv -1 \pmod{p-1}$. Then*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \pmod{p}$$

and both sides are p-integral.

Proof. Since $n \not\equiv -1$, $\omega^{n+1} \neq 1$. Also $\omega^n(p) = 0$ since $\omega^n \neq 1$. Therefore, by Corollary 5.13,

$$\begin{aligned} B_{1,\omega^n} &= (1 - \omega^n(p))B_{1,\omega^n} = -L_p(0, \omega^{n+1}) \\ &\equiv -L_p(1 - (n + 1), \omega^{n+1}) = (1 - p^n)\frac{B_{n+1}}{n+1} \equiv \frac{B_{n+1}}{n+1} \pmod{p}. \end{aligned}$$

The p-integrality also follows from Corollary 5.13. □

Theorem 5.16. *Let p be an odd prime and let h_p^- be the relative class number of $\mathbb{Q}(\zeta_p)$. Then $p \mid h_p^- \Leftrightarrow p$ divides the numerator of B_j for some $j = 2, 4, \ldots, p - 3$. (Later we shall show $p \mid h_p \Leftrightarrow p \mid h_p^-$.)*

Proof. The odd characters corresponding to $\mathbb{Q}(\zeta_p)$ are $\omega, \omega^3, \ldots, \omega^{p-2}$. Therefore, by Theorem 4.16

$$h_p^- = 2p \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-2} \left(-\tfrac{1}{2}B_{1,\omega^j}\right)$$

($Q = 1$ by Corollary 4.13; $w = 2p$). First, note that

$$B_{1,\omega^{p-2}} = B_{1,\omega^{-1}} = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv \frac{p-1}{p} \bmod \mathbb{Z}_p.$$

Therefore $(2p)(-\frac{1}{2}B_{1,\omega^{p-2}}) \equiv 1 \pmod p$, so we have

$$h_p^- \equiv \prod_{\substack{j=1\\ j\,\text{odd}}}^{p-4} (-\tfrac{1}{2}B_{1,\omega^j}) \pmod p.$$

By Corollary 5.15, this may be rewritten as

$$h_p^- \equiv \prod_{\substack{j=1\\ j\,\text{odd}}}^{p-4} \left(-\frac{1}{2}\frac{B_{j+1}}{j+1}\right) \pmod p.$$

The theorem follows immediately. □

As mentioned in Chapter 1, a prime is called irregular if p divides B_j for some $j = 2, 4, \ldots, p-3$.

Theorem 5.17. *There are infinitely many irregular primes.*

Proof. Suppose $p_1, \ldots, p_r$ are all the irregular primes and let $m = N(p_1 - 1) \cdots (p_r - 1)$, where N will be chosen later. It follows from Exercise 4.3 that $|B_n/n| \to \infty$ as $n \to \infty$, n even. If we choose N large enough, then $|B_m/m| > 1$. There then exists a prime p which divides the numerator of B_m/m. Since p_i is in the denominator of B_m for $i = 1, \ldots, r$ by Theorem 5.10, we cannot have $p = p_i$ for any i. Also $m \not\equiv 0 \pmod{p-1}$ for similar reasons. Let $m' \equiv m \pmod{p-1}$, $0 < m' < p-1$. Then

$$\frac{B_{m'}}{m'} \equiv \frac{B_m}{m} \pmod p,$$

so $p \mid B_{m'}$. Therefore, p is irregular. It follows that there must be infinitely many irregular primes, as claimed. □

It is not known whether or not there are infinitely many regular primes. However, numerical evidence indicates that about 61 % of all primes are regular. More precisely, let $i(p)$ be the number of B_j, $j = 2, 4, \ldots, p-3$, which are divisible by p. This number is usually called the index of irregularity. Assume that the Bernoulli numbers are random mod p in the sense that B_j is divisible by p with probability $1/p$. There are $(p-3)/2$ Bernoulli numbers in consideration for a prime p. The probability that $i(p) = k$ is therefore

$$\binom{\frac{p-3}{2}}{k}\left(1 - \frac{1}{p}\right)^{\frac{1}{2}(p-3)-k}\left(\frac{1}{p}\right)^k,$$

which approaches $(\frac{1}{2})^k e^{-1/2}/k!$ as $p \to \infty$ (Poisson distribution with parameter $\frac{1}{2}$). For $i(p) = 0$, we find that $e^{-1/2} \approx 60.65\%$ of all primes should be regular. The remaining 39.35% should be irregular of various indices. This heuristic argument agrees closely with the numerical evidence. For the 11733 odd primes less than 125000, the computer calculations of Wagstaff [1] yielded the following data:

$i(p)$	Fraction with $i(p)$	$\frac{1}{k!}\frac{1}{2^k}e^{-1/2}$
0	0.6075	0.6065
1	0.3033	0.3033
2	0.0746	0.0758
3	0.0130	0.0126
4	0.0014	0.0016
5	0.0002	0.0002
≥ 6	0.0000	0.0000

§5.4 The Value at $s = 1$

We now turn our attention to the evaluation of $L_p(1, \chi)$. The answer is the p-adic version of the classical formula with the Euler factor at p removed.

Theorem 5.18. *Let χ be an even nontrivial Dirichlet character of conductor f, let $\bar{\chi} = \chi^{-1}$, let ζ be a primitive fth root of unity, and let $\tau(\chi) = \sum_{a=1}^{f} \chi(a)\zeta^a$ be a Gauss sum. Then*

$$L_p(1, \chi) = -\left(1 - \frac{\chi(p)}{p}\right)\frac{\tau(\chi)}{f}\sum_{a=1}^{f} \bar{\chi}(a)\log_p(1 - \zeta^a).$$

Proof. (The proof is not especially enlightening. The reader could possibly omit it without seriously impairing the understanding of subsequent results.)

We shall consider the cases $f = p$ and $f \neq p$ separately.

I. $f = p$ (the argument in this case is essentially due to Kummer). Then $\chi = \omega^k$ for some even $k \not\equiv 0 \pmod{p-1}$, and p must be odd. Let $\phi(X) \in \mathbb{Q}[X]$ be a polynomial with p-integral coefficients such that $\phi(1) = 1$. Then $\phi(X) = 1 + b_1(X - 1) + b_2(X - 1)^2 + \cdots$ so we may formally expand

$$\log \phi(X) = -\sum_{i=1}^{\infty} \frac{(1 - \phi(X))^i}{i} = \sum_{i=1}^{\infty} \frac{C_i}{i}(1 - X)^i.$$

We claim the C_i's are p-integral. When

$$\frac{1}{i}(-b_1(X - 1) - b_2(X - 1)^2 - \cdots - b_k(X - 1)^k)^i$$

is expanded, we obtain terms of the form

$$(p\text{-integral coefficient})\frac{1}{i}\binom{i}{a_1, \ldots, a_k}(X-1)^{a_1}\cdots(X-1)^{ka_k},$$

where the expression in parentheses is a multinomial coefficient. Note that for any j with $a_j \neq 0$,

$$\frac{a_j}{i}\binom{i}{a_1, \ldots, a_k}$$

is another multinomial coefficient, hence integral. Therefore

$$\frac{1}{i}\binom{i}{a_1, \ldots, a_k}\sum ja_j \in \mathbb{Z}.$$

But this expression, times the "p-integral coefficient" above, is the form of the contributions to C_n, with $n = \sum ja_j$. This proves the claim.

Returning to the above formula, we expand further and obtain

$$\log \phi(X) = \sum_{i=1}^{\infty} \frac{C_i}{i}\left(\sum_{j=0}^{i}\binom{i}{j}(-1)^j X^j\right).$$

Now let $X = e^t$, so

$$\log \phi(e^t) = \sum_{i=1}^{\infty} \frac{C_i}{i} \sum_{j=0}^{i}\binom{i}{j}(-1)^j \sum_{m=0}^{\infty}\frac{j^m}{m!}t^m.$$

Lemma 5.19.

$$\sum_{j=0}^{i}\binom{i}{j}(-1)^j j^m = 0 \quad \text{for } i > m.$$

Proof. The left-hand side is the coefficient of $t^m/m!$ in the Taylor expansion of $(1-e^t)^i = t^i +$ higher terms. The result follows immediately. □

The lemma shows that the coefficient of $t^m/m!$ is a finite sum, in fact it is

$$\sum_{i=1}^{m}\frac{C_i}{i}\sum_{j=0}^{i}\binom{i}{j}(-1)^j j^m.$$

Now let g be a primitive root modulo p (so $g^a \equiv 1 \bmod p \Leftrightarrow p-1$ divides a) and let

$$\phi(X) = \frac{1}{g}\frac{X^g - 1}{X - 1} = \frac{1}{g}(X^{g-1} + X^{g-2} + \cdots + 1).$$

Then

$$\frac{d}{dt}\log \phi(e^t) = \frac{ge^{gt}}{e^{gt}-1} - \frac{e^t}{e^t - 1} = \frac{1}{t}\left(\frac{gt}{e^{gt}-1} - \frac{t}{e^t-1}\right) + g - 1$$

$$= g - 1 + \sum_{m=1}^{\infty}(g^m - 1)B_m\frac{t^{m-1}}{m!}.$$

It follows that the coefficient of $t^m/m!$ $(m \geq 2)$ for $\log \phi(e^t)$ is $(g^m - 1)(B_m/m)$, so

$$(g^m - 1)\frac{B_m}{m} = \sum_{i=1}^{\infty} \frac{C_i}{i} \sum_{j=1}^{i} \binom{i}{j}(-1)^j j^m.$$

Let $m = kp^n$. Then $\omega^{kp^n} = \omega^k$ and

$$L_p(1, \omega^k) = \lim_{n\to\infty} L_p(1 - kp^n, \omega^k) = \lim_{n\to\infty} -(1 - p^{kp^n})\frac{B_{kp^n}}{kp^n} = \lim_{n\to\infty} -\frac{B_{kp^n}}{kp^n}.$$

Since $g^{kp^n} \to \omega(g)^k$, we have

$$\begin{aligned}(\omega(g)^k - 1)L_p(1, \omega^k) &= \lim_{n\to\infty} -(g^{kp^n} - 1)\frac{B_{kp^n}}{kp^n} \\ &= \lim_{n\to\infty} -\sum_{i=1}^{\infty} \frac{C_i}{i} \sum_{j=1}^{i} \binom{i}{j}(-1)^j j^{kp^n} \\ &= \lim_{n\to\infty} -\sum_{i=1}^{\infty} C_i \sum_{j=1}^{i} \binom{i-1}{j-1}(-1)^j j^{kp^n-1} \\ &\left(\textit{Note}: \binom{i}{j} = \frac{i}{j}\binom{i-1}{j-1}\right).\end{aligned}$$

Since each C_i is p-integral, we may evaluate $\lim j^{kp^n-1}$ termwise. If $p \mid j$ then the limit is 0. Otherwise we obtain $\omega^k(j)/j$. Therefore

$$(\omega(g)^k - 1)L_p(1, \omega^k) = -\sum_{i=1}^{\infty} \frac{C_i}{i} \sum_{\substack{j=1 \\ p\nmid j}}^{i} \binom{i}{j}(-1)^j \omega^k(j).$$

We now return to the original formula for $\log \phi(X)$. Let $\zeta = \zeta_p$ be any primitive pth root of unity and let $(a, p) = 1$. Since $|\phi(\zeta^a) - 1| \leq |\zeta^a - 1| < 1$, we may expand

$$\begin{aligned}\log_p \phi(\zeta^a) &= -\sum_{i=1}^{\infty} \frac{(1 - \phi(\zeta^a))^i}{i} = \sum_{i=1}^{\infty} \frac{C_i}{i}(1 - \zeta^a)^i \\ &= \sum_{i=1}^{\infty} \frac{C_i}{i} \sum_{j=0}^{i} \binom{i}{j}(-1)^j \zeta^{aj},\end{aligned}$$

with the same C_i as above. Therefore,

$$\begin{aligned}\sum_{a=1}^{p-1} \omega^{-k}(a) \log_p \phi(\zeta^a) &= \sum_{i=1}^{\infty} \frac{C_i}{i} \sum_{j=0}^{i} \binom{i}{j}(-1)^j \sum_{a=1}^{p-1} \omega^{-k}(a)\zeta^{aj} \\ &= \tau(\omega^{-k}) \sum_{i=1}^{\infty} \frac{C_i}{i} \sum_{\substack{j=0 \\ p\nmid j}}^{\infty} \binom{i}{j}(-1)^j \omega^k(j)\end{aligned}$$

since

$$\sum_{a=1}^{p-1} \omega^{-k}(a)\zeta^{aj} = \omega^k(j)\tau(\omega^{-k}) \quad \text{if } p \nmid j$$

and equals 0 if $p|j$. We now have

$$\begin{aligned}\tau(\omega^{-k})(\omega(g)^k - 1)L_p(1, \omega^k) &= -\sum_{a=1}^{p-1} \omega^{-k}(a)\log_p \phi(\zeta^a)\\ &= -\sum_{a=1}^{p-1} \omega^{-k}(a)[-\log_p g + \log_p(1-\zeta^{ag}) - \log_p(1-\zeta^a)]\\ &= -(\omega(g)^k - 1)\sum_{a=1}^{p-1} \omega^{-k}(a)\log_p(1-\zeta^a).\end{aligned}$$

Finally, since $\tau(\omega^k)\tau(\omega^{-k}) = \omega^k(-1)p = p$ by Lemmas 4.7 and 4.8, we obtain (note $\omega^k(g) \equiv g^k \not\equiv 1 \bmod p$, so $\omega^k(g) \neq 1$)

$$L_p(1, \omega^k) = -\frac{\tau(\omega^k)}{p}\sum_{a=1}^{p-1} \omega^{-k}(a)\log_p(1-\zeta^a),$$

as desired. Note that the Euler factor $(1 - \omega^k(p)/p) = 1$ so it does not appear explicitly.

II. $f \neq p$.

Lemma 5.20. *Let $\chi \neq 1$ be a Dirichlet character of conductor f and let ζ be a primitive* fth *root of unity. Then for $n \geq 1$*

$$\frac{B_{n,\chi}}{n} = -\frac{\tau(\chi)}{f}\sum_{a=1}^{f-1}\sum_{i=1}^{n}\frac{\bar{\chi}(a)}{i(\zeta^a-1)^i}\sum_{j=1}^{i}\binom{i}{j}(-1)^{i-j}j^n$$

(we may also sum for $1 \leq i < \infty$ by Lemma 5.19.)

Proof. Let

$$\begin{aligned}f_a(t) &= \sum_{n=0}^{\infty}\sum_{i=1}^{\infty}\frac{1}{i(\zeta^a-1)^i}\sum_{j=0}^{i}\binom{i}{j}(-1)^{i-j}j^n\frac{t^n}{n!}\\ &= \sum_{i=1}^{\infty}\frac{1}{i(\zeta^a-1)^i}\sum_{j=0}^{i}\binom{i}{j}(-1)^{i-j}e^{jt} = \sum_{i=1}^{\infty}\frac{1}{i}\left(\frac{e^t-1}{\zeta^a-1}\right)^i.\end{aligned}$$

Then $f_a(0) = 0$ and $f_a'(t) = e^t/(\zeta^a - e^t)$.

Let $g(X) = \sum_{b=1}^{f-1}\chi(b)X^{b-1}$ and consider the partial fraction expansion

$$\frac{g(X)}{X^f-1} = \sum_{a=1}^{f}\frac{r_a}{X-\zeta^a}.$$

Computing residues at ζ^a, we obtain

$$r_a = \frac{g(\zeta^a)}{(f)(\zeta^a)^{f-1}} = \frac{\zeta^a}{f} g(\zeta^a) = \frac{1}{f}\sum \chi(b)\zeta^{ab} = \frac{\bar{\chi}(a)}{f}\tau(\chi).$$

Therefore

$$\sum_{n=1}^{\infty} B_{n,\chi}\frac{t^{n-1}}{n!} = \sum_{b=1}^{f}\frac{\chi(b)e^{bt}}{e^{ft}-1} = e^t\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\bar{\chi}(a)\frac{1}{e^t-\zeta^a}$$

$$= -\frac{\tau(\chi)}{f}\sum_{a=1}^{f-1}\bar{\chi}(a)f'_a(t).$$

Therefore

$$\sum_{n=1}^{\infty}\frac{B_{n,\chi}}{n}\frac{t^n}{n!} = -\frac{\tau(\chi)}{f}\sum_{a=1}^{f-1}\bar{\chi}(a)f_a(t).$$

If we equate the coefficients of $t^n/n!$, we obtain the lemma. □

As in the case $f = p$, we have

$$L_p(1,\chi) = \frac{\tau(\chi)}{f}\lim_{n\to\infty}\sum_{a=1}^{f-1}\sum_{i=1}^{(p-1)p^n}\frac{\bar{\chi}(a)}{i(\zeta^a-1)^i}\sum_{j=1}^{i}\binom{i}{j}(-1)^{i-j}j^{(p-1)p^n}.$$

Postponing for the moment the justification of the termwise evaluation of $\lim j^{(p-1)^n} = 1$ if $p\nmid j$, we obtain

$$\frac{\tau(\chi)}{f}\lim\sum_{a=1}^{f-1}\sum_{i=1}^{(p-1)p^n}\frac{\bar{\chi}(a)}{i(\zeta^a-1)^i}\sum_{\substack{j=1\\ p\nmid j}}^{i}\binom{i}{j}(-1)^{i-j}.$$

But

$$\sum_{j=0}^{i}\binom{i}{j}(-1)^{i-j} = (1-1)^i = 0,$$

so

$$\sum_{p\nmid j}\binom{i}{j}(-1)^{i-j} = -\sum_{p\mid j}\binom{i}{j}(-1)^{i-j} = -\frac{1}{p}\sum_{\alpha^p=1}\sum_{j=0}^{i}\binom{i}{j}(-1)^{i-j}\alpha^j$$

$$= -\frac{1}{p}\sum_{\alpha^p=1}(\alpha-1)^i.$$

We now have

$$-\frac{\tau(\chi)}{pf}\sum_{a=1}^{f-1}\sum_{\alpha^p=1}\sum_{i=1}^{\infty}\bar{\chi}(a)\frac{1}{i}\left(\frac{\alpha-1}{\zeta^a-1}\right)^i.$$

If ζ is not a p-power root of unity then $|\zeta^a - 1|_p = 1$ so $|(\alpha - 1)/(\zeta^\alpha - 1)|_p < 1$. If ζ is a p^nth root of unity then $n \geq 2$ ($f \neq p$). Therefore again we have $|(\alpha - 1)/(\zeta^a - 1)| < 1$. In both cases we have convergence, so we get

$$\begin{aligned}
&\frac{\tau(\chi)}{pf}\sum_a\sum_\alpha \bar{\chi}(a)\log_p\left(1 - \frac{\alpha - 1}{\zeta^a - 1}\right)\\
&= \frac{\tau(\chi)}{pf}\sum_a\sum_\alpha \bar{\chi}(a)\log_p\left(\frac{\alpha - \zeta^a}{1 - \zeta^a}\right)\\
&= \frac{\tau(\chi)}{pf}\sum_{a=1}^{f} \bar{\chi}(a)[\log_p(1 - \zeta^{ap}) - p\log_p(1 - \zeta^a)]\\
&= -\left(1 - \frac{\chi(p)}{p}\right)\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\bar{\chi}(a)\log_p(1 - \zeta^a),
\end{aligned}$$

as desired (the $\log_p(1 - \zeta^{ap})$ is treated by a change of variables if $p \nmid f$. If $p \mid f$ then use the same technique as in the proof of Lemma 4.7).

We now justify the termwise evaluation of $\lim j^{(p-1)p^n}$, as promised above (yes, even in the p-adics things like this need to be checked once in a while). We know that $j^{(p-1)p^n} = J + \text{small}$, where $J = 0$ or 1. Consider the inner sums over i and j. We have

$$\sum\sum(\text{coefficient})(J + \text{small}) = \sum\sum(\text{coeff.})(J) + \sum\sum(\text{coeff.})(\text{small}).$$

When the coefficients are p-integral, the second term is small. The problem is that the coefficients have $(\zeta - 1)^i$ in the denominator, so sometimes they are large. Therefore we must show that (large)(small) = small.

Lemma 5.21.

$$\sum_{j=1}^{i}\binom{i}{j}(-1)^{i-j}j^m \quad\text{and}\quad \sum_{\substack{j=1\\ p\nmid j}}^{i}\binom{i}{j}(-1)^{i-j}$$

are both divisible by $i!$ for $m \geq 1$, the first divisibility being in $\mathbb{Z}$, the second in $\mathbb{Z}_p$ (note that we do not get $\mathbb{Z}$-divisibility for the second expression: let $p = 3$, $i = 4$. Then 24 divides 3 in $\mathbb{Z}_3$ but not in $\mathbb{Z}$).

Proof. Write the monomial X^m as

$$X^m = \sum_{i=0}^{\infty} a_i\binom{X}{i}.$$

Then the a_i are uniquely determined and

$$a_i = \sum_{j=1}^{i}\binom{i}{j}(-1)^{i-j}j^m$$

(see the discussion preceding Proposition 5.8). Since we may obviously write any polynomial in $\mathbb{Z}[X]$, in particular X^m, as a $\mathbb{Z}$-linear combination of polynomials of the form $(X)(X-1)\cdots(X-j+1) = X^j +$ lower terms, we must have $a_i/i! \in \mathbb{Z}$. This proves the first half of the lemma. But for any i we may let $m = (p-1)p^n \to \infty$ to obtain the second expression, so the lemma is proved. □

If ζ is not of p-power order we have $|\zeta^a - 1| = 1$, so we may proceed as in the case $f = p$: write

$$\frac{1}{i}\binom{i}{j} j^{(p-1)p^n} = \binom{i-1}{j-1} j^{(p-1)} j^{(p-1)p^n - 1}.$$

Everything else inside the limit is p-integral so we may take the limit termwise.

But if ζ is a p^mth root of unity ($m \geq 2$), then $i(\zeta^a - 1)^i$ is very small p-adically for large i, so we must proceed more carefully. Fix n and first consider $i \leq n$. Then

$$v_p(i(\zeta^a - 1)^i) \leq \frac{\log i}{\log p} + \frac{i}{\phi(p^m)} \leq \frac{\log n}{\log p} + \frac{n}{(p-1)p}.$$

If $p \mid j$ then $v_p(j^{(p-1)p^n}) \geq (p-1)p^n$ which grows faster than $v_p(i(\zeta^a - 1)^i)$. So omitting the terms with $p \mid j$ does not change the limit. If $p \nmid j$ then

$$v_p(j^{(p-1)p^n} - 1) \geq n + 1.$$

Therefore $v_p(j^{(p-1)p^n} - 1) - v_p(i(\zeta^a - 1)^i) \to \infty$ as $n \to \infty$ uniformly for $i \leq n$. It follows that we may replace $j^{(p-1)p^n}$ by 1 for all terms with $i \leq n$.

Now consider $i > n$. By the above lemma

$$\begin{aligned} v_p\left(\frac{1}{i(\zeta^a - 1)^i} \sum_{j=1}^{i} (-1)^{i-j} \binom{i}{j} j^{(p-1)p^n}\right) j &\geq v_p\left(\frac{(i-1)!}{(\zeta^a - 1)^i}\right) \\ &\geq \frac{i-1-p}{p-1} - \frac{\log(i-1)}{\log p} - \frac{i}{(p-1)p} \geq ci \geq cn \end{aligned}$$

for some $c > 0$ (for the estimate on $(i-1)!$ see the discussion preceding Proposition 5.4). Therefore the terms with $i > n$ do not affect the limit. We obtain the same result when $j^{(p-1)p^n}$ is replaced by 1 ($p \nmid j$) or 0 ($p \mid j$).

To summarize, if $i \leq n$ then the denominator is not small enough to cause problems, so we may take the limit termwise. The terms for $i > n$ become 0 in the limit, so may be ignored. This completes the justification. The proof of Theorem 5.18 is now complete. □

The above reasoning also yields the following result, which shows that the p-adic L-functions are Iwasawa functions (see Exercise 12.3 and Theorem 7.10).

Proposition 5.22. *Suppose $\chi \neq 1, f \neq p, \zeta = \zeta_f$. Then for $s \in \mathbb{Z}_p$ we have*

$$L_p(s, \chi) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f-1} \bar{\chi}(a) \sum_{i=1}^{\infty} \frac{1}{i(\zeta^a - 1)^i} \sum_{\substack{j=1 \\ p \nmid j}}^{i} \binom{i}{j} (-1)^{i-j} \langle j \rangle^{1-s}.$$

Proof. $L_p(s, \chi) = \lim L_p(1 - n, \chi)$, where $n = (p - 1)m \to \infty$, and $m \to (1 - s)/(p - 1)$ p-adically. So

$$L_p(s, \chi) = \lim - (1 - \chi(p)p^{n-1})\frac{B_{n,\chi}}{n} = -\lim \frac{B_{n,\chi}}{n}.$$

Now use Lemma 5.20. Since $\lim j^n = \lim(\omega(j)\langle j\rangle)^n = \lim\langle j\rangle^n = \langle j\rangle^{1-s}$ if $p \nmid j$, we may use the above reasoning to justify the termwise evaluation of the limit and obtain the result. The details are left to the reader. □

§5.5 The p-adic Regulator

The question now arises regarding whether or not $L_p(1, \chi)$ is nonzero. As in the complex case, we have $L_p(1, \chi) \neq 0$, but it is a rather deep fact. However, we may quickly dispose of a special case.

Proposition 5.23. *If p is a regular prime and k is an even integer with $k \not\equiv 0 \pmod{p - 1}$, then $L_p(1, \omega^k) \not\equiv 0 \pmod p$. In particular, $L_p(1, \omega^k) \neq 0$.*

Proof. We know from Corollary 5.13 that $L_p(1, \omega^k) \equiv L_p(1 - k, \omega^k) = = -(1 - p^{k-1})(B_k/k) \not\equiv 0 \pmod p$, since $p \nmid B_k$. □

To treat the general case, we introduce the p-adic regulator. Let K be a number field. If we fix an embedding of $\mathbb{C}_p$ into $\mathbb{C}$, then any embedding of K into $\mathbb{C}_p$ becomes an embedding into $\mathbb{C}$, hence may be considered as real or complex, depending on the image of K (this classification possibly depends on the choice of the embedding of $\mathbb{C}_p$ into $\mathbb{C}$. We therefore sometimes obtain an ambiguity in the definition of the p-adic regulator. See Exercises 5.12 and 5.13). Let $r = r_1 + r_2 - 1$, with r_1, r_2 defined as usual for K. The embeddings of K into $\mathbb{C}_p$ may be listed as $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}$, where the σ_i, $1 \leq i \leq r_1$ are real in the above sense, and the other embeddings are complex. Let $\delta_i = 1$ if σ_i is real, $\delta_i = 2$ if σ_i is complex. Let $\varepsilon_1, \ldots, \varepsilon_r$ be independent units of K. Then

$$R_{K,p}(\varepsilon_1, \ldots, \varepsilon_r) = \det(\delta_i \log_p(\sigma_i \varepsilon_j))_{1 \leq i, j \leq r}.$$

Note that this regulator is only defined up to a change in sign, since changing the order of the σ_i's could introduce a factor of -1. We are mostly interested in p-divisibility properties, so this will not present a problem. Since there are additional ambiguities unless K is real, or *CM* (see Exercise 5.13), we shall usually only discuss p-adic regulators in these cases.

If $\{\varepsilon_1, \ldots, \varepsilon_r\}$ is a basis for the units of K modulo roots of unity, then $R_p(K) = R_{K,p}(\varepsilon_1, \ldots, \varepsilon_r)$ is called the p-adic regulator of K. In Chapter 8 we shall prove the following result. The proof will rely heavily on the above formula for $L_p(1, \chi)$.

Theorem 5.24. *Let K be a totally real abelian number field of degree n corresponding to a group X of Dirichlet characters. Then*

$$\frac{2^{n-1}h(K)R_p(K)}{\sqrt{d(K)}} = \prod_{\substack{\chi\in X\\ \chi\neq 1}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1, \chi).$$

(Since both $R_p(K)$ and $\sqrt{d(K)}$ are only determined up to sign, the above equality actually means that we can choose signs so as to obtain equality.)

If we define the p-adic zeta function of K to be

$$\zeta_{K,p}(s) = \prod_{\chi\in X} L_p(s, \chi)$$

then we obtain

$$\lim_{s\to 1} (s-1)\zeta_{K,p}(s) = \frac{2^{n-1}hR_p}{\sqrt{d}} \prod_{\chi\in X} \left(1 - \frac{\chi(p)}{p}\right),$$

so if $R_p \neq 0$ then $\zeta_{K,p}(s)$ has a simple pole at $s = 1$ with a residue which is the p-adic analogue of the residue for the complex case.

We shall prove that $R_p(K) \neq 0$ when K is abelian over $\mathbb{Q}$, so that $L_p(1, \chi) \neq 0$. From Proposition 5.23 combined with Theorem 5.24, we already have $R_p(K) \neq 0$ when $K = \mathbb{Q}(\zeta_p)^+$ and p is regular. In general, there is the following.

Leopoldt's Conjecture (Preliminary Form). $R_p(K) \neq 0$ *for all number fields* K.

At present, there is no general proof of this result, although it has been verified in several cases.

Theorem 5.25. *If $K/\mathbb{Q}$ is abelian then $R_p(K) \neq 0$.*

Proof. We shall need several preparatory results.

Lemma 5.26. *Let G be a finite abelian group and let f be a function on G with values in some field of characteristic* 0. *Then*

(a) $$\det(f(\sigma\tau^{-1}))_{\sigma,\tau\in G} = \prod_{\chi\in\hat{G}} \sum_{\sigma\in G} \chi(\sigma)f(\sigma),$$

(b) $$\det(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau\neq 1} = \prod_{\chi\neq 1} \sum_{\sigma\in G} \chi(\sigma)f(\sigma),$$

(c) *if* $\sum_\sigma f(\sigma) = 0$ *then*

$$\det(f(\sigma\tau^{-1}))_{\sigma,\tau\neq 1} = |G|^{-1} \cdot \prod_{\chi\neq 1} \sum_{\sigma\in G} \chi(\sigma)f(\sigma).$$

Proof. (a) Consider the finite-dimensional vector space V of all functions $h(X)$ on G. Then G acts on V by translation: $\sigma h(X) = h(\sigma X)$. Define the linear transformation $T = \sum_\sigma f(\sigma)\sigma$. Let $\phi_\tau(X)$ be the characteristic function of $\{\tau\} \subseteq G$, so $\phi_\tau(\sigma) = 1$ if $\sigma = \tau$ and 0 if $\sigma \neq \tau$. Then $\{\phi_\tau\}_{\tau \in G}$ forms a basis for V. Since

$$\begin{aligned} T\phi_\tau(X) &= \sum_\sigma f(\sigma)\phi_\tau(\sigma X) = \sum_\sigma f(\sigma)\phi_{\sigma^{-1}\tau}(X) \\ &= \sum_\alpha f(\tau\alpha^{-1})\phi_\alpha(X), \end{aligned}$$

the matrix $(f(\sigma\tau^{-1}))_{\sigma,\tau \in G}$ is the matrix for T with respect to this basis. Since the characters $\chi \in \hat{G}$ are linearly independent, they also form a basis for V (alternatively, since $\phi_\tau(X) = \sum_\chi \chi(\tau^{-1}X)$, they span V, hence form a basis). But $T\chi(X) = \sum_\sigma f(\sigma)\chi(\sigma)\chi(X)$, so the character χ is an eigenvector with eigenvalue $\sum \chi(\sigma)f(\sigma)$. Consequently, T is diagonal with respect to this basis. The determinant is the product of these eigenvalues, so the first part of the lemma is proved.

(b) Let W be the subspace consisting of functions $h(X)$ with $\sum_\sigma h(\sigma) = 0$. Let $\psi_\tau(X) = \phi_\tau(X) - 1/|G|$. Then $\{\psi_\tau(X) | \tau \neq 1\}$ forms a basis for W. Using the fact that $\psi_1(X) = -\sum_{\tau \neq 1} \psi_\tau(X)$, we easily find that $(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau \neq 1}$ is the matrix of T restricted to W for this basis. As before, the nontrivial characters diagonalize T restricted to W, so part (b) follows.

(c) Adjoin a row and column to $(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau \neq 1}$ to obtain the following (index the rows by σ, the columns by τ):

$$\begin{pmatrix} 1 & 0 & \cdots \\ f(\sigma) & f(\sigma\tau^{-1}) - f(\sigma) & \cdots \\ \vdots & \vdots & \end{pmatrix}$$

Now add the first column to each of the other columns, then add each of the columns of the resulting matrix onto the first column. The final result is

$$\begin{pmatrix} |G| & 1 & \cdots \\ 0 & f(\sigma\tau^{-1}) & \cdots \\ \vdots & \vdots & \end{pmatrix}$$

We have used the fact that $\sum_\sigma f(\sigma) = 0$ to obtain the zeroes in the first column. Using the result of part (b), we obtain the result. This completes the proof of Lemma 5.26. □

Lemma 5.27. *Let $K/\mathbb{Q}$ be a finite Galois extension. If K is real then let $\sigma_1, \ldots, \sigma_{r+1}$ be the elements of* $\mathrm{Gal}(K/\mathbb{Q})$. *If K is complex then let $\sigma_1, \ldots, \sigma_{r+1}$, $\bar{\sigma}_1, \ldots, \bar{\sigma}_{r+1}$ be the elements of* $\mathrm{Gal}(K/\mathbb{Q})$ *(we regard K as a subfield of* $\mathbb{C}$*). There exists a unit ε of K such that the set of units $\{\varepsilon^{\sigma_i} | 1 \leq i \leq r\}$ is multiplicatively independent, hence generates a subgroup of finite index in the full group of units (such a unit is called a Minkowski unit).*

Proof. We shall find a unit ε such that $|\varepsilon^{\sigma_1}| > 1$ but $|\varepsilon^{\sigma_i}| < 1$ for $i \neq 1$ (the absolute value is the complex absolute value corresponding to a fixed embedding of K into $\mathbb{C}$). The existence of such a unit is usually implicitly proved during the proof of Dirichlet's Unit Theorem. However, since it is rather difficult to isolate this step from many treatments of the subject, we shall reverse the steps and derive the existence of ε from the Unit Theorem.

Let E be the group of units of K and consider the mapping $L: E \to \mathbb{R}^r$ defined by

$$L(\eta) = (\log|\eta^{\sigma_2}|, \ldots, \log|\eta^{\sigma_{r+1}}|).$$

Note that $\log|\eta^{\sigma_1}| = -\sum_{i=2}^{r+1} \log|\eta^{\sigma_i}|$. The kernel of L is exactly the roots of unity in K by Lemma 1.6. By the Unit Theorem, the image must be a free abelian group of rank r. A bound on $L(\eta)$ gives a bound on the conjugates of η, hence on the coefficients of the irreducible polynomial for η. It follows that there are only finitely many images $L(\eta)$ is any bounded region of $\mathbb{R}^r$, so the image of L is discrete. Therefore it is a lattice M of maximal rank. Consider the "quadrant" $Q = \{(x_2, \ldots, x_{r+1}) \in \mathbb{R}^r | x_i < 0 \text{ for } 2 \le i \le r+1\}$. Then $M \cap Q \neq \phi$. Let $\varepsilon \in E$ satisfy $L(\varepsilon) \in M \cap Q$. Then $\log|\varepsilon^{\sigma_i}| < 0$ for $2 \le i \le r+1$ and $\log|\varepsilon^{\sigma_1}| = -\sum_{i=2}^{r+1} \log|\varepsilon^{\sigma_i}| > 0$. It follows that $|\varepsilon^{\sigma_i}| > 1$ but $|\varepsilon^{\sigma_i}| < 1$ for $i \neq 1$, as desired.

We claim that ε is a unit of the type asserted in the lemma. For the proof we need the following.

Lemma 5.28. *Let (a_{ij}) be a real square matrix with $a_{ii} > 0$, $a_{ij} \le 0$ for $i \neq j$, and such that $\sum_i a_{ij} > 0$ for all j. Then* $\det(a_{ij}) \neq 0$.

Proof. If $\det(a_{ij}) = 0$, there exists a non-zero vector (x_i) such that $\sum a_{ij} x_i = 0$ for each j. Let $|x_k|$ be maximal among the entries of the vector. By changing signs if necessary, we may assume $x_k > 0$, hence $x_k \ge x_i$ for all i. Then

$$\begin{aligned} 0 = \sum_i a_{ik} x_i &\ge \sum_i a_{ik} x_k \quad (\text{since } a_{ik} \le 0 \text{ for } i \neq k) \\ &= (\textstyle\sum a_{ik}) x_k > 0, \quad \text{contradiction.} \end{aligned}$$

□

Returning to the proof of Lemma 5.27, we may assume $\sigma_1 = id$ and let

$$a_{ij} = \delta_i \log|\varepsilon^{\sigma_j \sigma_i^{-1}}|.$$

Then $a_{ii} = \delta_i \log|\varepsilon^{\sigma_1}| > 0$ and $a_{ij} < 0$ for $i \neq j$. Since $\sum_{i=1}^{r+1} a_{ij} = 0$, we have $\sum_{i=1}^{r} a_{ij} = -a_{r+1,j} > 0$ for $j \neq r+1$. Lemma 5.28 implies that

$$R_K(\varepsilon^{\sigma_1}, \ldots, \varepsilon^{\sigma_r}) = |\det(a_{ij})| \neq 0.$$

Therefore $\varepsilon^{\sigma_1}, \ldots, \varepsilon^{\sigma_r}$ must be multiplicatively independent, otherwise there would be a linear relation among rows of the determinant. This completes the proof of Lemma 5.27. □

We now prove Theorem 5.25. We may assume that K is totally real, since if K is imaginary then $R_p(K) = (1/Q)2^r R_p(K^+)$ (use the same proof as for Proposition 4.15, changing log to $\log_p$). Fix an embedding of K into $\mathbb{C}_p$, let $\{1 = \sigma_1, \dots, \sigma_{r+1}\} = \mathrm{Gal}(K/\mathbb{Q})$, and let ε be as in Lemma 5.27. By Lemma 5.26(c) (this is where we need $G = \mathrm{Gal}(K/\mathbb{Q})$ to be abelian) we have

$$\begin{aligned} R_p(\varepsilon^{\sigma_2}, \dots, \varepsilon^{\sigma_{r+1}}) &= \det(\log_p(e^{\sigma_i \sigma_j^{-1}}))_{2 \le i, j \le r+1} \\ &= \frac{1}{|G|} \prod_{\substack{\chi \ne 1 \\ \chi \in \hat{G}}} \sum_{\sigma} \chi(\sigma) \log_p(\varepsilon^{\sigma}). \end{aligned}$$

We now need the following deep result, which is the p-adic analogue of a theorem of Baker.

Theorem 5.29. *Let* $\alpha_1, \dots, \alpha_n$ *be algebraic over* $\mathbb{Q}$ *and suppose* $\log_p \alpha_1, \dots, \log_p \alpha_n$ *are linearly independent over* $\mathbb{Q}$. *Then they are linearly independent over* $\bar{\mathbb{Q}}$ *= the algebraic closure of* $\mathbb{Q}$ *in* $\mathbb{C}_p$ *(for a proof, see Brumer* [1]*).* □

Since $\varepsilon^{\sigma_1}, \dots, \varepsilon^{\sigma_r}$ are multiplicatively independent, it follows easily that $\log_p(\varepsilon^{\sigma_1}), \dots, \log_p(\varepsilon^{\sigma_r})$ are linearly independent over $\mathbb{Q}$ (we need Proposition 5.6). Since

$$\log_p(\varepsilon^{\sigma_{r+1}}) = -\sum_{i=1}^{r} \log_p(\varepsilon^{\sigma_i}),$$

we have

$$\sum_{\sigma} \chi(\sigma) \log_p(\varepsilon^{\sigma}) = \sum_{i=1}^{r} (\chi(\sigma_i) - \chi(\sigma_{r+1})) \log_p(\varepsilon^{\sigma_i}).$$

If $\chi \ne 1$ then $\chi(\sigma_i) \ne \chi(\sigma_{r+1})$ for some i, so not all coefficients are zero. By the above theorem, the sum does not vanish. Therefore

$$R_p(\varepsilon^{\sigma_2}, \dots, \varepsilon^{\sigma_{r+1}}) . \ne 0.$$

But $R_p(\varepsilon^{\sigma_2}, \dots, \varepsilon^{\sigma_{r+1}}) = [E : E'] R_p(K)$, where E is the full group of units of K and E' is the subgroup generated by ± 1 and $\varepsilon^{\sigma_2}, \dots, \varepsilon^{\sigma_{r+1}}$, which is the same as the subgroup generated by ± 1 and $\{\varepsilon^{\sigma_i} \mid 1 \le i \le r\}$. This completes the proof of Theorem 5.25. □

Corollary 5.30. *Let* $\chi \ne 1$ *be an even Dirichlet character. Then* $L_p(1, \chi) \ne 0$. □

By Theorem 5.18, we know that $L_p(1, \chi)$ is essentially a linear form in logarithms. So why did we not apply Theorem 5.29 directly? The problem is that the logarithms in question are generally not independent over $\mathbb{Q}$. In certain cases we know all relations. For example, the only relation among $\{\log_p(1 - \zeta_p^a) \mid 1 \le a \le (p-1)/2)$ is that the sum is 0. So we may use the argument used above to obtain a situation where Theorem 5.29 is applicable. But in the general situation, there can be many more relations and the analysis becomes much more complicated. We shall discuss this matter more fully in Chapter 8.

For later reference, we now give another version of Leopoldt's Conjecture. Let K be a number field. For each prime $\not{p}$ lying above p, let $U_{\not{p}}$ denote the local units of $K_{\not{p}}$ and $U_{1,\not{p}}$ denote the principal units, that is, the units congruent to 1 modulo $\not{p}$. Let

$$U = \prod_{\not{p}|p} U_{\not{p}} \quad \text{and} \quad U_1 = \prod_{\not{p}|p} U_{1,\not{p}}.$$

We may embed the global units E in U:

$$\begin{aligned} E &\hookrightarrow U \\ \varepsilon &\mapsto (\varepsilon, \ldots, \varepsilon). \end{aligned}$$

Let E_1 denote those ε whose images are in U_1. Then E_1 is a subgroup of E of finite index (since $\varepsilon^{N\not{p}-1} \in U_{1,\not{p}}$), so E_1 is an abelian group of rank $r = r_1 + r_2 - 1$. Let $\bar{E}_1$ denote the closure of E_1 in the topology of U_1. Since U_1 is a $\mathbb{Z}_p$-module ($s\colon u \mapsto u^s$), $\bar{E}_1$ is also a $\mathbb{Z}_p$-module. What is its rank?

Leopoldt's Conjecture. *The $\mathbb{Z}_p$-rank of $\bar{E}_1$ is $r_1 + r_2 - 1$.*

Theorem 5.31. *Let K be totally real. Then $R_p(K) \neq 0 \Leftrightarrow$ the $\mathbb{Z}_p$-rank of $\bar{E}_1$ is $r_1 - 1$.*

Remarks. One may be tempted to think that $\bar{E}_1$ must have rank $r_1 + r_2 - 1$ since E_1 has that for its $\mathbb{Z}$-rank. But consider the following. The group generated by 7 and 13 in $\mathbb{Q}_3^\times$ has $\mathbb{Z}$-rank 2. But $7^{\log_3 13} = 13^{\log_3 7}$, and $\log_3 13/\log_3 7 \in \mathbb{Z}_3$. Therefore 7 generates the closure of the group, so the $\mathbb{Z}_3$-rank of the closure is 1.

If there is only one $\not{p}$ above p in K, then the theorem says that $R_p(K) \neq 0 \Leftrightarrow$ units which are independent over $\mathbb{Z}$ are independent over $\mathbb{Z}_p$. This is not necessarily true for nonunits, as the above example with 7 and 13 shows.

Also, if there are several primes above p, it is not sufficient to consider only one $U_{1,\not{p}}$. For example, if p splits completely then each $U_{1,\not{p}}$ is a $\mathbb{Z}_p$-module of rank 1; so if $r_1 + r_2 + 1 > 1$ then the units must be $\mathbb{Z}_p$-dependent in each $U_{1,\not{p}}$. But the relations are different for different $\not{p}$, so it is still possible for the units to be $\mathbb{Z}_p$-independent in U_1.

To be more precise, suppose $\varepsilon_1, \ldots, \varepsilon_r$ are $\mathbb{Z}_p$-dependent in U_1. Then there exist $a_1, \ldots, a_r \in \mathbb{Z}_p$ such that $\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} = 1$ in $K_{\not{p}}$ for all $\not{p}$. This means that if $a_{i,n}$ are rational integers with $a_{i,n} \to a_i$ p-adically ,then

$$\varepsilon_1^{a_{1,n}} \cdots \varepsilon_r^{a_{r,n}} \to 1 \quad \text{in } K_{\not{p}} \text{ for each } \not{p}.$$

Since the $\not{p}$-adic valuations are different for different $\not{p}$, the fact that the limit is 1 for one $K_{\not{p}}$ does not imply anything about the limit for other $\not{p}$. However, if the units are $\mathbb{Z}_p$-dependent then it is possible to get 1 as a limit for all $K_{\not{p}}$ simultaneously.

Proof of Theorem 5.31. Suppose the $\mathbb{Z}_p$-rank of $\bar{E}_1$ is less than $r = r_1 - 1$. Let $\varepsilon_1, \ldots, \varepsilon_r$ be a $\mathbb{Z}$-basis for E_1 modulo roots of unity. Then $\varepsilon_1, \ldots, \varepsilon_r$ must be $\mathbb{Z}_p$-dependent in U_1, say

$$\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} = 1 \qquad (a_i \in \mathbb{Z}_p, \text{ some } a_i \neq 0).$$

Let L be the Galois closure of $K/\mathbb{Q}$. Suppose that $|x|_{\mathfrak{p}_1}$ and $|x|_{\mathfrak{p}_2}$ are the absolute values corresponding to primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of K lying above p. When these absolute values are extended to L they are related by $|x|_{\mathfrak{p}_1} = |\sigma x|_{\mathfrak{p}_2}$ for some $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ (in fact, $\sigma\mathcal{P}_1 = \mathcal{P}_2$, where $\mathcal{P}_i$ lies above $\mathfrak{p}_i$). Therefore, if

$$\varepsilon_1^{a_{1n}} \cdots \varepsilon_r^{a_{rn}} \to 1 \quad \text{in } K_{\mathfrak{p}_1} \text{ (hence in } (L_{\mathcal{P}_1})$$

then

$$(\varepsilon_1^{\sigma})^{a_{1n}} \cdots (\varepsilon_r^{\sigma})^{a_{rn}} \to 1 \quad \text{in } L_{\mathcal{P}_2}.$$

Fix a prime $\mathfrak{p}_0$ lying above p in K and a prime $\mathcal{P}_0$ lying above $\mathfrak{p}_0$ in L. Then

$$\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} = 1 \quad \text{in } K_{\mathfrak{p}} \text{ for all } \mathfrak{p}$$

if and only if

$$(\varepsilon_1^{\sigma})^{a_1} \cdots (\varepsilon_r^{\sigma})^{a_r} = 1 \quad \text{in } L_{\mathcal{P}_0} \text{ for all } \sigma \in \mathrm{Gal}(L/\mathbb{Q})$$

(does $(\varepsilon^{\sigma})^a = (\varepsilon^a)^{\sigma}$? No, since σ is not always an automorphism of $L_{\mathcal{P}_0}/\mathbb{Q}_p$; it does not necessarily fix $\mathbb{Q}_p$ if p splits, so σ does not even make sense as a p-adic map. It is defined only before embedding in $L_{\mathcal{P}_0}$).

Taking logarithms (we may assume $L_{\mathcal{P}_0} \subset \mathbb{C}_p$), we have

$$\sum_i a_i \log_p(\varepsilon_i^{\sigma}) = 0 \quad \text{for all } \sigma.$$

Clearly this implies that $R_p(\varepsilon_1, \ldots, \varepsilon_r) = 0$, hence $R_p(K) = 0$.

Conversely, suppose $R_p(K) = 0$. Then there exist $a_i \in L_{\mathcal{P}_0}$ such that

$$\sum_i a_i \log_p(\varepsilon_i^{\sigma}) = 0 \quad \text{for all } \sigma;$$

but we want $a_i \in \mathbb{Z}_p$. We may assume that one of the a_i's equals 1. Let $\tau \in \mathrm{Gal}(L_{\mathcal{P}_0}/\mathbb{Q}_p)$. Then

$$\sum_i a_i^{\tau} \log_p(\varepsilon_i^{\tau\sigma}) = 0 \quad \text{for all } \sigma;$$

since τ permutes the σ's, we have

$$\sum_i a_i^{\tau} \log_p(\varepsilon_i^{\sigma}) = 0 \quad \text{for all } \sigma.$$

Letting T denote the trace from $L_{\mathcal{P}_0}$ to $\mathbb{Q}_p$, we obtain

$$\sum_i T(a_i) \log_p(\varepsilon_i^{\sigma}) = 0 \quad \text{for all } \sigma.$$

Since one $a_i = 1$, at least one of the $T(a_i) \neq 0$. Upon clearing denominators we obtain a relation with coefficients in $\mathbb{Z}_p$. Reversing the steps from the first half, we find that (we now may assume $a_i \in \mathbb{Z}_p$ for all i)

$$(\varepsilon_1^\sigma)^{a_1} \cdots (\varepsilon_r^\sigma)^{a_r} = (\text{root of unity}) \quad \text{in } L_{\mathscr{P}_0}$$

for all σ. If we multiply each a_i by the same integer, chosen suitably, we may assume the root of unity is 1. Then, continuing backwards through the above, we have $\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} = 1$ in $K_{\not{p}}$ for all $\not{p}$, so $\varepsilon_1, \ldots, \varepsilon_r$ are $\mathbb{Z}_p$-dependent in U_1. Since $\bar{E}_1$ is generated (modulo torsion) over $\mathbb{Z}_p$ by $\varepsilon_1, \ldots, \varepsilon_r$, we must have the $\mathbb{Z}_p$-rank of $\bar{E}_1 < r = r_1 - 1$. This completes the proof. □

Corollary 5.32. *If $K/\mathbb{Q}$ is abelian then the $\mathbb{Z}_p$-rank of $\bar{E}_1$ is $r_1 + r_2 - 1$.*

Proof. If K is real, use Theorems 5.25 and 5.31. If K is complex, then the corollary is true for K^+. Since $r_1 + r_2 - 1$ is the same for both fields, the result follows easily. □

§5.6 Applications of the Class Number Formula

We now use the p-adic class number formula (Theorem 5.24) to deduce results on class numbers.

Proposition 5.33. *Suppose K is a totally real abelian number field. If p does not divide $\deg(K/\mathbb{Q})$, if there is only one prime of K above p, and if the ramification index of p is at most $p - 1$, then*

$$\left| \frac{R_p(K)}{\sqrt{d(K)}} \right|_p \leq 1.$$

Proof. Let K_p denote the completion of K at the prime above p and let $\mathcal{O}_p$ be the ring of integers of K_p. By the assumptions on p, $\deg(K_p/\mathbb{Q}_p) = \deg(K/\mathbb{Q})$ and also the Galois groups may be identified.

If $x \in K_p$ and $|x| < 1$ then $|x| \leq p^{-1/(p-1)}$. Therefore (cf. Lemma 5.5)

$$\log_p(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \in \mathcal{O}_p$$

since all terms in the sum are in $\mathcal{O}_p$. It follows easily from the definition of the extension of $\log_p$ that $\log_p \varepsilon \in \mathcal{O}_p$ for all $\varepsilon \in K_p$.

Let $\varepsilon_1, \ldots, \varepsilon_{n-1}$ ($n = \deg(K/\mathbb{Q})$) be a basis for the units of K modulo $\{\pm 1\}$, and let $\beta_i = \log_p \varepsilon_i$, $1 \leq i \leq n - 1$. Let $\beta_n = 1$. Then $\{\beta_1, \ldots, \beta_n\}$ generates a $\mathbb{Z}_p$-submodule of $\mathcal{O}_p$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for $\mathcal{O}_p$ as a $\mathbb{Z}_p$-module. Then we can write

$$\beta_i = \sum_{j=1}^{n} a_{ij} \alpha_j \quad \text{with} \quad a_{ij} \in \mathbb{Z}_p.$$

Let $\varepsilon \in \mathrm{Gal}(K_p/\mathbb{Q}_p)$. Then $\beta_i^\sigma = \sum a_{ij}\alpha_j^\sigma$, so

$$\det(\beta_i^\sigma)_{i,\sigma} = \det(a_{ij})_{i,j}\det(\alpha_j^\sigma)_{j,\sigma}.$$

The p-part of the discriminant of K is the discriminant of $K_p/\mathbb{Q}_p$ (there is only one prime above p), so we have

$$|\sqrt{d(K)}|_p = |\sqrt{d(K_p)}|_p = |\det(\alpha_j^\sigma)|_p.$$

Also

$$\det(\beta_i^\sigma) = \det\begin{pmatrix} \cdots & \log_p(\varepsilon_i^\sigma) & \cdots \\ \cdots & 1 & \cdots \end{pmatrix}.$$

Since $\sum_\sigma \log_p(\varepsilon^\sigma) = 0$, we may add all the columns onto the last one to obtain

$$\det(\beta_i^\sigma) = \deg(K/\mathbb{Q})R_p(K).$$

Therefore, since $p \nmid \deg(K/\mathbb{Q})$, we have

$$\left|\frac{R_p(K)}{\sqrt{d(K)}}\right|_p = \left|\frac{\det(\beta_i^\sigma)}{\det(\alpha_j^\sigma)}\right|_p = |\det(a_{ij})|_p \leq 1,$$

because $a_{ij} \in \mathbb{Z}_p$ for all i, j. This completes the proof. □

Remark. Actually, the proposition is true in much more generality. Let K be totally real of degree n and for each prime $\not{p}$ above p let $N\not{p}$ denote its norm and $v_{\not{p}}$ the number of p-power roots of unity in $K_{\not{p}}$. Then

$$\left|\frac{npR_p}{\sqrt{d}}\prod_{\not{p}|p}\frac{1}{(N\not{p})(v_{\not{p}})}\right|_p \leq 1.$$

In particular,

$$\left|\frac{nR_p}{\sqrt{d}}\right|_p \leq 1.$$

The proof involves an extension of the above ideas (see Coates [7]).

Theorem 5.34. *If $p \mid h^+(\mathbb{Q}(\zeta_p))$ then $p \mid h^-(\mathbb{Q}(\zeta_p))$. Therefore $p \mid h(\mathbb{Q}(\zeta_p)) \Leftrightarrow p$ divides B_j for some $j = 2, 4, \ldots, p-3$.*

Remark. At present, there are no known examples where $p \mid h^+(\mathbb{Q}(\zeta_p))$. It is a conjecture of Vandiver that this never happens.

Proof of Theorem 5.34. The characters corresponding to $\mathbb{Q}(\zeta_p)^+$ are $1, \omega^2, \ldots, \omega^{p-3}$. Let $n = \frac{1}{2}(p-3)$. Then

$$\frac{2^{n-1}h^+R_p^+}{\sqrt{d^+}} = \prod_{\substack{j=2 \\ j\,\text{even}}}^{p-3} L_p(1, \omega^j).$$

Since $\mathbb{Q}(\zeta_p)^+$ satisfies the hypotheses of Proposition 5.33, we have $|R_p^+/\sqrt{d^+}| \leq 1$. If $p|h^+$ then $p|L_p(1, \omega^j)$ for some $j = 2, 4, \ldots, p-3$. By Corollary 5.13,

$$\begin{aligned} 0 &\equiv L_p(1, \omega^j) \equiv L_p(0, \omega^j) \\ &\equiv -(1-\omega^{j-1}(p))B_{1,\omega^{j-1}} = -B_{1,\omega^{j-1}} \pmod{p}. \end{aligned}$$

Since

$$h^- \equiv \prod_{\substack{i=1 \\ i \text{ odd}}}^{p-4} (-\tfrac{1}{2}B_{1,\omega^i}) \pmod{p}$$

(see the proof of Theorem 5.16), and since all these B_{1,ω^i} are p-integral (Corollary 5.13), we have $p|h^-$, as desired. This completes the proof. □

Later, we shall give another proof of Theorem 5.34 which depends on class field theory but not on p-adic L-functions.

Before giving more applications, we need to know about logarithms of units.

Lemma 5.35. *Let $K/\mathbb{Q}$ be an extension of degree n, with $n \leq p-1$. Assume that p is totally ramified: $(p) = \mathfrak{p}^n$. Suppose ε is a unit of K which is congruent to a rational integer modulo $\mathfrak{p}^c$ ($c > 0$). Then* $\log_p \varepsilon \equiv 0 \bmod \mathfrak{p}^c$.

Proof. Let π generate $\mathfrak{p}$ in $\mathcal{O}_\mathfrak{p}$, so $\varepsilon = a + b\pi^c + \cdots = a(1 + (b/a)\pi^c + \cdots)$ with $a, b, \ldots \in \mathbb{Z}$. Since

$$|\pi^c| = p^{-c/n} \leq p^{-1/(p-1)},$$

we have $\log_p(1 + (b/a)\pi^c + \cdots) \equiv 0 \bmod \mathfrak{p}^c$ by Lemma 5.5. So $\log_p \varepsilon \equiv \log_p a$. Let N denote the norm from $K_\mathfrak{p}$ to $\mathbb{Q}_p$ (which may be identified with the norm from K to $\mathbb{Q}$). Then

$$\pm 1 = N\varepsilon \equiv Na = a^n \bmod \mathfrak{p}^c.$$

Therefore $n \log_p a = \log_p a^n = \log_p(\pm a^n) \equiv 0 \bmod \mathfrak{p}^c$. Since $p \nmid n$, the proof is complete. □

We are now able to prove a famous result of Kummer which will be useful for treating the second case of Fermat's Last Theorem.

Theorem 5.36. *Assume p is a regular prime and let ε be a unit of $\mathbb{Q}(\zeta_p)$. If ε is congruent to a rational integer* mod p *then ε is the* pth *power of a unit of $\mathbb{Q}(\zeta_p)$.*

(Note that the congruence is mod p, which is much stronger than mod$(1-\zeta)$, which always holds. Also, the converse of the theorem is true (Lemma 1.8). See also Exercise 8.1.)

Proof. We may write $\varepsilon = \zeta^a \varepsilon_1$ with ε_1 real, by Proposition 1.5. Every element of $\mathbb{Z}[\zeta + \zeta^{-1}]$ is congruent mod$(1-\zeta)(1-\zeta^{-1}) = 2 - (\zeta + \zeta^{-1})$ to a rational integer (simply replace $\zeta + \zeta^{-1}$ by 2). Also $\zeta^a = (1 + (\zeta - 1))^a \equiv 1 + a(\zeta - 1) \bmod (\zeta - 1)^2$. If $\zeta^a \varepsilon_1$ is congruent to a rational integer $\bmod (\zeta - 1)^2$, we must have $p \mid a$. Therefore $\varepsilon = \varepsilon_1$ is real.

From now on we work with $K = \mathbb{Q}(\zeta_p)^+$. Let $\not{p} = ((1 - \zeta)(1 - \zeta^{-1}))$, the prime above p. Then $\not{p}^{(p-1)/2} = (p)$. By Lemma 5.35, $\log_p \varepsilon \equiv 0 \pmod p$, so $(1/p) \log_p \varepsilon \in \mathcal{O}_{\not{p}}$.

Suppose ε is not a pth power. Then we may find (real) units $\varepsilon_2, \dots, \varepsilon_r$ $(r = (p - 3)/2)$ such that the group E' generated by $\pm 1, \varepsilon, \varepsilon_2, \dots, \varepsilon_r$ is a subgroup of index prime to p in the full group of units E (Proof: Let $\eta_1, \dots, \eta_r$ be a basis for E, so $\varepsilon = \pm \prod \eta_i^{a_i}$ with some $a_i \not\equiv 0 \bmod p$, say $i = 1$. Let $\varepsilon_j = \eta_j$ for $j \geq 2$. Then E' has index $\pm a_1 \not\equiv 0 \pmod p$.) Therefore

$$|R_p(E')| = |[E : E^+] R_p(K)| = |R_p(K)|.$$

Let $\beta_1 = (1/p) \log_p \varepsilon_1$, $\beta_i = \log_p \varepsilon_i$, $2 \leq i \leq r$, $\beta_{r+1} = 1$. Then $\beta_1, \dots, \beta_{r+1}$ generate a $\mathbb{Z}_p$-submodule of $\mathcal{O}_{\not{p}}$. As in the proof of Proposition 5.33, we have

$$\left| \frac{\det(\beta_i^\sigma)}{\sqrt{d(K)}} \right| \leq 1 \quad \text{and} \quad \det(\beta_i^\sigma) = \frac{1}{p} \cdot \deg(\mathbb{Q}(\zeta_p^+)/\mathbb{Q}) \cdot R_p(E').$$

Therefore

$$\left| \frac{R_p(K)}{\sqrt{d}} \right| \leq |p| < 1.$$

But

$$\frac{2^r h^+ R_p}{\sqrt{d}} = \prod_{\substack{j=2 \\ j \text{ even}}}^{p-3} L_p(1, \omega^j),$$

so p must divide $L_p(1, \omega^j)$ for some j. This contradicts Proposition 5.23. The proof is complete. □

We now give another proof using class field theory. As above, we may assume ε is real. Raising ε to the $(p - 1)$st power if necessary, we may assume that $\varepsilon \equiv 1 \pmod p$ (ε^{p-1} is a pth power $\Leftrightarrow$ ε is a pth power). Let $\pi = \zeta_p - 1$. Note that π^{p-1}/p is a unit of $\mathbb{Z}[\zeta]$ and that every element of $\mathbb{Z}[\zeta]$ is congruent to a rational integer modulo π. We may write

$$\varepsilon = 1 + pa + p\pi y \quad \text{with} \quad y \in \mathbb{Z}[\zeta] \quad \text{and} \quad a \in \mathbb{Z}.$$

Then

$$1 = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\varepsilon) \equiv (1 + pa)^{p-1} \equiv 1 + (p - 1)pa \equiv 1 - pa \pmod{p\pi},$$

so $\pi \mid a$ and $\varepsilon \equiv 1 \bmod p\pi$. Since $\varepsilon - 1$ is real, $v_p(\varepsilon - 1)$ is a multiple of $2/(p - 1) (= 1/e$ for $\mathbb{Q}(\zeta_p)^+)$. Therefore

$$v_p(\varepsilon - 1) \geq 1 + \frac{2}{p - 1}, \quad \text{or} \quad \varepsilon \equiv 1 \bmod p\pi^2 \quad (\text{or} \bmod \pi^{p+1}).$$

Consider the polynomial

$$f(X) = \frac{(\pi X - 1)^p + \varepsilon}{\pi^p}.$$

Clearly $f(X)$ is monic and since $\varepsilon \equiv 1 \bmod \pi^{p+1}$, the constant term is in $\mathbb{Z}[\zeta]$. But $p \mid \binom{p}{j}$ for $1 \leq j \leq p-1$, so the other coefficients are also in $\mathbb{Z}[\zeta]$. Since $f(0) = (-1+\varepsilon)/\pi^p \equiv 0 \pmod{\pi}$ and $f'(0) = p/\pi^{p-1} \not\equiv 0 \pmod{\pi}$, Hensel's Lemma implies that $f(X) = 0$ has a solution in the completion $\mathbb{Z}[\zeta]$. It follows that $\varepsilon^{1/p} \in \mathbb{Z}_p[\zeta]$ (alternatively, since $\varepsilon \equiv 1 \bmod \pi^{p+1}$, we find that $\exp((1/p)\log_p \varepsilon)$ converges, and its pth power is ε).

Suppose now that ε is not a pth power. Then $\mathbb{Q}(\zeta_p, \varepsilon^{1/p})\mathbb{Q}(\zeta_p)$ is a nontrivial abelian extension of degree p. Since $\varepsilon^{1/p} \in \mathbb{Q}_p(\zeta_p)$, the prime (π) splits completely; in particular, it does not ramify. The archimedean primes are all complex, so cannot ramify. Let $g(X) = X^p - \varepsilon$. The relative discriminant divides $N(g'(\varepsilon^{1/p})) = N(p\varepsilon^{(p-1)/p}) = (\pi)^{(p-1)p}$, where N is the relative ideal norm. Therefore the primes other than (π) are also unramified. The extension is therefore unramified everywhere. By class field theory, the degree of the maximal unramified abelian extension equals the class number. Consequently, p divides $h(\mathbb{Q}(\zeta_p))$, which contradicts the assumption that p is regular. Therefore ε is a pth power, and the proof is complete. □

We conclude this chapter with two results on quadratic fields.

Theorem 5.37 (Ankeny–Artin–Chowla). *Let* $p \equiv 1 \pmod 4$ *and let* h *and* $\varepsilon = (t + u\sqrt{p})/2 > 1$ *be the class number and fundamental unit for* $\mathbb{Q}(\sqrt{p})$. *Then*

$$\frac{u}{t} h \equiv B_{(p-1)/2} \pmod{p}.$$

PROOF. Until now we have been able to ignore the ambiguity in sign for the p-adic regulator. But now we are forced to choose signs.

From the classical class number formula for $\mathbb{Q}(\sqrt{p})$, we have (Exercise 4.6)

$$\varepsilon^{-2h} = \prod_{a=1}^{p-1} (1 - \zeta_p^a)^{\chi(a)},$$

where $\zeta_p = e^{2\pi i/p}$ and χ is the character for $\mathbb{Q}(\sqrt{p})$. We also have the Gauss sum $\tau(\chi) = \sum \chi(a)\zeta_p^a = \sqrt{p}$. Note that if we had chosen a different pth root of unity for ζ_p, we could have had $\tau(\chi) = -\sqrt{p}$, and also ε^{+2h} could have appeared on the left-hand side of the above formula. We also made the choice $\varepsilon > 1$. However, in the p-adics, there is no canonical way to choose ζ_p, $\sqrt{p}$, and ε. But we can choose them so that the above relation holds and also $\tau(\chi) = \sqrt{p}$: Fix an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$(note that since $\chi(a) = \pm 1$ or 0, everything is algebraic). Since the above is an equality in $\bar{\mathbb{Q}}$, it holds in $\mathbb{C}_p$. Now take p-adic logarithms:

$$\begin{aligned} 2h \log_p \varepsilon &= -\sum_{a=1}^{p-1} \chi(a) \log_p(1-\zeta_p^a) \\ &= -\frac{\tau(\chi)\sqrt{p}}{p} \sum \chi(a) \log_p(1-\zeta_p^a) \\ &= \sqrt{p}\left(1-\frac{\chi(p)}{p}\right)^{-1} L_p(1,\chi) \\ &= \sqrt{p} L_p(1,\chi). \end{aligned}$$

Therefore

$$\frac{2h \log_p \varepsilon}{\sqrt{p}} = L_p(1,\chi),$$

which is the class number formula with no ambiguity of sign. Clearly $\chi = \omega^{(p-1)/2}$ since χ is quadratic of conductor p. By Corollary 5.13,

$$\begin{aligned} L_p(1,\chi) &\equiv L_p\left(1-\frac{p-1}{2},\chi\right) \\ &= -(1-p^{(p-1)/2})\frac{B_{(p-1)/2}}{(p-1)/2} \\ &\equiv 2B_{(p-1)/2} \pmod{p}. \end{aligned}$$

But (cf. Exercise 5.15)

$$\begin{aligned} \log_p \varepsilon &= \log_p\left(\frac{t}{2}\right) + \log_p\left(1+\frac{u}{t}\sqrt{p}\right) \\ &\equiv 0 + \frac{u}{t}\sqrt{p} \pmod{p}. \end{aligned}$$

Therefore

$$\frac{hu}{t} \equiv B_{(p-1)/2} \pmod{\sqrt{p}},$$

but since both sides are rational, the congruence actually holds (mod p). This completes the proof. □

Since it can be shown that $h < \sqrt{p}$, this congruence actually determines h if $u \not\equiv 0 \pmod{p}$, or equivalently if p does not divide $B_{(p-1)/2}$ (note $p \nmid t$ since $\sqrt{p} \nmid \varepsilon$). For $p < 6{,}270{,}713$, no examples of $u \equiv 0$ are known (Beach, Williams and Zarnke [1]). However, if we assume $B_{(p-1)/2}$ to be random mod p (but see Exercise 5.9), then the number of $p \leq x$ with $p \mid B_{(p-1)/2}$ (and $p \equiv 1 \bmod 4$) should be

$$\sum_{\substack{p \leq x \\ p \equiv 1(4)}} \frac{1}{p} \sim \tfrac{1}{2} \log \log x;$$

so up to 6,270,713 one would expect only around one or two examples. Therefore the fact that none exist should not be considered decisive.

Proposition 5.38. *Let $m \geq 1$ be squarefree and assume 3 does not split completely in $\mathbb{Q}(\sqrt{-m})$. If 3 divides the class number of $\mathbb{Q}(\sqrt{3m})$ then 3 divides the class number of $\mathbb{Q}(\sqrt{-m})$ (we allow $3 \mid m$, in which case $\mathbb{Q}(\sqrt{3m}) = \mathbb{Q}(\sqrt{m/3})$).*

Remark. The result is also true if 3 splits, but our proof does not work. Later we shall prove the following more precise result, due to Scholz: Let r and s be the 3-ranks of the ideal class groups of $\mathbb{Q}(\sqrt{3m})$ and $\mathbb{Q}(\sqrt{-m})$, respectively. Then $r + 1 \geq s \geq r$. Whether $s = r$ or $r + 1$ depends partly on the units of $\mathbb{Q}(\sqrt{3m})$. That the units could have an effect can be seen in the present proof.

If $m = 3387$ then the class number of $\mathbb{Q}(\sqrt{3m}) = \mathbb{Q}(\sqrt{1129})$ is 9, but the class number of $\mathbb{Q}(\sqrt{-3387})$ is 12. Therefore we cannot replace 3 by 9 in the proposition.

Proof of Proposition 5.38. We may assume $m \geq 3$ since the proposition is vacuously true for $m < 3$. Let χ be the character for $\mathbb{Q}(\sqrt{-m})$. Then $\chi\omega = \chi\omega_3$ is the character for $\mathbb{Q}(\sqrt{3m})$. Let ε, h, and D be the fundamental unit, class number, and discriminant for $\mathbb{Q}(\sqrt{3m})$. As in the proof of Theorem 5.37, or by the class number formula since we need not worry about signs here, we obtain

$$\left(1 - \frac{\chi\omega(3)}{3}\right) \frac{2h \log_3 \varepsilon}{\sqrt{D}} = L_3(1, \chi\omega) \equiv L_3(0, \chi\omega) = -(1 - \chi(3))B_{1,\chi} \pmod{3}.$$

If $3 \nmid m$ then $3 \mid D$. As in the previous proof, or by Proposition 5.33, we have $|\log_3 \varepsilon/\sqrt{D}| \leq 1$. Also in this case $\chi\omega(3) = 0$, so the Euler factor disappears. If $3 \mid m$ then $3 \nmid D$, so $\chi\omega(3) \neq 0$. Therefore the Euler factor contributes a 3 to the denominator. But $|\log_3 \varepsilon| < 1$ so $\log_3 \varepsilon \equiv 0 \bmod 3$ (since $\mathbb{Q}_3(\varepsilon)/\mathbb{Q}_3$ is unramified, 3 generates the maximal ideal). This cancels the denominator. Consequently, in both cases the right-hand side is h times something integral.

If $3 \mid h$, we therefore find that 3 divides $(1 - \chi(3))B_{1,\chi}$ (note that if $\log_3 \varepsilon \equiv 0 \pmod{9}$ then we do not need $3 \mid h$). Since we have assumed 3 does not split in $\mathbb{Q}(\sqrt{-m})$, $\chi(3) \neq 1$. Therefore 3 divides $-B_{1,\chi} = h(\mathbb{Q}\sqrt{-m}))$. This completes the proof. □

The general philosophy to be learned from the proofs of Theorem 5.34 and Proposition 5.38 is that the p-adic L-functions at $s = 1$ contain information about units and class numbers for real fields, while at $s = 0$ they contain information about relative class numbers. Since we have congruences between these values, we can obtain results as above. However, the character ω appears, so it is helpful to have $\mathbb{Q}(\zeta_p)$ nearby, either explicitly, as in Theorem 5.34, or implicitly, as in Proposition 5.38. All this will be made more precise later, when we discuss reflection theorems.

Notes

For more on p-adic analysis, see Amice [1], Iwasawa [23], Koblitz [1], or Mahler [1]. A simple proof of Mahler's theorem is in Lang [4]. A version of the p-adic logarithm and exponential appeared in the work of Eisenstein [1] and of Kummer [3].

The construction of p-adic L-functions given above and the analogy with the values at positive integers is from Washington [2]. Other constructions can be found, for example, in Kubota-Leopoldt [1] (= the original construction), Amice-Fresnel [1], Coates [7], Fresnel [1], Iwasawa [18], [23], Serre [2], and Lang [4]. For other treatments of the positive integers, see Diamond [3], Hatada [1], Shiratani [5], and Koblitz [3].

p-adic L-functions have been constructed for all totally real fields by Barsky [4], Cassou-Noguès [4], and Deligne–Ribet [1]. See also Katz [7].

For p-adic L-functions in other settings, see Amice–Vélu [1], Cassou-Noguès [6], Coates–Wiles [4], Lichtenbaum [4], Manin [2], [3], [4], Manin–Višik [1], Višik [2], Mazur–Swinnerton-Dyer [1], and several of the papers of Katz.

For work on the zeros of p-adic L-functions, see Barsky [6], Sunseri [1], Wagstaff [2], and Washington [12].

For information about the behavior of p-adic L-functions at $s = 0$, see Federer–Gross [1], Gross [2], Ferrero-Greenberg [1], Lang [5], and Koblitz [4]. The last three give the relationship with the p-adic Γ-function (Morita [1]).

Theorem 5.16 is due to Kummer. For generalizations, see Adachi [1], R. Greenberg [3], and Kudo [3].

Theorem 5.17 has been generalized: for any $N > 2$ and for any proper subgroup H of $(\mathbb{Z}/N\mathbb{Z})^\times$, there are infinitely many irregular primes not in H. See Metsänkylä [9]. The probability arguments seem to have originated with Lehmer [1] and Siegel [1].

The calculation of $L_p(1, \chi)$ given above is partly from Washington [6], which is based on ideas of Kummer, and partly from a modification of Washington [4], which is based on the proof of Leopoldt [10] (see also Iwasawa [23]). Other methods may be found in Amice–Fresnel [1], Koblitz [3], [4], and Shiratani [3].

It is possible to determine the sign of $R_p/\sqrt{d}$ canonically: choose orderings in the determinants for R and $\sqrt{d}$ so that the archimedean $R/\sqrt{d}$ is positive. Then use the same orderings in the p-adic case. This gives the correct sign in the class number formula. See Amice–Fresnel [1].

Leopoldt's conjecture is from Leopoldt [9]. The reduction of the conjecture to the p-adic version of Baker's theorem (proved by Brumer) is due to Ax. For other work on the conjecture, see Bertrandias–Payan [1], Gillard [3], G. Gras [1], Serre [3], and Waldschmidt [1]. The last paper shows that the $\mathbb{Z}_p$-rank of the units is always at least half of the $\mathbb{Z}$-rank. There have been occasional papers claiming to prove Leopoldt's conjecture, but they all appear to be incorrect.

Some of the congruences of Ankeny–Artin–Chowla [1] were also discovered by Kiselev [1].

Exercises

5.1. Let K be a finite extension of $\mathbb{Q}_p$ of degree n. Show that there is a constant C depending on n, but not on K, such that $|\log_p x| \leq C$ for all $x \in K$.

5.2. Show that $\log_p \colon \mathbb{C}_p \to \mathbb{C}_p$ is surjective.

5.3. Let K be a number field and let S be a finite set of places of K including the archimedean places. An S-unit $\alpha \in K$ is an element satisfying $|\alpha|_v = 1$ for all places $v \notin S$. Show that if S is sufficiently large then Leopoldt's Conjecture is not true for S-units; namely $\mathbb{Z}_p$-rank $<$ $\mathbb{Z}$-rank $= \#(S) - 1$.

5.4. Show that

$$L_p(1, \chi) = \frac{1}{F} \sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a)\left(-\log_p\langle a\rangle + \sum_{j=1}^{\infty} \frac{B_j}{j}\left(\frac{-F}{a}\right)^j\right)$$

(there does not appear to be an easy way to transform this expression into that of Theorem 5.18).

5.5. Let K be an abelian field with X its group of Dirichlet characters. Let

$$\zeta_{K,p}(s) = \prod_{\chi \in X} L_p(s, \chi).$$

Show that $\zeta_{K,p}(1-n) = \zeta_K(1-n)\prod_\chi (1 - \chi(p)p^{n-1})$ if $n > 0, n \equiv 0 \pmod{p-1}$. Show that $\zeta_{K,p}(s)$ vanishes identically if K is complex.

5.6. Let i be even, $0 < i < p - 1$. Let u_i be the smallest integer $u \geq 0$ such that $B_{ip^u} \not\equiv 0 \pmod{p^{2u+1}}$. Show that $u_i = v_p(L_p(1, \omega^i))$. (*Hint*: Theorem 5.12.)

5.7. Let ε be a unit of $\mathbb{Q}(\zeta_p)$. Show that if ε is congruent to a rational integer modulo a sufficiently large power of p then ε is a pth power (this result will be refined in Chapter 8).

5.8. (Ankeny–Artin–Chowla). Let $m > 1$ be square-free, $m \equiv 1 \pmod 3$. Let $(t + u\sqrt{3m})/2$ *be* the fundamental unit for $\mathbb{Q}(\sqrt{3m})$. Show that $h(\mathbb{Q}(\sqrt{-m})) \equiv -(u/t)h(\mathbb{Q}(\sqrt{3m})) \pmod 3$. (*Be careful*: it is necessary to expand $\log_3$ to the third term.)

5.9. Let $p \equiv 3 \pmod 4$. Use the Brauer–Siegel theorem to show that $\log h(\mathbb{Q}(\sqrt{-p})) \sim \log\sqrt{p}$. Conclude that $p \nmid B_{(p+1)/2}$ for all sufficiently large p. Also, show that if $b \equiv B_{(p+1)/2} \pmod p$, $0 < b < p$, then $b/p \to 0$ as $p \to \infty$. Therefore $B_{(p+1)/2}$ is not "random" mod p. (Actually, $h < \sqrt{p}\log p$, hence $p \nmid B_{(p+1)/2}$, for all $p \equiv 3 \pmod 4$).

5.10. (J. C. Adams) Show that if $(p-1) \nmid i$ but $p^g \mid i$, then $p^g \mid B_i$.

5.11. (a) Show that $L_p(s, 1) = (1-(1/p))(s-1)^{-1} + a_0 + a_1(s-1) + \cdots$ where $a_i \in \mathbb{Z}_p$ for $i \geq 0$.
(b) (Carlitz) Show that if $p^g(p-1) \mid i$, then $p^g \mid (B_i + 1/p - 1)$.

5.12. Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$. The fundamental unit is $\alpha - 1$. Let $\phi_i : K \to \mathbb{C}_p$, $i = 1, 2, 3$, be the embeddings of K into $\mathbb{C}_p$. Show that for any i we may choose the embedding $\mathbb{C}_p \to \mathbb{C}$ so that ϕ_i is real and the other two embeddings are complex. We therefore have three possible regulators: R_1, R_2, R_3. Show that if $i \neq j$ then R_i/R_j is transcendental (use Theorem 5.29).

5.13. Use Theorem 4.12 to show that if K is a CM-field then the p-adic regulator is independent of the choice of labelings of the embeddings of K in $\mathbb{C}_p$.

5.14. Let $\pi = \zeta_p - 1$. Suppose ε is a unit of $\mathbb{Z}[\zeta_p]$ such that $\varepsilon \equiv a + b\pi^c \bmod \pi^{c+1}$ with $a, b \in \mathbb{Z}$, $p \nmid ab$, and $c \geq 2$. Show that if $c/(p-1) \notin \mathbb{Z}$ then $v_p(\log_p \varepsilon) = c/(p-1)$. In fact, show that $\log_p \varepsilon \equiv (b/a)\pi^c \bmod \pi^{c+1}$. (*Hint*: look at the proof of Lemma 5.35.)

5.15. (a) Show that if $r \in \mathbb{Q}$ then $\log_p r \equiv 0 \bmod p$.
(b) Let $\pi = \zeta_p - 1$, and let $\alpha \in \mathbb{Q}(\zeta_p)$. Show that $\alpha^{p-1} = rst$, where $r \in \mathbb{Q}$ (possibly divisible by p), s is a root of unity, and $t \equiv 1 \bmod \pi^2$.
(c) Let $\alpha \in \mathbb{Q}(\zeta_p)$. Show that $\log_p \alpha \equiv 0 \bmod \pi^2$.

5.16. (a) Let χ be an even Dirichlet character. Show that $L_p(s, \chi) = 0$ if and only if $\chi\omega^{-1}(p) = 1$.
(b) Show that there exist quadratic odd characters χ_1 and χ_2 with $\chi_1(p) = 1$ and $\chi_2(p) = -1$. (*Hint*: Quadratic reciprocity plus Dirichlet's theorem).
(c) The classical complex L-functions for even characters satisfy a functional equation of the form $f(s)L(s, \chi) = h_\chi(s)g(s)L(1-s, \bar{\chi})$, where f and g are analytic and independent of χ, while $h_\chi(s)$ may depend on χ but is nonvanishing. Show that there is no such functional equation for p-adic L-functions (of course, we do not allow f and g to be identically zero).

Chapter 6

Stickelberger's Theorem

The aim of this chapter is to give, for any abelian number field, elements of the group ring of the Galois group which annihilate the ideal class group. They will form the Stickelberger ideal. The proof involves factoring Gauss sums as products of prime ideals, and since Gauss sums generate principal ideals, we obtain relations in the ideal class group. As an application, we prove Herbrand's theorem which relates the nontriviality of certain parts of the ideal class group of $\mathbb{Q}(\zeta_p)$ to p dividing corresponding Bernoulli numbers. Then we calculate the index of the Stickelberger ideal in the group ring for $\mathbb{Q}(\zeta_{p^n})$ and find it equals the relative class number. Finally, we prove a result, essentially due to Eichler, on the first case of Fermat's Last theorem. In the next chapter we shall use Stickelberger elements to give Iwasawa's construction of p-adic L-functions.

§6.1 Gauss Sums

In order to prove Stickelberger's theorem, we need to study Gauss sums, which are also interesting in their own right. The Gauss sums used here are not the same as those used earlier, but there are many similarities.

Let $\mathbb{F} = \mathbb{F}_q$ be the finite field with q elements, q being a power of the prime p. Let ζ_p be a fixed primitive pth root of unity and let T be the trace from $\mathbb{F}$ to $\mathbb{Z}/p\mathbb{Z}$. Define

$$\psi: \mathbb{F} \to \mathbb{C}^\times, \qquad \psi(x) = \zeta_p^{T(x)},$$

which is easily seen to be a well-defined, nontrivial (T is surjective) character of the additive group of $\mathbb{F}$. Let

$$\chi: \mathbb{F}^\times \to \mathbb{C}^\times$$

be a multiplicative character of $\mathbb{F}^\times$. We extend χ to all of $\mathbb{F}$ by setting $\chi(0) = 0$ (even if χ is the trivial character). Note that χ^{q-1} is the trivial character, so the order of χ is prime to p. If $q \neq p$, such characters are not the Dirichlet characters studied earlier. The concept of conductor will not enter into the present discussion.

Define the Gauss sum

$$g(\chi) = -\sum_{a \in \mathbb{F}} \chi(a)\psi(a)$$

If χ has order m, then $g(\chi) \in \mathbb{Q}(\zeta_{mp})$. A quick calculation shows that $g(1) = 1$.

Lemma 6.1. (a) $g(\bar{\chi}) = \chi(-1)\overline{g(\chi)}$;

(b) *if* $\chi \neq 1$, $g(\chi)g(\bar{\chi}) = \chi(-1)q$;
(c) *if* $\chi \neq 1$, $g(\chi)\overline{g(\chi)} = q$.

Proof. (a) is straightforward. (b) follows from (a) and (c). For (c),

$$\begin{aligned} g(\chi)\overline{g(\chi)} &= \sum_{a,b \neq 0} \chi(ab^{-1})\psi(a-b) \\ &= \sum_{b,c \neq 0} \chi(c)\psi(bc-b) \quad (\textit{let } c = ab^{-1}) \\ &= \sum_{b \neq 0} \chi(1)\psi(0) + \sum_{c \neq 0,1} \chi(c) \sum_{b \neq 0} \psi(b(c-1)) \\ &= (q-1) + \sum_{c \neq 0,1} \chi(c)(-1) = q. \end{aligned}$$

This completes the proof. □

If χ_1, χ_2 are two multiplicative characters, we define the Jacobi sum

$$J(\chi_1, \chi_2) = -\sum_{a \in \mathbb{F}} \chi_1(a)\chi_2(1-a).$$

More generally, we have

$$J(\chi_1, \ldots, \chi_n) = -\sum_{a_1 + \cdots + a_n = 1} \chi_1(a_1) \cdots \chi_n(a_n),$$

but we do not need this for $n > 2$. Note that if χ_1 and χ_2 have orders dividing m then $J(\chi_1, \chi_2)$ is an algebraic integer in $\mathbb{Q}(\zeta_m)$.

Lemma 6.2. (a) $J(1, 1) = 2 - q$;
(b) $J(1, \chi) = J(\chi, 1) = 1$ *if* $\chi \neq 1$;
(c) $J(\chi, \bar{\chi}) = \chi(-1)$ *if* $\chi \neq 1$;
(d) $J(\chi_1, \chi_2) = g(\chi_1)g(\chi_2)/g(\chi_1\chi_2)$ *if* $\chi_1 \neq 1$, $\chi_2 \neq 1$, *and* $\chi_1\chi_2 \neq 1$.

Proof. (a) and (b) are easy. To prove (c) and (d), we compute

$$\begin{aligned} g(\chi_1)g(\chi_2) &= \sum_{a,b} \chi_1(a)\chi_2(b)\psi(a+b) \\ &= \sum_{a,b} \chi_1(a)\chi_2(b-a)\psi(b) \\ &= \sum_{\substack{a,b \\ b\neq 0}} \chi_1(a)\chi_2(b-a)\psi(b) + \sum_a \chi_1(a)\chi_2(-a). \end{aligned}$$

If $\chi_1\chi_2 \neq 1$, then the second sum vanishes. If $\chi_1\chi_2 = 1$, then it equals $\chi_1(-1)(q-1)$. The first sum equals (let $a = bc$)

$$\sum_{\substack{b,c \\ b\neq 0}} \chi_1(b)\chi_2(b)\chi_1(c)\chi_2(1-c)\psi(b) = g(\chi_1\chi_2)J(\chi_1, \chi_2).$$

If $\chi_1\chi_2 \neq 1$, we obtain (d). If $\chi_1\chi_2 = 1$, use Lemma 6.1(b), along with $g(1) = 1$, to obtain (c). This completes the proof. □

Corollary 6.3. *If χ_1, χ_2 are characters of orders dividing m, then*

$$\frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$$

is an algebraic integer in $\mathbb{Q}(\zeta_m)$.

Proof. If χ_1, χ_2, and $\chi_1\chi_2$ are nontrivial, use the above result. The remaining cases are quickly checked individually. □

The significance of this result is twofold: not only is the expression integral, it also eliminates ζ_p. This will be useful later.

Let m be an integer with $(m, p) = 1$. Then the fields $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_p)$ are disjoint. Let $(b, m) = 1$. We may define $\sigma_b \in \mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_p)/\mathbb{Q})$ by

$$\sigma_b \colon \zeta_p \mapsto \zeta_p, \zeta_m \mapsto \zeta_m^b.$$

(perhaps it would be better to use double indices and call this $\sigma_{1,b}$, but usually ζ_p will drop out early, leaving only ζ_m).

Lemma 6.4. *Assume χ^m is trivial. Then*

$$\frac{g(\chi)^b}{g(\chi)^{\sigma_b}} = g(\chi)^{b-\sigma_b} \in \mathbb{Q}(\zeta_m),$$

and $g(\chi)^m \in \mathbb{Q}(\zeta_m)$.

PROOF. The second follows from the first if we let $b = 1 + m$. For the first, we have

$$g(\chi)^{\sigma_b} = -\sum \chi(a)^b \psi(a) = g(\chi^b).$$

Let $\tau \in \operatorname{Gal}(\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m))$, so $\tau\colon \zeta_m \mapsto \zeta_m$, $\zeta_p \mapsto \zeta_p^c$ for some c, $(c, p) = 1$. Then

$$\begin{aligned} g(\chi)^\tau &= -\sum \chi(a)\psi(ca) \\ &= -\chi(c)^{-1} \sum \chi(a)\psi(a) = \chi(c)^{-1} g(\chi), \end{aligned}$$

and similarly

$$g(\chi^b)^\tau = \chi(c)^{-b} g(\chi^b).$$

Therefore τ fixes $g(\chi)^{b-\sigma_b}$. The result follows. □

Lemma 6.5. $g(\chi^p) = g(\chi)$.

PROOF. Since $a \mapsto a^p$ is an automorphism over $\mathbb{Z}/p\mathbb{Z}$, $T(a) = T(a^p)$, and a^p yields a permutation of $\mathbb{F}$. Therefore

$$\begin{aligned} g(\chi^p) &= -\sum \chi(a^p)\zeta_p^{T(a)} \\ &= -\sum \chi(a^p)\zeta_p^{T(a^p)} = g(\chi). \end{aligned}$$ □

This completes our list of basic properties of Gauss sums. We now digress to give an application to the Fermat curve.

We wish to count the number of solutions of

$$X^d + Y^d = 1, \quad \text{with } X, Y \in \mathbb{F}_q.$$

As is usually the case, it is more natural to count points in projective space. That is, we consider solutions, except (0, 0, 0), of

$$X^d + Y^d = Z^d,$$

and identify two solutions if they differ by a scalar multiple. If $Z \neq 0$, we may identify (X, Y, Z) with $(X/Z, Y/Z, 1)$ and obtain a solution of the original equation. But if $Z = 0$, we obtain the "points at infinity" $(X/0 = \infty)$, which correspond to solutions of $X^d + Y^d = 0$. Since we do not count $(0, 0, 0)$, we must have $Y \neq 0$, so any solution $(X, Y, 0)$ may be put in the form $(X/Y, 1, 0)$. The number of points at infinity is exactly the number of solutions in $\mathbb{F}_q$ of $X^d = -1$.

Despite all this, we shall start by counting the solutions of $X^d + Y^d = 1$, and make the correction later. We first assume d divides $q - 1$. Since $\mathbb{F}_q^\times$ is cyclic of order $q - 1$, there exists a character χ of $\mathbb{F}_q^\times$ of order exactly d. The cyclicity implies that $\chi(u) = 1$ if and only if $u \in \mathbb{F}_q^\times$ is a dth power. For $u \in \mathbb{F}_q^\times$, let $N_d(u)$ be the number of solutions in $\mathbb{F}_q$ of $X^d = u$, so

$$N_d(u) = \begin{cases} 1, & u = 0 \\ 0, & u \neq 0, u \neq d\text{th power} \\ d, & u \neq 0, u = d\text{th power (since } d \mid q - 1). \end{cases}$$

It follows easily that

$$N_d(u) = \sum_{a=1}^{d} \chi^a(u) \quad \text{if } u \neq 0.$$

Therefore, the number of solutions of $X^d + Y^d = 1$ is

$$\sum_{\substack{u+v=1\\ uv\neq 0}} N_d(u)N_d(v) + 2d$$

(the second term corresponds to $X = 0$ or $Y = 0$)

$$= 2d + \sum_{u\neq 0,1} \sum_{a=1}^{d} \sum_{b=1}^{d} \chi^a(u)\chi^b(1-u)$$

$$= 2d - \sum_{a=1}^{d} \sum_{b=1}^{d} J(\chi^a, \chi^b).$$

From Lemma 6.2 we see that the term $a = b = d$ contributes $2 - q$; the terms with either $a = d$ or $b = d$, but not both, contribute a total of $2(d-1)$; those with $a + b = d$ yield $\sum_{a=1}^{d-1} \chi^a(-1) = N_d(-1) - 1$; and the remaining terms can be expressed in terms of Gauss sums via Lemma 6.2(d). Using the fact that $N_d(-1)$ is the number of points at infinity, we find that the number of solutions of $X^d + Y^d = Z^d$ in projective space is

$$q + 1 - \sum_{\substack{a,b=1\\ a+b\neq d}}^{d-1} J(\chi^a, \chi^b).$$

Since $|g(\chi)| = \sqrt{q}$ if $\chi \neq 1$, we have, using Lemma 6.2(d), that

$$\left|\sum J(\chi^a, \chi^b)\right| \leq (d-1)(d-2)\sqrt{q}.$$

If $\overline{N}$ denotes the number of solutions,

$$|\overline{N} - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

This is a special case of a more general result which states that for a curve of genus g we have

$$|\overline{N} - (q+1)| \leq 2g\sqrt{q}.$$

Note that $q + 1$ is the number of points on a line $aX + bY = cZ$, so the number of points on a curve is approximately the same as for a line, the possible error being bounded in terms of the genus.

Now assume d is arbitrary, so we do not necessarily have $d \mid q - 1$. Let $e = (d, q-1)$. Then $N_d(u) = N_e(u)$, so

$$\begin{aligned}\overline{N} &= \#\{X^d + Y^d = Z^d \mid (X, Y, Z) \neq (0,0,0)\}/(q-1)\\ &= \sum_{u+v=w} N_d(u)N_d(v)N_d(w)/(q-1)\\ &= \#\{X^e + Y^e = Z^e \mid (X, Y, Z) \neq (0,0,0)\}/(q-1).\end{aligned}$$

Since e divides $q - 1$, we have

$$|\bar{N} - (q + 1)| \le (e - 1)(e - 2)\sqrt{q} \le (d - 1)(d - 2)\sqrt{q},$$

so we have proved the following.

Proposition 6.6. *Let $\bar{N}$ denote the number of projective space solutions of*

$$X^d + Y^d = Z^d$$

in $\mathbb{F}_q$. Then

$$|\bar{N} - (q + 1)| \le (d - 1)(d - 2)\sqrt{q}. \qquad \square$$

Corollary 6.7. *For any given d, $X^d + Y^d \equiv 1 \pmod{p}$ has solutions with $XY \not\equiv 0 \pmod{p}$, for all sufficiently large p.*

Proof. From the above, the number of points at infinity is $N_d(-1)$ (or $N_e(-1)$), which is at most d. The number of solutions with $X \equiv 0$ or $Y \equiv 0$ is at most $2d$. Therefore we have a nontrivial solution as soon as $\bar{N} > 3d$. Since $\bar{N} - p = 0(\sqrt{p})$, the result follows. □

This corollary shows that it would be difficult to prove Fermat's Last Theorem using only congruences.

To finish this digression we show that Proposition 6.6 is essentially the Riemann hypothesis for the Fermat curve. Fix d and p and let $\bar{N}_n$ be the number of solutions of $X^d + Y^d = Z^d$ in projective space over $\mathbb{F}_{p^n}$. The zeta function $\zeta_d(s)$ of the curve may be defined as follows:

Define $Z(T)$ by

$$\frac{Z'(T)}{Z(T)} = \sum_{n=1}^{\infty} \bar{N}_n T^{n-1}, \qquad Z(0) = 1.$$

Then

$$\zeta_d(s) = Z(p^{-s}).$$

This function satisfies many properties similar to those for Dedekind zeta functions: for example, there is an Euler product, and also there is a functional equation relating the values at s and $1 - s$. It can be shown that $Z(T)$ is a rational function of the form

$$Z(T) = \frac{P(T)}{(1 - T)(1 - pT)}, \quad \text{where } P(T) \in \mathbb{Z}[T],\ P(0) = 1.$$

(for further properties and proofs, see Weil [6] or Eichler [3]).

Writing $P(T) = \prod_i (1 - \alpha_i T)$, we see that

$$\frac{Z'(T)}{Z(T)} = \sum_{n=1}^{\infty} \left(1 + p^n - \sum_i \alpha_i^n\right) T^{n-1},$$

so

$$\bar{N}_n = 1 + p^n - \sum_i \alpha_i^n.$$

To answer the question that arises when one compares this with a previous formula, yes, the α_i's are Jacobi sums, but we shall not prove this here. It follows easily from the Davenport–Hasse relations (see the Exercises).

From Proposition 6.6 we have

$$\left|\sum_i \alpha_i^n\right| \le (d-1)(d-2)p^{n/2}.$$

Lemma 6.8.

$$\limsup_{n\to\infty}\left|\sum_i \alpha_i^n\right|^{1/n} = \operatorname*{Max}_i |\alpha_i|.$$

Proof. The only problem arises when two α's have the same absolute value, in which case a straightforward proof would have to show that "cancellation" does not decrease the lim sup. However, there is the following classical trick. Consider the complex function

$$f(z) = \sum_i \frac{1}{1-\alpha_i z} = \sum_{n=0}^{\infty}\left(\sum_i \alpha_i^n\right)z^n.$$

The radius of convergence of the power series is the distance to the nearest singularity, namely $1/\operatorname{Max}|\alpha_i|$. But it is also the reciprocal of lim sup$|\sum \alpha_i^n|^{1/n}$. The result follows. □

We now have $|\alpha_i| \le \sqrt{p}$ for each i. Returning to $\zeta_d(s)$, we see that $\zeta_d(s) = 0 \Leftrightarrow p^s = \alpha_i$ for some i. Therefore $\operatorname{Re}(s) \le \frac{1}{2}$. But the functional equation for $\zeta_d(s)$ implies that if $\zeta_d(s) = 0$ then $\zeta_d(1-s) = 0$. Therefore $\operatorname{Re}(s) = \frac{1}{2}$ for each zero s. This is the Riemann hypothesis for the Fermat curve.

All of the above is part of a much more general situation, which applies not only to cuves but also to higher dimensional varieties (the Weil conjectures, now Deligne's theorem). The reader is strongly urged to read the classic papers of Weil ([1], [2]), where this is discussed and where additional results on Gauss and Jacobi sums are proved.

§6.2 Stickelberger's Theorem

Let $M/\mathbb{Q}$ be a finite abelian extension, so $M \subseteq \mathbb{Q}(\zeta_m)$ for some m (by the Kronecker–Weber theorem, proved in Chapter 14). We assume m is minimal. $G = \operatorname{Gal}(M/\mathbb{Q})$ may be regarded as a quotient of $(\mathbb{Z}/m\mathbb{Z})^\times$. We let σ_a, $(a, m) = 1$, denote both the element of $\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and its restriction to M. Let $\{x\}$ denote the fractional part of the real number x; so $x - \{x\} \in \mathbb{Z}$ and $0 \le \{x\} < 1$. Define the *Stickelberger element*

$$\theta = \theta(M) = \sum_{\substack{a \pmod m\\ (a,m)=1}} \left\{\frac{a}{m}\right\}\sigma_a^{-1} \in \mathbb{Q}[G].$$

The *Stickelberger ideal* $I(M)$ is defined to be $\mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$, in other words, those $\mathbb{Z}[G]$-multiples of θ which have integral coefficients.

Lemma 6.9. *Suppose $M = \mathbb{Q}(\zeta_m)$. Let I' be the ideal of $\mathbb{Z}[G]$ generated by elements of the form $c - \sigma_c$, with $(c, m) = 1$. Let $\beta \in \mathbb{Z}[G]$. Then*

$$\beta\theta \in \mathbb{Z}[G] \Leftrightarrow \beta \in I'.$$

Therefore $I = I'\theta$.

Proof. Since

$$(c - \sigma_c)\theta = \sum_a \left(c\left\{\frac{a}{m}\right\} - \left\{\frac{ac}{m}\right\}\right)\sigma_a^{-1} \in \mathbb{Z}[G],$$

we have "$\Leftarrow$". To prove the converse, first note that $m = (1 + m) - \sigma_{1+m} \in I'$. Suppose $(\sum_a x_a\sigma_a)\theta \in \mathbb{Z}[G]$, with $x_a \in \mathbb{Z}$. A short calculation shows that

$$\left(\sum_a x_a\sigma_a\right)\left(\sum_c \left\{\frac{c}{m}\right\}\sigma_c^{-1}\right) = \sum_b \left(\sum_a x_a\left\{\frac{ab}{m}\right\}\right)\sigma_b^{-1}.$$

Looking at the coefficient of σ_1^{-1}, we find that m divides $\sum x_a a$. Since $m \in I'$, so is $\sum x_a a$. Therefore

$$\sum x_a\sigma_a = \sum x_a(\sigma_a - a) + \sum x_a a \in I'.$$

This completes the proof. □

This result is not true in general if M is a proper subfield of $\mathbb{Q}(\zeta_m)$. The problem is that $\sigma_b = 1$ for several b, so the "coefficient of σ_1^{-1}" involves a sum over various values of b. For example, let $M = \mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{11}) \subset \mathbb{Q}(\zeta_{12})$. Then $\sigma_1 = \sigma_{11} = 1$, while $\sigma_5 = \sigma_7 = \sigma$, say. We have $\theta(M) = 1 + \sigma \in \mathbb{Z}[G]$, so $1 \cdot \theta \in \mathbb{Z}[G]$. But I' is generated by $\{5 - \sigma, 7 - \sigma, 11 - 1\}$, therefore by $\{2, 1 + \sigma\}$. In particular, $1 \notin I'$.

If $x = \sum x_\sigma\sigma \in \mathbb{Z}[G]$ then x acts on ideals and ideal classes in the natural way: $A^x = \prod_\sigma (A^\sigma)^{x_\sigma}$.

Theorem 6.10 (Stickelberger's Theorem). *Let A be a fractional ideal of M, let $\beta \in \mathbb{Z}[G]$, and suppose $\beta\theta \in \mathbb{Z}[G]$. Then $A^{\beta\theta}$ is principal. Therefore, the Stickelberger ideal annihilates the ideal class group of M.*

Before starting the proof, we give two examples.

(a) Suppose M is real. Then $\sigma_a = \sigma_{-a}$ and $\langle a/m\rangle + \langle -a/m\rangle = 1$, so

$$\theta(M) = \frac{1}{2}\sum_{a(\text{mod } m)} \sigma_a = \frac{\phi(m)}{2 \deg M}\,\text{Norm}_{M/\mathbb{Q}}.$$

In this case we find that the norm, or some multiple of it, annihilates the ideal class group. This of course is already obvious, since $\mathbb{Q}$ has class number one. We therefore can obtain nontrivial results only if we look at imaginary fields.

(b) Suppose $M = \mathbb{Q}(\sqrt{-m})$ is imaginary quadratic. $\mathrm{Gal}(M/\mathbb{Q}) = \{1, \sigma\}$, where σ is complex conjugation. Since $A^{1+\sigma}$ is an ideal of $\mathbb{Q}$, hence principal, σ acts by inversion on the ideal class group. Let $\beta = m$. Then $\beta\theta = \sum a\sigma_a^{-1} \in \mathbb{Z}[G]$, and in the ideal class group $\beta\theta$ acts as $\sum a\chi(a)$, where χ is the quadratic character for M. We find that $\sum a\chi(a) = mB_{1,\chi}$ annihilates the ideal class group. Of course, the class number formula implies that this number is just $-mh$ (if $m > 4$), so what we have is a weak form of the analytic class number formula; however, it will be proved algebraically.

More generally, let F be any totally real number field and M/F a finite abelian extension. Let $G = \mathrm{Gal}(M/F)$. Via the Artin map $A \mapsto \sigma_A \in G$, one can define partial zeta functions for $\sigma \in G$:

$$\zeta_F(\sigma, s) = \sum_{\sigma_A = \sigma} \frac{1}{NA^s} \qquad (\mathrm{Re}(s) > 1).$$

These may be meromorphically continued to the whole complex plane, and the values $\zeta_F(\sigma, -n)$ are rational numbers for $n \geq 0$. Define

$$\theta_n(M/F) = \sum_{\sigma \in G} \zeta_F(\sigma, -n)\sigma^{-1},$$

and let $I_n(M/F)$ be the ideal generated by elements of the form

$$(NA^{n+1} - \sigma_A)\theta_n(M/F),$$

where A ranges over a set of integral ideals of F not divisible by a certain finite set of prime ideals. Then $I_n(M/F)$ should annihilate some natural object, perhaps a K-group. For example, $I_1(M/\mathbb{Q})$ annihilates $K_2\mathcal{O}_M$, except possibly for the 2-part, where $\mathcal{O}_m$ is the ring of integers of M. When $M = \mathbb{Q}(\zeta_m)$ and $F = \mathbb{Q}$, we have

$$\zeta(\sigma_a, s) = \sum_{\substack{b \equiv a(m) \\ b > 0}} \frac{1}{b^s},$$

which is essentially a Hurwitz zeta function. If $n = 0$, we have

$$\theta_0\left(\frac{M}{\mathbb{Q}}\right) = \sum_{c (\mathrm{mod}\, m)} \left(\frac{1}{2} - \left\{\frac{c}{m}\right\}\right)\sigma_c^{-1},$$

which differs from θ by half the norm (in fact, we shall need θ_0 later). Since $K_0\mathcal{O}_m$ is essentially the ideal class group of M, the above may be regarded as an appropriate generalization of Stickelberger's Theorem. For details, see Coates [7].

We are now ready to start the proof of Stickelberger's theorem. The major step will be the factorization of certain Gauss sums. Let p be a prime and let $q = p^f$ be a power of p. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\zeta_{q-1})$ lying above p. Since $\mathbb{Z}[\zeta_{q-1}]$ mod $\mathfrak{p}$ is the finite field with q elements ($f=$ residue class degree by Theorem 2.13), and since the $(q-1)$st roots of unity are distinct mod $\mathfrak{p}$, there is an isomorphism

$$\omega = \omega_{\mathfrak{p}}\colon \mathbb{F}_q^\times \to (q-1)\text{st roots of } 1$$

satisfying

$$\omega(a) \bmod \mathfrak{p} = a \in \mathbb{F}_q^\times .$$

This ω is essentially a generalization of the ω of the previous chapter. Let $\tilde{\mathfrak{P}}$ be the prime of $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ lying above $\mathfrak{p}$. For $\alpha \in \mathbb{Z}$, let $s(\alpha) = v_{\tilde{\mathfrak{P}}}(g(\omega^{-\alpha}))$, where $v_{\tilde{\mathfrak{P}}}$ is the $\tilde{\mathfrak{P}}$-adic valuation. Clearly $s(\alpha)$ depends only on $\alpha \pmod{q-1}$.

Lemma 6.11. (a) $s(0) = 0$;
(b) $0 \le s(\alpha + \beta) \le s(\alpha) + s(\beta)$;
(c) $s(\alpha + \beta) \equiv s(\alpha) + s(\beta) \pmod{p-1}$;
(d) $s(p\alpha) = s(\alpha)$;
(e) $\sum_{\alpha=1}^{q-2} s(\alpha) = (q-2)(f)(p-1)/2$.

PROOF. (a) is obvious; (b) and (d) follow from Corollary 6.3 and Lemma 6.5, respectively. Since $\tilde{\mathfrak{P}}^{p-1} = \mathfrak{p}$, the values of $v_{\tilde{\mathfrak{P}}}$ on $\mathbb{Q}(\zeta_{q-1})$ are divisible by $p-1$. Therefore (c) also follows from Corollary 6.3. Since $g(\omega^{-\alpha})g(\omega^{\alpha}) = \pm q = \pm p^f$, we have $s(\alpha) + s(q-1-\alpha) = v_{\tilde{\mathfrak{P}}}(p^f) = (p-1)f$. Pairing up the terms in the sum (the term for $\alpha = (q-1)/2$ pairs with itself), we obtain (e). This completes the proof. □

Lemma 6.12. $s(\alpha) > 0$ *if* $\alpha \not\equiv 0 \pmod{q-1}$, *and* $s(1) = 1$.

PROOF. Since $\pi = \zeta_p - 1 \in \tilde{\mathfrak{P}}$,

$$g(\omega^{-\alpha}) = -\sum \omega^{-\alpha}(a)\zeta_p^{T(a)} \equiv -\sum \omega^{-\alpha}(a) \equiv 0 \pmod{\tilde{\mathfrak{P}}}.$$

Therefore $s(\alpha) > 0$. Also,

$$\begin{aligned} g(\omega^{-1}) &= -\sum \omega^{-1}(a)\zeta_p^{T(a)} \\ &= -\sum \omega^{-1}(a)(1+\pi)^{T(a)} \equiv -\sum \omega^{-1}(a)(1+\pi T(a)) \pmod{\tilde{\mathfrak{P}}^2}. \\ &\equiv -\pi \sum \omega^{-1}(a)T(a). \end{aligned}$$

Regarding $\mathbb{F}_q$ as $\mathbb{Z}[\zeta_{q-1}]$ mod $\mathfrak{p}$, we have

$$T(a) = a + a^p + \cdots + a^{p^{f-1}} \pmod{\mathfrak{p}}$$

(since $a \mapsto a^p$ generates the Galois group mod $\mathfrak{p}$), and

$$\sum \omega^{-1}(a)T(a) \equiv \sum_{\substack{a \not\equiv 0 \\ a \bmod \mathfrak{p}}} a^{-1}(a + a^p + \cdots + a^{p^{f-1}}) \pmod{\mathfrak{p}}.$$

If $0 < b < f$, then $\sum_{a \neq 0} a^{p^b - 1} \equiv 0 \pmod{\mathfrak{p}}$, so the sum reduces to $\sum_{a \neq 0} 1 = q - 1 \equiv -1$. Therefore

$$g(\omega^{-1}) \equiv \pi \pmod{\tilde{\mathfrak{P}}^2},$$

hence $s(1) = v_{\tilde{\mathfrak{P}}}(\pi) = 1$ (since $\mathbb{Q}(\zeta_{q-1}, \zeta_p)/\mathbb{Q}(\zeta_p)$ is unramified at p). This completes the proof. □

Proposition 6.13. *Let* $0 \leq \alpha < q - 1$ *and let* $\alpha = a_0 + a_1 p + \cdots + a_{f-1} p^{f-1}$, $0 \leq a_i \leq p - 1$, *be the standard p-adic expansion of* α. *Then*

$$s(\alpha) = a_0 + a_1 + \cdots + a_{f-1}.$$

PROOF. From Lemma 6.11(a), (b), (c) and Lemma 6.12 we immediately have $s(\alpha) = \alpha$ for $0 \leq \alpha \leq p - 2$. If $q = p$, we are done. Otherwise, $s(p-1) > 0$ and we similarly obtain $s(p-1) = p - 1$. Lemma 6.11(b) and (d) imply that $s(\alpha) \leq a_0 + \cdots + a_{f-1}$. When α runs through the integers from 0 to $q - 1$, inclusive, each coefficient of the p-adic expansion takes on each of the values from 0 to $p - 1$ exactly p^{f-1} times, so

$$\sum_{\alpha=0}^{q-1} (a_0 + \cdots + a_{f-1}) = \frac{p(p-1)}{2} (f) p^{f-1} = \frac{p-1}{2} fq.$$

If we omit $\alpha = q - 1 = (p-1) + \cdots + (p-1)p^{f-1}$, we obtain

$$\sum_{\alpha=0}^{q-2} (a_0 + \cdots + a_{f-1}) = \frac{p-1}{2} fq - (p-1)f = \sum_{\alpha=0}^{q-2} s(\alpha),$$

by Lemma 6.11(e). The result follows. □

Remark. Let $\pi = \zeta_p - 1$ and $0 \leq \alpha < q - 1$, as above. Then

$$g(\omega^{-\alpha}) \equiv \frac{\pi^{a_0 + \cdots + a_{f-1}}}{(a_0!) \cdots (a_{f-1}!)} \pmod{\pi^{a_0 + \cdots + a_{f-1} + 1}}.$$

(see Lang [4], [5]). In Lemma 6.12 we verified a special case of this formula. The general argument follows a similar line, but involves a rather delicate analysis of binomial coefficients.

Now fix a positive integer m. Let p be a prime, $(p, m) = 1$, and let f be the order of $p \pmod{m}$, so m divides $p^f - 1 = q - 1$. Fix a prime $\mathfrak{p}_0$ of $\mathbb{Q}(\zeta_m)$ lying above p; let $\tilde{\mathfrak{p}}_0$ be the prime of $\mathbb{Q}(\zeta_m, \zeta_p)$ above $\mathfrak{p}_0$, so $\tilde{\mathfrak{p}}_0^{p-1} = \mathfrak{p}_0$; let $\mathfrak{P}_0$ be a prime of $\mathbb{Q}(\zeta_{q-1})$ lying above $\mathfrak{p}_0$; and let $\tilde{\mathfrak{P}}_0$ be the prime of $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ lying above $\mathfrak{P}_0$ (and $\tilde{\mathfrak{p}}_0$). Let $\omega = \omega_{\mathfrak{P}_0}$ be as above and let $\chi = \omega^{-d}$, where $d = (q-1)/m$. Then $\chi^m = 1$, so $g(\chi) \in \mathbb{Q}(\zeta_m, \zeta_p)$. Since $g(\chi)\overline{g(\chi)} = q = p^f$, the factorization of $g(\chi)$ involves only primes of $\mathbb{Q}(\zeta_m, \zeta_p)$ above p, that is, the conjugates over $\mathbb{Q}$ of $\tilde{\mathfrak{p}}_0$. Let $(a, m) = 1$ and let $\sigma_a \in \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ be the corresponding element of the Galois group. For each such a, fix an extension of σ_a to $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ such that $\zeta_p^{\sigma_a} = \zeta_p$.

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_{q-1}, \zeta_p)\ \ \tilde{\mathscr{P}}_0 \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_{q-1})\ \ \mathscr{P}_0 \arrow[dr, dash] & & \mathbb{Q}(\zeta_m, \zeta_p)\ \ \tilde{\wp}_0 \arrow[dl, dash] \\
& \mathbb{Q}(\zeta_m)\ \ \wp_0 \arrow[d, dash] & \\
& \mathbb{Q}\ \ p &
\end{tikzcd}$$

The decomposition group for p in $(\mathbb{Z}/m\mathbb{Z})^\times$ is generated by $p \pmod{m}$ (see the discussion after Theorem 2.13). Let R denote a set of representatives for $(\mathbb{Z}/m\mathbb{Z})^\times$ modulo this decomposition group. Then $\{\wp_0^{\sigma_a^{-1}} \mid a \in R\}$ is the set of conjugates of $\wp_0$. Since $\tilde{\wp}_0$ is the unique prime above $\wp_0$, all conjugates of $\tilde{\wp}_0$ have the form $\tilde{\wp}_0^{\sigma_a^{-1}}$. Let $\tilde{\wp} = \tilde{\wp}_0^{\sigma_a\ 1}$ be one of them. Then

$$v_{\tilde{\wp}}(g(\chi)) = v_{\tilde{\wp}_0}(g(\chi)^{\sigma_a}) = v_{\tilde{\wp}_0}(g(\chi^a)) = v_{\tilde{\mathscr{P}}_0}(g(\chi^a)) = s(ad)$$

($v_{\tilde{\wp}_0} = v_{\tilde{\mathscr{P}}_0}$ since $\tilde{\mathscr{P}}_0/\tilde{\wp}_0$ is unramified). Therefore

$$(g(\chi)) = \wp_0^{\sum_R s(ad)\sigma_a^{-1}}.$$

Lemma 6.14. *Let* $0 \le h < q - 1$. *Then*

$$s(h) = (p-1)\sum_{i=0}^{f-1}\left\{\frac{p^i h}{q-1}\right\}.$$

Proof. Let $h = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$. Then

$$p^i h \equiv a_0 p^i + a_1 p^{i+1} + \cdots + a_{f-1}p^{i-1} \pmod{q-1}.$$

It follows that

$$\left\{\frac{p^i h}{q-1}\right\} = \frac{1}{q-1}(a_0 p^i + \cdots + a_{f-1}p^{i-1}).$$

Summing over i, we obtain the result. □

We now have $s(ad) = (p-1)\sum_{i=0}^{f-1}\{p^i a/m\}$, so

$$\sum_R s(ad)\sigma_a^{-1} = (p-1)\sum_{i=0}^{f-1}\sum_R\left\{\frac{p^i a}{m}\right\}\sigma_a^{-1}.$$

Since $\tilde{\wp}_0^{p-1} = \wp_0$ and since $\sigma_{p^i}(\wp_0) = \wp_0$ (definition of decomposition group),

$$(g(\chi)^m) = \wp_0^{m\Sigma\Sigma\{p^i a/m\}\sigma_{ap^i}^{-1}} = \wp_0^{m\theta},$$

where $\theta = \sum_{b=1,(b,m)=1}^{m} \{b/m\}\sigma_b^{-1}$ is the Stickelberger element (we raise to the mth power to avoid denominators).

We now have a partial result: If $\wp_0$ is a prime of $\mathbb{Q}(\zeta_m)$ with $\wp_0 \nmid m$, then $\wp_0^{m\theta}$ is principal in $\mathbb{Q}(\zeta_m, \zeta_p)$. The main problem is now to get down to $\mathbb{Q}(\zeta_m)$, then to M.

Suppose that A is an ideal of $M \subseteq \mathbb{Q}(\zeta_m)$ with $(A, m) = 1$. Let $A = \prod \wp_i$ be its factorization into (not necessarily distinct) prime ideals in $\mathbb{Q}(\zeta_m)$. Then

$$A^{m\theta} = (\prod g(\chi_{\wp_i})^m),$$

where we write $\chi_{\wp_i}$ to indicate that χ depends on $\wp_i$. Suppose $\beta \in \mathbb{Z}[G]$ ($G = \mathrm{Gal}(M/\mathbb{Q})$) and $\beta\theta \in \mathbb{Z}[G]$. Extending the elements of G, we may regard $\beta\theta$ as an element of $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{mp})/\mathbb{Q})]$. Then

$$A^{m\beta\theta} = (\gamma^{\beta m}), \quad \text{where} \quad \gamma = \prod g(\chi_{\wp_i}) \in \mathbb{Q}(\zeta_{Pm}),$$

where $P = \prod p_i$ is the product of the rational primes divisible by the $\wp_i$'s. Since $\gamma^{m\beta} \in \mathbb{Q}(\zeta_m)$ by Lemma 6.4, and it is the mth power of an ideal of $\mathbb{Q}(\zeta_m)$, namely $A^{\beta\theta}$, it follows that the extension $\mathbb{Q}(\zeta_m, \gamma^\beta)/\mathbb{Q}(\zeta_m)$ can be ramified only at primes dividing m (*proof*: locally, $A^{\beta\theta}$ is principal, so we are adjoining the mth root of a local unit). But

$$\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_m, \gamma^\beta) \subseteq \mathbb{Q}(\zeta_m, \zeta_P),$$

Therefore, ramification can occur only at p_i's. Since $(P, m) = 1$, the extension must be unramified.

Lemma 6.15. *If $\mathbb{Q}(\zeta_m) \subseteq K \subseteq \mathbb{Q}(\zeta_n)$ and $K/\mathbb{Q}(\zeta_m)$ is unramified at all primes, then $K = \mathbb{Q}(\zeta_m)$.*

PROOF. Suppose $K \neq \mathbb{Q}(\zeta_m)$. Then there is a character χ for K of conductor not dividing m. By Theorem 3.5, $K/\mathbb{Q}(\zeta_m)$ must be ramified at some prime. Contradiction. □

We find that $\gamma^\beta \in \mathbb{Q}(\zeta_m)$. Therefore $A^{\beta\theta} = (\gamma^\beta)$ is principal as an ideal of $\mathbb{Q}(\zeta_m)$. But this does not necessarily mean that it is principal as an ideal of M. So we show that $\gamma^\beta \in M$, which suffices, since if two ideals of M are equal in $\mathbb{Q}(\zeta_m)$ they must have been equal originally because of unique factorization.

Let $\mathscr{P}$ be a prime of $\mathbb{Q}(\zeta_{q-1})$ lying over one of the prime factors $\wp_i$ of A. Then $\chi_{\wp_i}$ *a priori* depends on the choice of $\mathscr{P}$, so we temporarily let $\chi_{\wp_i} = \chi_{\mathscr{P}}$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/M)$. Then

$$\sigma\colon \mathbb{Z}[\zeta_{q-1}] \bmod \mathscr{P} \xrightarrow{\sim} \mathbb{Z}[\zeta_{q-1}] \bmod \mathscr{P}^\sigma$$

and correspondingly if $\chi_{\mathscr{P}}(a) = \zeta$ then $\chi_{\mathscr{P}^\sigma}(a) = \zeta^\sigma$. Therefore $\chi_{\mathscr{P}}^\sigma = \chi_{\mathscr{P}^\sigma}$. But $\chi_{\mathscr{P}}^m = 1$, so $\chi_{\mathscr{P}^\sigma} = \chi_{\mathscr{P}}$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}(\zeta_m))$. Therefore $\chi_{\mathscr{P}}$ depends only on $\not{p}_i$, so we may return to the notation $\chi_{\not{p}_i}$. The above reasoning shows that $\chi_{\not{p}_i}^{\sigma} = \chi_{\not{p}_i^{\sigma}}$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/M)$. If we extend σ by letting $\sigma(\zeta_p) = \zeta_p$, then $g(\chi_{\not{p}_i})^{\sigma} = g(\chi_{\not{p}_i}^{\sigma}) = g(\chi_{\not{p}_i^{\sigma}})$.

Since $A^{\sigma} = A$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/M)$, σ permutes the $\not{p}_i$'s. Therefore

$$\gamma^{\beta\sigma} = \prod g(\chi_{\not{p}_i})^{\beta\sigma} = \prod g(\chi_{\not{p}_i^{\sigma}})^{\beta} = \gamma^{\beta}.$$

But we already have $\gamma^{\beta} \in \mathbb{Q}(\zeta_m)$; hence $\gamma^{\beta} \in M$. So $A^{\beta\theta}$ is principal in M.

Finally, if A is an arbitrary ideal of M, we may write $A = (a)A_1$, with $a \in M$ and $(A_1, m) = 1$. Then

$$A^{\beta\theta} = (a^{\beta\theta})A_1^{\beta\theta},$$

which is principal. This completes the proof of Stickelberger's theorem. □

§6.3 Herbrand's Theorem

Let G be a finite abelian group and $\hat{G}$ its character group. Let $\chi \in \hat{G}$ and define

$$\varepsilon_{\chi} = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in \bar{\mathbb{Q}}[G],$$

where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. One may easily verify the following relations:

(a) $\varepsilon_{\chi}^2 = \varepsilon_{\chi}$;
(b) $\varepsilon_{\chi}\varepsilon_{\psi} = 0$ if $\chi \neq \psi$;
(c) $1 = \sum_{\chi \in \hat{G}} \varepsilon_{\chi}$;
(d) $\varepsilon_{\chi}\sigma = \chi(\sigma)\varepsilon_{\chi}$.

The ε_{χ}'s are called the orthogonal idempotents of the group ring $\bar{\mathbb{Q}}[G]$. If M is a module over $\bar{\mathbb{Q}}[G]$ then we may write

$$M = \bigoplus_{\chi} M_{\chi}, \quad \text{where } M_{\chi} = \varepsilon_{\chi} M$$

(use (c) to get the sum; if $0 = \sum \varepsilon_{\chi} a_{\chi}$, then use (b) and (a) to show $\varepsilon_{\chi} a_{\chi} = 0$ for all χ). Each $\sigma \in G$ acts on M, and M_{χ} is the eigenspace with eigenvalue $\chi(\sigma)$, by (d).

Of course, all the above works if $\bar{\mathbb{Q}}$ is replaced by any (commutative) ring which contains the values of all $\chi \in \hat{G}$ and in which $|G|$ is invertible.

In particular, let p be an odd prime and let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^{\times}$. Then $\hat{G} = \{\omega^i | 0 \leq i \leq p-2\}$. We shall work in the group ring $\mathbb{Z}_p[G]$. The idempotents are

$$\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1}, \qquad 0 \leq i \leq p-2.$$

Later, we shall also need

$$\varepsilon_- = \frac{1-\sigma_{-1}}{2} = \sum_{i\,\mathrm{odd}} \varepsilon_i \quad \text{and} \quad \varepsilon_+ = \frac{1+\sigma_{-1}}{2} = \sum_{i\,\mathrm{even}} \varepsilon_i .$$

There is a decomposition $A = A^- \oplus A^+$ for any $\mathbb{Z}_p[G]$-module, for example the p-Sylow subgroup of the ideal class group.

Let $\theta = (1/p)\sum_{a=1}^{p-1} a\sigma_a^{-1}$ be the Stickelberger element. Using (d), we find that

$$\varepsilon_i\theta = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-i}(a)\varepsilon_i = B_{1,\omega^{-i}}\varepsilon_i$$

and

$$\varepsilon_i(c - \sigma_c)\theta = (c - \omega^i(c))B_{1,\omega^{-i}}\varepsilon_i .$$

Let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$. Since $p^nA = 0$ for sufficiently large n, we may make A into a $\mathbb{Z}_p$-module by defining

$$\left(\sum_{j=0}^{\infty} b_jp^j\right)a = \sum_{j=0}^{\infty} (b_jp^ja),$$

since the latter sum is finite. G also acts on A, so A is a $\mathbb{Z}_p[G]$-module. Let

$$A = \bigoplus_{i=0}^{p-2} A_i$$

be the decomposition as above. Stickelberger's theorem implies that $(c - \sigma_c)\theta$ annihilates A, hence each A_i. Therefore we have proved the following: Let $c \in \mathbb{Z}$, $(c, p) = 1$. Then $(c - \omega^i(c))B_{1,\omega^{-i}}$ annihilates A_i.

Remark. Since $p\theta \equiv (p-1)\varepsilon_1 (\mathrm{mod}\ p)$, it is not very surprising that $p\theta$ annihilates A_i for $i \neq 1$. The fact that it annihilates A_1, however, requires Stickelberger's theorem.

Now, suppose $i \neq 0$ is even. Then $B_{1,\omega^{-i}} = 0$ so the above says nothing. If $i = 0$ then $(c-1)/2$ annihilates A_0, so $A_0 = 0$. But this is already obvious since $\varepsilon_1 = (\mathrm{Norm})/(p-1)$.

Let i be odd. Consider first the case $i = 1$. Let $c = 1 + p$, so we have

$$\begin{aligned}(c - \omega(c))B_{1,\omega^{-1}} = pB_{1,\omega^{-1}} &= \sum_{a=1}^{p-1} a\omega^{-1}(a) \\ &\equiv p - 1 \not\equiv 0 \ (\mathrm{mod}\ p).\end{aligned}$$

Since A_1 is a p-group, we must have $A_1 = 0$. (It is easily seen that $A_1 = 0$ is related to von Staudt–Clausen, which is related to the fact that the p-adic zeta function has a pole. Perhaps this explains why A_1 is a special case). If $i \neq 1$, we may choose an integer c, for example a primitive root (mod p), such that $c \not\equiv c^i \equiv \omega^i(c)$ (mod p). We may consequently ignore the factor $c - \omega^i(c)$, so we obtain the following.

Proposition 6.16. $A_0 = A_1 = 0$. *For* $i = 3, 5, \ldots, p-2$, $B_{1,\omega^{-i}}$ *annihilates* A_i. □

Suppose $A_i \neq 0$. Then we must have $B_{1,\omega^{-i}} \equiv 0 \pmod{p}$. But $B_{1,\omega^{-i}} \equiv B_{p-i}/(p-i) \pmod{p}$ by Corollary 5.15. We have proved the following.

Theorem 6.17 (Herbrand). *Let i be odd*, $3 \leq i \leq p-2$. *If* $A_i \neq 0$ *then* $p \mid B_{p-i}$. □

This theorem is much stronger than the theorem "$p \mid h \Rightarrow p$ divides some Bernoulli number" since it gives a "piece-by-piece" description of the criterion. Even better, the following is true.

Theorem 6.18 (Ribet). *Let i be odd*, $3 \leq i \leq p-2$. *If* $p \mid B_{p-i}$ *then* $A_i \neq 0$.

We shall not give the proof, which is very deep. It uses delicate techniques from algebraic geometry to construct an abelian unramified extension of degree p which corresponds by class field theory to A_i. See Ribet [2].

One corollary of Ribet's theorem is that the p-rank of the ideal class group of $\mathbb{Q}(\zeta_p)$ is at least the index of irregularity (p-rank = number of summands when A is decomposed as a direct sum of cyclic groups of p-power order). However, it is not known whether or not there is equality, since the rank of some A_i could possibly be two or larger. If $p \nmid h(\mathbb{Q}(\zeta_p)^+)$ then we do have equality, as we shall prove in Chapter 10.

§6.4 The Index of the Stickelberger Ideal

Let p be an odd prime, $n \geq 1$, $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$, and $R = \mathbb{Z}[G]$. As before,

$$\theta = \frac{1}{p^n} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} a\sigma_a^{-1}$$

is the Stickelberger element and $I = R\theta \cap R$ is the Stickelberger ideal. Let $J = \sigma_{-1}$ denote complex conjugation. Then

$$R^- = \{x \in R \mid Jx = -x\} = (1-J)R,$$

the first equality being the definition, the second following from a short calculation. We define

$$I^- = I \cap R^- = R\theta \cap R^-.$$

Note that we have to be careful about using the idempotent $(1-J)/2$ since it has a denominator. However, observe that $x \in R^- \Leftrightarrow [(1-J)/2]x = x$.

Theorem 6.19 (Iwasawa). $[R^- : I^-] = h^-(\mathbb{Q}(\zeta_{p^n}))$.

Remark. The above definitions hold for arbitrary $\mathbb{Q}(\zeta_m)$. Sinnott has shown in this case that

$$[R^- : I^-] = 2^a h^-(\mathbb{Q}(\zeta_m)),$$

where a is defined as follows: Let g be the number of distinct primes dividing m. Then $a = 0$ if $g = 1$, and $a = 2^{g-2} - 1$ if $g > 1$.

Proof of Theorem 6.19. The proof will proceed by considering completions, since we can then work with one prime at a time, which is slightly easier. Let q be a prime, $R_q = \mathbb{Z}_q[G]$, $I_q = R_q I$. Clearly I is dense in I_q in the natural q-adic topology. Also, $R_q^- = (1 - J)R_q$ and $I_q^- = I_q \cap R_q^-$.

Lemma 6.20. (a) $I_q = R_q\theta \cap R_q$, (b) $I_q^- = R_q\theta \cap R_q^-$, (c) $I_q^- = I^- \cdot \mathbb{Z}_q$, (d) *If* $p \neq q$ *then* $I_q = R_q\theta$.

Proof. The proof of Lemma 6.9 works for both R and R_q, with $I'_q = I'\mathbb{Z}_q$, so we obtain

$$R_q\theta \cap R_q = I'_q\theta = I'\mathbb{Z}_q\theta = I'\theta\mathbb{Z}_q = I\mathbb{Z}_q = I_q.$$

This proves (a). Part (b) follows easily from (a). If $p \neq q$ then $\theta \in R_q$, so (d) also follows from (a).

We now prove (c). Since $\{z\} + \{-z\} = 1$ for $z \notin \mathbb{Z}$, we have

$$(1 + J)\theta = N, \quad \text{where } N = \sum_{\sigma \in G} \sigma.$$

Let $x \in I'$. Then $x\theta \in I$, and we have

$$x\theta \in I^- \Leftrightarrow (1 + J)x\theta = 0 \Leftrightarrow xN = 0.$$

Similarly, suppose $y \in I'_q$. Then $y\theta \in I'_q\theta = I_q$, from the above, and

$$y\theta \in I_q^- \Leftrightarrow yN = 0.$$

Clearly $I^-\mathbb{Z}_q \subseteq I_q^-$. Suppose now that $y\theta \in I_q^-$, with $y \in I'_q$. We may write

$$y = \sum_c \sum_\sigma a_\sigma^c \sigma(c - \sigma_c), \qquad a_\sigma^c \in \mathbb{Z}_q.$$

The condition $yN = 0$ becomes $\sum_c \sum_\sigma a_\sigma^c(c - 1) = 0$. We want to approximate y by an element $x \in I'$ such that $xN = 0$. This then will give us an element $x\theta$ of I^- near $y\theta$, which will show that $I_q^- \subseteq$ closure of $I^- = I^-\mathbb{Z}_q$, as desired. The approximation will reduce to the following.

Fact. *Suppose* $b_i \in \mathbb{Z}$, $s_i \in \mathbb{Z}_q$, *and suppose* $\sum_{i=1}^m b_i s_i = 0$. *Then there is a sequence* $(t_1^{(n)}, \ldots, t_m^{(n)}) \in \mathbb{Z}^m$ *whose limit is* $(s_1, \ldots, s_m)$ *and such that* $\sum b_i t_i^{(n)} = 0$.

Proof. We may assume $(q, b_1) = 1$. For $2 \leq i \leq m$, choose $t_i^{(n)} \equiv 0 \bmod b_1$ with $t_i^{(n)}$ near s_i (this is where $(q, b_1) = 1$ is needed). Then $\sum b_i t_i^{(n)} \equiv 0 \bmod b_1$, so we can choose $t_1^{(n)} \in \mathbb{Z}$. Since $t_i^{(n)}$ is near s_i for $i \neq 1$, we must also have $t_1^{(n)}$ near s_1. This completes the proof of the fact.

If we let $a_\sigma^c = s_{\sigma,c}(=s_i)$, $c - 1 = b_{\sigma,c}$, and $x = \sum t_{\sigma,c}^{(n)}\sigma(c - \sigma_c) \in I'$, then x is near y and $xN = 0$, as desired. This completes the proof of Lemma 6.20. □

We have $R_q \simeq R \otimes \mathbb{Z}_q$, and under this isomorphism $R_q^- \simeq R^- \otimes \mathbb{Z}_q$ and $I_q^- \simeq I^- \otimes \mathbb{Z}_q$, by (c). It follows easily that $R_q^-/I_q^- \simeq (R^-/I^-) \otimes \mathbb{Z}_q$, which is isomorphic to the q-part of R^-/I^-. Therefore it suffices to prove the following.

Theorem 6.21. $[R_q^- : I_q^-] =$ *q-part of* $h^-(\mathbb{Q}(\zeta_{p^n}))$.

Proof. We first consider $q \neq 2, p$. Then $(1 \pm J)/2 \in R_q$; and we get $R_q = R_q^+ \oplus R_q^-$ and $I_q = I_q^+ \oplus I_q^-$ from the relation $1 = (1 + J)/2 + (1 - J)/2$. Therefore

$$I_q^- = \frac{1 - J}{2} I_q = \frac{1 - J}{2} R_q\theta = R_q^-\theta.$$

Consider the linear map

$$A: R_q^- \to R_q^-, \qquad x \mapsto x\theta.$$

By the theory of elementary divisors, as in the proof of Lemma 4.14, we have $[R_q^- : R_q^-\theta] = q$-part of $\det(A)$. But $\det(A)$ may be computed by working in $\bar{\mathbb{Q}}_q[G]^-$, which has the advantage of being a vector space over an algebraically closed field. We have

$$\bar{\mathbb{Q}}_q[G]^- = \bigoplus_{\chi\,\text{odd}} \varepsilon_\chi \bar{\mathbb{Q}}_q[G]$$

where $\varepsilon_\chi = (1/p^n) \sum_{a=1,(a,p)=1}^{p^n} \chi(a)\sigma_a^{-1}$ and each direct summand is one-dimensional. As in the previous section,

$$\varepsilon_\chi\theta = B_{1,\bar{\chi}}\varepsilon_\chi,$$

so A becomes a diagonal matrix. Therefore $\det(A) = \prod_{\chi\,\text{odd}} B_{1,\bar{\chi}}$, hence

$$\begin{aligned}[R_q^- : I_q^-] &= q\text{-part of} \prod_\chi B_{1,\bar{\chi}} \\ &= q\text{-part of } 2p^n \prod \left(-\tfrac{1}{2}B_{1,\bar{\chi}}\right) \\ &= q\text{-part of } h^-(\mathbb{Q}(\zeta_{p^n})).\end{aligned}$$

For $q = 2$, the argument must change slightly since $(1 + J)/2 \notin R_2$, so $R_2 \neq R_2^+ \oplus R_2^-$. Also, there is a power of 2 in the class number formula which must be accounted for.

Since we are restricted in our use of $(1 - J)/2$, we modify θ to obtain an element already in $\mathbb{Q}_2[G]^-$. Let

$$\tilde{\theta} = \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} \left(\frac{a}{p^n} - \frac{1}{2}\right)\sigma_a^{-1} = \theta - \tfrac{1}{2}N,$$

where N is the norm (one could also call it the trace). Clearly $\tilde{\theta} \notin R_2$, but a short calculation shows that

$$\frac{1-J}{2}\tilde{\theta} = \tilde{\theta}$$

so $\tilde{\theta}$ is in the "$-$" component. We recall that $\tilde{\theta}$ is perhaps a better Stickelberger element than θ, since it is the one that generalizes most readily (see the discussion after the statement of Theorem 6.10).

Lemma 6.22. (a) $I_2^- \subseteq R_2\tilde{\theta}$;
(b) $[R_2\tilde{\theta} : I_2^-] = 2$.

Proof. For the first statement, suppose $x \in R_2$ and $x\theta \in I_2^- = R_2\theta \cap R_2^-$. Then $x\theta = [(1-J)/2]x\theta = x[(1-J)/2](\tilde{\theta} + \frac{1}{2}N) = x\tilde{\theta} \in R_2\tilde{\theta}$.

For (b), we claim that if $x \in R_2$ then either $x\tilde{\theta} \in R_2$ or $x\tilde{\theta} - \tilde{\theta} \in R_2$. To prove this, we note that $x\tilde{\theta} = x\theta - \frac{1}{2}xN \in R_2 \Leftrightarrow \frac{1}{2}xN \in R_2$ and similarly for $(x-1)$. Let $x = \sum x_\sigma \sigma$. Then $xN = (\sum x_\sigma)N$ and $(x-1)N = (-1 + \sum x_\sigma)N$. Since either $(\sum x_\sigma)$ or $(-1 + \sum x_\sigma)$ is even, the claim is established.

The claim implies that $[R_2\tilde{\theta} : R_2\tilde{\theta} \cap R_2] = 2$ (the index is not 1 since $\tilde{\theta} \notin R_2$). The proof of the lemma will be complete if we can show that $R_2\tilde{\theta} \cap R_2 = R_2\theta \cap R_2^- = I_2^-$. We have already shown that $I_2^- \subseteq R_2\tilde{\theta} \cap R_2$. Now, let $x\tilde{\theta} \in R_2\tilde{\theta} \cap R_2$, where $x = \sum x_\sigma \sigma \in R_2$. Then, as above, $x\tilde{\theta} \in R_2 \Rightarrow \frac{1}{2}xN \in R_2 \Rightarrow \sum x_\sigma \equiv 0 \pmod 2$. Let $y_\sigma = x_\sigma$ for $\sigma \neq 1, J$, and let $y_1 = x_1 - \frac{1}{2}\sum x_\sigma$ and $y_J = x_J - \frac{1}{2}\sum x_\sigma$. Then $\sum y_\sigma = 0$, so $y = \sum y_\sigma \sigma \in R_2$ satisfies $yN = 0$. Also, $x - y = (\frac{1}{2}\sum x_\sigma)(1 + J)$, so $(x-y)\tilde{\theta} = 0$. Hence

$$x\tilde{\theta} = y\tilde{\theta} = y\theta - \tfrac{1}{2}yN = y\theta \in R_2\theta.$$

Since $x\tilde{\theta} \in R_2$ and satisfies $[(1-J)/2]x\tilde{\theta} = x\tilde{\theta}$, we have

$$x\tilde{\theta} \in R_2\theta \cap R_2^- = I_2^-, \quad \text{so} \quad R_2\tilde{\theta} \cap R_2 = I_2^-.$$

This completes the proof of Lemma 6.22. □

Just as for the other primes, we have a linear map

$$A : R_2^- \to R_2^-, \qquad x \mapsto \tilde{\theta}x$$

(since $x \in R_2^-$, $\frac{1}{2}xN = 0$, so there is no 2 in the denominator), and

$$\begin{aligned}
[R_2^- : R_2^-\tilde{\theta}] &= \text{2-part of } \det(A) \\
&= \text{2-part of } \prod_{\chi \text{ odd}} B_{1,\bar{\chi}} \qquad (\chi \text{ odd} \Rightarrow \varepsilon_\chi \tilde{\theta} = \varepsilon_\chi \theta) \\
&= 2^{\frac{1}{2}|G|} \cdot \tfrac{1}{2} \cdot (\text{2-part of } h^-).
\end{aligned}$$

Since this index is finite we must have

$$\tfrac{1}{2}|G| = \mathbb{Z}_2\text{-rank of } R_2^- = \mathbb{Z}_2\text{-rank of } R_2^-\tilde{\theta}.$$

Observe that $R_2^-\tilde{\theta} = (1-J)R_2\tilde{\theta} = R_2(2\tilde{\theta}) = 2R_2\tilde{\theta}$. Therefore

$$[R_2\tilde{\theta} : R_2^-\tilde{\theta}] = 2^{\frac{1}{2}|G|}.$$

But

$$[R_2\tilde{\theta} : I_2^-] = 2,$$

from Lemma 6.22. Putting everything together, we obtain

$$[R_2^- : I_2^-] = 2\text{-part of } h^-,$$

as desired.

Finally, we consider $q = p$. The main problem is that θ has p^n in its denominator. Let $\tilde{\theta} = \theta - \frac{1}{2}N$ be as above. Suppose $x = \sum_{(b,p)=1} x_b\sigma_b \in R_p$. Then $x\tilde{\theta} \in R_p^- \Leftrightarrow x\theta \in R_p$. We have

$$x\theta = \frac{1}{p^n}\sum_c \sum_a a x_{ac}\sigma_c;$$

hence $x\theta \in R_p \Leftrightarrow \sum_a a x_{ac} \equiv 0 \pmod{p^n}$ for all c with $(c, p) = 1$. But

$$\sum_a a x_{ac} \equiv c^{-1}\sum_a ac\, x_{ac} \equiv c^{-1}\sum_a a x_a \pmod{p^n},$$

so we only need $\sum a x_a \equiv 0 \pmod{p^n}$. It follows easily that $(x - b)\theta \in R_p$ for exactly one integer $b \pmod{p^n}$. Therefore

$$[R_p\tilde{\theta} : R_p\tilde{\theta} \cap R_p^-] = p^n.$$

But

$$R_p\tilde{\theta} = R_p^-\tilde{\theta} = R_p^-(\theta - \tfrac{1}{2}N) = R_p^-\theta, \quad \text{since}\, \frac{1-J}{2}N = 0,$$

Therefore

$$R_p\tilde{\theta} \cap R_p^- = R_p^-\theta \cap R_p^- \subseteq R_p\theta \cap R_p^- = I_p^-.$$

If $x\theta \in R_p^-$, then $x\theta = [(1 - J)/2]x\theta \in R_p^-\theta$; hence $R_p\theta \cap R_p^- \subseteq R_p^-\theta \cap R_p^-$. Therefore

$$I_p^- = R_p\tilde{\theta} \cap R_p^-.$$

From the above,

$$[R_p^-\theta : I_p^-] = p^n.$$

Let

$$A: R_p^- \to R_p^-, \qquad x \mapsto p^n\theta x.$$

Then

$$\begin{aligned}[R_p^- : p^n R_p^-\theta] &= p\text{-part of } \det(A)\\ &= p\text{-part of } p^{(n/2)|G|}\prod B_{1,\bar{\chi}}\\ &= p^{(n/2)|G|}\left(\frac{1}{p^n}\right)(p\text{-part of } h^-).\end{aligned}$$

But $[R_p^-\theta : p^n R_p^-\theta] = p^{(n/2)|G|}$, so

$$[R_p^- : I_p^-] = p\text{-part of } h^-.$$

This completes the proof of Theorems 6.19 and 6.21. □□

The formula $[R^- : I^-] = h^-$ may be regarded as an algebraic interpretation of the class number formula. It should be considered as being of a similar nature to the formula $[E^+ : C^+] = h^+$, which will be proved in Chapter 8.

The natural question arises: is there an isomorphism of G-modules

$$R^-/I^- \simeq C/C^+?$$

(C = class group, C^+ = class group of the real subfield). After all, both sides have the same order. In general, there is not such an isomorphism. Let $p = 4027$. The class group C_1 of $\mathbb{Q}(\sqrt{-4027})$ is $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Note that since $1 + J$ is the norm to $\mathbb{Q}$, J acts by inversion on the ideal class group. Therefore $C_1^- = C_1$ and $C_1^+ = 1$. Since $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})$ is totally ramified (at p), it follows from class field theory that the norm map on the ideal class groups is surjective. Suppose $R^-/I^- \simeq C/C^+$. Since R^-/I^- is cyclic over R, generated by $1 - J$, a similar statement holds for C/C^+; so there exists $c \in C$ such that $C/C^+ = cR \bmod C^+$. Therefore $C_1 = \text{Norm}(C) = \text{Norm}(C/C^+)$ (since $\text{Norm}(C^+) \subseteq C_1^+ = 1$) is generated by $c_1 = \text{Norm}(c)$ over R. If $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ then $\sigma | \mathbb{Q}(\sqrt{-p}) = 1$ or J. Therefore $c_1^\sigma = c_1^{\pm 1}$. It follows that $c_1 R$ is the subgroup generated by c_1, hence $c_1 R \neq C_1 \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Therefore R^-/I^- is not isomorphic to C/C^+.

However, we may hope for less. Let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_{p^n})$, so $A = A^+ \oplus A^-$. Then is there a G-isomorphism

$$R_p^-/I_p^- \simeq A^-?$$

Again, both sides have the same order. We shall show in Chapter 10 that if $p \nmid h^+(\mathbb{Q}(\zeta_p))$ then the above holds, so A^- is cyclic (i.e., generated by one element) as a module over the group ring in that case.

§6.5 Fermat's Last Theorem

Theorem 6.23. *Suppose p is prime and suppose the index of irregularity of p (=the number of Bernoulli numbers divisible by p) satisfies $i(p) < \sqrt{p} - 2$. Then*

$$X^p + Y^p = Z^p, \qquad (XYZ, p) = 1,$$

has no integer solutions.

Remark. This theorem was proved by Eichler under the assumption that the p-rank of the minus part of the ideal class group is less than $\sqrt{p} - 2$. It was noticed (independently) by Brückner, Iwasawa, and Skula that it is possible to use $i(p)$ instead. This yields a stronger theorem. Ribet's theorem shows that $i(p) \leq$ rank, but since possibly some component A_i could have rank greater than 1, we could have strict inequality. Also, it is easier to compute $i(p)$.

Up to 125000, the largest value of $i(p)$ is 5, and probability arguments indicate that we should have $i(p) = 0(\log p/\log\log p)$. Therefore, the theorem gives perhaps the best evidence yet for the first case of Fermat's Last Theorem. In fact, the probability that $i(p) > \sqrt{p} - 2$ is

$$\sum_{k > \sqrt{p}-2} e^{-1/2} \frac{(\frac{1}{2})^k}{k!}$$

(see the discussion following Theorem 5.17), which is easily seen to be at most $(1/2^k)(1/k!)$, with $k = [\sqrt{p}] - 1$. Since the first case of Fermat's Last Theorem is known at present for all $p < 6 \times 10^9$, we only need to consider larger p. Therefore, the total number of expected exceptions to the first case of Fermat's Last Theorem is at most

$$\sum_{p > 6 \times 10^9} \left(\frac{1}{2}\right)^{[\sqrt{p}]-1} \frac{1}{([\sqrt{p}] - 1)!},$$

which is less than $10^{-300000}$.

Proof of Theorem 6.23. Let $\zeta = \zeta_p$. As in Chapter 1, we assume we have a solution and obtain

$$(x + \zeta^i y) = C_i^p, \qquad i = 0, \ldots, p - 1,$$

where C_i is an ideal of $\mathbb{Q}(\zeta_p)$. Let C be the subgroup of the ideal class group generated by $C_1, \ldots, C_{p-1}$. Then C is an elementary p-group, so $\mathbb{Z}_p[G]$ acts on C, where $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Since $C_1^{\sigma_a} = C_a$, C_1 generates C over the group ring, and

$$\bigoplus_i \langle \varepsilon_i C_1 \rangle = C$$

($\langle x \rangle$ denotes the cyclic subgroup generated by x). Also,

$$\bigoplus_{i \text{ odd}} \langle \varepsilon_i C_1 \rangle = C^-.$$

Therefore

$$\begin{aligned} p\text{-rank } C^- &= \#\{\varepsilon_i C_1 \neq 0, i \text{ odd}\} \\ &\leq \#\{A_i \neq 0, i \text{ odd}\} \\ &\leq i(p) \quad \text{(by Herbrand's theorem)} \\ &< \sqrt{p} - 2 \quad \text{(by assumption).} \end{aligned}$$

This type of inequality can prove useful whenever one is working with a group, such as C, which is cyclic as a module over the group ring, since in essence we have reversed the inequality "rank $\geq i(p)$."

We now proceed with the proof of the theorem, following Eichler's argument. We may assume $p > 3$. Let $r = [\sqrt{p}] - 1$. Consider the set of all products $C_1^{b_1} \cdots C_r^{b_r}$ with $0 \le b_i < p$. The number of such products is $p^r > p^{\operatorname{rank}(C^-)} = |C^-|$. Therefore, two of them must agree in their C^--components, so we may divide and obtain

$$\prod_{i=1}^{r} C_i^{a_i} \in C^+, \quad \text{with } -p < a_i < p,$$

and some a_i is nonzero. Therefore

$$\prod C_i^{a_i} = (\rho)S,$$

with $\rho \in \mathbb{Q}(\zeta_p)$ and S an ideal with $\bar{S} = S$, so

$$\left(\prod_{i=1}^{r} (x + \zeta^i y)^{a_i}\right) = (\rho^p)S^p.$$

Since all the C_i's are prime to p, we may assume ρ and S are prime to p. The above implies that S^p is principal in $\mathbb{Q}(\zeta_p)$. Since the ideal class group of $\mathbb{Q}(\zeta_p)^+$ injects into that of $\mathbb{Q}(\zeta_p)$, by Theorem 4.14, S^p is principal in $\mathbb{Q}(\zeta_p)^+$: $S^p = (\alpha)$, with $\bar{\alpha} = \alpha$. Since any unit of $\mathbb{Q}(\zeta_p)$ is a root of unity times a real unit, we obtain

$$\prod_{i=1}^{r} (x + \zeta^i y)^{a_i} = \zeta^{\mu} \varepsilon \alpha \rho^p, \quad \text{with } \mu \in \mathbb{Z} \text{ and } \varepsilon \text{ a real unit.}$$

Therefore

$$\prod_{i=1}^{r} (x + \zeta^{-i} y)^{a_i} = \zeta^{-\mu} \varepsilon \alpha \bar{\rho}^p.$$

By Lemma 1.8, $\rho^p \equiv \bar{\rho}^p \equiv$ rational integer (mod p), so

$$\prod_{i=1}^{r} \left(\frac{x + \zeta^i y}{x + \zeta^{-i} y}\right)^{a_i} \equiv \zeta^{2\mu} \pmod{p},$$

and

$$\prod_{i=1}^{r} \left(\frac{x + \zeta^i y}{y + \zeta^i x}\right)^{a_i} \equiv \zeta^{v} \pmod{p},$$

with $v \equiv 2\mu - \sum i a_i (\operatorname{mod} p)$, $v \ge 0$. Let

$$x_i = \begin{cases} y, & \text{if } a_i < 0 \\ x, & \text{if } a_i \ge 0, \end{cases} \qquad y_i = \begin{cases} x, & \text{if } a_i < 0 \\ y, & \text{if } a_i \ge 0, \end{cases}$$

$$F(T) = \prod (x_i + T^i y_i)^{|a_i|}, \qquad G(T) = \prod (y_i + T^i x_i)^{|a_i|}.$$

Then F yields the numerator and G yields the denominator of the above expression, so

$$F(\zeta) \equiv \zeta^v G(\zeta) \pmod{p},$$

so

$$F(\zeta) = \zeta^v G(\zeta) + pK(\zeta), \quad \text{for some } K(T) \in \mathbb{Z}[T].$$

It follows that $F(T) = T^v G(T) + pK(T) + (1 + T + \cdots + T^{p-1})H(T)$ for some polynomial $H(T) \in \mathbb{Q}(T)$, but since everything else has integral coefficients, $H(T) \in \mathbb{Z}[T]$. Multiply by $1 - T$, differentiate with respect to T, set $X = \zeta$, and reduce mod p. Then

$$(1 - \zeta)F'(\zeta) - F(\zeta) \equiv (1 - \zeta)\zeta^v G'(\zeta) - \zeta^v G(\zeta) + v(1 - \zeta)\zeta^{v-1} G(\zeta) \pmod{p}.$$

Dividing by $F(\zeta) \equiv \zeta^v G(\zeta) \pmod{p}$, we find that

$$(1 - \zeta)\frac{F'(\zeta)}{F(\zeta)} - 1 \equiv (1 - \zeta)\frac{G'(\zeta)}{G(\zeta)} - 1 + v(1 - \zeta)\zeta^{-1} \pmod{p}.$$

This is essentially the same as what we would have obtained if we could have taken the logarithmic derivative of $F(\zeta) \equiv \zeta^v G(\zeta)$ with respect to ζ. The above may be rewritten as

$$\begin{aligned}(1 - \zeta)\sum_{i=1}^{r} i|a_i|\zeta^{i-1}\frac{y_i}{x_i + \zeta^i y_i} \\ \equiv (1 - \zeta)\sum_{i=1}^{r} i|a_i|\zeta^{i-1}\frac{x_i}{y_i + \zeta^i x_i} + v(1 - \zeta)\zeta^{-1},\end{aligned}$$

which is the same as

$$(1 - \zeta)\sum_{i=1}^{r} ia_i\zeta^i\left(\frac{y}{x + \zeta^i y} - \frac{x}{y + \zeta^i x}\right) \equiv v(1 - \zeta) \pmod{p}.$$

Multiply by $\prod_{i=1}^{r}(x + \zeta^i y)(y + \zeta^i x)$, which is a polynomial of degree $r(r + 1)$ in ζ. Let i_0 be the index of the first nonzero a_i. On the left we obtain a polynomial in ζ of degree

$$1 + i_0 + r(r + 1) - 2i_0 = 1 + r(r + 1) - i_0$$

with leading coefficient $i_0 a_{i_0}(x^2 - y^2)x^r y^r$. On the right we have a polynomial in ζ of degree $1 + r(r + 1)$ with leading coefficient $-x^r y^r v$. But

$$1 + r(r + 1) < 1 + (\sqrt{p} - 1)(\sqrt{p}) < p - 1,$$

so we have a polynomial in ζ of degree less than $p - 1$. By Lemma 1.9, corresponding coefficients are congruent mod p. It follows that $v \equiv 0 \pmod{p}$, so the right-hand side vanishes. The leading coefficient on the left now must vanish (mod p), so $x^2 \equiv y^2$, hence $x \equiv \pm y \pmod{p}$.

Interchanging y and z, we may also obtain $x \equiv \pm z \pmod{p}$, so

$$\pm x^p \pm x^p \equiv \pm x^p,$$

which is impossible for $p > 3$. This completes the proof. □

Notes

A good reference for much of this chapter is Coates [7]. See also the new edition of Ireland–Rosen [1].

For more on Gauss sums, see Ireland-Rosen [1] and Weil [1], [2], [3], [4].

Stickelberger's theorem was proved for $\mathbb{Q}(\zeta_p)$ by Kummer [1], and in general by Stickelberger [1]. For a proof which does not use Gauss sums, see Fröhlich [4].

There is a beautiful relation between Gauss sums and the p-adic Γ-function. See Gross–Koblitz [1], Lang [5], and Koblitz [4].

There are also analogues of Stickelberger's theorem for totally real fields (G. Gras [10], Oriat [3]), for group rings (McCulloh [1], [2]), and K-groups (Coates–Sinnott [1], [3]). For another extension, using Hecke characters, see Iwasawa [28].

Theorem 6.19 is due to Iwasawa [11]. The analogous formula for $\mathbb{Q}(\zeta_n)$ and some other abelian fields has been proved by Sinnott [1], [2], [3]. For the general theory of Stickelberger ideals, see the papers of Kubert–Lang.

Theorem 6.23 has been improved slightly by Uehara [2].

Exercises

6.1. Let $\mathbb{F}$ be a finite field. Show that the characters $\psi_c(x) = \psi(cx)$ for $c \in \mathbb{F}$ are distinct. Conclude that all additive characters of $\mathbb{F}$ are of this form.

6.2. Suppose the characters χ_i are multiplicative characters of $\mathbb{F}^\times$ and that $\chi_i^m = 1$ for all i. Let $e_i \in \mathbb{Z}$. Show that

$$\prod_i g(\chi_i)^{e_i} \in \mathbb{Q}(\zeta_m) \Leftrightarrow \prod \chi_i^{e_i}(a) = 1 \quad \text{for all } a \in (\mathbb{Z}/p\mathbb{Z})^\times.$$

6.3. Let $p \equiv 3 \pmod 4$ be prime, let R denote the number of quadratic residues mod p in the interval $(0, p/2)$, and let N denote the number of nonresidues in this interval. Use Stickelberger's theorem to show that $R - N$ annihilates the ideal class group of $\mathbb{Q}(\sqrt{-p})$. (Historically, this was known before the class number formula) (*Hint*: Exercise 4.5).

6.4. Let $\mathbb{E}/\mathbb{F}$ be an extension of finite fields, $[\mathbb{E}:\mathbb{F}] = n$, and let N be the norm for this extension. Let $\psi_{\mathbb{E}}$ and $\psi_{\mathbb{F}}$ be the additive characters. Let $\chi_{\mathbb{F}}$ be a multiplicative character of $\mathbb{F}$ and let $\chi_{\mathbb{E}} = \chi_{\mathbb{F}} \circ N$, a multiplicative character of $\mathbb{E}$. Let

$$R = \frac{g(\chi_{\mathbb{E}})}{g(\chi_{\mathbb{F}})^n}$$

(a) If $\chi_{\mathbb{F}}^m = 1$, show that $R \in \mathbb{Q}(\zeta_m)$.
(b) Show that R is a unit.
(c) Show that R has absolute value 1, hence is a root of 1.
(d) Use the Remark following Proposition 6.13 to show that R is congruent to 1 modulo primes above p (=characteristic of $\mathbb{F}$).

(e) (Davenport–Hasse) Conclude that for $p > 2$, $g(\chi_{\mathbb{E}}) = g(\chi_{\mathbb{F}})^n$ (this also works for $p = 2$; see the original paper by Davenport and Hasse. For a different proof, see Weil [1]).

(f) Show that if $\chi_{\mathbb{F}}$ has order exactly d then $\chi_{\mathbb{E}}$ has order exactly d.

(d) Suppose $\mathbb{F}$ has q elements and $d \mid q - 1$. Show that the number of solutions in projective space over $\mathbb{E}$ of $X^d + Y^d = Z^d$ is $1 + q^n - \sum_{a,b=1,a+b\neq d}^{d-1} J(\chi_{\mathbb{F}}^a, \chi_{\mathbb{F}}^b)^n$.

(h) Let α be a root of the polynomial in the numerator of the zeta function for $X^d + Y^d = Z^d$ over $\mathbb{Z}/p\mathbb{Z}$. Suppose $[\mathbb{F} : \mathbb{Z}/p\mathbb{Z}] = e$. Show that $\alpha^e = J(\chi_{\mathbb{F}}^a, \chi^b)$ for some a, b.

6.5. Show that for each positive integer d, the equation $X^d + Y^d = Z^d$ has nontrivial p-adic solutions for all p.

6.6. (a) Use the Brauer–Siegel theorem (or Theorem 4.19) to show that the index of irregularity satisfies $i(p) \leq p/4 + o(p)$.

(b) The probability that $i(p) = k$ is $e^{-1/2}(\frac{1}{2})^k/k!$ (see the discussion after Theorem 5.17). Let x be such that the expected number of $p \leq x$ with $i(p) = k$ is 1. Show that $\log x$ is approximately $k \log k$. Assuming that x is approximately equal to the first p with $i(p) = k$, conclude that we should have $i(p) = 0(\log p/\log \log p)$. This gives a fairly accurate estimate. The first p with $i(p) = 5$ is 78233, and $\log p/\log \log p = 4.65$.

Chapter 7

Iwasawa's Construction of p-adic L-functions

Following Iwasawa, we show how Stickelberger elements may be used to construct p-adic L-functions. The result yields a very useful representation of these functions in terms of a power series. As an application, we obtain information about the behavior of the p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension and prove that the Iwasawa μ-invariant vanishes for abelian number fields. Also, we show how many of the formulas we obtain have analogues in the theory of function fields over finite fields.

§7.1 Group Rings and Power Series

Let $\mathcal{O}$ be the ring of integral elements in a finite extension of $\mathbb{Q}_p$. For example, $\mathcal{O} = \mathcal{O}_\chi = \mathbb{Z}_p[\chi(1), \chi(2), \ldots]$ for some Dirichlet character χ. Let $\not{p}$ be the maximal ideal of $\mathcal{O}$ and let π be a generator of $\not{p}$, so $(\pi) = \not{p}$.

Let Γ be a multiplicative topological group isomorphic to the additive group $\mathbb{Z}_p$. Let γ be a fixed topological generator of Γ; i.e., the cyclic subgroup generated by γ is dense in Γ. For example, we may let γ correspond to $1 \in \mathbb{Z}_p$ under the above isomorphism, since 1 generates $\mathbb{Z}$, which is dense in $\mathbb{Z}_p$. Since the closed subgroups of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$, the closed subgroups of Γ are of the form Γ^{p^n}. Let $\Gamma_n = \Gamma/\Gamma^{p^n}$, so Γ_n is cyclic of order p^n, generated by the coset of γ.

Consider the group ring $\mathcal{O}[\Gamma_n]$. If $m \geq n \geq 0$ there is a natural map $\phi_{m,n}\colon \mathcal{O}[\Gamma_m] \to \mathcal{O}[\Gamma_n]$ induced by the map $\Gamma_m \to \Gamma_n$. Clearly

$$\mathcal{O}[\Gamma_n] \simeq \mathcal{O}[T]/((1 + T)^{p^n} - 1),$$

where the isomorphism is defined by

$$\gamma \bmod \Gamma^{p^n} \mapsto 1 + T \bmod((1 + T)^{p^n} - 1).$$

Since $(1+T)^{p^n}-1$ divides $(1+T)^{p^m}-1$ when $m \geq n \geq 0$, there is a natural map in the polynomial rings corresponding to $\phi_{m,n}$. If we take the inverse limit of the group rings $\mathcal{O}[\Gamma_n]$ with respect to the maps $\phi_{m,n}$ we get $\mathcal{O}[[\Gamma]]$, the so-called profinite group ring of Γ. Clearly $\mathcal{O}[\Gamma] \subseteq \mathcal{O}[[\Gamma]]$, since an element $\alpha \in \mathcal{O}[\Gamma]$ gives a sequence of elements $\alpha_n \in \mathcal{O}[\Gamma_n]$ such that $\phi_{m,n}(\alpha_m) = \alpha_n$. However, as we shall see, $\mathcal{O}[[\Gamma]]$ contains more elements. In effect, it is the compactification of $\mathcal{O}[\Gamma]$ and contains certain "infinite sums" of elements of Γ. To understand $\mathcal{O}[[\Gamma]]$ better, let us look at polynomial rings, since clearly

$$\mathcal{O}[[\Gamma]] \simeq \varprojlim \mathcal{O}[T]/((1+T)^{p^n}-1).$$

Theorem 7.1. $\mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T]]$, *the isomorphism being induced by* $\gamma \mapsto 1+T$.

Before proceeding with the proof, we shall prove two preliminary results which are useful in their own right.

Proposition 7.2. *Let* f, $g \in \mathcal{O}[[T]]$ *and assume* $f = a_0 + a_1 T + \cdots$, *with* $a_i \in \not{p}$ *for* $0 \leq i \leq n-1$, *but* $a_n \in \mathcal{O}^\times$. *Then we may uniquely write*

$$g = qf + r,$$

where $q \in \mathcal{O}[[T]]$ *and where* $r \in \mathcal{O}[T]$ *is a polynomial of degree at most* $n-1$.

Proof. We first prove uniqueness, which reduces to considering $qf + r = 0$. If $q, r \neq 0$, we may assume that either $\pi \nmid r$ or $\pi \nmid q$. Reduction mod π shows that $\pi | r$, so $\pi | qf$. An easy argument shows that since $\pi \nmid f$ we must have $\pi | q$, which gives a contradiction. So $q = r = 0$.

The existence is a little more difficult. Define an operator $\tau = \tau_n \colon \mathcal{O}[[T]] \to \mathcal{O}[[T]]$ by

$$\tau\left(\sum_{i=0}^{\infty} b_i T^i\right) = \sum_{i=n}^{\infty} b_i T^{i-n}.$$

In essence, τ is a "shift operator." Clearly τ is $\mathcal{O}$-linear and satisfies

(i) $\tau(T^n h(T)) = h(T)$ for all $h(T) \in \mathcal{O}[[T]]$;
(ii) $\tau(h(T)) = 0 \Leftrightarrow h(T) \in \mathcal{O}[T]$ with $\deg h(T) \leq n-1$.

We may write

$$f(T) = \pi P(T) + T^n U(T),$$

where $P(T)$ is a polynomial of degree less than n and $U(T) = a_n + a_{n+1}T + \cdots = \tau(f(T))$. Since $a_n \in \mathcal{O}^\times$, $U(T)$ is a unit of the power series ring. Let

$$q(T) = \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g).$$

Here, for example,

$$\left(\tau \circ \frac{P}{U}\right)^2 \circ \tau(g) = \tau\left(\frac{P}{U}\tau\left(\frac{P}{U}\tau(g)\right)\right).$$

Note that possibly each summand contributes, say, to the constant term. But the factor π^j makes the sum of these contributions converge. So $q(T)$ is well-defined power series in $\mathcal{O}[[T]]$. Since

$$qf = \pi qP + T^n qU,$$

we have

$$\tau(qf) = \pi\tau(qP) + \tau(T^n qU) = \pi\tau(qP) + qU.$$

But

$$\begin{aligned}\pi\tau(qP) &= \pi\left(\tau \circ \frac{P}{U}\right) \circ \left(\sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g)\right) \\ &= \tau(g) - qU.\end{aligned}$$

Therefore

$$\tau(qf) = \tau(g).$$

By (ii) above, $g = qf + r$, where $\deg r \leq n - 1$. This completes the proof of Proposition 7.2. □

Definition. $P(T) \in \mathcal{O}[T]$ is called *distinguished* if $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ with $a_i \in \mathfrak{p}$ for $0 \leq i \leq n - 1$. (Note that $P(T)$ is almost an Eisenstein polynomial. But we allow $\pi^2 | a_0$, so we do not necessarily have irreducibility).

Theorem 7.3 (p-adic Weierstrass Preparation Theorem). *Let*

$$f(T) = \sum_{i=0}^{\infty} a_i T^i \in \mathcal{O}[[T]],$$

and assume for some n we have $a_i \in \mathfrak{p}$, $0 \leq i \leq n - 1$, but $a_n \notin \mathfrak{p}$ (so $a_n \in \mathcal{O}^\times$). Then f may be uniquely written in the form $f(T) = P(T)U(T)$, where $U(T) \in \mathcal{O}[[T]]$ is a unit and $P(T)$ is a distinguished polynomial of degree n.

More generally, if $f(T) \in \mathcal{O}[[T]]$ is nonzero, then we may uniquely write

$$f(T) = \pi^\mu P(T)U(T)$$

with P and U as above and μ a nonnegative integer.

Proof. The second part clearly follows from the first part if we factor as large a power of π as possible from the coefficients of $f(T)$.

To prove the first part, let $g(T) = T^n$ in Proposition 7.2. Then

$$T^n = q(T)f(T) + r(T), \quad \text{with } \deg r \leq n - 1.$$

Since

$$q(T)f(T) \equiv q(T)(a_n T^n + \text{higher terms}) \pmod{\pi},$$

we must have $r(T) \equiv 0 \pmod{\pi}$. Therefore $P(T) = T^n - r(T)$ is a distinguished polynomial of degree n. Let q_0 be the constant term of $q(T)$. Comparing coefficients of T^n, we have $1 \equiv q_0 a_n \pmod{\pi}$. Therefore $q_0 \in \mathcal{O}^\times$, so $q(T)$ is a unit. Let $U(T) = 1/q(T)$. Then $f(T) = P(T)U(T)$, as desired. Since any distinguished polynomial of degree n can be written as $P(T) = T^n - r(T)$, we may transform the equation $f(T) = P(T)U(T)$ back to

$$T^n = U(T)^{-1}f(T) + r(T).$$

The uniqueness statement of Proposition 7.2 now implies the uniqueness of P and U. This completes the proof of Theorem 7.3. □

Corollary 7.4. *Let $f(T) \in \mathcal{O}[[T]]$ be nonzero. Then there are only finitely many $x \in \mathbb{C}_p$, $|x| < 1$, with $f(x) = 0$.*

Proof. Assume $f(x) = 0$. Write $f(T) = \pi^\mu P(T)U(T)$, as above. Since $U(T)$ is invertible, $U(x) \neq 0$. Therefore $P(x) = 0$. The result follows. □

Lemma 7.5. *Suppose $P(T) \in \mathcal{O}[T]$ is a distinguished polynomial, and let $g(T) \in \mathcal{O}[T]$ be arbitrary. If $g(T)/P(T) \in \mathcal{O}[[T]]$ then $g(T)/P(T) \in \mathcal{O}[T]$.*

Proof. Suppose $g(T) = f(T)P(T)$ for some $f(T) \in \mathcal{O}[[T]]$. Let $x \in \mathbb{C}_p$ be a zero of $P(T)$. Then

$$0 = P(x) = x^n + (\text{multiple of } \pi),$$

so $|x| < 1$. Hence $f(x)$ converges, so $g(x) = 0$. Dividing by $T - x$, and working in a larger ring if necessary, we continue this process and find that $P(T)$ divides $g(T)$ as polynomials, therefore in $\mathcal{O}[T]$. This completes the proof of Lemma 7.5. □

We now prove Theorem 7.1. It suffices to show that

$$\mathcal{O}[[T]] \simeq \varprojlim \mathcal{O}[T]/((1 + T)^{p^n} - 1).$$

Note that $P_n(T) = (1 + T)^{p^n} - 1$ is a distinguished polynomial. In fact, we can say more. The ideal $(\pi, T) \supseteq (p, T)$ is a maximal ideal of $\mathcal{O}[T]$ and also gives the maximal ideal of $\mathcal{O}[[T]]$. Clearly $P_0(T) \in (p, T)$. Since

$$\frac{P_{n+1}(T)}{P_n(T)} = (1 + T)^{p^n(p-1)} + (1 + T)^{p^n(p-2)} + \cdots + 1 \in (p, T)$$

(i.e., p divides the constant term), induction implies that $P_n(T) \in (p, T)^{n+1}$.

By Proposition 7.2, there is a natural map from $\mathcal{O}[[T]]$ to $\mathcal{O}[T]$ mod $P_n(T)$ for each n. Namely, $f(T) \mapsto f_n(T)$, where $f(T) = q_n(T)P_n(T) + f_n(T)$, with deg $f_n < p^n$. If $m \geq n \geq 0$, then

$$f_m(T) - f_n(T) - \left(q_n - \frac{P_m}{P_n} q_m\right)P_n.$$

By Lemma 7.5, $f_m \equiv f_n \pmod{P_n}$, as polynomials. Therefore

$$(f_0, f_1, \ldots) \in \varprojlim \mathcal{O}[T]/(P_n(T)).$$

This gives us the map from the power series ring to the inverse limit. If $f_n = 0$ for all n then P_n divides f for all n. Therefore $f \in \bigcap_{n=0}^{\infty} (p, T)^{n+1} = 0$, so the map is injective.

We now show it is surjective. Suppose $(f_0, f_1, \ldots)$ is in the inverse limit. Then, for $m \geq n \geq 0$, $f_m \equiv f_n \pmod{P_n}$, therefore $(\mathrm{mod}(p, T)^{n+1})$. Therefore, the constant terms are congruent mod p^{n+1}, the linear terms mod p^n, etc. So the coefficients of the terms form Cauchy sequence (Alternatively, $f = \lim f_n$ exists since $\mathcal{O}[[T]]$ is complete in the (p, T)-adic topology). Let $f(T) = \lim f_n(T) \in \mathcal{O}[[T]]$. We must show $f \mapsto (f_0, f_1, \ldots)$. If $m \geq n \geq 0$ then $f_m - f_n = q_{m,n}P_n$ for some $q_{m,n} \in \mathcal{O}[T]$. Let $m \to \infty$. Then

$$q_{m,n} = \frac{f_m - f_n}{P_n} \to \frac{f - f_n}{P_n}.$$

Since $q_{m,n} \in \mathcal{O}[T]$, the limit must be in $\mathcal{O}[[T]]$ (i.e., no denominators), so

$$f = (P_n)\left(\lim_m q_{m,n}\right) + f_n.$$

Therefore $f \mapsto (f_0, f_1, \ldots)$. This completes the proof of Theorem 7.1. □

§7.2 p-adic L-functions

We can now construct p-adic L-functions. The strategy is as follows. First, we use Stickelberger elements to obtain an element of $\mathcal{O}[\Gamma_n]$ for each n, where $\mathcal{O}$ is an approximate ring. These elements are "compatible," so they give an element of $\mathcal{O}[[\Gamma]]$, therefore a power series in $\mathcal{O}[[T]]$. This power series will give us the p-adic L-functions.

Let $q = p$ if $p \neq 2$, $q = 4$ if $p = 2$. The Galois group of $\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q}$ is $(\mathbb{Z}/qp^n\mathbb{Z})^\times$. If we let

$$\mathbb{Z}(\zeta_{qp^\infty}) = \bigcup_{n \geq 0} \mathbb{Q}(\zeta_{qp^n}),$$

then it follows from infinite Galois theory that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{qp^\infty})/\mathbb{Q}) = \varprojlim(\mathbb{Z}/qp^n\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

More explicitly, let $a = \sum a_i p^i \in \mathbb{Z}_p^\times$, and let $\zeta = \zeta_{p^n}$ for some n. Then

$$\sigma_a(\zeta) = \zeta^a = \prod_i \zeta^{a_i p^i},$$

which is a finite product since $\zeta^{p^i} = 1$ for $i \geq n$. Clearly σ_a gives an automorphism of $\mathbb{Q}(\zeta_{qp^\infty})$, and a moment's reflection shows that every automorphism must be of this form, since we know what happens at each finite level. Now,

$$\mathbb{Z}_p^\times \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times (1 + q\mathbb{Z}_p) \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times \mathbb{Z}_p,$$

the isomorphism being given by

$$a \mapsto (\omega(a) \bmod q, \langle a \rangle) \mapsto \left(\omega(a) \bmod q, \frac{\log_p\langle a \rangle}{\log_p(1 + q)}\right).$$

Also, observe that $1 + q$ is a topological generator for $1 + q\mathbb{Z}_p$; i.e., $(1 + q)^{\mathbb{Z}_p} = 1 + q\mathbb{Z}_p$.

Let d be a positive integer with $(p, d) = 1$. We assume $d \not\equiv 2 \pmod 4$ (hence $qp^n d \not\equiv 2 \pmod 4$ for $n \geq 0$). Let $q_n = qp^n d$, $K_n = \mathbb{Q}(\zeta_{q_n})$, and $K_\infty = \bigcup_{n \geq 0} \mathbb{Q}(\zeta_{q_n})$. Then $K_n = K_0(\zeta_{qp^n})$ and $K_\infty = K_0(\zeta_{qp^\infty})$. It follows easily that

$$\mathrm{Gal}(K_\infty/\mathbb{Q}) \simeq \Delta \times \Gamma.$$

where

$$\Delta = \mathrm{Gal}(K_0/\mathbb{Q}) \quad \text{and} \quad \Gamma = \mathrm{Gal}(K_\infty/K_0) \simeq \mathbb{Z}_p.$$

More explicitly, $\Gamma = 1 + q_0\mathbb{Z}_p = (1 + q_0)^{\mathbb{Z}_p}$, so $1 + q_0$ gives a topological generator. The elements of Γ which fix K_n are clearly those in

$$1 + q_n\mathbb{Z}_p = (1 + q_0)^{p^n\mathbb{Z}_p} = \Gamma^{p^n}.$$

Therefore $\mathrm{Gal}(K_n/K_0) = \Gamma/\Gamma^{p^n} = \Gamma_n$. Finally,

$$\mathrm{Gal}(K_n/\mathbb{Q}) \simeq \Delta \times \Gamma_n.$$

Corresponding to this decomposition, we write

$$\sigma_a = \delta(a)\gamma_n(a), \quad \text{with } \delta(a) \in \Delta, \gamma_n(a) \in \Gamma_n.$$

Let χ be a Dirichlet character whose conductor is of the form dp^j for some $j \geq 0$. Regarding χ as a character of $\mathrm{Gal}(K_n/\mathbb{Q})$, we see that we may uniquely write

$$\chi = \theta\psi,$$

where $\theta \in \hat{\Delta}$, $\psi \in \hat{\Gamma}_n$. Then θ is a character with conductor d or qd (hence $pq \nmid f_\theta$), while ψ is a character of Γ_n, so ψ has p-power order and is either trivial or has conductor of the form qp^j with $j \geq 1$. We call θ a character of the first kind and ψ a character of the second kind. Note that the characters of the first kind are associated with K_0, while those of the second kind are associated with the subfield of $\mathbb{Q}(\zeta_{qp^n})$ of degree p^n over $\mathbb{Q}$. Therefore the characters of the first kind correspond to tame ramification at p (i.e., p does not divide the ramification index of p), if $p \neq 2$, while those of the second kind correspond to wild ramification. Observe that ψ is an even character since it corresponds to a real field. Therefore, if χ is even then θ is even.

We now consider Stickelberger elements. Assume $\chi = \theta\psi$ is an even character, and let $\theta^* = \omega\theta^{-1}$, so θ^* is odd. Let

$$\xi_n = -\frac{1}{q_n} \sum_{\substack{0<a<q_n \\ (a,q_0)=1}} a\delta(a)^{-1}\gamma_n(a)^{-1}$$

$(=(-1) \times$ Stickelberger), and let

$$\begin{aligned}\eta_n &= (1-(1+q_0)\gamma_n(1+q_0)^{-1})\xi_n \\ &= -\sum_a \left(\left\{\frac{a(1+q_0)}{q_n}\right\} - (1+q_0)\left\{\frac{a}{q_n}\right\}\right)\delta(a)^{-1}\gamma_n(a)^{-1}\gamma_n(1+q_0)^{-1}.\end{aligned}$$

Note that $\eta_n \in \mathbb{Z}_p[\Delta \times \Gamma_n]$. Let

$$\varepsilon_{\theta^*} = \frac{1}{|\Delta|}\sum_{\delta\in\Delta} \theta^*(\delta)\delta^{-1}$$

be the idempotent for θ^*. Then $\varepsilon_{\theta^*}\xi_n = \xi_n(\theta)\varepsilon_{\theta^*}$ and $\varepsilon_{\theta^*}\eta_n = \eta_n(\theta)\varepsilon_{\theta^*}$, where

$$\xi_n(\theta) = -\frac{1}{q_n}\sum_a a\theta\omega^{-1}(a)\gamma_n(a)^{-1} \in K_\theta[\Gamma_n]$$

and

$$\begin{aligned}\eta_n(\theta) &= (1-(1+q_0)\gamma_n(1+q_0)^{-1})\xi_n(\theta) \\ &= \sum_a \left((1+q_0)\left\{\frac{a}{q_n}\right\} - \left\{\frac{a(1+q_0)}{q_n}\right\}\right) \times \theta\omega^{-1}(a)\gamma_n(a)^{-1}\gamma_n(1+q_0)^{-1} \\ &\in \mathcal{O}_\theta[\Gamma_n].\end{aligned}$$

$$(K_\theta = \mathbb{Q}_p(\theta(1), \theta(2), \ldots), \mathcal{O}_\theta = \mathbb{Z}_p[\theta(1), \theta(2), \ldots]).$$

Proposition 7.6. (a) $\frac{1}{2}\eta_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$;

(b) *if* $\theta \neq 1$ *then* $\frac{1}{2}\xi_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$;

(c) if $m \geq n \geq 0$ *then* $\eta_m(\theta) \mapsto \eta_n(\theta)$ *and* $\xi_m(\theta) \mapsto \xi_n(\theta)$ *under the natural map from* $K_\theta[\Gamma_m]$ *to* $K_\theta[\Gamma_n]$.

PROOF. (a) is obvious except when $p = 2$. To take care of this case, note that $\gamma_n(a) = \gamma_n(q_n - a)$ but $\theta\omega^{-1}(q_n - a) = -\theta\omega^{-1}(a)$. The terms for a and $q_n - a$ in $\frac{1}{2}\eta_n(\theta)$ combine to give

$$\begin{aligned}&\frac{1}{2}\left((1+q_0)\left\{\frac{a}{q_n}\right\} - \left\{\frac{a(1+q_0)}{q_n}\right\} - (1+q_0)\left(1-\left\{\frac{a}{q_n}\right\}\right) + \left(1-\left\{\frac{a(1+q_0)}{q_n}\right\}\right)\right) \\ &\qquad = (1+q_0)\left\{\frac{a}{q_n}\right\} - \left\{\frac{a(1+q_0)}{q_n}\right\} - \frac{q_0}{2} \in \mathbb{Z}_p.\end{aligned}$$

This proves (a).

We now prove (c). Under the map $\Gamma_m \to \Gamma_n$, we have $\gamma_m(a) \mapsto \gamma_n(a)$. Therefore

$$\xi_m(\theta) \mapsto \xi_n'(\theta) \overset{\text{def}}{=} -\frac{1}{q_m} \sum_{\substack{0<a<q_m \\ (a,q_0)=1}} a\theta\omega^{-1}(a)\gamma_n(a)^{-1}.$$

The set of $\gamma_m(a)$ which map to $\gamma_n(b)$ is

$$\{\gamma_m(b + iq_n) \mid 0 \le i < p^{m-n}\}.$$

Since

$$\sum_{0 \le i < p^{m-n}} (b + iq_n)\theta\omega^{-1}(b + iq_n)$$
$$= \theta\omega^{-1}(b) \sum_i (b + iq_n) = \frac{q_m}{q_n}\theta\omega^{-1}(b)\left(b + \frac{p^{m-n}-1}{2} q_n\right),$$

we have

$$\xi_n'(\theta) = \xi_n(\theta) - \frac{(p^{m-n}-1)}{2} \sum_{\substack{0<b<q_n \\ (b,q_0)=1}} \theta\omega^{-1}(b)\gamma_n(b)^{-1}.$$

Since $\gamma_n(b) = \gamma_n(q_n - b)$, but $\theta\omega^{-1}(q_n - b) = -\theta\omega^{-1}(b)$, the second sum vanishes. Therefore $\xi_m(\theta) \mapsto \xi_n(\theta)$.

Also, $1 - (1 + q_0)\gamma_m(1 + q_0)^{-1} \mapsto 1 - (1 + q_0)\gamma_n(1 + q_0)^{-1}$, so $\eta_m(\theta) \mapsto \eta_n(\theta)$. This proves (c).

For (b), we use a slightly longer proof than is necessary, since it gives additional information which will be useful later.

Lemma 7.7. $\gamma_n(a) = \gamma_n(b) \Leftrightarrow \langle a \rangle \equiv \langle b \rangle \bmod qp^n$.

PROOF. The decomposition $\sigma_a = \delta(a)\gamma_n(a)$ corresponds to $\mathbb{Q}(\zeta_{q_n}) = \mathbb{Q}(\zeta_{q_0}) \cdot \mathbb{B}_n$, where $\mathbb{B}_n$ is the subfield of $\mathbb{Q}(\zeta_{qp^n})$ which is cyclic of degree p^n over $\mathbb{Q}$. Since σ_a restricted to $\mathbb{B}_n$ depends only on $\langle a \rangle$ (mod qp^n) (the $\omega(a)$-part gives the action on $\mathbb{Q}(\zeta_q)$), the lemma follows. □

Let R denote the set of $(p-1)$st roots of unity (2nd roots of 1 if $p = 2$) in $\mathbb{Z}_p$. Then $\gamma_n(a) = \gamma_n(b) \Leftrightarrow \langle a/b \rangle \equiv 1 \pmod{qp^n} \Leftrightarrow a/b \equiv \omega(a/b) \Leftrightarrow a \equiv b\alpha$ (mod qp^n) for some $\alpha \in R$. If $a \in \mathbb{Z}_p$, let $s_n(a)$ be the unique integer satisfying

$$s_n(a) \equiv a \pmod{qp^n}, \qquad 0 \le s_n(a) < qp^n.$$

Actually, $s_n(a)$ is a partial sum of the p-adic expansion of a. The above may be rephrased as $s_n(a) = s_n(b\alpha)$. The set of numbers a with $0 < a < q_n$ such that $s_n(a) = s_n(b\alpha)$ is

$$\{s_n(b\alpha) + iqp^n \mid 0 \le i \le d - 1\}.$$

(Recall $q_0 = dq$). Finally, let T denote a set of representatives of elements of $(\mathbb{Z}/q_n\mathbb{Z})^\times$ such that

$$\Gamma_n = \{\gamma_n(b) \mid b \in T\}.$$

We have

$$\begin{aligned} \tfrac{1}{2}\xi_n(\theta) &= -\frac{1}{2q_n}\sum_{b\in T}\ \sum_{\gamma_n(a)=\gamma_n(b)} a\theta\omega^{-1}(a)\gamma_n(b)^{-1} \\ &= -\frac{1}{2q_n}\sum_{b\in T}\sum_{\alpha\in R}\sum_{i=0}^{d-1}(s_n(b\alpha)+iqp^n)\theta\omega^{-1}(s_n(b\alpha)+iqp^n)\gamma_n(b)^{-1}. \end{aligned}$$

If $\alpha \in R$ then $-\alpha \in R$, so we let R' be a set of representatives for $R \bmod \{\pm 1\}$. Clearly

$$s_n(-b\alpha) = qp^n - s_n(b\alpha) \quad (\text{if } b\alpha \not\equiv 0),$$

so

$$\begin{aligned} \theta\omega^{-1}(s_n(-b\alpha)+(d-1-i)qp^n) &= \theta\omega^{-1}(-s_n(b\alpha)-iqp^n+dqp^n) \\ &= -\theta\omega^{-1}(s_n(b\alpha)+iqp^n). \end{aligned}$$

(Recall $f_{\theta\omega^{-1}}$ divides $q_n = dqp^n$).

We now assume $d > 1$. Combining the term (α, i) with $(-\alpha, d-1-i)$, we obtain

$$\begin{aligned} &-\frac{1}{2q_n}\sum_{b\in T}\sum_{\alpha\in R'}\sum_{i=0}^{d-1}(s_n(b\alpha)+iqp^n-qp^n+s_n(b\alpha) \\ &\qquad\qquad -(d-1-i)qp^n)\theta\omega^{-1}(s_n(b\alpha)+iqp^n)\gamma_n(b)^{-1} \\ &= -\frac{1}{q_n}\sum_{b\in T}\sum_{\alpha\in R'}\sum_{i=0}^{d-1}\left(s_n(b\alpha)+iqp^n-\frac{q_n}{2}\right)\theta\omega^{-1}(s_n(b\alpha)+iqp^n)\gamma_n(b)^{-1}. \end{aligned}$$

Lemma 7.8. *Suppose $s, t \in \mathbb{Z}$, $(t, d) = 1$. Then*

$$\sum_{i=0}^{d-1}\theta\omega^{-1}(s+itq) = 0.$$

Proof. If $p \nmid f_{\theta\omega^{-1}}$, then $f_{\theta\omega^{-1}} = d$. Since $s + itq$ runs through a complete set of residue classes mod d, the result follows. Now suppose $p \mid f_{\theta\omega^{-1}}$, so the conductor is qd. If $p \mid s$ then all terms in the sum are 0. If $p \nmid s$ then $s + itq$ runs through all residue classes mod d, but is fixed mod p. Since $f_{\theta\omega^{-1}} > q$, there is an integer $u \equiv 1 \pmod q$ with $\theta\omega^{-1}(u) \neq 1, 0$. Multiplication by $\theta\omega^{-1}(u)$ permutes the sum, which must therefore be 0. This proves the lemma. □

We now have

$$\tfrac{1}{2}\xi_n(\theta) = -\sum_{b\in T}\sum_{\alpha\in R'}\sum_{i=0}^{d-1}\frac{i}{d}\theta\omega^{-1}(s_n(b\alpha)+iqp^n)\gamma_n(b)^{-1}.$$

Since $p \nmid d$, it follows that $\tfrac{1}{2}\xi_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$.

If $d = 1$, then θ is a power of ω and $q_n = qp^n$. Since $\theta \neq 1$ and θ is even, we cannot have $p = 2$ (or 3). Therefore we may ignore the 2 in the denominator. We find from the above that

$$\tfrac{1}{2}\xi_n(\theta) = -\frac{1}{2qp^n}\sum_{b\in T}\sum_{\alpha\in R} s_n(b\alpha)\theta\omega^{-1}(s_n(b\alpha))\gamma_n(b)^{-1}.$$

Since $s_n(b\alpha) \equiv b\alpha \pmod{qp^n}$, we have

$$\theta\omega^{-1}(s_n(b\alpha)) = \theta\omega^{-1}(b)\theta\omega^{-1}(\alpha) = \theta\omega^{-1}(b)\theta(\alpha)\alpha^{-1}.$$

Consequently

$$\begin{aligned}\tfrac{1}{2}\xi_n(\theta) &\equiv -\frac{1}{2qp^n}\sum_{b\in T}\sum_{\alpha\in R} b\alpha\theta\omega^{-1}(b)\theta(\alpha)\alpha^{-1}\gamma_n(b)^{-1}\\ &\equiv 0 \bmod \mathcal{O}_\theta, \quad \text{since} \textstyle\sum\theta(\alpha) = 0.\end{aligned}$$

This completes the proof of (b), hence of Proposition 7.6. □

For future reference, we record part of what we just proved.

Proposition 7.9. *Assume $\theta \neq 1$.*

(a) *If $f_\theta = q$, then*

$$\tfrac{1}{2}\xi_n(\theta) = -\frac{1}{2qp^n}\sum_{b\in T}\sum_{\alpha\in R} s_n(b\alpha)\theta\omega^{-1}(b\alpha)\gamma_n(b)^{-1};$$

(b) *if $f_\theta \neq q$, then*

$$\tfrac{1}{2}\xi_n(\theta) = -\frac{1}{d}\sum_{b\in T}\sum_{\alpha\in R'}\sum_{i=0}^{d-1} i\theta\omega^{-1}(s_n(b\alpha) + iqp^n)\gamma_n(b)^{-1}.$$ □

Combining Theorem 7.1 and Proposition 7.6, we find that there are power series $f, g, h \in \mathcal{O}_\theta[[T]]$ such that

$$\lim \xi_n(\theta) \leftrightarrow f(T, \theta) \quad (\text{if } \theta \neq 1)$$

$$\lim \eta_n(\theta) \leftrightarrow g(T, \theta)$$

$$\lim 1 - (1 + q_0)\gamma_n(1 + q_0)^{-1} \leftrightarrow h(T, \theta).$$

It is easy to see that

$$h(T, \theta) = 1 - \frac{1 + q_0}{1 + T}.$$

Also,

$$f(T, \theta) = \frac{g(T, \theta)}{h(T, \theta)}.$$

If $\theta = 1$, we take this as the definition of $f(T, \theta)$.

Theorem 7.10. *Let $\chi = \theta\psi$ be an even Dirichlet character (θ = first kind, ψ = second kind), and let $\zeta_\psi = \psi(1 + q_0)^{-1} = \chi(1 + q_0)^{-1}$ (= a root of unity of p-powder order). Then*

$$L_p(s, \chi) = f(\zeta_\psi(1 + q_0)^s - 1, \theta).$$

Remark. This is a very useful result. Note the essential difference between the contributions from the characters of the first and second kinds. This will be used in the proof of Theorem 7.14, and it is what one expects from analogy with function fields (Section 7.4).

Proof. Observe first that if $|s| < qp^{-1/(p-1)}$ then

$$|(1 + q_0)^s - 1| = |\exp(s \log_p(1 + q_0)) - 1| < 1,$$

and since ζ_ψ is of p-power order, $|\zeta_\psi(1 + q_0)^s - 1| < 1$. Therefore the right-hand side converges and is an analytic function of s. Consequently, we only need to prove the above equality for $s = 1 - m$, where m is a positive integer.

We shall work with $\eta_n(\theta)$ and $g(T, \theta)$ since, in all cases, they have integral coefficients. Let $i(a) = \log_p\langle a\rangle/\log_p(1 + q_0)$. Since $\gamma_n(1 + q_0)$ corresponds to $1 + T$, it follows that $\gamma_n(a) = \gamma_n(1 + q_0)^{i(a)}$ corresponds to $(1 + T)^{i(a)}$ $(\text{mod}(1 + T)^{p^n} - 1)$. From the definition of $\eta_n(\theta)$, we have

$$g(T, \theta) \equiv \sum_{\substack{0<a<q_n\\(a, q_0)=1}} \left((1 + q_0)\left\{\frac{a}{q_n}\right\} - \left\{\frac{(1 + q_0)a}{q_n}\right\}\right) \times \theta\omega^{-1}(a)(1 + T)^{-i(a)-1}$$
$$(\text{mod}(1 + T)^{p^n} - 1).$$

Let $(1 + q_0)a = a_1 + a_2 q_n$, with $0 \le a_1 < q_n$. Then $i(a) + 1 = i((1 + q_0)a) \equiv i(a_1) \bmod p^n$, and

$$g(T, \theta) \equiv \sum_a a_2\theta\omega^{-1}(a_1)(1 + T)^{-i(a_1)}(\text{mod } (1 + T)^{p^n} - 1).$$

If m is a positive integer and n is sufficiently large, then

$$g(\zeta_\psi(1 + q_0)^{1-m} - 1, \theta) \equiv \sum_a a_2\theta\omega^{-1}(a_1)(\zeta_\psi^{-1}(1 + q_0)^{m-1})^{i(a_1)} \bmod q_n,$$

since

$$\begin{aligned}(1 + T)^{p^n} - 1 &= (\zeta_\psi(1 + q_0)^{1-m})^{p^n} - 1\\ &= (1 + q_0)^{(1-m)p^n} - 1 \equiv 0 \ (\text{mod } q_n).\end{aligned}$$

But $\zeta_\psi^{-i(a_1)} = \psi(1 + q_0)^{i(a_1)} = \psi(a_1)$, and $(1 + q_0)^{i(a_1)} = \langle a_1\rangle$. Therefore

$$\begin{aligned}g(\zeta_\psi(1 + q_0)^{1-m} - 1, \theta) &\equiv \sum_a a_2\theta\omega^{-1}(a_1)\psi(a_1)\langle a_1\rangle^{m-1}\\ &\equiv \sum_a a_2\chi\omega^{-m}(a_1)a_1^{m-1} \ (\text{mod } q_n).\end{aligned}$$

If n is large enough that $f_\chi | q_n$, then $\chi\omega^{-m}((1+q_0)a) = \chi\omega^{-m}(a_1)$. Also,

$$((1+q_0)a)^m \equiv a_1^m + m a_1^{m-1} q_n a_2 \pmod{q_n^2},$$

so

$$\chi\omega^{-m}(1+q_0)(1+q_0)^m \sum_a \chi\omega^{-m}(a)a^m$$
$$\equiv \sum \chi\omega^{-m}(a_1)a_1^m + mq_n \sum a_2 \chi\omega^{-m}(a_1)a_1^{m-1} \pmod{q_n^2}.$$

Note that this last term is the one we need to evaluate in the above. As a runs from 1 to q_n, so does a_1, so the first two terms are the same. Also, $\chi\omega^{-m}(1+q_0) = \chi(1+q_0)$. We obtain

$$g(\zeta_\psi(1+q_0)^{1-m} - 1, \theta)$$
$$= ((1+q_0)^m \chi(1+q_0) - 1)\frac{1}{m} \lim_{n\to\infty} \frac{1}{q_n} \sum_{\substack{0<a<q_n\\(a,q_0)=1}} \chi\omega^{-m}(a)a^m$$
$$= -h(\zeta_\psi(1+q_0)^{1-m} - 1)\frac{1}{m} \lim_{n\to\infty} \frac{1}{q_n} \sum_a \chi\omega^{-m}(a)a^m.$$

The following lemma completes the proof of the theorem.

Lemma 7.11.

$$\lim_{n\to\infty} \frac{1}{q_n} \sum_{\substack{0<a<q_n\\(a,q_0)=1}} \chi\omega^{-m}(a)a^m = (1 - \chi\omega^{-m}(p)p^{m-1})B_{m,\chi\omega^{-m}}.$$

Proof. From Proposition 4.1 (recall $B_m(X) = \sum \binom{m}{i} B_i X^{m-i}$),

$$B_{m,\chi\omega^{-m}} = \frac{1}{q_n} \sum_{j=1}^{q_n} \chi\omega^{-m}(j) q_n^m B_m\left(\frac{j}{q_n}\right)$$
$$\equiv \frac{1}{q_n} \sum_j \chi\omega^{-m}(j)\left(j^m - \frac{m}{2} j^{m-1} q_n\right)\left(\operatorname{mod} \frac{1}{p} q_n\right)$$

($1/p$ takes care of the 6 in the denominator of B_2). Since

$$\chi\omega^{-m}(q_n - j)\cdot(q_n - j)^{m-1} \equiv -\chi\omega^{-m}(j)j^{m-1} \pmod{q_n},$$

we may pair terms to obtain

$$\sum_j \chi\omega^{-m}(j)j^{m-1} \equiv 0 \pmod{q_n}.$$

Therefore

$$B_{m,\chi\omega^{-m}} = \lim_{n\to\infty} \frac{1}{q_n} \sum_{j=1}^{q_n} \chi\omega^{-m}(j)j^m.$$

Finally, we obtain

$$\begin{aligned}(1-\chi\omega^{-m}(p)p^{m-1})B_{m,\chi\omega^{-m}} &= \lim \frac{1}{q_n}\sum_{j=1}^{q_n}\chi\omega^{-m}(j)j^m - \lim\frac{1}{q_n}\sum_{j=1}^{q_{n-1}}\chi\omega^{-m}(pj)(pj)^m \\ &= \lim\frac{1}{q_n}\sum_{\substack{j=1\\ p\nmid j}}^{q_n}\chi\omega^{-m}(j)j^m \\ &= \lim\frac{1}{q_n}\sum_{\substack{j=1\\ (j,q_0)=1}}^{q_n}\chi\omega^{-m}(j)j^m.\end{aligned}$$

This completes the proof of the lemma, and also of Theorem 7.10. □□

§7.3 Applications

Theorem 7.10 has many applications. For example, the congruences of Chapter 5 may be generalized (see the Exercises). In the following, we shall give an application to class numbers, but first we need a result about $g(T, \theta)$.

Lemma 7.12. *If $\theta = 1$, then $\frac{1}{2}g(T, \theta)$ is a unit of $\mathbb{Z}_p[[T]]$.*

Proof. By Theorem 7.10,

$$f(0, 1) = -B_{1,\omega^{-1}} = -\frac{1}{q}\sum_{\substack{a=1\\ p\nmid a}}^{q}\omega^{-1}(a)a \equiv \frac{1}{p}\bmod \mathbb{Z}_p,$$

since $\omega(a) \equiv a \pmod q$. Also

$$h(0, 1) = -q.$$

Therefore

$$\tfrac{1}{2}g(0, 1) = \tfrac{1}{2}f(0, 1)h(0, 1) \equiv \frac{-q}{2p} \bmod \frac{q}{2}\mathbb{Z}_p.$$

It follows that $\frac{1}{2}g(0, 1) \not\equiv 0 \pmod p$, so the constant term of $\frac{1}{2}g$ is a unit. This completes the proof. □

Theorem 7.13. *Let $(d, p) = 1$, $q_n = qdp^n$, and $h_n^- = h^-(\mathbb{Q}(\zeta_{q_n}))$. We assume $d \not\equiv 2 \pmod 4$. Then*

$$\frac{h_n^-}{h_0^-} = \prod_{\substack{\theta\neq 1\\ f_\theta \mid q_0\\ \theta \text{ even}}}\ \prod_{\substack{\zeta^{p^n}=1\\ \zeta\neq 1}} \tfrac{1}{2}f(\zeta-1, \theta) \times (p\text{-adic unit}).$$

PROOF. From the analytic class number formula we have

$$h_0^- = 2q_0 Q \prod_{\substack{\theta \neq 1 \\ f_\theta | q_0 \\ \theta \text{ even}}} (-\tfrac{1}{2} B_{1,\theta\omega^{-1}})$$

and

$$h_n^- = 2q_n Q \prod_{\substack{\chi \neq 1 \\ f_\chi | q_n \\ \chi \text{ even}}} (-\tfrac{1}{2} B_{1,\chi\omega^{-1}}).$$

The number Q equals 1 or 2, but is the same for all $n \geq 0$ by Corollary 4.13. Writing $\chi = \theta\psi$, where θ is of the first kind and ψ is of the second kind, we obtain

$$\prod_{\chi \neq 1} (-\tfrac{1}{2} B_{1,\chi\omega^{-1}}) = \prod_{\theta \neq 1} (-\tfrac{1}{2} B_{1,\theta\omega^{-1}}) \prod_{\psi \neq 1} (-\tfrac{1}{2} B_{1,\psi\omega^{-1}}) \prod_{\substack{\theta \neq 1 \\ \psi \neq 1}} (-\tfrac{1}{2} B_{1,\theta\psi\omega^{-1}}).$$

The first product is the same as that for h_0^-. To treat the second product, note that

$$-B_{1,\psi\omega^{-1}} = L_p(0, \psi) = \frac{g(\zeta_\psi - 1, 1)}{h(\zeta_\psi - 1, 1)}$$

($\psi\omega^{-1}(p) = 0$, so the Euler factor disappears. It is because of the Euler factors for the other characters that we must take the ratio h_n^-/h_0^- and require $\zeta \neq 1$; otherwise the formulas could reduce to $0 = 0$). From Lemma 7.12, $\frac{1}{2}g(\zeta_\psi - 1, 1)$ is a unit; and

$$h(\zeta_\psi - 1, 1) = 1 - \frac{1+q}{\zeta_\psi} \equiv 1 - \zeta_\psi^{-1} \pmod{q}.$$

Since ζ_ψ equals ψ evaluated at a generator of Γ_n, ζ_ψ determines ψ. Since there are p^n elements of $\hat{\Gamma}_n$, it follows that as ψ runs through the characters of the second kind, ζ_ψ runs through all p^nth roots of unity. Putting everything together, we find that

$$v_p\left(\prod_{\psi \neq 1} (-\tfrac{1}{2} B_{1,\psi\omega^{-1}})\right) = v_p\left(\prod_{\substack{\zeta^{p^n} = 1 \\ \zeta \neq 1}} (1 - \zeta^{-1})^{-1}\right) = v_p(p^{-n}) = v_p\left(\frac{q_0}{q_n}\right).$$

For the third product, we proceed as above (again, since $\psi \neq 1$, the Euler factor disappears):

$$-\tfrac{1}{2} B_{1,\theta\psi\omega^{-1}} = \tfrac{1}{2} f(\zeta_\psi - 1, \theta),$$

so

$$\prod_{\substack{\theta \neq 1 \\ \psi \neq 1}} (-\tfrac{1}{2} B_{1,\theta\psi\omega^{-1}}) = \prod_{\theta \neq 1} \prod_{\substack{\zeta^{p^n} = 1 \\ \zeta \neq 1}} \tfrac{1}{2} f(\zeta - 1, \theta).$$

Combining all the above, we obtain the theorem. □

Theorem 7.14. *Let $p^{e_n^-}$ be the exact power of p dividing h_n^-, in the notation of the previous theorem. There exist integers λ, μ, and ν, independent of n, with $\lambda \geq 0$, $\mu \geq 0$, such that*

$$e_n^- = \lambda n + \mu p^n + \nu$$

for all n sufficiently large.

Proof. In the notation of the previous theorem, let

$$A(T) = \prod_{\theta \neq 1} \tfrac{1}{2} f(T, \theta) \in \mathbb{Z}_p[[T]].$$

Then

$$\frac{h_n^-}{h_0^-} = \prod_{\substack{\zeta^{p^n}=1 \\ \zeta \neq 1}} A(\zeta - 1) \times (p\text{-adic unit}).$$

By the Weierstrass Preparation Theorem,

$$A(T) = p^\mu P(T) U(T),$$

where $\mu \geq 0$, $P(T)$ is a distinguished polynomial, and $U(T)$ is a unit of $\mathbb{Z}_p[[T]]$. Therefore

$$v_p(h_n^-) = v_p(h_0^-) + (p^n - 1)\mu + v_p\left(\prod_{\substack{\zeta^{p^n}=1 \\ \zeta \neq 1}} P(\zeta - 1) \right).$$

Let $\lambda = \deg P(T)$, so $P(T) = T^\lambda + a_{\lambda-1}T^{\lambda-1} + \cdots + a_0$ with $p \mid a_i$ for $0 \leq i \leq \lambda - 1$. If n is large enough and if ζ is a primitive p^nth root of unity, then

$$v_p((\zeta - 1)^\lambda) = \frac{\lambda}{\phi(p^n)} < v_p(p).$$

Hence $v_p(P(\zeta - 1)) = v_p((\zeta - 1)^\lambda)$. It follows that for n sufficiently large,

$$v_p\left(\prod_{\substack{\zeta^{p^n}=1 \\ \zeta \neq 1}} P(\zeta - 1) \right) = v_p(\prod (\zeta - 1)^\lambda) + C = v_p(p^{n\lambda}) + C = \lambda n + C,$$

where C is independent of n (it absorbs the effect of low-order roots of unity). The theorem follows easily. □

The above is part of a much more general theory of Iwasawa, which we shall consider in a later chapter. Suppose we have a sequence of number fields

$$K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \bigcup K_n,$$

with $\text{Gal}(K_n/K_0) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Then $\text{Gal}(K_\infty/K_0) = \varprojlim(\mathbb{Z}/p^n\mathbb{Z}) = \mathbb{Z}_p$, so the extension K_∞/K_0 is called a *$\mathbb{Z}_p$-extension* (or Γ-extension). Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there exist integers λ, μ, ν, as above, such that

$$e_n = \lambda n + \mu p^n + \nu$$

for all sufficiently large n. If the fields K_n are CM-fields, then

$$h_n = h_n^+ h_n^-, \qquad e_n = e_n^+ + e_n^-, \qquad \mu = \mu^+ + \mu^-, \quad \text{etc.}$$

So what we have proved above is the existence of λ^-, μ^-, ν^-.

We shall show later (Chapter 13) that for a given base field K_0 there are at least (exactly if Leopoldt's Conjecture is true) $r_2 + 1$ independent $\mathbb{Z}_p$-extensions, so, for example, real fields should have only one $\mathbb{Z}_p$-extension, while imaginary quadratic fields have two independent $\mathbb{Z}_p$-extensions. For the moment, we content ourselves with showing that every number field has at least one $\mathbb{Z}_p$-extension.

Let $\mathbb{B}_n$ be the unique (unless $p = 2$ and $n = 1$) subfield of $\mathbb{Q}(\zeta_{qp^n})$ which is cyclic of degree p^n over $\mathbb{Q}$ (use the isomorphism $(\mathbb{Z}/qp^n\mathbb{Z})^\times \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times$ (cyclic of order p^n); let $\mathbb{B}_n$ be the fixed field of $(\mathbb{Z}/q\mathbb{Z})^\times$). Then $\mathbb{Q} = \mathbb{B}_0$ and $\mathbb{B}_\infty/\mathbb{Q}$ is a $\mathbb{Z}_p$-extension. It corresponds to the group of all characters of the second kind. Now let K be any number field and let $K_\infty = K\mathbb{B}_\infty$. We claim that K_∞/K is a $\mathbb{Z}_p$-extension. Let $\mathbb{B}_e = K \cap \mathbb{B}_\infty$. Then $\mathrm{Gal}(K_\infty/K) \simeq \mathrm{Gal}(\mathbb{B}_\infty/\mathbb{B}_\infty \cap K) \simeq p^e\mathbb{Z}_p \simeq \mathbb{Z}_p$, as desired. The extension K_∞/K is called the *cyclotomic $\mathbb{Z}_p$-extension* of K. If K contains $\mathbb{Q}(\zeta_q)$ then the extension is obtained by simply adjoining all p^nth roots of unity for all n. This is what happened in Theorems 7.13 and 7.14.

§7.4 Function Fields

The theory of cyclotomic $\mathbb{Z}_p$-extensions has a strong analogue in the theory of function fields over finite fields. Let $\mathbb{F}_q$ be the finite field with q elements (no relation to the previous q; but this is the standard notation). Let X, Y be indeterminates related by a polynomial equation over $\mathbb{F}_q$, so $k = \mathbb{F}_q(X, Y)$ has transcendence degree one. We assume $k \cap \overline{\mathbb{F}}_q = \mathbb{F}_q$. The field k is called a function field (of one variable) over $\mathbb{F}_q$. It is well known that there are close connections between the arithmetic behavior of number fields and that of function fields; for example, both have zeta functions, satisfy class field theory, and have finite residue class fields at all (nonarchimedean) places.

Let $\zeta_k(s)$ be the zeta function of k. Then

$$\zeta_k(s) = \frac{R(q^{-s} - 1)}{(1 - q^{-s})(1 - q^{1-s})}$$

where $R(T) \in \mathbb{Z}[T]$ (we have used a nonstandard normalization of the numerator; usually $P(T) = R(T - 1)$ is used). The zeta function of the field $\mathbb{F}_q(X)$, the analogue of $\mathbb{Q}$, is simply

$$\frac{1}{(1 - q^{-s})(1 - q^{1-s})}$$

so the numerator is a product of L-series (at least when k is abelian over $\mathbb{F}_q(X)$).

Returning temporarily to number fields, we assume, for simplicity, that $K = \mathbb{Q}(\zeta_p)^+$ and let

$$\zeta_{K,p}(s) = \prod_{\substack{\theta\,\text{even} \\ f_\theta | p}} L_p(s, \theta).$$

Then $\zeta_{K,p}(s)$ is the p-adic zeta function of K. Let

$$A(T) = g(T, 1) \prod_{\theta \neq 1} f(T, \theta) \in \mathbb{Z}_p[[T]].$$

Then

$$\zeta_{K,p}(s) = \frac{A((1+p)^s - 1)}{h((1+p)^s - 1)},$$

which is a formula remarkably similar to the one above, except that A is a power series instead of a polynomial. But the Weierstrass Preparation Theorem says that a power series is "almost" a polynomial. Note in addition that h has a relatively simple form, and it may be traced to $\zeta_{\mathbb{Q},p}(s)$ (i.e., $\theta = 1$), again in analogy with the function field case. Of course, this may also be done for fields other than $\mathbb{Q}(\zeta_p)^+$, but then we must use q_0 in place of p. However, q_0 depends on the character θ; so either the above formula becomes a little more complicated, or we change variables in the $f(T, \theta)$ so that we may still use p (change T to $(1 + T)^a - 1$, where $a = \log_p(1 + q_0)/\log_p(1 + p)$).

We now return to function fields. The polynomial $R(T)$ satisfies the following properties:

(1) $R(T) = \prod_{j=1}^{2g} (1 - \alpha_j(T + 1))$ where the α_j's are algebraic integers of absolute value $q^{1/2}$ (the Riemann Hypothesis) and $g \geq 0$ is an integer called the genus of k.

(2) $R(0) = \prod (1 - \alpha_j) = h(k) =$ the number of divisor classes of degree 0 for k. This number is the analogue of the class number.

(3) If $\mathbb{F}/\mathbb{F}_q$ is an extension of degree m then $k' = k\mathbb{F}$ is a function field over $\mathbb{F}$. The numerator of the zeta function of k' is

$$R_{k'}(T - 1) = \prod_{j=1}^{2g} (1 - a_j^m T^m) = \prod_{\zeta^m = 1} R_k(\zeta T - 1).$$

From the theory of finite fields, there is a unique sequence of fields

$$\mathbb{F}_q \subset \mathbb{F}_{qp} \subset \cdots \subset \mathbb{F}_{qp^n} \subset \cdots \subset \mathbb{F} = \bigcup_n \mathbb{F}_{qp^n},$$

which is clearly a $\mathbb{Z}_p$-extension. Therefore, if $k_n = k\mathbb{F}_{qp^n}$, then

$$k = k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots \subset k_\infty$$

is also a $\mathbb{Z}_p$-extension. Since everything except 0 in a finite field is a root of unity, we have obtained this extension by adjoining roots of unity; and if $\mathbb{F}_q$ contains the pth roots of unity (remember, p and q are not related) then the extension k_∞ is obtained by adjoining the p-power roots of 1 (since reducing the rings $\mathbb{Z}[\zeta_{p^n}]$ modulo appropriate primes gives a $\mathbb{Z}_p$-extension of finite fields). Therefore k_∞/k is analogous to the cyclotomic $\mathbb{Z}_p$-extension of a number field.

Combining (2) and (3) above, we find that

$$\frac{h(k_n)}{h(k_0)} = \prod_{\substack{\zeta^{p^n}=1 \\ \zeta \neq 1}} R(\zeta - 1)$$

(the analogue of Theorem 7.13). The polynomial $R(T)$ is not necessarily distinguished, so we write $R(T) = p^\mu P(T)U(T)$, where $\mu \geq 0$, $P(T) \in \mathbb{Z}_p[T]$ is a distinguished polynomial (of degree $\leq 2g$), and $U(T)$ is a unit of $\mathbb{Z}_p[[T]]$ (actually, $U(T)$ is a polynomial by Lemma 7.5). Since $R(-1) = 1$, by (1), $\mu = 0$. Alternatively, when $R(T)$ is expanded as a polynomial in $1 + T$, one of the coefficients, in this case the constant term, is not divisible by p. This is essentially what we shall do to prove $\mu = 0$ in the number field case. Now let p^{e_n} be the exact power of p dividing $h(k_n)$. As in the proof of Theorem 7.14, we find that

$$e_n = \lambda n + \nu \quad \text{for } n \text{ sufficiently large,}$$

where $\lambda \leq 2g$ is the degree of $P(T)$. Because of the strong analogy between cyclotomic $\mathbb{Z}_p$-extensions and the above situation for function fields, plus some numerical evidence, Iwasawa was led to conjugate that $\mu = 0$ for cyclotomic $\mathbb{Z}_p$-extensions of number fields. For the special (and most important) case of $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)$, Iwasawa and Sims showed that $\mu = 0$ for $p \leq 4001$. Subsequent calculations (on a computer, of course) by Johnson and then Wagstaff extended the result to $p < 125000$. In the next section we shall extend the result up to $p < \infty$.

§7.5 $\mu = 0$

Theorem 7.15. *Let K be an abelian extension of $\mathbb{Q}$, let p be any prime, and let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension of K. Then $\mu = 0$.*

Remark. Iwasawa has constructed examples of noncyclotomic $\mathbb{Z}_p$-extensions with $\mu > 0$. See (Iwasawa [24]).

Proof of Theorem 7.15. Before starting the main part of the proof, we state some facts, some of which will be proved in later chapters but which are needed now.

I. K is contained in a cyclotomic field (Kronecker–Weber theorem).

II. If $K \subseteq K'$ then $\mu \leq \mu'$.

PROOF. Lift the p-part of the Hilbert class field H_n of K_n up to K_n'. The compositum $H_n K_n'$ is contained in the class field of K_n'. Since H_n and K_n' might not be disjoint, we could lose a factor of at most $[K_n' : K_n] \leq [K' : K]$. Therefore $e_n' + O(1) \geq e_n$. The result follows easily. □

III. Assume the pth roots of unity are in K. Then $\mu = \mu^+ + \mu^-$, and if $\mu^- = 0$ then $\mu^+ = 0$ (proof in Chapter 13).

IV. Suppose $e_n = \lambda n + \mu p^n + \nu$ for K_∞/K_0. Let $K' = K_m'$. Then K_∞/K' is a $\mathbb{Z}_p$-extension and

$$\lambda' = \lambda, \qquad \mu' = \mu p^m, \qquad \nu' = \nu + \lambda m.$$

PROOF. $e_n' = e_{n+m} = \lambda n + (\mu p^m)p^n + (\nu + \lambda m)$. □

We now claim that it suffices to prove $\mu^- = 0$ for K of the form $\mathbb{Q}(\zeta_{qd})$, where $q = p$ or 4 and $(d, p) = 1$. (These are exactly those to which Theorems 7.13 and 7.14 apply). For if K is arbitrary, $K \subseteq \mathbb{Q}(\zeta_{qp^n d})$ for some n and d. If $\mu^- = 0$ for $\mathbb{Q}(\zeta_{qd})$ then $\mu^+ = \mu = 0$ by III. By IV, $\mu = 0$ for $\mathbb{Q}(\zeta_{qp^n d})$, and by II, $\mu = 0$ for K.

If $\theta \neq 1$ is an even character of $\mathbb{Q}(\zeta_{qd})$ then $\frac{1}{2}f(T, \theta)$ has p-integral coefficients. If we can show that for each θ, $\frac{1}{2}f(T, \theta)$ has at least one coefficient relatively prime to p ("$\mu_\theta = 0$"), then it follows easily that $\mu^- = 0$ (see the proof of Theorem 7.14). This is what we shall do. As in the function field case, it will be more convenient to work with $1 + T$ than with T.

Recall that if $\alpha \in \mathbb{Z}_p$ then $s_n(\alpha)$ is the unique integer satisfying $0 \leq s_n(\alpha) < qp^n$ and $s_n(\alpha) \equiv \alpha \pmod{qp^n}$. For $p \neq 2$, let

$$\alpha = \sum_{j=0}^{\infty} t_j(\alpha)p^j, \qquad 0 \leq t_j(\alpha) \leq p - 1,$$

be the standard p-adic expansion. Then $s_n(\alpha) = \sum_{j=0}^{n} t_j(\alpha)p^j$ (we do not need $t_j(\alpha)$ for $p = 2$).

Proposition 7.16. *Let R be the set of $(p - 1)$st roots of unity in $\mathbb{Z}_p$ ($R = \{\pm 1\}$ if $p = 2$) and let R' be a set of representatives for R modulo $\{\pm 1\}$.*

(a) *Suppose $\theta = \omega^k$, $k \not\equiv 0 \pmod{p - 1}$, k even. Then $\mu_\theta = 0 \Leftrightarrow$ there exists $\beta \in \mathbb{Z}_p^\times$ and $n \geq 1$ such that*

$$\sum_{\alpha \in R} t_n(\beta\alpha)\alpha^{k-1} \not\equiv 0 \pmod{p}.$$

(b) *Suppose θ is not a power of ω. Then $\mu_\theta = 0 \Leftrightarrow$ there exists $\beta \in \mathbb{Z}_p^\times$ and $n \geq 0$ such that*

$$\sum_{\alpha \in R'} \sum_{i=0}^{d-1} i\theta\omega^{-1}(s_n(\beta\alpha) + iqp^n) \not\equiv 0 \pmod{\not{p}},$$

where $\not{p}$ is the prime of $\mathcal{O}_\theta$ above p, and d or dq is the conductor of θ.

PROOF. (a) Since $\theta \neq 1$ is even, we must have $p \geq 5$, so we have the luxury of ignoring 2 and letting $p = q$. In the notation of Proposition 7.9, we see that if $\frac{1}{2}\xi_n(\theta)$ is expressed as a polynomial in $1 + T$, modulo $(1 + T)^{p^n} - 1$, then each $\gamma_n(b)^{-1}$ corresponds to a different power of $1 + T$. Let $\gamma_n(b)^{-1} \leftrightarrow (1 + T)^{a_b}$, $0 \leq a_b < p^n$. Then (T = set $\neq$ T = variable)

$$\tfrac{1}{2}f(T, \theta) \equiv -\frac{1}{2p^{n+1}} \sum_{b \in T} \sum_{\alpha \in R} s_n(b\alpha)\theta\omega^{-1}(b\alpha)(1 + T)^{a_b} \bmod (1 + T)^{p^n} - 1.$$

Since $(1 + T)^{p^n} - 1 \equiv T^{p^n} \pmod{p}$, the above congruence determines the coefficients of $\frac{1}{2}f(T, \theta)$ modulo p, up to $T^{p^n - 1}$. Suppose $\mu_\theta > 0$, so p divides all the coefficients of $\frac{1}{2}f$. Then p divides all coefficients of the above polynomial when it is expressed as a polynomial in T, or in $1 + T$. Consequently,

$$\mu_\theta \neq 0 \Leftrightarrow \sum_{\alpha \in R} s_n(b\alpha)\theta\omega^{-1}(b\alpha) \equiv 0 \pmod{p^{n+2}},$$

for all n and all $b \in T$. But we can arbitrarily change the choice of the set of representatives T (this does not change the sum since we sum over R). Therefore we can consider all $b \in \mathbb{Z}$, $(b, p) = 1$. It is more convenient to consider all $b \in \mathbb{Z}_p^\times$; this does not affect anything since we are only looking at the beginning of the p-adic expansions. Since $\theta = \omega^k$ and $\omega(\alpha) = \alpha$, $\theta\omega^{-1}(\alpha) = \alpha^{k-1}$. Also, we may factor off and ignore $\theta\omega^{-1}(b)$. Writing

$$s_n(b\alpha) = s_{n+1}(b\alpha) - t_{n+1}(b\alpha)p^{n+1} \equiv b\alpha - t_{n+1}(b\alpha)p^{n+1} \pmod{p^{n+2}},$$

we have

$$\mu_\theta \neq 0 \Leftrightarrow \sum_{\alpha \in R} (b\alpha - t_{n+1}(b\alpha)p^{n+1})\alpha^{k-1} \equiv 0 \pmod{p^{n+2}}$$

$$\Leftrightarrow \sum_{\alpha \in R} t_{n+1}(b\alpha)\alpha^{k-1} \equiv 0 \pmod{p},$$

for all $n \geq 0$ and all $b \in \mathbb{Z}_p^\times$. This proves (a).

(b) This part follows immediately from Proposition 7.9, in a manner similar to part (a). □

Proposition 7.17. *Let m, d be positive integers with $(p, d) = 1$. For all n sufficiently large, there exist β_1, $\beta_2 \in \mathbb{Z}_p$, both congruent to* 1 mod p^m, *and there exists $\alpha_0 \in R'$ such that*

$$s_{n+m}(\beta_1\alpha) = s_n(\beta_1\alpha) \equiv 0 \pmod{d} \quad \text{for all } \alpha \in R',$$

$$s_{n+m}(\beta_2\alpha) = s_n(\beta_2\alpha) \equiv 0 \pmod{d} \quad \text{for all } \alpha \neq \alpha_0, \alpha \in R',$$

$$s_{n+m}(\beta_2\alpha_0) = s_n(\beta_2\alpha_0) + qp^n \equiv 0 \pmod{d}.$$

Remark. What this means is that the p-adic expansion of each $\beta_1\alpha$ and $\beta_2\alpha$ $(\alpha \neq \alpha_0)$ has m consecutive 0's starting with the $(n + 1)$st place, while $\beta_2\alpha_0$ has a 1 followed by $m - 1$ 0's. If α is a normal number (i.e., all possible combinations of digits occur with the expected frequency) then there are arbitrarily long sequences of 0's. But we do not know whether or not any α is normal (even though almost all numbers are normal), so we must use β_1 and β_2 to help. Also, we are requiring the desired patterns to occur for all α simultaneously, which causes additional problems, especially since there are usually dependence relations among the α's.

We shall postpone the proof of Proposition 7.17 in order to complete the proof of Theorem 7.15.

We first treat criterion (a) of Proposition 7.16. Since

$$0 = p \cdot p^m + (p-1)p^{m+1} + (p-1)p^{m+2} + \cdots,$$

we have

$$t_n(-y) = t_n(0-y) = p - 1 - t_n(y) \quad \text{if } n > v_p(y).$$

Since $k-1$ is odd, we may combine the terms for α and $-\alpha$ to obtain

$$\mu_\theta \neq 0 \Leftrightarrow 2 \sum_{\alpha \in R'} t_n(\beta\alpha)\alpha^{k-1} \equiv (p-1) \sum_{\alpha \in R'} \alpha^{k-1} \pmod p$$

for all $\beta \in \mathbb{Z}_p^\times$ and all $n \geq 1$. Note that the right side is independent of β and n. In Proposition 7.17 let $m = d = 1$. Then for n sufficiently large we have β_1, β_2 such that

$$\begin{aligned} t_{n+1}(\beta_1\alpha) &= 0 \quad \text{for all } \alpha \in R', \\ t_{n+1}(\beta_2\alpha) &= 0 \quad \text{for all } \alpha \neq \alpha_0, \alpha \in R', \\ t_{n+1}(\beta_2\alpha_0) &= 1. \end{aligned}$$

Therefore if $\mu_\theta \neq 0$, the above criterion (with $n+1$ instead of n) yields

$$0 \equiv (p-1) \sum \alpha^{d-1} \qquad (\beta = \beta_1),$$

and

$$2\alpha_0^{d-1} \equiv (p-1) \sum \alpha^{d-1} \qquad (\beta = \beta_2).$$

This is impossible (recall $p \neq 2$ in this case), so $\mu_\theta = 0$.

We now consider part (b) of Proposition 7.16. Assume $\mu_\theta \neq 0$, so

$$\sum_{\alpha \in R'} \sum_{i=0}^{d-1} i\theta\omega^{-1}(s_n(\beta\alpha) + iqp^n) \equiv 0 \pmod{\mathfrak{p}}$$

for all $n \geq 0$ and all $\beta \in \mathbb{Z}_p^\times$. In Proposition 7.17, let $m = 2$, $d = d$. If n is sufficiently large, there exist $\beta_1, \beta_2 \equiv 1 \pmod{p^2}$, in particular $\beta_1, \beta_2 = 1 \pmod q$, satisfying the criteria of Proposition 7.17. Therefore

$$s_n(\beta_1\alpha) \equiv \beta_1\alpha \equiv \alpha \equiv \beta_2\alpha \equiv s_n(\beta_2\alpha) \pmod q,$$

and

$$s_n(\beta_1\alpha) \equiv 0 \equiv s_n(\beta_2\alpha) \pmod d \quad \text{for } \alpha \neq \alpha_0.$$

Hence

$$s_n(\beta_1\alpha) \equiv s_n(\beta_2\alpha) \pmod{dq}, \qquad \alpha \neq \alpha_0,$$

and

$$\theta\omega^{-1}(s_n(\beta_1\alpha) + iqp^n) = \theta\omega^{-1}(s_n(\beta_2\alpha) + iqp^n)$$

for all i and all $\alpha \neq \alpha_0$. Similarly,

$$s_n(\beta_1\alpha_0) \equiv s_n(\beta_2\alpha_0) \equiv s_n(\beta_2\alpha_0) + qp^n \pmod{q}$$

and

$$0 \equiv s_n(\beta_1\alpha_0) \equiv s_n(\beta_2\alpha_0) + qp^n \pmod{d},$$

so

$$\theta\omega^{-1}(s_n(\beta_1\alpha_0) + iqp^n) = \theta\omega^{-1}(s_n(\beta_2\alpha_0) + (i+1)qp^n).$$

Let $a_0 = s_n(\beta_2\alpha_0)$, for convenience. Comparing terms above for $\beta = \beta_1$ and $\beta = \beta_2$, we find that we must have

$$\begin{aligned}\sum_{i=0}^{d-1} i\theta\omega^{-1}(a_0 + iqp^n) &\equiv \sum_{i=0}^{d-1} i\theta\omega^{-1}(s_n(\beta_1\alpha_0) + iqp^n)\\ &\equiv \sum_{i=0}^{d-1} i\theta\omega^{-1}(a_0 + (i+1)qp^n)\\ &\equiv \sum_{j=1}^{d} j\theta\omega^{-1}(a_0 + jqp^n) - \sum_{j=1}^{d} \theta\omega^{-1}(a_0 + jqp^n)\\ &\equiv \sum_{i=0}^{d-1} i\theta\omega^{-1}(a_0 + iqp^n) + d\theta\omega^{-1}(a_0 + dqp^n) - \sum_{j=1}^{d} \theta\omega^{-1}(a_0 + jqp^n).\end{aligned}$$

The last sum vanishes by Lemma 7.8. Consequently,

$$d\theta\omega^{-1}(a_0 + dqp^n) \equiv 0 \pmod{\not{p}}.$$

But $p \nmid d$ and $\theta\omega^{-1}(a_0 + dqp^n) = \theta\omega^{-1}(a_0)$, so $\theta\omega^{-1}(a_0) = 0$. But $a_0 = s_n(\beta_2\alpha_0) \equiv -qp^n \pmod{d}$, so $(a_0, d) = 1$. Also, $s_n(\beta_2\alpha_0) \equiv \beta_2\alpha_0 \equiv \alpha_0 \pmod{q}$, so $(a_0, q) = 1$. Therefore $(a_0, f_{\theta\omega^{-1}}) = 1$, hence $\theta\omega^{-1}(a_0) \neq 0$. This contradiction completes the proof of Theorem 7.15. □

Proof of Proposition 7.17. Let r be a positive integer. A sequence of vectors $x_n \in [0, 1)^r$ is called uniformly distributed mod 1 if for every open set $U \subseteq [0, 1)^r$ we have

$$\lim_{N\to\infty} \frac{\#\{n \leq N \mid x_n \in U\}}{N} = \text{meas}(U),$$

where we take the usual measure, normalized by meas$([0, 1)^r) = 1$. There is the following well-known criterion of Weyl:

The sequence $\{x_n\}$ *is uniformly distributed* mod 1 $\Leftrightarrow$ *for every* $z \in \mathbb{Z}^r$, $z \neq 0$, *we have*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i x_n \cdot z} = 0$$

($x_n \cdot z$ *is the usual dot product; note that if* $z = 0$, *the limit is* 1).

The proof of the criterion may be sketched as follows: the trigonometric polynomials are dense in the set of continuous functions on $(\mathbb{R}/\mathbb{Z})^r$, and $\int e^{2\pi i x \cdot z}\, dx = 0$ if $z \neq 0$, so the above is equivalent to

$$\frac{1}{N} \sum_{n=1}^{N} f(x_n) \to \int f(x)\, dx \quad \text{for all continuous } f.$$

Now, if f approximates the characteristic function of an open set U then $\sum f(x_n)$ is approximately $\#\{n \leq N \mid x_n \in U\}$, while $\int f(x)\, dx$ is approximately meas(U). Since step functions can be used to approximate continuous functions, the argument also works in reverse. For fuller details, see (Kuipers and Niederreiter [1]).

Lemma 7.18. *For* $\beta \in \mathbb{Z}_p$, *let* $x_n(\beta) = q^{-1}p^{-n}s_n(\beta)$. *For almost all* $\beta \in \mathbb{Z}_p$ (*i.e., except for a set of measure* 0 *for the usual Haar measure on* $\mathbb{Z}_p$), *the sequence of numbers* $x_n(\beta) \in [0, 1)$ *is uniformly distributed* mod 1

Proof. Let $S(N, \beta) = (1/N) \sum_{n=1}^{N} e(x_n(\beta))$, where $e(x) = e^{2\pi i x}$. Then

$$\int_{\beta \in \mathbb{Z}_p} |S(N, \beta)|^2\, d\beta = \frac{1}{N} + \frac{1}{N^2} \sum_{m \neq n} \int_{\beta \in \mathbb{Z}_p} e(x_n(\beta) - x_m(\beta))\, d\beta.$$

Suppose $n > m$. We claim that the map

$$\mathbb{Z}/qp^n\mathbb{Z} \to \mathbb{Z}/qp^n\mathbb{Z}, \quad \alpha \mapsto s_n(\alpha) - p^{n-m}s_m(\alpha)$$

is a bijection. For suppose

$$s_n(\alpha) - p^{n-m}s_m(\alpha) \equiv s_n(\beta) - p^{n-m}s_m(\beta) \pmod{qp^n}.$$

Then

$$\begin{aligned} \alpha - \beta &\equiv s_n(\alpha) - s_n(\beta) \\ &\equiv p^{n-m}(s_m(\alpha) - s_m(\beta)) \equiv p^{n-m}(\alpha - \beta) \pmod{qp^n}. \end{aligned}$$

It follows that $\alpha - \beta \equiv 0$, so the map is injective, hence bijective. Since

$$x_n(\beta) - x_m(\beta) = q^{-1}p^{-n}(s_n(\beta) - p^{n-m}s_m(\beta)),$$

it follows that if β runs through the congruence classes mod qp^n in $\mathbb{Z}_p$, $e(x_n(\beta) - x_m(\beta))$ runs through all qp^nth roots of 1. Since each congruence class has the same measure, namely $q^{-1}p^{-n}$, it follows that the integral above vanishes. Similarly, the integral is 0 if $n < m$. Therefore

$$\int |S(N, \beta)|^2 \, d\beta = \frac{1}{N},$$

so

$$\int \sum_{m=1}^{\infty} |S(m^2, \beta)|^2 \, d\beta = \sum_{m=1}^{\infty} \int |S(m^2, \beta)|^2 \, d\beta = \sum_{m=1}^{\infty} \frac{1}{m^2} < \infty.$$

Consequently $\sum |S(m^2, \beta)|^2 \in L^1(\mathbb{Z}_p)$, hence the sum must converge for almost all β. Therefore $\lim |S(m^2, \beta)|^2 = 0$ for almost all β.

For arbitrary N, choose m such that $m^2 \leq N < (m + 1)^2$. Trivial estimates yield

$$|S(N, \beta)| \leq |S(m^2, \beta)| + \frac{2m}{N} \to 0 \quad \text{as } N \to \infty$$

for almost all $\beta \in \mathbb{Z}_p$.

Now let $z \in \mathbb{Z}$, $z \neq 0$. Since

$$zs_n(\beta) \equiv z\beta \equiv s_n(z\beta) \pmod{qp^n},$$

we have

$$e(zx_n(\beta)) = e(x_n(z\beta)).$$

By the above,

$$\frac{1}{N} \sum_{n=1}^{N} e(zx_n(\beta)) = \frac{1}{N} \sum_{n=1}^{N} e(x_n(z\beta)) = S(N, z\beta) \to 0$$

for almost all β. Each z excludes a set of measure 0. Since $\mathbb{Z}$ is countable, we exclude altogether only a set of measure 0. For the remaining β's, we may apply the Weyl criterion ($r = 1$). This completes the proof of Lemma 7.18. □

Remark. A p-adic number β is called normal if for every $k \geq 1$ and every string of integers of length k, consisting of integers in $\{0, 1, \ldots, p - 1\}$, the standard p-adic expansion of β contains this string infinitely often, with asymptotic frequency p^{-k}. It is not hard to see that β is normal if and only if $x_n(\beta)$ is uniformly distributed mod 1 (see Exercises). Therefore, almost all $\beta \in \mathbb{Z}_p$ are normal. Since the digits of the p-adic expansion can be regarded as independent identically distributed random variables, this fact may also be approached via theorems of probability theory.

Lemma 7.19. *Suppose $\gamma_1, \ldots, \gamma_r \in \mathbb{Z}_p$ are linearly independent over $\mathbb{Q}$. For almost all $\beta \in \mathbb{Z}_p$ the sequence of vectors*

$$X_n = X_n(\beta) = (x_n(\beta\gamma_1), \ldots, x_n(\beta\gamma_r)) \in [0, 1)^r$$

is uniformly distributed mod 1.

Proof. Let $z = (z_1, \ldots., z_r) \in \mathbb{Z}^r$, $z \neq 0$, let $\beta \in \mathbb{Z}_p$, and let $y_n = X_n \cdot z = q^{-1}p^{-n} \sum_i z_i s_n(\beta\gamma_i)$. Since

$$\sum_i z_i s_n(\beta\gamma_i) \equiv \sum z_i \beta\gamma_i \equiv s_n(\beta \sum z_i \gamma_i) \pmod{qp^n},$$

we have

$$y_n \equiv q^{-1}p^{-n}s_n(\beta\gamma) \pmod 1, \quad \text{where } \gamma = \sum z_i\gamma_i.$$

Note that $\gamma \neq 0$ since the γ_i's are linearly independent. By Lemma 7.19 and the Weyl criterion (with $r = 1$),

$$\frac{1}{N} \sum_{n=1}^{N} e(X_n \cdot z) = \frac{1}{N} \sum_{n=1}^{\infty} e(x_n(\beta\gamma)) \to 0$$

for almost all $\beta \in \mathbb{Z}_p$. As in the previous lemma, each z excludes only a set of measure 0, and $\mathbb{Z}^r$ is countable, hence the Weyl criterion (with $r = r$) completes the proof of Lemma 7.19. □

Lemma 7.20. *Suppose $\gamma_1, \ldots, \gamma_r \in \mathbb{Z}_p$ are linearly independent over $\mathbb{Q}$. Let $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_r) \in (0, 1)^r$, let $\varepsilon > 0$, and let m and d be positive integers with $(d, p) = 1$. For each n sufficiently large, there exists $\beta \in \mathbb{Z}_p$ such that*

(1) $\beta \equiv 1 \pmod{p^m}$,
(2) $|x_n(\beta\gamma_j) - \bar{x}_j| < \varepsilon$ *for* $1 \leq j \leq r$,
(3) $s_n(\beta\gamma_j) \equiv 0 \pmod d$ *for* $1 \leq j \leq r$.

Proof. For $t \in \mathbb{R}$, or $\mathbb{R}/\mathbb{Z}$, let $\|t\|$ denote the distance from t to the nearest integer, and let $\|(t_1, \ldots, t_r)\| = \max \|t_i\|$. Let $\varepsilon' = \varepsilon/2d$ and $x' = \bar{x}/d$. We assume ε is small enough that $\bar{x}_j + \varepsilon < 1$ and $\bar{x}_j - \varepsilon > 0$ for all j.

Since $[0, 1]^r$ is compact, there exist $y_1, \ldots, y_D \in (0, 1)^r$, for some D, such that for each $y \in [0, 1]^r$ we have $\|y - y_i\| < \varepsilon'$ for some i. By Lemma 7.19, for each y_i there exists $\beta_i \in \mathbb{Z}_p$ and $n_i \in \mathbb{Z}$ such that $\|X_{n_i}(\beta_i) - y_i\| < \varepsilon'$. Let $n_0 = m + \max n_i$. We claim that if $n \geq n_0$ we can satisfy (1), (2), (3). Choose y_i such that

$$\left\|x' - X_n\left(\frac{1}{d}\right) - y_i\right\| < \varepsilon' \qquad \left(\text{note } \frac{1}{d} \in \mathbb{Z}_p\right).$$

Let $\beta' = 1/d + p^{n-n_i}\beta_i$. Then

$$\begin{aligned}\|x' - X_n(\beta')\| \leq {} & \left\| x' - X_n\left(\frac{1}{d}\right) - y_i\right\| \\ & + \|y_i - X_{n_i}(\beta_i)\| \\ & + \left\|X_n\left(\frac{1}{d}\right) + X_{n_i}(\beta_i) - X_n(\beta')\right\|.\end{aligned}$$

But

$$\begin{aligned} s_n(\beta'\gamma_j) &\equiv s_n\left(\frac{1}{d}\gamma_j\right) + s_n(p^{n-n_i}\beta_i\gamma_j) \\ &\equiv s_n\left(\frac{1}{d}\gamma_j\right) + p^{n-n_i}s_{n_i}(\beta_i\gamma_j) \pmod{qp^n} \end{aligned}$$

for $1 \leq j \leq r$. Therefore

$$X_n(\beta') \equiv X_n\left(\frac{1}{d}\right) + X_{n_i}(\beta_i) \pmod{1},$$

so the last term in the above sum vanishes. Hence

$$\|x' - x_n(\beta')\| < \varepsilon' + \varepsilon' + 0 = \frac{\varepsilon}{d},$$

so

$$\|\bar{x} - dX_n(\beta')\| < \varepsilon, \quad \text{and} \quad |\bar{x}_j - dq^{-1}p^{-n}s_n(\beta'\gamma_j)| < \varepsilon$$

for each j. Since $\bar{x}_j + \varepsilon < 1$ and $\bar{x}_j - \varepsilon > 0$ by assumption, $0 < ds_n(\beta'\gamma_j) < qp^n$. It follows that

$$s_n(d\beta'\gamma_j) = ds_n(\beta'\gamma_j) \equiv 0 \pmod{d}, \quad \text{and} \quad dX_n(\beta') = X_n(d\beta').$$

Since $n - n_i \geq m$, we have $d\beta' \equiv 1 \pmod{p^m}$. It follows that $\beta = d\beta'$ satisfies the conditions of the lemma. This completes the proof of Lemma 7.20. □

Remark. The location of the vector $X_n(\beta)$ depends on the coefficients of the p-adic expansions of the $\beta\gamma_j$'s near the nth digit. By the choice of $y_1, \ldots, y_D$, the vectors $X_{n_i}(\beta_i)$ are distributed throughout all of $(0, 1)^r$. Hence they give us a wealth of possible patterns of coefficients. We can add these onto existing patterns to obtain any desired pattern. In effect, this is accomplished by the term $p^{n-n_i}\beta_i$ in the definition of β'. This is what allows us to get close to $\bar{x}$ and also obtain the congruence mod d (cf. Ferrero–Washington [1]).

We can now prove Proposition 7.17. We cannot apply Lemma 7.20 directly since the elements of R' are not necessarily linearly independent. If R' is linearly independent ($\Leftrightarrow p$ is a Fermat prime) then the following argument can be simplified to yield the result. Therefore assume R' has dependence relations. If α is a primitive $(p-1)$st root of unity and $r = \phi(p-1)$, then $1, \alpha, \ldots, \alpha^{r-1}$ forms an integral basis for $\mathbb{Z}[\alpha]$. Consequently we may choose $\alpha_1, \ldots, \alpha_r \in R'$ (let $\alpha_{r+1}, \ldots, \alpha_t$, $t = (p-1)/2$, be the other elements) such that

$$\alpha_j = \sum_{i=1}^{r} a_{ji}\alpha_i, \qquad a_{ji} \in \mathbb{Z}, \qquad j = r+1, \ldots, t.$$

We may assume $a_{j1} \neq 0$ for some j. Order $\alpha_{r+1}, \ldots, \alpha_t$ lexicographically according to $|a_{ji}|$, $1 \leq i \leq r$. That is, let $\alpha_j > \alpha_l$ if for some i_0 we have $|a_{ji}| = |a_{li}|$ for $i < i_0$ and $|a_{ji_0}| > |a_{li_0}|$. Let α_{j_0} be a maximal element for this ordering (we do not care whether or not a_{j_0} is unique). If necessary, change the signs of $\alpha_1, \ldots, \alpha_r$ so that $a_{j_0 i} \geq 0$ for $1 \leq i \leq r$ (this changes R'). Note that $a_{j_0 1} \geq 1$ (since $a_{j1} \neq 0$ for some j) and $a_{j_0 i} > 0$ for some other i (since $\alpha_{j_0}/\alpha_i \notin \mathbb{Z}$). Now change the signs of α_j, $r + 1 \leq j \leq t$, if necessary, so that the first nonzero a_{ji}, $1 \leq i \leq r$, is positive for each such j.

Let $x_1, \ldots, x_r \in (0, 1)$ be such that x_i is much larger than x_{i+1} for each i. Define

$$x_j = \sum_{i=1}^{r} a_{ji} x_i, \quad r + 1 \leq j \leq t.$$

Since the first nonzero coefficient a_{ji} is positive and since x_i is much larger than x_{i+1}, x_{i+2}, etc., we must have $x_j > 0$ for each j. By the choice of j_0, $x_{j_0} > x_j$ for $r + 1 \leq j \leq t$, $j \neq j_0$ (even if α_{j_0} is not the unique maximal element, we have $a_{j_0 i} \geq 0$ for all i; so any other maximal element must have a negative coefficient, hence a smaller x_j). Also, $x_{j_0} > a_{j_0 1} x_1 \geq x_1$ (since $a_{j_0 i} > 0$ for some $i \neq 1$), so $x_{j_0} > x_i$ for $1 \leq i \leq r$.

Replacing x_i by cx_i for a suitable constant c, we may arrange that

$$0 < x_j < p^{-m} \quad \text{for } 1 \leq j \leq t, j \neq j_0,$$

and

$$p^{-m} < x_{j_0} < 2p^{-m}.$$

By Lemma 7.20, for all n sufficiently large there exists $\beta \equiv 1 \pmod{p^m}$ such that

$$|q^{-1}p^{-n}s_n(\beta\alpha_i) - x_i| < \varepsilon \quad (\varepsilon \text{ very small})$$

and

$$s_n(\beta\alpha_i) \equiv 0 \ (\mathrm{mod}\ d) \quad \text{for } i = 1, \ldots, r.$$

If ε is small enough,

$$0 < \sum_{i=1}^{r} a_{ji} q^{-1} p^{-n} s_n(\beta\alpha_i) < p^{-m} \quad \text{for } r + 1 \leq j \leq t, j \neq j_0,$$

and

$$p^{-m} < \sum_{i=1}^{r} a_{j_0 i} q^{-1} p^{-n} s_n(\beta\alpha_i) < 2p^{-m}.$$

Also,

$$\sum a_{ji} s_n(\beta\alpha_i) \equiv \sum a_{ji} \beta\alpha_i \ (\mathrm{mod}\ qp^n)$$

and satisfies the appropriate inequality, so

$$s_n(\beta\alpha_j) = s_n(\beta \sum a_{ji}\alpha_i) = \sum a_{ji} s_n(\beta\alpha_i).$$

Therefore

$$s_n(\beta\alpha_j) \equiv 0 \pmod{d} \quad \text{for } 1 \leq j \leq t,$$

and

$$0 < q^{-1}p^{-n}s_n(\beta\alpha_j) < p^{-m}, \qquad 1 \leq j \leq t, j \neq j_0,$$
$$p^{-m} < q^{-1}p^{-n}s_n(\beta\alpha_{j_0}) < 2p^{-m}.$$

For $j \neq j_0$ we have

$$0 < s_n(\beta\alpha_j) < qp^{n-m} \quad \text{and} \quad s_n(\beta\alpha_j) \equiv \beta\alpha_j \pmod{qp^{n-m}},$$

hence

$$s_n(\beta\alpha_j) = s_{n-m}(\beta\alpha_j).$$

Similarly,

$$0 < s_n(\beta\alpha_{j_0}) - qp^{n-m} < qp^{n-m},$$

and

$$s_n(\beta\alpha_{j_0}) - qp^{n-m} \equiv \beta\alpha_{j_0} \pmod{qp^{n-m}},$$

so

$$s_n(\beta\alpha_{j_0}) - qp^{n-m} = s_{n-m}(\beta\alpha_{j_0}).$$

Therefore β gives us β_2 in the statement of the proposition (change n to $n + m$ and change $n - m$ to n). To get β_1, let c be small enough that $0 < x_j < p^{-m}$ for all j, including j_0, then proceed as above. This completes the proof of Proposition 7.17. □

Notes

The construction given here is due to Iwasawa [18], [23]. For another approach, see Coates [7].

The proof that $\mu = 0$ had its origins in the work of Gold [1], who considered certain quadratic fields. Later progress appears in Ferrero [2]. The proof given above follows Oesterlé [1] (see also Gillard [5]). For a different, but equivalent, approach see the original paper by Ferrero–Washington [1], which also treats the simpler case of $\mathbb{Q}(\zeta_p)$ separately. The idea of the proof is summarized in Washington [10].

Iwasawa [24] has constructed examples of noncyclotomic $\mathbb{Z}_p$-extensions with $\mu > 0$.

For the non-p-part of the class number, see Washington [7]. For composites of cyclotomic $\mathbb{Z}_p$-extensions ($p = p_1, \ldots, p_s$), see Friedman [1].

For values of the λ-invariant, see Ernvall–Metsänkylä [1], Ferrero [3], Kida [1], and several of the papers of Gold. For a heuristic estimate of λ for $\mathbb{Q}(\zeta_p)$, see the appendix to Chapter 10 of Lang [5]. For upper bounds for λ, see Ferrero [1], Metsänkylä [12], and the end of Ferrero–Washington [1].

Exercises

7.1. Let $\mathcal{O}$ be a ring. Show that $f(T) \in \mathcal{O}[[T]]$ is a unit $\Leftrightarrow f(0) \in \mathcal{O}^\times$.

7.2. Using the fact that every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some n (Kronecker–Weber theorem), show that $\mathbb{B}_\infty/\mathbb{Q}$ is the only $\mathbb{Z}$-${}_p$extension of $\mathbb{Q}$ ($\mathbb{B}_\infty$ is defined after Theorem 7.14).

7.3. (a) Show that Theorems 7.13 and 7.14 can be generalized to any imaginary abelian field all of whose Dirichlet characters are of the first kind.
(b) Let K be an arbitrary abelian number field and let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension. Show that there is a field F, all of whose characters are of the first kind, such that for some $e \geq 0$ and all n sufficiently large $F_{n+e} = K_n$ (*Hint*: Let $\chi = \theta\psi$ run through the characters of K. Let F correspond to the group of θ's. Note that ψ's correspond to $\mathbb{B}$'s).
(c) Show that for arbitrary imaginary abelian K a modified version of Theorem 7.13 holds, and deduce Theorem 7.14 for K.

7.4. (a) Let $\chi \neq 1$ be an even character of the first kind. Show that the constant term of $f(T, \chi)$ is $-(1 - \chi\omega^{-1}(p))B_{1,\chi\omega^{-1}}$.
(b) Suppose p is regular. Show that $p \nmid h^-(\mathbb{Q}(\zeta_{p^n}))$ for all n (note that for $p = 2$ we have an empty product in Theorem 7.13, so the result is trivially true!).
(c) Let K be an imaginary abelian field. Show that $\lambda^- \geq \#\{\chi \mid \chi$ is odd and $\chi(p) = 1\}$.
(d) The class number of $\mathbb{Q}(\sqrt{-5})$ is 2, and 3 splits in $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. Show that although $3 \nmid h(K_0)$, we have $3 \mid h(K_n)$ for all $n \geq 1$, where K_∞/K_0 is the $\mathbb{Z}_3$-extension of $K_0 = \mathbb{Q}(\sqrt{-5})$.

7.5. Suppose $\chi \neq 1$ is not a character of the second kind (but also not necessarily of the first kind). Show that for $n \geq 1$, $(1/n)B_{n,\chi\omega^{-n}}$ is p-integral, and if $m \equiv n \pmod{p^a}$ then

$$(1 - \chi\omega^{-m}(p)p^{m-1})\frac{B_{m,\chi\omega^{-m}}}{m} \equiv (1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n} \pmod{p^{a+1}}$$

(this of course contains the Kummer congruences).

7.6. (a) Suppose $\chi = 1$. Show that

$$f(0, 1) \equiv \frac{1}{p} \pmod{\mathbb{Z}_p},$$

hence that

$$g(0, 1) \equiv -1 \pmod{p} \quad \text{if } p \neq 2, \qquad g(0, 1) \equiv 2 \pmod{4} \quad \text{if } p = 2.$$

(b) Show that $1 - (1 + q)^n \equiv -nq \pmod{nqp\mathbb{Z}_p}$.
(c) (von Staudt–Clausen) Show that if $p - 1 \mid n$ then $B_n \equiv -(1/p) \pmod{\mathbb{Z}_p}$.
(d) More generally, show that for $n \geq 1$, $B_{n,\omega^{-n}} \equiv -(1/p) \pmod{\mathbb{Z}_p}$.

7.7. Suppose $\chi \neq 1$ is of the second kind and of conductor qp^m. Show that for $n \geq 1$,

$$\frac{B_{n,\chi\omega^{-n}}}{n} \equiv \frac{q}{p}\frac{1}{1 - \zeta^{-1}} \left(\text{mod}\ \frac{q}{p}\mathbb{Z}_p\right),$$

where $\zeta = \chi(1 + q)$.

7.8. Let R' be as defined in this chapter. Show that R' is linearly independent over $\mathbb{Q} \Leftrightarrow (p - 1)/2 = \phi(p - 1) \Leftrightarrow p$ is a Fermat prime.

7.9. (a) Show that $\beta \in \mathbb{Z}_p$ is normal $\Leftrightarrow$ the sequence $q^{-1}p^{-n}s_n(\beta)$ is uniformly distributed mod 1.

(b) Let $\gamma_1, \ldots, \gamma_r \in \mathbb{Z}_p$. Figure out a suitable definition of "joint normality" and show that it is equivalent to the sequence of vectors

$$(q^{-1}p^{-n}s_n(\gamma_1), \ldots, q^{-1}p^{-n}s_n(\gamma_r))$$

being uniformly distributed mod 1.

(c) Show that if $\gamma_1, \ldots, \gamma_r$ are linearly dependent over $\mathbb{Q}$ then they cannot be jointly normal.

7.10. Let k_0 be a function field over a finite field and let k_∞/k_0 be the "cyclotomic" $\mathbb{Z}_p$-extension. Let $l \neq p$ be another prime and let l^{e_n} be the exact power of l dividing $h(k_n)$. Show that e_n is bounded as $n \to \infty$. (The analogous result has been proved for cyclotomic $\mathbb{Z}_p$-extensions of abelian number fields. The proof involves uniform distribution mod 1, but works directly with the class number formula, rather than with Iwasawa's power series. See Washington [7]).

Chapter 8

Cyclotomic Units

The determination of the unit group of an algebraic number field is rather difficult in general. However, for cyclotomic fields, it is possible to give explicitly a group of units, namely the cyclotomic units, which is of finite index in the full unit group. Moreover, this index is closely related to the class number, a fact which allows us to prove Leopoldt's p-adic class number formula. Finally, we study more closely the units of the pth cyclotomic field, and give relations with p-adic L-functions and with Vandiver's conjecture.

§8.1 Cyclotomic Units

Let $n \not\equiv 2 \bmod 4$ and let V_n be the multiplicative group generated by

$$\{\pm\zeta_n, 1 - \zeta_n^a \mid 1 < a \leq n - 1\}.$$

Let E_n be the group of units of $\mathbb{Q}(\zeta_n)$ and define

$$C = C_n = V_n \cap E_n.$$

C is called the group of cyclotomic units of $\mathbb{Q}(\zeta_n)$. More generally, if K is an abelian number field, we can define the cyclotomic units of K by letting $K \subseteq \mathbb{Q}(\zeta_n)$ with n minimal and defining $C_K = E_K \cap C_n$. This works well for $\mathbb{Q}(\zeta_n)^+$. For other K, it is perhaps better to take norms, from $\mathbb{Q}(\zeta_n)$ to K, of cyclotomic units. See (Sinnott [2]).

Since the real units multiplied by roots of unity are of index 1 or 2 in the full group of units (Theorem 4.12), it will usually be sufficient to work with real units. The following observation will be useful:

$$\zeta_n^{(1-a)/2}\frac{1-\zeta_n^a}{1-\zeta_n} = \pm\frac{\sin(\pi a/n)}{\sin(\pi/n)}$$

is real, and if a is changed to $-a$ then we obtain the same unit multiplied by -1.

Lemma 8.1. *Let p be prime and $m \geq 1$.*

(a) *The cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$ are generated by -1 and the units*

$$\xi_a = \zeta_{p^m}^{(1-a)/2}\frac{1-\zeta_{p^m}^a}{1-\zeta_{p^m}}, \qquad 1 < a < \tfrac{1}{2}p^m, (a, p) = 1.$$

(b) *The cyclotomic units of $\mathbb{Q}(\zeta_{p^m})$ are generated by ζ_{p^m} and the cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$.*

Proof. Let $\zeta = \zeta_{p^m}$. The definition of the cyclotomic units involves $1 - \zeta^a$ for all $a \not\equiv 0 \bmod p^m$. If $k < m$ and $(b, p) = 1$, then, using the relation $1 - X^{p^k} = \prod (1 - \zeta^{p^{m-k}}X)$, we obtain

$$1 - \zeta^{bp^k} = \prod_{j=0}^{p^k-1}(1 - \zeta^{b+jp^{m-k}}).$$

Since $(p, b + jp^{m-k}) = 1$, we are reduced to considering only those a with $(a, p) = 1$. Also, $1 - \zeta^a$ and $1 - \zeta^{-a}$ differ only by a power of ζ, so we need only consider $1 \leq a < \frac{1}{2}p^m$. Suppose now that

$$\xi = \pm\zeta^d \prod_{\substack{1 < a < \frac{1}{2}p^m \\ (a,p)=1}} (1 - \zeta^a)^{c_a}$$

is a unit of $\mathbb{Q}(\zeta)$. Since the ideals $(1 - \zeta^a)$ are all the same, $\sum c_a = 0$. Therefore

$$\xi = \pm\zeta^d \prod \left(\frac{1-\zeta^a}{1-\zeta}\right)^{c_a}$$
$$= \pm\zeta^e \prod_{a\neq 1} \xi_a,$$

where $e = d + \frac{1}{2}\sum c_a(a - 1)$. Note that if $p = 2$ then $(a, p) = 1$ requires a to be odd, so ζ^e is in $\mathbb{Q}(\zeta)$ in all cases. This completes the proof of (*b*). If $\xi \in \mathbb{Q}(\zeta)^+$ then since each factor in the above product is real, $\pm\zeta^e$ must be real, hence ± 1. This completes the proof. □

Remark. If n is not a prime power, not every cyclotomic unit is a product of roots of unity and numbers of the form $(1 - \zeta_n^a)/(1 - \zeta_n)$ with $(a, n) = 1$. Namely, each such product is a real unit times a root of unity, while the cyclotomic unit $1 - \zeta_n$ is not of this form (see the proof of Corollary 4.13).

Our goal is to show that the cyclotomic units are of finite index in the full group of units. It suffices to work in the real subfield. We start with the important, and easier, case of prime powers.

Theorem 8.2. *Let p be a prime and $m \geq 1$. The cyclotomic units $C_{p^m}^+$ of $\mathbb{Q}(\zeta_{p^m})^+$ are of finite index in the full unit group $E_{p^m}^+$, and*

$$h_{p^m}^+ = [E_{p^m}^+ : C_{p^m}^+],$$

where $h_{p^m}^+$ is the class number of $\mathbb{Q}(\zeta_{p^m})^+$.

Proof. We shall show that the regulator of the units ξ_a of Lemma 8.1 is nonzero. Let $\zeta = \zeta_{p^m}$. As usual, let $\sigma_a : \zeta \to \zeta^a$ be in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. The elements σ_a, $1 \leq a < \frac{1}{2}p^m$, $(a, p) = 1$, yield $G = \mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})$. We may write

$$\xi_a = \frac{(\zeta^{-1/2}(1-\zeta))^{\sigma_a}}{\zeta^{-1/2}(1-\zeta)}$$

(if $p = 2$, extend σ_a to $\mathbb{Q}(\zeta_{2^{m+1}})$. Everything below works, since

$$|(\zeta^{-1/2}(1-\zeta))^{\sigma_a}|$$

is all that matters, and it is independent of the choice of the extension). We now apply Lemma 5.26. Let

$$f(\sigma) = \log|(\zeta^{-1/2}(1-\zeta))^{\sigma}| = \log|(1-\zeta)^{\sigma}|, \qquad \sigma \in G.$$

Then the regulator is

$$\begin{aligned} R(\{\xi_a\}) &= \pm\det[\log|\xi_a^{\tau}|]_{a,\tau\neq 1} \\ &= \pm\det[f(\sigma\tau) - f(\tau)]_{\sigma,\tau\neq 1} \\ &= \pm\det[f(\tau\sigma^{-1}) - f(\tau)]_{\sigma,\tau\neq 1} \\ &= \pm\prod_{\substack{\chi\neq 1\\ \chi\in\hat{G}}} \sum_{\sigma\in G} \chi(\sigma)\log|(1-\zeta)^{\sigma}| \\ &= \pm\prod \sum_{1\leq a<\frac{1}{2}p^m} \chi(a)\log|1-\zeta^a| \\ &= \pm\prod \frac{1}{2}\sum_{a=1}^{p^m} \chi(a)\log|1-\zeta^a|. \end{aligned}$$

If $f_\chi = p^k$ with $1 \leq k \leq m$, then, using the relation

$$\prod_{\substack{1<a<p^m\\ a\equiv b(p^k)}} (1-\zeta_{p^m}^a) = 1-\zeta_{p^k}^b,$$

we obtain

$$\begin{aligned} \sum_{a=1}^{p^m} \chi(a)\log|1-\zeta^a| &= \sum_{b=1}^{p^k} \chi(b)\log|1-\zeta_{p^k}^b| \\ &= -\frac{f_\chi}{\tau(\bar{\chi})} L(1,\bar{\chi}) = -\tau(\chi)L(1,\bar{\chi}). \end{aligned}$$

Therefore,

$$R(\{\xi_a\}) = \pm \prod_{\chi \neq 1} -\tfrac{1}{2}\tau(\chi)L(1, \bar{\chi}) = h^+R^+ \neq 0,$$

where R^+ is the regulator of $\mathbb{Q}(\zeta_{p^m})^+$ (we have used Corollary 4.6 to handle $\tau(\chi)$). Therefore the $\pm\xi_a$'s generate a subgroup, namely C^+, of finite index in the full group of units, and

$$[E_{p^m}^+ : C_{p^m}^+] = \frac{R(\{\xi_a\})}{R^+} = h^+$$

by Lemma 4.14. This completes the proof. □

Remark. This result should be regarded as the analogue for h^+ of Theorem 6.19. A similar question arises: is E^+/C^+ isomorphic to the ideal class group of $\mathbb{Q}(\zeta_{p^m})^+$ as modules over $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})^+/\mathbb{Q})]$? Let $p \equiv 1 \bmod 4$, so $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)^+$. Since $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}(\sqrt{p})$ is totally ramified, the norm map on the ideal class groups is surjective (see the appendix on class field theory). Also, the norm of E^+ is contained in the units of $\mathbb{Q}(\sqrt{p})$, hence $N(E^+)/N(C^+)$ is either cyclic or $(\mathbb{Z}/2\mathbb{Z}) \times$ (cyclic). Therefore, if E^+/C^+ is isomorphic to the ideal class group as modules over the Galois group, then the ideal class group of $\mathbb{Q}(\sqrt{p})$ must be cyclic (since $p \equiv 1 \bmod 4$, the 2-part is trivial). For $p = 62501$, Schaffstein found that the class group is $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Therefore, the isomorphism does not always hold. Whether or not there is an isomorphism as abelian groups appears to be an open question. Finding nontrivial examples appears to be difficult since $h_n^+ = 1$ for small n and for large n the calculations required to determine E^+ or the class group are extremely lengthy. The next question is whether or not the p-part of E^+/C^+ is isomorphic to the p-Sylow subgroup of the class group of $\mathbb{Q}(\zeta_{p^m})^+$. In this case, it is hard to know what to expect. Vandiver's conjecture predicts that the p-Sylow subgroup of the class group, hence of both groups, is trivial. This is true for $p < 125000$, but it is not clear that it should be true in general. Recent work of Mazur and Wiles on the "Main Conjecture" has yielded the following: Decompose the p-Sylow $(E^+/C^+)_p$ of E^+/C^+ and the p-Sylow A of the ideal class group of $\mathbb{Q}(\zeta_p)$ via the idempotents ε_i of Chapter 6. Then

$$|\varepsilon_i(E^+/C^+)_p| = |\varepsilon_i A|.$$

We shall return to $\mathbb{Q}(\zeta_p)$ later, but now we treat the case of $\mathbb{Q}(\zeta_n)$ for general n. We do not give a set of independent generators for the full group of cyclotomic units. However, we exhibit a set of independent units that generate a subgroup of finite index, which suffices to show that the cyclotomic units have finite index. One's first guess for a set of independent units would probably be

$$\zeta_n^{(1-a)/2}\frac{1-\zeta_n^a}{1-\zeta_n}, \qquad 1 < a < \tfrac{1}{2}n, (a, n) = 1.$$

This set has $\frac{1}{2}\phi(n) - 1$ elements and is the obvious generalization of Lemma 8.1. Unfortunately, this set does not always work. We shall show below

(Corollary 8.8) that there are sometimes multiplicative dependence relations. Therefore, we use a set of units discovered by Ramachandra.

Theorem 8.3. *Let $n \not\equiv 2 \bmod 4$, and let $n = \prod_{i=1}^{s} p_i^{e_i}$ be its prime factorization. Let I run through all subsets of $\{1, \ldots, s\}$, except $\{1, \ldots, s\}$, and let $n_I = \prod_{i \in I} p_i^{e_i}$. For $1 < a < \frac{1}{2}n$, $(a, n) = 1$, define*

$$\xi_a = \zeta_n^{d_a} \prod_I \frac{1 - \zeta_n^{an_I}}{1 - \zeta_n^{n_I}}, \qquad d_a = \tfrac{1}{2}(1 - a) \sum_I n_I.$$

Then $\{\xi_a\}$ forms a set of multiplicatively independent units for $\mathbb{Q}(\zeta_n)^+$. If C_n' denotes the group generated by -1 and the ξ_a's, and E_n^+ denotes the group of units of $\mathbb{Q}(\zeta_n)^+$, then

$$[E_n^+ : C_n'] = h_n^+ \prod_{\chi \neq 1} \prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i)) \neq 0,$$

where h_n^+ is the class number of $\mathbb{Q}(\zeta_n)^+$ and χ runs through the nontrivial even characters of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Remarks. The difference between the units $(1 - \zeta^a)/(1 - \zeta)$ and the present units is that these new ones contain contributions from the units of proper subfields.

We have not obtained generators for the full group of cyclotomic units of $\mathbb{Q}(\zeta_n)^+$. Sinnott has calculated the index of the full group of cyclotomic units to be

$$[E_n^+ : C_n^+] = 2^b h_n^+,$$

where $b = 0$ if $g = 1$ and $b = 2^{g-2} + 1 - g$ if $g \geq 2$, and g is the number of distinct prime factors of n. See (Sinnott [1]).

Proof of Theorem 8.3. The proof will be similar in many ways to that of Theorem 8.2, but will be more technical. As in the proof of that theorem, we have

$$R(\{\xi_a\}) = \pm \prod_{\chi \neq 1} \frac{1}{2} \sum_{\substack{a=1 \\ (a,n)=1}}^{n} \chi(a) \sum_I \log|1 - \zeta_n^{an_I}|,$$

where χ runs through the nontrivial even characters mod n. Clearly, this product should reduce to an expression involving $\prod L(1, \chi)$, but there are a few problems: n might not be f_χ, the restriction $(a, n) = 1$ may leave out some terms with $(a, n) \neq 1$ but $(a, f_\chi) = 1$, and $\zeta_n^{n_I}$ is not necessarily ζ_{f_χ}. The following lemmas treat these difficulties.

Lemma 8.4. *If $f_\chi \nmid (n/m)$ then*

$$\sum_{\substack{a=1 \\ (a,n)=1}}^{n} \chi(a) \log|1 - \zeta_n^{am}| = 0.$$

PROOF. We claim that there exists $b \equiv 1 \bmod (n/m)$ such that $(b, n) = 1$ and $\chi(b) \neq 1$. If not, then $\chi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ may be factored through $(\mathbb{Z}/(n/m)\mathbb{Z})^\times$, so $f_\chi | (n/m)$, contradiction. Since $\zeta_n^{am} = \zeta_n^{abm}$,

$$\begin{aligned}\sum \chi(a) \log|1 - \zeta_n^{am}| &= \sum \chi(a) \log|1 - \zeta_n^{abm}| \\ &= \chi(b)^{-1} \sum \chi(a) \log|1 - \zeta_n^{am}|,\end{aligned}$$

so the sum vanishes. □

Lemma 8.5. *Let $n = mm'$ with $(m, m') = 1$, and suppose $f_\chi | m$. Then*

$$\sum_{\substack{a=1 \\ (a,n)=1}}^{n} \chi(a) \log|1 - \zeta_n^{am'}| = \phi(m') \sum_{\substack{b=1 \\ (b,m)=1}}^{m} \chi(b) \log|1 - \zeta_m^b|$$

PROOF. Write $a = b + cm$ with $1 \le b < m$, $0 \le c < m'$. If $(a, n) = 1$ then $(b, m) = 1$. Conversely, for each b with $(b, m) = 1$ there are $\phi(m')$ choices of c such that $(b + cm, m') = 1$, hence $(b + cm, n) = 1$ (since $(m, m') = 1$). Since $\chi(a)$ and $\zeta_n^{am'}$ depend only on b, the lemma follows. □

Lemma 8.6. *Suppose F, g, t are positive integers with $f_\chi | F$ and $g | F$. Then*

$$\sum_{\substack{a=1 \\ (a,g)=1}}^{Ft} \chi(a) \log|1 - \zeta_{Ft}^a| = \sum_{\substack{b=1 \\ (b,g)=1}}^{F} \chi(b) \log|1 - \zeta_F^b|.$$

PROOF. Write $a = b + cF$, $1 \le b \le F$, $0 \le c < t$. Then $(a, g) = 1 \Leftrightarrow (b, g) = 1$. Since

$$\prod_{c=0}^{t-1} (1 - \zeta_{Ft}^{b+cF}) = 1 - \zeta_F^b,$$

and since $\chi(a)$ depends only on b, the lemma follows easily. □

Lemma 8.7. *Assume $f_\chi | m$. Then*

$$\sum_{\substack{b=1 \\ (b,m)=1}}^{m} \chi(b) \log|1 - \zeta_m^b| = \left[\prod_{p|m} (1 - \chi(p))\right] \sum_{b=1}^{m} \chi(b) \log|1 - \zeta_m^b|.$$

PROOF. Let $p, q, \ldots$ represent the primes dividing m. We only need to consider those which do not divide f_χ. The right-hand side equals

$$\begin{aligned}&\sum_{b=1}^{m} \chi(b) \log|1 - \zeta_m^b| - \sum_p \chi(p) \sum_{b=1}^{m} \chi(b) \log|1 - \zeta_m^b| \\ &\qquad + \sum_{\substack{p,q \\ p \neq q}} \chi(pq) \sum_{b=1}^{m} \chi(b) \log|1 - \zeta_m^b| - \cdots \\ &= \sum_{b=1}^{m} \chi(b) \log|1 - \zeta_m^b| - \sum_p \chi(p) \sum_{b=1}^{m/p} \chi(b) \log|1 - \zeta_{m/p}^b| + \cdots\end{aligned}$$

(by Lemma 8.6 with $g = 1$. Since $p \nmid f_\chi$, we have $f_\chi | m/p$)

$$= \sum_{b=1}^{m} \chi(b) \log|1 - \zeta_m^b| - \sum_p \sum_{\substack{b=1 \\ p|b}}^{m} \chi(b) \log|1 - \zeta_m^b| + \cdots$$

$$= \sum_{\substack{b=1 \\ (b,m)=1}}^{m} \chi(b) \log|1 - \zeta_m^b|$$

(e.g., if $pq|b$ then $\sum_p$ subtracts the term for b twice but $\sum_{p \neq q}$ adds it back once; this is essentially the relation $\sum_{j=0}^{n} (-1)^j \binom{n}{j} = 0$ if $n > 0$).

This completes the proof of Lemma 8.7. □

We may now finish the proof of Theorem 8.3. If $m' = n_I$ for some I then $n = mm'$ with $(m, m') = 1$. If $f_\chi | m$ then

$$\sum_{\substack{a=1 \\ (a,n)=1}}^{n} \chi(a) \log|1 - \zeta_n^{am'}| = \phi(m') \sum_{\substack{b=1 \\ (b,m)=1}}^{m} \chi(b) \log|1 - \zeta_m^b|$$

$$= \phi(m')\left[\prod_{p|m}(1 - \chi(p))\right] \sum_{b=1}^{m} \chi(b) \log|1 - \zeta_m^b|$$

$$= \phi(m')\left[\prod_{p|m}(1 - \chi(p))\right] \sum_{a=1}^{f_\chi} \chi(a) \log|1 - \zeta_{f_\chi}^a|$$

$$= -\phi(m') \frac{f_\chi}{\tau(\bar{\chi})} L(1, \bar{\chi}) \prod_{p|m} (1 - \chi(p))$$

$$= -\phi(m')\tau(\chi)L(1, \bar{\chi}) \prod_{p|m} (1 - \chi(p)).$$

Therefore (let $n = n_I n_I'$, so $n_I = m'$ and $n_I' = m$)

$$\sum_{\substack{a=1 \\ (a,n)=1}}^{n} \chi(a) \sum_I \log|1 - \zeta_n^{an_I}| = -\tau(\chi)L(1, \bar{\chi}) \sum_{\substack{I \\ f_\chi | n_I'}} \phi(n_I) \prod_{p | n_I'} (1 - \chi(p)).$$

Consequently

$$R(\{\xi_a\}) = \pm \prod_{\chi \neq 1} \tfrac{1}{2}\tau(\chi)L(1, \bar{\chi}) \sum_{\substack{I \\ f_\chi | n_I'}} \phi(n_I) \prod_{p | n_I'} (1 - \chi(p))$$

$$= h_n^+ R_n^+ \prod_{\chi \neq 1} \left(\sum_{\substack{I \\ f_\chi | n_I'}} \phi(n_I) \prod_{p | n_I'} (1 - \chi(p)) \right),$$

where h_n^+ and R_n^+ are the class number and regulator of $\mathbb{Q}(\zeta_n)^+$, respectively.

Recall $n = \prod_{i=1}^{s} p_i^{e_i}$. We claim that

$$\sum_{\substack{I \\ f_\chi | n_I'}} \phi(n_I) \prod_{p | n_I'} (1 - \chi(p)) = \prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i)).$$

If the right-hand side is expanded out, we obtain

$$\sum_J \phi\left(\sum_{i \in J} p_i^{e_i}\right) \prod_{i \notin J} (1 - \chi(p_i)),$$

where J runs through all subsets of $\{i \mid p_i \nmid f_\chi\}$. If $p \mid f_\chi$ then $1 - \chi(p_i) = 1$. Therefore we enlarge the set of $i \notin J$ to include all $i \notin J$ with $1 \leq i \leq s$. If we let $n_J = \prod_{i \in J} p_i^{e_i}$ and $n'_J = \prod_{i \notin J} p_i^{e_i}$ then we obtain

$$\sum_J \phi(n_J) \prod_{p \mid n'_J} (1 - \chi(p)).$$

Since J is included in the sum $\Leftrightarrow (n_J, f_\chi) = 1 \Leftrightarrow f_\chi \mid n'_J$, the claim is proved. Note that $f_\chi \neq 1 \Rightarrow n_J \neq 1 \Rightarrow J \neq \{1, \ldots, s\}$, as required.

Finally, since the real part of $\phi(p_i^{e_i}) + 1 - \chi(p_i)$ is positive, the above product is nonzero. Since the index $[E_n^+ : C'_n]$ is the ratio of regulators $R(\{\xi_a\})/R_n^+$, the proof of Theorem 8.3 is complete. □

Corollary 8.8. *Let C''_n be the group generated by* -1 *and the units of the form*

$$\zeta_n^{(1-a)/2} \frac{1 - \zeta_n^a}{1 - \zeta_n}, \qquad 1 < a < \tfrac{1}{2}n, (a, n) = 1.$$

Then

$$[E_n^+ : C''_n] = h_n^+ \prod_{\chi \neq 1} \prod_{p \mid n} (1 - \chi(p)),$$

where χ runs through the nontrivial even characters mod n, *and the index is infinite if the right-hand side is* 0.

Proof. The regulator of C''_n is

$$\pm \prod_{\chi \neq 1} \frac{1}{2} \sum_{\substack{a=1 \\ (a,n)=1}}^{n} \chi(a) \log|1 - \zeta_n^a|.$$

By the above calculations (plus Lemmas 8.7 and 8.6), we find that this expression equals

$$\pm \prod_{\chi \neq 1} \left[\tfrac{1}{2}\tau(\chi) L(1, \bar{\chi}) \prod_{p \mid n} (1 - \chi(p)) \right] = h_n^+ R_n^+ \prod_{\chi \neq 1} \prod_{p \mid n} (1 - \chi(p)).$$

This completes the proof. □

It is easy to see that there are many examples where C''_n is not of maximal rank. For example, if $n = 55$, then 11 splits in $\mathbb{Q}(\sqrt{5})$, so $\chi(11) = 1$ for the quadratic character of conductor 5. Therefore $[E_{55}^+ : C''_{55}]$ is infinite. If n has 4 distinct prime factors then the index is automatically infinite (see Exercises).

In the above, we have used only two basic relations, namely

$$1-\zeta_n^{-a}=-\zeta_n^{-a}(1-\zeta_n^a)$$

and

$$1-\zeta_m^a=\prod_{j=0}^{(n/m)-1}(1-\zeta_n^{a+mj})\quad \text{if } m\mid n.$$

The following theorem of Bass shows that these generate almost all relations.

Theorem 8.9. *Let $n \not\equiv 2 \bmod 4$ and let $(A_n^0)^+$ be the additive abelian group with generators*

$$\left\{g\left(\frac{a}{n}\right)\,\middle|\,\frac{a}{n}\in\frac{1}{n}\mathbb{Z}/\mathbb{Z},\ \frac{a}{n}\neq 0\right\}$$

and relations

$$g\left(\frac{-a}{n}\right)=g\left(\frac{a}{n}\right)$$

and

$$g\left(\frac{a}{m}\right)=\sum_{j=0}^{(n/m)-1}g\left(\frac{a+mj}{n}\right)\quad \textit{if } m\mid n \text{ (and } a/m\neq 0).$$

Let $\tilde{C}_n$ be the group generated by $\{1-\zeta_n^a \mid 1\le a<n\}$. ($\tilde{C}_n$ contains some nonunits). Then, for some c, there is an exact sequence

$$0\to(\mathbb{Z}/2\mathbb{Z})^c\to(A_n^0)^+\to\tilde{C}_n/\langle\pm\zeta_n\rangle\to 0,$$

where

$$g\left(\frac{a}{n}\right)\mapsto 1-\zeta_n^a \bmod\langle\pm\zeta_n\rangle.$$

Proof. The proof uses distributions, hence will be postponed until Chapter 12.

§8.2 Proof of the p-adic Class Number Formula

In order to prove the p-adic class number formula (Theorem 5.24), we study the units of an arbitrary totally real abelian number field K of degree r over $\mathbb{Q}$. Let $K\subseteq\mathbb{Q}(\zeta_n)^+$ and let N be the norm from $\mathbb{Q}(\zeta_n)^+$ to K. Let E_n^+ and E_K be the respective unit groups, and C_n^+ and C_K the cyclotomic units (we can take $C_K=E_K\cap C_n^+$ or $N(C_n^+)$; either definition works here). If $\varepsilon\in E_K$ then $N\varepsilon=\varepsilon^d$, where $d=\deg(\mathbb{Q}(\zeta_n)^+/K)$. Therefore $N(E_n^+)$ contains E_K^d, hence is of finite index in E_K. Since $[E_n^+ : C_n^+]$ is finite, and $N(C_n^+)\subseteq C_K$, it follows that $[E_K : C_K]$ is finite. But we need to be more explicit.

Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)^+/\mathbb{Q}) = \{\sigma_a \mid 1 \le a < \frac{1}{2}n,\ (a, n) = 1\}$, and let $H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)^+/K)$. Then $G/H = \mathrm{Gal}(K/\mathbb{Q})$. Let $R \subseteq G$ be a set of coset representatives for G/H and $R' \subset R$ a set of representatives for $G/H - \{H\}$. In Theorem 8.3,

$$\xi_a = \zeta_n^{d_a}\frac{\alpha^{\sigma_a}}{\alpha}, \quad \text{where } \alpha = \prod_I (1 - \zeta_n^{n_I}).$$

Letting $\beta = N(\alpha)$, we have $N(\xi_a) = \zeta_n^{d_a'}(\beta^{\sigma_a}/\beta)$ with $d_a' \in \mathbb{Z}$. Clearly $\beta^{\sigma_a}/\beta = \beta^{\sigma_b}/\beta$ if $\sigma_a\sigma_b^{-1} \in H$. So we only need to consider

$$\{N\xi_a \mid \sigma_a \in R'\}.$$

We have

$$\begin{aligned} R(\{N\xi_a\}) &= \pm\det(\log|N\xi_a^{\sigma}|)_{\substack{a \in R' \\ \sigma \in G/H,\, \sigma \ne 1}} \\ &= \pm\det(\log|\beta^{\sigma\sigma_a}| - \log|\beta^{\sigma}|) \\ &= \pm\det(\log|\beta^{\sigma\tau^{-1}}| - \log|\beta^{\sigma}|)_{\substack{\sigma, \tau \in G/H \\ \sigma, \tau \ne 1}} \\ &= \pm \prod_{\substack{\chi \in (G/H)^\wedge \\ \chi \ne 1}} \sum_{\sigma \in G/H} \chi(\sigma)\log|\beta^{\sigma}| \qquad \text{(Lemma 5.26)} \\ &= \pm \prod_{\chi \ne 1} \sum_{\sigma} \chi(\sigma) \sum_{\tau \in H} \log|\alpha^{\sigma\tau}|. \end{aligned}$$

Extending χ to G by letting $\chi(H) = 1$, we obtain

$$\pm \prod_{\chi \ne 1} \sum_{\sigma \in G} \chi(\sigma)\log|\alpha^{\sigma}| = \pm \prod_{\chi \ne 1} \frac{1}{2} \sum_{\substack{a = 1 \\ (a, n) = 1}} \chi(a)\log|\alpha^{\sigma_a}|.$$

But these factors are exactly the ones that were evaluated in Theorem 8.3. Therefore, as before,

$$\begin{aligned} R(\{N\xi_a\}) &= \pm \prod_{\chi \ne 1}\left[\tfrac{1}{2}\tau(\chi)L(1, \bar{\chi}) \prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i))\right] \\ &= h_K R_K \prod_{\chi \ne 1} \prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i)) \ne 0, \end{aligned}$$

so the group generated by $\{N\xi_a\}$ and -1 has index

$$i_K = h_K \prod_{\chi \ne 1} \prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i))$$

in the full group of units.

Observe that the preceding calculation of $R(\{N\xi_a\})$ would have worked just as well with $\log_p$ in place of log, except for the use of the relation

$$\prod_{\chi \ne 1} L(1, \chi) = \frac{2^{r-1}h_K R_K}{\sqrt{d_K}}.$$

Also note that (Theorem 5.18)

$$\sum_{a=1}^{f_\chi} \chi(a)\log_p(1-\zeta_{f_\chi}^a) = -\left(1-\frac{\bar{\chi}(p)}{p}\right)^{-1}\tau(\chi)L_p(1,\bar{\chi}),$$

so an Euler factor appears in the calculations. Therefore

$$\begin{aligned} R_p(\{N\xi_a\}) &= \pm\prod_{\chi\neq 1}\left[\tfrac{1}{2}\tau(\chi)\left(1-\frac{\bar{\chi}(p)}{p}\right)^{-1}L_p(1,\bar{\chi})\prod_{p_i\nmid f_\chi}(\phi(p_i^{e_i})+1-\chi(p_i))\right] \\ &= \pm\frac{i_K}{h_K}2^{1-r}\sqrt{d_K}\prod_{\chi\neq 1}\left(1-\frac{\bar{\chi}(p)}{p}\right)^{-1}L_p(1,\bar{\chi}). \end{aligned}$$

But

$$i_K = \frac{R_p(\{N\xi_a\})}{R_{K,p}} \quad (p\text{-adic version of Lemma 4.14}),$$

so

$$\pm\frac{2^{r-1}h_K R_{K,p}}{\sqrt{d_K}} = \prod_{\chi\neq 1}\left(1-\frac{\chi(p)}{p}\right)^{-1}L_p(1,\chi).$$

Since $R_{K,p}$ is only determined up to sign, we may choose $R_{K,p}$ so as to eliminate the " ± ". This completes the proof of Theorem 5.24. □

§8.3 Units of $\mathbb{Q}(\zeta_p)$ and Vandiver's Conjecture

We now study more closely the units of $\mathbb{Q}(\zeta_p)$ for p an odd prime. Let $\zeta = \zeta_p$ and let $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. The characters of G are of the form ω^i, $0 \le i \le p-2$, where ω is the Teichmüller character. Correspondingly, we have the idempotents

$$\varepsilon_i = \frac{1}{p-1}\sum_{a=1}^{p-1}\omega^i(a)\sigma_a^{-1} = \frac{1}{p-1}\sum_{a=1}^{p-1}\omega^{-i}(a)\sigma_a \in \mathbb{Z}_p[G].$$

It is easy to see that

$$\sum_{i=0}^{p-2}\varepsilon_i = 1 \quad\text{and}\quad \varepsilon_i\varepsilon_j = \begin{cases}\varepsilon_i, & i=j\\ 0, & i\neq j.\end{cases}$$

Let E be the units of $\mathbb{Q}(\zeta_p)$. For $N>0$, let

$$E_{p^N} = E/E^{p^N}$$

Usually we shall take N sufficiently large; if we wanted to, we could take the inverse limit for $N \to \infty$, but this is not necessary. Since $E = WE^+$, where W is the group of roots of unity, we have

$$E/E^{p^N} \simeq \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p^N\mathbb{Z})^{(p-3)/2}, \quad \text{as groups.}$$

We wish to study the action of G, and $\mathbb{Z}_p[G]$, on E_{p^N}. If $\eta \in E_{p^N}$ and $a \in \mathbb{Z}_p$ then η^a is defined in the natural way: let $a \equiv a_0 \bmod p^N$ with $a_0 \in \mathbb{Z}$; then $\eta^a = \eta^{a_0}$. Consequently ε_i acts on E_{p^N} for each i, so

$$E_{p^N} = \bigoplus_{i=0}^{p-2} \varepsilon_i E_{p^N}.$$

We now analyze each summand. First, suppose $i = 0$. Then ε_0 is just a multiple of the norm, hence

$$\varepsilon_0 E_{p^N} \subseteq \text{Norm}(E_{p^N}) \subseteq 1 \bmod E^{p^N} = 1.$$

Next, let i be arbitrary. Let $\eta \in E$, so $\eta = \zeta^r \eta_0$, where $r \in \mathbb{Z}$ and $\bar{\eta}_0 = \eta_0$. Since $\sigma_a(\zeta) = \zeta^{\omega(a)}$, and since this equation characterizes $\varepsilon_1 E_{p^N}$, the subgroup generated by ζ lies in $\varepsilon_1 E_{p^N}$. Now consider the real unit η_0:

$$\varepsilon_i(\eta_0)^{p-1} \equiv \prod_{a=1}^{p-1} \sigma_a^{-1}(\eta_0)^{\omega^i(a)} \bmod E^{p^N}$$

If i is odd, $\omega^i(a) = -\omega^i(-a)$ while $\sigma_a^{-1}(\eta_0) = \sigma_{-a}^{-1}(\eta_0)$. The factors for a and $-a$ cancel, so $\varepsilon_i(\eta_0) \equiv 1 \bmod E^{p^N}$. We have proved the following.

Proposition 8.10.

$$E_{p^N} = \langle\zeta\rangle \oplus \bigoplus_{\substack{i=2 \\ i \text{ even}}}^{p-3} \varepsilon_i E_{p^N} \quad \textit{and} \quad E_{p^N}^+ = E^+/(E^+)^{p^N} = \bigoplus_{\substack{i=2 \\ i \text{ even}}}^{p-3} \varepsilon_i E_{p^N}^+$$

($\langle\zeta\rangle = \varepsilon_1 E_{p^N}$ is the subgroup generated by ζ). □

Note that $E_{p^N}^+$ is a direct sum of $(p - 3)/2$ cyclic groups of order p^N (by the Dirichlet Unit Theorem) and that there are $(p - 3)/2$ summands in the above formula. One therefore might expect that each summand is a cyclic group. We shall show that this is the case, using the cyclotomic units.

Proposition 8.11. *Let g be a primitive root* mod p^n. *Then*

$$\zeta_{p^n}^{(1-g)/2} \frac{1 - \zeta_{p^n}^g}{1 - \zeta_{p^n}}$$

generates $C_{p^n}^+$ as a module over $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta_{p^n})^+/\mathbb{Q})]$.

Proof. During this proof, let $\zeta = \zeta_{p^n}$. Let $(a, p) = 1$. Then $a \equiv g^r \bmod p^n$ for some $r > 0$, so

$$\zeta^{(1-a)/2}\frac{1-\zeta^a}{1-\zeta} = \zeta^{(1-g^r)/2}\frac{1-\zeta^{g^r}}{1-\zeta} = \prod_{i=0}^{r-1}\zeta^{(g^i-g^{i+1})/2}\frac{1-\zeta^{g^{i+1}}}{1-\zeta^{g^i}}$$

$$= \prod_{i=0}^{r-1}\left(\zeta^{(1-g)/2}\frac{1-\zeta^g}{1-\zeta}\right)^{\sigma_g^i}.$$

The result follows from Lemma 8.1. □

Remark. The above works for $p = 2$ if we let $g \equiv 5 \bmod 8$ and note that either $a \equiv g^r$ or $-a \equiv g^r \bmod 2^n$.

Actually, Proposition 8.11 is a more explicit version of Lemma 5.27.

Fix the primitive root g mod p and let i be even, $2 \le i \le p - 3$. Let

$$\omega_N(a) \equiv \omega(a) \bmod p^N, \qquad \omega_N(a) \in \mathbb{Z}.$$

Define

$$E_i^{(N)} = \prod_{a=1}^{p-1}\left(\zeta^{(1-g)/2}\,\frac{1-\zeta^g}{1-\zeta}\right)^{\omega_N(a)^i\sigma_a^{-1}},$$

so

$$E_i^{(N)} \equiv \left(\zeta^{(1-g)/2}\frac{1-\zeta^g}{1-\zeta}\right)^{(p-1)\varepsilon_i} \bmod (E^+)^{p^N}.$$

and

$$E_i^{(N)} \in \varepsilon_i E^+_{p^N}$$

In particular, define

$$E_i \overset{\text{def}}{=} E_i^{(1)} = \prod_{a=1}^{p-1}\left(\zeta^{(1-g)/2}\frac{1-\zeta^g}{1-\zeta}\right)^{a^i\sigma_a^{-1}}$$

$$\equiv \prod_{a=1}^{p-1}\left(\zeta^{a(1-g)/2}\frac{1-\zeta^{ag}}{1-\zeta^a}\right)^{a^{p-1-i}} \bmod (E^+)^p$$

(change a to a^{-1} and note $\sigma_a\zeta = \zeta^a$).

Since $\omega_N(a) \equiv a \bmod p$ it follows that

$$E_i^{(N)} \text{ is a } p\text{th power} \Leftrightarrow E_i \text{ is a } p\text{th power}.$$

This fact will prove useful in the following. For technical reasons it will often be convenient to let N be large. But we still obtain information about the case $N = 1$. Since $\log_p \zeta = 0$, we have (change a to a^{-1})

$$\begin{aligned}\log_p E_i^{(N)} &= \sum_{a=1}^{p-1} \omega_N(a^{-1})^i \log_p\left(\frac{1-\zeta^{ag}}{1-\zeta^a}\right)\\ &\equiv \sum_{a=1}^{p-1} \omega(a)^{-i} \log_p\left(\frac{1-\zeta^{ag}}{1-\zeta^a}\right) (\text{mod } p^N)\end{aligned}$$

(since $\log_p \mathbb{Q}(\zeta_p) \subseteq \mathbb{Z}_p[\zeta_p]$; see Exercise 5.15(*c*))

$$\equiv -(\omega^i(g) - 1)\tau(\omega^{-i})L_p(1, \omega^i) \, (\text{mod } p^N).$$

From Proposition 6.13, we know that $v_p(\tau(\omega^{-i})) = i/(p-1)$ (see also Exercise 8.12). Since $\omega^i(g) - 1 \equiv g^i - 1 \not\equiv 0 \bmod p$, we have proved the following.

Proposition 8.12. *If* $N \geq 1 + v_p(L_p(1, \omega^i))$, *then*

$$v_p(\log_p E_i^{(N)}) = \frac{i}{p-1} + v_p(L_p(1, \omega^i)). \qquad \square$$

Proposition 8.13. *Let* $N \geq 1$ *and let* i *be even*, $2 \leq i \leq p-3$. *Then*

$$\varepsilon_i E_{p^N}^+ \simeq \mathbb{Z}/p^N\mathbb{Z}.$$

Proof. Since $L_p(1, \omega^i) \neq 0$, $E_i^{(N)} \neq 1$, hence $\varepsilon_i E_{p^N}^+ \neq 0$, for large N. Since $E_{p^N}^+ \simeq (\mathbb{Z}/p^N\mathbb{Z})^{(p-3)/2}$, and $\varepsilon_i E_{p^N}^+$ is a direct summand, $\varepsilon_i E_{p^N}^+ \simeq (\mathbb{Z}/p^N\mathbb{Z})^{a_i}$, for some $a_i \geq 1$. But $\sum a_i = (p-3)/2$, so each $a_i = 1$. This proves the proposition for large N.

If N is arbitrary (i.e., smaller), we may choose $M \geq N$ large and take a quotient. Then

$$\varepsilon_i E_{p^N}^+ \simeq \varepsilon_i(E_{p^M}^+/(E_{p^M}^+)^{p^N}) \simeq \mathbb{Z}/p^N\mathbb{Z},$$

as desired. $\square$

Recall that $h^+ = [E^+ : C^+]$. Let $C_{p^N}^+$ be the group generated by C^+ mod$(E^+)^{p^N}$. If $p^N > h^+$ then

$$(E^+/C^+)_p \simeq E_{p^N}^+/C_{p^N}^+,$$

where, for a finite abelian group A, we let $(A)_p$ denote its p-Sylow subgroup. From Proposition 8.11, $\varepsilon_i C_{p^N}^+$ is generated by the unit $E_i^{(N)}$, so

$$(E^+/C^+)_p \simeq \bigoplus_{\substack{i=2\\ i \text{ even}}}^{p-3} \varepsilon_i E_{p^N}^+/\langle E_i^{(N)}\rangle.$$

Since $\varepsilon_i E_{p^N}^+$ is a cyclic group of p-power order, the ith summand is nontrivial if and only if $E_i^{(N)}$ is a pth power. Since $E_i^{(N)}$ is a pth power if and only if E_i is a pth power, we obtain the following important result.

Theorem 8.14. *$p \mid h^+(\mathbb{Q}(\zeta_p)) \Leftrightarrow$ some E_i (i even, $2 \le i \le p-3$) is a pth power of a unit of $\mathbb{Q}(\zeta_p)^+$.* □

Corollary 8.15. *If $p \nmid h^+(\mathbb{Q}(\zeta_p))$ then the E_i's generate $E^+/(E^+)^p$ (this is also obvious from Theorem 8.2).* □

Theorem 8.16. *E_i is a pth power $\Rightarrow p \mid B_i$.*

Proof. We may replace E_i with $E_i^{(N)}$ for N sufficiently large. If $E_i^{(N)} = \eta^p$ then $\log_p E_i^{(N)} = p \log_p \eta$. Since $\log_p \eta \in \mathbb{Z}_p[\zeta_p]$ (cf. Exercise 5.15(c)),

$$1 \le v_p(\log_p E_i^{(N)}) = \frac{i}{p-1} + v_p(L_p(1, \omega^i)),$$

so

$$v_p(L_p(1, \omega^i)) > 0.$$

Since

$$L_p(1, \omega^i) \equiv L_p(1 - i, \omega^i) \equiv -\frac{B_i}{i} \pmod p$$

by Corollary 5.13, we have $p \mid B_i$. This completes the proof. □

Remark. The converse is not true. In fact, for $p < 125000$, $p \nmid h^+$, so E_i is not a pth power.

Corollary 8.17. *$p \mid h^+(\mathbb{Q}(\zeta_p)) \Rightarrow p \mid h^-(\mathbb{Q}(\zeta_p))$ (this is the same as Theorem 5.33).*

Proof. Theorems 8.14, 8.16, and 5.16. □

We have mentioned that $p \nmid h^+(\mathbb{Q}(\zeta_p))$ for $p < 125000$. The way this is verified (on a computer) is via the corollary of the following result. Its advantage is that it uses only rational arithmetic, hence is suitable for computer calculations.

Proposition 8.18. *Let i be even, $2 \le i \le p-3$. Let l be a prime with $l \equiv 1$ mod p, say $l = kp + 1$, and let t be an integer satisfying $(t, l) = 1$ and $t^k \not\equiv 1$ mod l. Define*

$$d = d_i = 1^{p-i} + 2^{p-i} + \cdots + \left(\frac{p-1}{2}\right)^{p-i}$$

and

$$Q_i = t^{-kd/2} \prod_{b=1}^{(p-1)/2} (t^{kb} - 1)^{b^{p-1-i}}.$$

Let $\tilde{l}$ be the prime of $\mathbb{Q}(\zeta_p)$ above l such that $t^k \equiv \zeta_p \bmod \tilde{l}$ (see the discussion following Proposition 2.14). Then

$$Q_i^k \equiv 1 \bmod l \Leftrightarrow E_i \textit{ is a } p\textit{th power} \bmod \tilde{l}.$$

Proof. Let $R_i = \prod_{a=1}^{p-1} (\zeta^{a/2} - \zeta^{-a/2})^{a^{p-1-i}}$. Recall that g is a primitive root mod p. Changing a to ag, we find that

$$R_i = \prod_{a=1}^{p-1} (\zeta^{ag/2} - \zeta^{-ag/2})^{(ag)^{p-1-i}} \cdot (p\text{th power}),$$

so

$$R_i^{g^i-1} = \prod_{a=1}^{p-1} \left(\frac{\zeta^{ag/2} - \zeta^{-ag/2}}{\zeta^{a/2} - \zeta^{-a/2}}\right)^{a^{p-1-i}} \cdot (p\text{th power})$$
$$= E_i A^p \text{ for some } A \in \mathbb{Q}(\zeta)^\times.$$

Note that the only prime ideal which can divide R_i is $(1 - \zeta)$; therefore $R_i \equiv 0 \bmod \tilde{l}$ will never happen. Since $(g^i - 1, p) = 1$, E_i is a pth power mod $\tilde{l}$ if and only if R_i is a pth power mod $\tilde{l}$. The terms for a and $p - a$ in the definition of R_i differ by a pth power (note $-1 = (-1)^p$), so we may combine terms and find that R_i is a pth power mod $\tilde{l}$ if and only if the same holds for

$$\prod_{b=1}^{(p-1)/2} (\zeta^{b/2} - \zeta^{-b/2})^{b^{p-1-i}} = \zeta^{-d/2} \prod_{b=1}^{(p-1)/2} (\zeta^b - 1)^{b^{p-1-i}}.$$

Since $t^k \not\equiv 1 \bmod l$ but $t^{kp} = t^{l-1} \equiv 1 \bmod l$, t^k is a pth root of unity mod l. Proposition 2.14 yields the prime ideal $\tilde{l}$ of $\mathbb{Q}(\zeta)$ lying above l such that $t^k \equiv \zeta \bmod \tilde{l}$. Since $(\mathbb{Z}[\zeta]/\tilde{l})^\times$ is cyclic of order $l - 1 = kp$, it follows that $Q_i^k \equiv 1 \bmod l$, or mod $\tilde{l}$, if and only if Q_i is a pth power mod $\tilde{l}$. Since

$$Q_i \equiv \zeta^{-d/2} \prod_{b=1}^{(p-1)/2} (\zeta^b - 1)^{b^{p-1-i}} \bmod \tilde{l},$$

the proof is complete. □

Corollary 8.19. *Let p be an irregular prime and let $i_1, \ldots, i_s$ be the even indices $2 \le i \le p - 3$ such that $p \mid B_i$. Suppose there exists a prime $l \equiv 1 \bmod p$ and an integer t, as in Proposition 8.18, such that $Q_i^k \not\equiv 1 \bmod l$ for all $i \in \{i_1, \ldots, i_s\}$. Then $p \nmid h^+(\mathbb{Q}(\zeta_p))$.*

Proof. Theorems 8.14 and 8.16, and Proposition 8.18. □

Remark. Of course, we could have used a different prime l for each index i, but the above form is what will be needed in Chapter 9 when we treat Fermat's Last Theorem. The converse of Corollary 8.19 is also true. Suppose $p \nmid h^+$. Then none of the E_i's are pth powers. The density of the prime ideals $\tilde{l}$ such that a given E_i is a pth power mod $\tilde{l}$ is $1/p$ by the Tchebotarev Density Theorem. Since there are less than p units E_i, there must be infinitely many $\tilde{l}$

such that none of the E_i's are pth powers mod $\tilde{l}$. As usual, only primes $\tilde{l}$ with residue class degree 1 over $\mathbb{Q}$ need to be considered, but these are precisely the primes that lie over rational primes $l \equiv 1 \bmod p$. Proposition 8.18 now applies and we have $Q_i^k \not\equiv 1 \bmod l$ for all i, for an appropriate choice of t.

Remark. *Vandiver's conjecture* states that $p \nmid h^+(\mathbb{Q}(\zeta_p))$ for all p (Serge Lang has pointed out that the conjecture actually originated with Kummer: in a letter to Kronecker, Kummer refers to $p \nmid h^+$ as a "noch zu beweisenden Satz" (see Kummer's *Collected Works*, vol. I, p. 85)). The conjecture has been verified for all $p < 125000$. What are the chances that it is true in general? First, consider a probability argument similar to that used for h^- in Section 5.3. Suppose each E_i is a pth power with probability $1/p$. There are $(p-3)/2$ indices i, so the probability that $p \nmid h^+$ would be

$$\left(1 - \frac{1}{p}\right)^{(p-3)/2} \rightarrow e^{-1/2} = 0.6065\ldots.$$

This does not agree at all with the numerical evidence, Perhaps, then, is there something yet undiscovered which causes the E_i's to be non-pth powers? If so, could this force be strong enough to make Vandiver's conjecture true for all p? This question remains open. Another probability argument that could be used is a refinement of the above. Since the only E_i's which can possibly be pth powers occur when $p \mid B_i$, we consider only such indices i and suppose that the probability of being a pth power is again $1/p$. The index of irregularity should take on the value k with probability $e^{-1/2}/2^k k!$ (see the discussion following Theorem 5.17), so the number of exceptions to Vandiver's conjecture for $p \leq x$ should be approximately

$$\begin{aligned}
&\sum_{p \leq x} \sum_{k=0}^{\infty} (\text{Prob. } i(p) = k)(\text{Prob. some } E_i \text{ is a } p\text{th power}) \\
&= \sum_{p \leq x} \sum_{k=0}^{\infty} \left(\frac{e^{-1/2}}{2^k k!}\right)\left(1 - \left(1 - \frac{1}{p}\right)^k\right) \\
&= \sum_{p \leq x} (1 - e^{-1/2p}) \sim \sum_{p \leq x} \frac{1}{2p} \sim \tfrac{1}{2} \log \log x.
\end{aligned}$$

Since $\frac{1}{2} \log \log(125000) = 1.23 \ldots$, it is not surprising that no exceptions have been found. Moreover, most of the contributions to this sum come from the first few primes. If we started the sum at the first irregular prime $p = 37$, we would obtain a much smaller number.

Finally, we could use a more naive approach. Suppose $p \mid h^+$ with probability $1/p$. Then the number of exceptions to Vandiver's conjecture for $p \leq x$ should be

$$\sum_{p \leq x} \frac{1}{p} \sim \log \log x.$$

The comments for the previous approach apply here also. However, another point arises. For h^- we used Bernoulli numbers which were much larger than p. Hence it was reasonable to expect that they were random mod p. But it is possible that h^+ is often small. In fact, very little is known about h^+. For small values of p, $h^+ = 1$. For some p we know $h^+ > 1$. For example $3 | h_{257}^+$ since $h(\mathbb{Q}(\sqrt{257})) = 3$. But, at present, for each p with $h^+ > 1$ we do not know the exact value. The computer calculations would be too lengthy. In any case, assuming h^+ is random mod p is rather dangerous.

Whether or not Vandiver's conjecture is always true, the above arguments indicate that it should hold for most primes. In Chapter 10, several important consequences of the conjecture will be given.

§8.4 p-adic Expansions

We now examine the p-adic expansions of units. Our main goal is to prove Theorem 8.22. Let $\zeta = \zeta_p$ and let

$$\pi = \zeta - 1 \quad \text{and} \quad \lambda = (\zeta - 1)(\zeta^{-1} - 1) = 2 - (\zeta + \zeta^{-1}),$$

so (π) and (λ) are the prime ideals lying above p in $\mathbb{Z}[\zeta]$ and $\mathbb{Z}[\zeta + \zeta^{-1}]$, respectively. Note that any element of $\mathbb{Z}[\zeta + \zeta^{-1}] = \mathbb{Z}[\lambda]$ is congruent to a rational integer mod λ. Since $(\lambda)^{(p-1)/2} = (p)$, we have

$$\lambda^{(p-1)/2} = \alpha p + \beta \lambda p + \cdots \quad \text{with } \alpha, \beta \in \mathbb{Z}.$$

Let $\eta \neq \pm 1$ be a real unit. We may write

$$\eta = a + b\lambda^c + d\lambda^{c+1} + \cdots$$

where $p \nmid ab$ and $c \not\equiv 0 \bmod (p-1)/2$ (if $p | b$, add $(p-1)/2$ to c. If $c \equiv 0$, use the formula for $\lambda^{(p-1)/2}$ above, and then modify a. If $p | a$, then η is not a unit). Note that c is the largest integer n such that η is congruent to a rational integer mod λ^n. Hence c is uniquely determined by η. The integers a and b are unique mod λ^{c+1} and mod p, respectively.

With the above notation, we may use Exercise 5.14 to conclude that

$$v_p(\log_p \eta) = \frac{2c}{p-1},$$

so this gives us a method for determining c. For example, if N is large enough, Proposition 8.12 imples that

$$E_i^{(N)} \equiv a_i + b_i \lambda^{c_i} \bmod \lambda^{c_i + 1}$$

with

$$c_i = \frac{i}{2} + \frac{p-1}{2} v_p(L_p(1, \omega^i)).$$

Proposition 8.20. *Let i be even, $2 \le i \le p-3$. If $N > 2c/(p-1)$ and*

$$\eta = a + b\lambda^c + \cdots \in \varepsilon_i E^+_{p^N}$$

then

$$c \equiv \frac{i}{2} \bmod \frac{p-1}{2}.$$

PROOF. Let $(\alpha, p) = 1$. Since $\pi^{\sigma_\alpha} = \zeta^\alpha - 1 = (\pi + 1)^\alpha - 1 = \alpha\pi + \cdots$, it follows that

$$\sigma_\alpha(\lambda) \equiv \alpha^2\lambda \bmod \lambda^2 \quad \text{and} \quad \sigma_\alpha(\lambda^c) \equiv \alpha^{2c}\lambda^c \bmod \lambda^{c+1}.$$

Therefore

$$\sigma_\alpha(\eta) \equiv a + b\alpha^{2c}\lambda^c \bmod \lambda^{c+1}.$$

From Exercise 5.14,

$$\log_p \eta \equiv \frac{b}{c}\lambda^c \bmod \lambda^{c+1},$$

$$\log_p \eta^{\sigma_\alpha} \equiv \frac{b\alpha^{2c}}{a}\lambda^c \bmod \lambda^{c+1}.$$

Since $\eta \in \varepsilon_i E^+_{p^N}$,

$$\log_p \eta^{\sigma_\alpha} \equiv \omega^i(\alpha) \log_p \eta \bmod p^N.$$

Since $N > 2c/(p-1)$, we obtain

$$\omega^i(\alpha)\frac{b}{a}\lambda^c \equiv \frac{b\alpha^{2c}}{a}\lambda^c \bmod \lambda^{c+1},$$

hence

$$\omega^i(\alpha) \equiv \alpha^{2c} \bmod p, \quad \text{for all } (\alpha, p) = 1.$$

Therefore $i \equiv 2c \bmod (p-1)$, as desired. □

Lemma 8.21. *Let i be even, $2 \le i \le p-3$, and let $\tilde{\eta}_i$ be a generator for $\varepsilon_i E^+_{p^N}$. If $N \ge 1 + v_p(L_p(1, \omega^i))$ then*

$$\tilde{\eta}_i \equiv a_i' + b_i'\lambda^{c_i'} \bmod \lambda^{c_i'+1}\left(p \nmid a_i'b_i',\ c_i' \not\equiv 0 \bmod \frac{p-1}{2}\right)$$

with

$$c_i' \le \frac{i}{2} + \frac{p-1}{2} v_p(L_p(1, \omega^i)).$$

PROOF. We have $E_i^{(N)} = \tilde{\eta}_i^{d_i}\gamma^{p^N}$ for some $d_i \in \mathbb{Z}$, $\gamma \in E^+$. Therefore

$$\log_p E_i^{(N)} \equiv d_i \log_p \tilde{\eta}_i \bmod p^N.$$

By Proposition 8.12,

$$v_p(\log_p E_i^{(N)}) = \frac{i}{p-1} + v_p(L_p(1, \omega^i)) < N.$$

Therefore

$$v_p(\log_p E_i^{(N)}) = v_p(d_i \log_p \tilde{\eta}_i) \geq v_p(\log_p \tilde{\eta}_i),$$

so

$$c_i' = \frac{p-1}{2} v_p(\log_p \tilde{\eta}_i) \leq \frac{i}{2} + \frac{p-1}{2} v_p(L_p(1, \omega^i)), \text{ as desired.} \qquad \square$$

Remark. Since $v_p(d_i) = v_p(\log_p E_i^{(N)}) - v_p(\log_p \tilde{\eta}_i) = [2/(p-1)](c_i - c_i')$, we have from the discussion preceding Theorem 8.14,

$$v_p(h^+(\mathbb{Q}(\zeta_p))) = \frac{2}{p-1} \sum_{\substack{i=2 \\ i\,\text{even}}}^{p-3} (c_i - c_i').$$

We may now generalize Theorem 5.36 (see also Exercise 5.7).

Theorem 8.22. *Let $M = \max_i v_p(L_p(1, \omega^i))$, where i is even, $2 \leq i \leq p-3$. If η is a unit of $\mathbb{Z}[\zeta_p]$ which is congruent to a rational integer* mod p^{M+1} *then η is a pth power of a unit.*

Proof. As in the proof of Theorem 5.35, we may assume η is real. Write

$$\eta = a + b\lambda^c + \cdots.$$

Then, by hypothesis,

$$c > \frac{p-1}{2}(M+1), \quad \text{so } v_p(\log_p \eta) = \frac{2c}{p-1} > M + 1.$$

Let $N \geq M + 1$ and let $\tilde{\eta}_2, \ldots, \tilde{\eta}_{p-3}$ be as in Lemma 8.21. We may write

$$\eta = \gamma^{p^N} \prod \tilde{\eta}_i^{g_i}$$

with $g_i \in \mathbb{Z}, \gamma \in E^+$. We shall show that $p | g_i$ for all i. Since

$$\frac{2c_i'}{p-1} = v_p(\log_p \tilde{\eta}_i) \equiv \frac{i}{p-1} \bmod 1$$

by Proposition 8.20, it follows that the numbers $v_p(g_i \log_p \tilde{\eta}_i)$ are distinct mod 1, hence distinct. Therefore

$$v_p(\sum g_i \log_p \tilde{\eta}_i) = \min v_p(g_i \log_p \tilde{\eta}_i).$$

Also,

$$\begin{aligned} v_p(\sum g_i \log_p \tilde{\eta}_i) &= v_p(\log_p \eta - p^N \log_p \gamma) \\ &\geq \min(v_p(\log_p \eta), v_p(p^N \log_p \gamma)) \\ &\geq \min(M+1, N) = M + 1. \end{aligned}$$

Therefore, for each i, the above, plus Lemma 8.21, yields

$$M + 1 \leq v_p(g_i \log_p \tilde{\eta}_i) \leq v_p(g_i) + \frac{i}{p-1} + v_p(L_p(1, \omega^i)) < v_p(g_i) + 1 + M.$$

Consequently $v_p(g_i) > 0$ for each i and η is a pth power. This completes the proof. □

Corollary 8.23. *Suppose $p^3 \nmid B_{pi}$ for all even i, $2 \leq i \leq p-3$. If η is a unit of $\mathbb{Z}[\zeta_p]$ which is congruent to a rational integer* mod p^2 *then η is a pth power.*

Proof. By Theorem 5.12,

$$L_p(s, \omega^i) = a_0 + a_1(s-1) + \cdots$$

with $a_i \in \mathbb{Z}_p$ for all i, and $p \mid a_i$ for $i \geq 1$. Therefore

$$\begin{aligned} -\frac{B_{pi}}{pi} &\equiv -(1 - p^{pi-1})\frac{B_{pi}}{pi} = L_p(1 - pi, \omega^i) \\ &\equiv a_0 = L_p(1, \omega^i) \bmod p^2. \end{aligned}$$

If $p^3 \nmid B_{pi}$ then $v_p(L_p(1, \omega^i)) \leq 1$, so $M \leq 1$. The result now follows from the theorem. □

We have been considering local properties of global units. As a final result, we consider the global units as a subgroup of the local units. We continue to assume p is an odd prime. Let

$$U_1 = \{x \in \mathbb{Z}_p[\lambda] \mid x \equiv 1 \bmod \lambda\}.$$

Then U_1 is a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)^+/\mathbb{Q})]$-module, so

$$U_1 = \prod_{\substack{i=0 \\ i \text{ even}}}^{p-3} \varepsilon_i U_1.$$

Let

$$U_1' = \prod_{\substack{i=2 \\ i \text{ even}}}^{p-3} \varepsilon_i U_1.$$

Since the norm to $\mathbb{Q}_p$ is $(p-1)\varepsilon_0$,

$$U_1' = \{x \in U_1 \mid \mathrm{Norm}(x) = 1\}.$$

Lemma 8.24. *Let i be even, $2 \leq i \leq p-3$. Then $\varepsilon_i U_1$ is a cyclic $\mathbb{Z}_p$-module with*

$$\xi_i = (1 + \lambda^{i/2})^{(p-1)\varepsilon_i}$$

as a generator.

Proof. As in the proof of Proposition 8.20,

$$\sigma_\alpha(\lambda^{i/2}) \equiv \alpha^i\lambda^{i/2} \bmod \lambda^{i/2+1}$$

Therefore

$$\begin{aligned}(1 + \lambda^{i/2})^{(p-1)\varepsilon_i} &= 1 + \left(\sum_{\alpha=1}^{p-1} \omega^{-i}(\alpha)\alpha^i\right)\lambda^{i/2} + \cdots \\ &\equiv 1 - \lambda^{i/2} \bmod \lambda^{i/2+1}.\end{aligned}$$

It is easy to see that any set of elements whose λ-adic expansions start with

$$1 - \lambda^{i/2}, \qquad i = 2, 4, \ldots, p-3,$$

plus the element $\xi_0 = 1 + p$, may be used as a set of $\mathbb{Z}_p$-generators of U_1. Since $\xi_i \in \varepsilon_i U_1$ for all i, including 0, we must have $\varepsilon_i U_1$ generated by ξ_i, as desired. □

Let $C_1^+ = C^+ \cap U_1 = C^+ \cap U_1'$ (if $\eta \in C^+ \cap U_1$ then $\varepsilon_0(\eta)$ is a power of Norm(η), hence equals 1. Therefore $C^+ \cap U_1 = C^+ \cap U_1'$). If $\eta \in C^+$ then $\eta^{p-1} \in C_1^+$. If N is chosen large enough that $C^+ \cap (E^+)^{p^N} \subseteq (C^+)^p$, then $E_2^{(N)}, \ldots, E_{p-3}^{(N)}$ generate $C^+/(C^+)^p$, hence

$$(E_2^{(N)})^{p-1}, \ldots, (E_{p-3}^{(N)})^{p-1} \text{ generate } C_1^+/(C_1^+)^p.$$

The standard recursive procedure shows that C_1^+ is contained in the $\mathbb{Z}_p$-submodule of U_1 generated by these elements; therefore the closure $\bar{C}_1^+$ of C_1^+ in U_1 is exactly the $\mathbb{Z}_p$-submodule generated by the $(E_i^{(N)})^{p-1}$, $i = 2, 4, \ldots, p-3$.

Theorem 8.25. *Let i be even, $2 \leq i \leq p-3$. Then*

$$[\varepsilon_i U_1' : \varepsilon_i \bar{C}_1^+] = p^{v_p(L_p(1,\omega^i))}.$$

Proof. Let d be the index, which must be a power of p since we are working with $\mathbb{Z}_p$-modules. Let ξ_i be as in Lemma 8.24 and let $(E_i^{(N)})^{p-1}$ be as above. Then

$$\xi_i^d = (E_i^{(N)})^{(p-1)u},$$

where u is a p-adic unit. Consequently (with N sufficiently large),

$$v_p(d \log_p \xi_i) = v_p(\log_p E_i^{(N)}) = \frac{i}{p-1} + v_p(L_p(1, \omega^i)).$$

But $\log_p \xi_i = \log_p(1 - \lambda^{i/2} + \cdots) = -\lambda^{i/2} \bmod \lambda^{i/2+1}$ (cf. Lemma 5.5), so

$$v_p(\log_p \xi_i) = \frac{i}{p-1}.$$

Therefore $v_p(d) = v_p(L_p(1, \omega^i))$. The proof is complete. □

Corollary 8.26. $\operatorname{Res}_{s=1} \zeta_{\mathbb{Q}(\zeta_p)^+, p}(s) = (1 - 1/p)[U_1' : \bar{C}_1^+] \cdot u$, *where u is a p-adic unit.*

Proof. We know from Chapter 5 that the residue is

$$\left(1 - \frac{1}{p}\right) \prod L_p(1, \omega^i).$$

The result now follows easily from the theorem. □

The above results will be generalized in Chapter 13.

Notes

Theorem 8.2 is due to Kummer [4]. Many of the results in this chapter had their origins in his work, and also in that of Vandiver. The index of the cyclotomic units in the general case of $\mathbb{Q}(\zeta_n)$ has been determined by Sinnott [1], [2], [3]. Other results have been obtained by Leopoldt [2] and C.-G. Schmidt [2]. For the case of function fields, see Galovich–Rosen [1].

The cyclotomic units can be used to obtain information about class numbers, especially their parity. See D. Davis [1], Garbanati [1], Schertz [1], and several papers of G. Gras and M.-N. Gras.

For elliptic analogues of cyclotomic units, see the papers of Robert, Gillard, and Kersey.

For a nonnumber-theoretic application, see Plymen [1].

Vandiver states that he conjectured $p \nmid h_p^+$ in Vandiver [1]. Kummer tried but was unable to prove the conjecture (Letter to Kronecker, April 24, 1853; *Collected Papers*, vol. I, 123–124).

The last section is from Washington [8], which is based on ideas of Dénes [1], [2], [3].

Exercises

8.1. Suppose $p \nmid h^+(\mathbb{Q}(\zeta_p))$ but $p \mid h^-(\mathbb{Q}(\zeta_p))$ (such p are called "properly irregular"). Show that there exists a unit in $\mathbb{Q}(\zeta_p)$, in fact one of the E_i's, which is congruent to a rational integer mod p but which is not a pth power.

8.2. Let ξ_a be as in Lemma 8.1. Show that

$$\xi_a = \pm\sqrt{\frac{(1 - \zeta^a)(1 - \zeta^{-a})}{(1 - \zeta)(1 - \zeta^{-1})}}$$

8.3. Let p be odd and let N be the norm from $\mathbb{Q}(\zeta_p)^+$ to $\mathbb{Q}$.
(a) Show that $\xi_a = \zeta_p^{(1-a)/2}(\zeta_p^a - 1)/(\zeta_p - 1) \equiv a \bmod (\zeta_p - 1)$.
(b) Show that $N(\xi_a) \equiv a^{(p-1)/2} \bmod p$.
(c) Show that if the Legendre symbol $(a/p) = -1$ then $N(\xi_a) = -1$.
(d) Let $p \equiv 1 \bmod 4$ and let ε be the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Show that $\operatorname{Norm}(\varepsilon) = -1$, where the norm is from $\mathbb{Q}(\sqrt{p})$ to $\mathbb{Q}$.

8.4. Let N be the norm from $\mathbb{Q}(\zeta_{p^{n+1}})$ to $\mathbb{Q}(\zeta_{p^n})$. Show
(a) $N(\zeta^a_{p^{n+1}} - 1) = \zeta^a_{p^n} - 1$, $(a, p) = 1$;
(b) $N(\zeta^a_{p^{n+1}}) = \zeta^a_{p^n}$;
(c) $N : C_{p^{n+1}} \to C_{p^n}$ and $N : C^+_{p^{n+1}} \to C^+_{p^n}$ are surjective.

8.5. Show that $[E : C] = [E^+ : C^+]$ for $\mathbb{Q}(\zeta_n)$.

8.6. Let $\tilde{C}_n$ be as in Theorem 8.9. Show $\pm\zeta_n \in \tilde{C}_n$.

8.7. Corollary 8.8 implies that there is a relation in C''_{39}. Find one.

8.8. Let $n \not\equiv 2 \bmod 4$ have at least 4 distinct prime factors, say $p < q < r < s$. Show that at least one of the quadratic characters χ of $(\mathbb{Z}/qrs\mathbb{Z})^\times$ is even and satisfies $\chi(p) = 1$. Conclude that $[E^+_n : C''_n]$ is infinite in the notation of Corollary 8.8. Show, however, that if $n = 3 \cdot 7 \cdot 11$ then the index is finite.

8.9. Suppose $p \nmid h^+(\mathbb{Q}(\zeta_p))$. Let $i_1, \ldots, i_s$ be the irregular indices. Show that the extension

$$\mathbb{Q}(\zeta_p, E^{1/p}_{i_1}, \ldots, E^{1/p}_{i_s})/\mathbb{Q}(\zeta_p)$$

is unramified (see Exercise 9.3) and has Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^s$. Under the assumption $p \nmid h^+$, s is the rank of the ideal class group (Corollary 10.14), so this shows how to generate the "p-elementary" Hilbert class field of $\mathbb{Q}(\zeta_p)$. In fact, for $p < 125000$ the ideal class group is $(\mathbb{Z}/p\mathbb{Z})^s$, so we get the entire Hilbert class field.

8.10. Suppose we have units $\eta_2, \eta_4, \ldots, \eta_{p-3}$ of $\mathbb{Q}(\zeta_p)^+$ such that

$$\eta_i \equiv a_i + b_i\lambda^{c_i} \bmod \lambda^{c_i+1}, \qquad p \nmid a_i b_i,$$

and suppose the c_i are distinct $\bmod (p-1)/2$ (for example, $c_i \equiv i/2$). Let $g_2, \ldots, g_{p-3}$ be integers. Show that

$$\prod_{i=2}^{p-3} \eta_i^{g_i} \equiv a + b\lambda^c \bmod \lambda^{c+1}$$

with $p \nmid ab$ and with $c = \min_i (c_i + [(p-1)/2]v_p(g_i))$.

8.11. For $i = 2, 4, \ldots, p-3$, let $E_i = a_i + b_i\lambda^{c_i}$ (mod λ^{c_i+1}), with $p \nmid a_i b_i$ and $c_i \not\equiv 0$ (mod $p-1$). Suppose $p \nmid B_i$. Show that $c_i = i/2$.

8.12. (a) Show that $0 < v_p(\tau(\omega^{-i})) < 1$ ($i \not\equiv 0$ (mod $p-1$)).
(b) Use Proposition 8.20 plus the proof of Proposition 8.12 (without Proposition 6.13) to show that $v_p(\tau(\omega^{-i})) \equiv i/(p-1)$(mod 1).
(c) Conclude that $v_p(\tau(\omega^{-i})) = i/(p-1)$.

Chapter 9

The Second Case of Fermat's Last Theorem

In Chapters 1 and 6 we treated the first case of Fermat's Last Theorem, showing that there are no solutions provided certain conditions are satisfied by the class number. We now study the second case, namely

$$x^p + y^p = z^p, \qquad p \nmid xy, p \mid z, z \neq 0.$$

Again, the class number plays a role, but the units are also very important, which makes things much more difficult than in the first case. In fact, the second case is only known to hold for $p < 125000$, while the first case is known at present for $p < 6 \times 10^9$.

In the following, we first give the basic argument which underlies all of the theorems we shall prove. Then we show how various assumptions make the argument work. A basic component of all the proofs is Vandiver's conjecture that $p \nmid h^+(\mathbb{Q}(\zeta_p))$. In fact, if a prime is ever found for which Vandiver's conjecture fails, it is not clear that we could prove the second case of Fermat's Last Theorem for that prime. However, the first case is probably safe, since Theorem 6.23 and also some other independent criteria all have a very low chance of failing, either simultaneously or even individually.

§9.1 The Basic Argument

Consider the equation

$$\omega^p + \theta^p = \eta\lambda^m\xi^p$$

where

$p \geq 3$;
$\lambda = (1 - \zeta)(1 - \zeta^{-1}), (\zeta = \zeta_p)$;

$\lambda, \omega, \theta, \xi \in \mathbb{Z}[\lambda]$ are pairwise relatively prime;
η is a (real) unit of $\mathbb{Z}[\lambda]$; and

$m \geq p(p - 1)/2$.

We shall show that under certain conditions this equation has no solutions. If this is the case then

$$x^p + y^p = z^p, \qquad p \nmid xy, p \mid z, z \neq 0.$$

has no solutions. Otherwise we could assume $(x, y, z) = 1$ and let $\omega = x$, $\theta = y$, and $\xi = z/p^a$, where $a = v_p(z)$. Then $m = pa(p - 1)/2 \geq p(p - 1)/2$, and $\eta = p^{ap}/\lambda^m$ is a unit.

Suppose we have a solution. Then

$$\prod_{a=0}^{p-1} (\omega + \zeta^a\theta) = \eta\lambda^m\xi^p.$$

Suppose $\not{p}$ is a prime ideal of $\mathbb{Z}[\zeta]$ such that

$$\not{p} \mid \omega + \zeta^a\theta \quad \text{and} \quad \not{p} \mid \omega + \zeta^b\theta, \quad \text{where } a \not\equiv b \bmod p.$$

Then

$$\not{p} \mid (\zeta^a - \zeta^b)\theta = (\text{unit})(1 - \zeta)\theta$$

and

$$\not{p} \mid \zeta^{b-a}(\omega + \zeta^a\theta) - (\omega + \zeta^b\theta) = (\text{unit})(1 - \zeta)\omega.$$

If $\not{p} \neq (1 - \zeta)$ then $\not{p} \mid \theta$ and $\not{p} \mid \omega$, contradiction. Therefore $\not{p} = (1 - \zeta)$. Since λ and θ are relatively prime, $\not{p} \nmid \theta$; hence $\not{p}^2 \nmid (\omega + \zeta^a\theta) - (\omega + \zeta^b\theta)$. Therefore $\not{p}^2 = (\lambda)$ divides at most one of the factors $(\omega + \zeta^a\theta)$. Since $\omega + \theta \equiv \omega^p + \theta^p \equiv 0 \bmod \lambda$, and since similarly $\omega + \zeta^a\theta \equiv 0 \bmod(1 - \zeta)$, we may write

$$(\omega + \theta) \prod_{a=1}^{p-1} \left(\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\right) = (\text{unit})\lambda^{m-(p-1)/2}\xi^p$$

where the factors on the left are pairwise relatively prime algebraic integers and

$$(1 - \zeta) \nmid \frac{\omega + \zeta^a\theta}{1 - \zeta^a}, \qquad 1 \leq a \leq p - 1.$$

It follows that there are ideals $B_a, 0 \leq a \leq p - 1$, in $\mathbb{Z}[\zeta]$ such that

$$\left(\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\right) = B_a^p, \qquad 1 \leq a \leq p - 1,$$

and

$$(\omega + \theta) = (\lambda)^{m-(p-1)/2} B_0^p.$$

Note that the ideals B_a are pairwise relatively prime. For later reference, we also observe that

$$(\xi) = B_0 B_1 \cdots B_{p-1} \quad \text{and} \quad (1 - \zeta) \nmid B_a \quad \text{for } 0 \leq a \leq p - 1.$$

It is easy to see that B_{p-a} is the complex conjugate of B_a. We shall write B_{-a} instead of B_{p-a}. We now need our first assumption.

Assumption I. $p \nmid h^+(\mathbb{Q}(\zeta_p))$ (Vandiver's conjecture).

Assuming this, we claim that B_0 is principal in $\mathbb{Z}[\lambda]$. Note that $\bar{B}_0 = B_0$ and $(1-\zeta) \nmid B_0$, so B_0 arises from $\mathbb{Z}[\lambda]$. Since B_0^p is principal in $\mathbb{Z}[\lambda]$, because $\omega + \theta$ and λ are real, Assumption I implies that

$$B_0 = (\rho_0), \quad \text{with } \rho_0 \text{ real,}$$

as claimed. Consequently,

$$\omega + \theta = \eta_0 \lambda^{m-(p-1)/2} \rho_0^p,$$

where η_0 is a unit which must be real since everything else is real.

Now let $a \not\equiv 0 \bmod p$ and let

$$\alpha = \left(\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\right)\left(\frac{\omega + \zeta^{-a}\theta}{1-\zeta^{-a}}\right)^{-1} = -\zeta^{-a}\frac{\omega + \zeta^a\theta}{\omega + \zeta^{-a}\theta}$$

$$= -\zeta^{-a}\frac{\omega(1-\zeta^a) + (\omega+\theta)\zeta^a}{\omega(1-\zeta^{-a}) + (\omega+\theta)\zeta^{-a}} \equiv 1 \bmod (1-\zeta)^{2m-p},$$

since $\omega + \theta \equiv 0 \bmod \lambda^{m-(p-1)/2}$ therefore $\bmod (1-\zeta)^{2m-p+1}$. Since $2m - p \geq p(p-1) - p = p(p-2) \geq p$, we have

$$\alpha \equiv 1 \bmod (1-\zeta)^p.$$

Lemma 9.1. *If* $\alpha \in \mathbb{Z}[\zeta_p]$ *satisfies* $\alpha \equiv 1 \bmod (1-\zeta)^p$ *then*

$$\mathbb{Q}(\zeta_p, \alpha^{1/p})/\mathbb{Q}(\zeta_p)$$

is unramified at $(1-\zeta)$.

Proof. Let

$$f(X) = \frac{((1-\zeta)X + 1)^p - \alpha}{(1-\zeta)^p}.$$

Clearly f is monic, and since p divides the binomial coefficients $\binom{p}{j}$, $1 \leq j \leq p-1$, it follows that $f(X)$ has coefficients in $\mathbb{Z}[\zeta]$. A root β of f generates the same extension as $\alpha^{1/p}$ .The different of this extension divides

$$f'(\beta) = \frac{p}{(1-\zeta)^{p-1}}((1-\zeta)\beta + 1)^{p-1}$$

$$\equiv \frac{p}{(1-\zeta)^{p-1}} \bmod (1-\zeta).$$

Since $p/(1-\zeta)^{p-1}$ is a unit, the different is relatively prime to $(1-\zeta)$, so $(1-\zeta)$ is unramified. This completes the proof of the lemma. □

Since $\alpha = (B_a/B_{-a})^p$, the extension in Lemma 9.1 is also unramified at all other primes (Exercise 9.1).

Lemma 9.2. *Assume $p \nmid h^+(\mathbb{Q}(\zeta_p))$. Suppose $\alpha \in \mathbb{Q}(\zeta_p)$ satisfies $\bar{\alpha} = \alpha^{-1}$ and suppose the extension $\mathbb{Q}(\zeta_p, \alpha^{1/p})/\mathbb{Q}(\zeta_p)$ is unramified. Then α is a pth power in $\mathbb{Q}(\zeta_p)$.*

PROOF. Assume the extension is nontrivial, hence of degree p. Let

$$\sigma\colon \alpha^{1/p} \mapsto \zeta_p \alpha^{1/p}$$

generate the Galois group and let J denote complex conjugation, extended so that $J(\alpha^{1/p}) = (J\alpha)^{1/p}$. Since $J\alpha = \alpha^{-1}$,

$$J\sigma(\alpha^{1/p}) = J(\zeta\alpha^{1/p}) = \frac{1}{\zeta\alpha^{1/p}},$$

and

$$\sigma J(\alpha^{1/p}) = \sigma(\alpha^{-1/p}) = \zeta^{-1}\alpha^{-1/p}.$$

Therefore $J\sigma = \sigma J$, so σJ has order $2p$ and fixes $\mathbb{Q}(\zeta_p)^+$. Since

$$[\mathbb{Q}(\zeta_p, \alpha^{1/p})\colon \mathbb{Q}(\zeta_p)^+] = 2p,$$

σJ generates the Galois group. Let K be the fixed field of J, so $K/\mathbb{Q}(\zeta_p)^+$ is abelian of degree p. If a prime ideal $\not{p}$ of $\mathbb{Q}(\zeta_p)^+$ were to ramify in this extension, it would have ramification index $p > 2$, so the ramification could not be absorbed by $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)^+$. Hence $\mathbb{Q}(\zeta_p, \alpha^{1/p})/\mathbb{Q}(\zeta_p)$ would be ramified, contrary to hypothesis. Therefore $K/\mathbb{Q}(\zeta_p)^+$ is unramified and abelian of degree p, so $p \mid h^+(\mathbb{Q}(\zeta_p))$, which is a contradiction. This proves the lemma. □

Remark. Note that the fact that $\bar{\alpha} = \alpha^{-1}$, hence α is in the "$-$" component, caused $\alpha^{1/p}$ to yield an extension of the real subfield, which is the "$+$" component of $\mathbb{Q}(\zeta_p)$. This phenomenon will occur again in Chapter 10.

By the lemma, we have

$$\alpha = \left(\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\right)\left(\frac{\omega + \zeta^{-a}\theta}{1 - \zeta^{-a}}\right)^{-1} = \alpha_1^p$$

for some $\alpha_1 \in \mathbb{Q}(\zeta)$. But, as ideals,

$$\left(\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\,\frac{\omega + \zeta^{-a}\theta}{1 - \zeta^{-a}}\right) = (B_a B_{-a})^p.$$

By the same reasoning as was used above for B_0, we have

$$\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\,\frac{\omega + \zeta^{-a}\theta}{1 - \zeta^{-a}} = \eta'(\beta')^p,$$

where η' is a real unit and β' is real. Therefore

$$\left(\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\right)^2 = \eta'(\alpha_1\beta')^p.$$

Raising both sides of the $(p + 1)/2$th power, we obtain

$$\frac{\omega + \zeta^a\theta}{1 - \zeta^a} = \eta_a\rho_a^p,$$

where η_a is a real unit (so $\eta_a = \eta_{-a}$) and $\rho_a \in \mathbb{Z}[\zeta]$. Changing a to $-a$, we we find that $(\bar{\rho}_a)^p = \rho_{-a}^p$, so we may change ρ_{-a} by a power of ζ and assume

$$\bar{\rho}_a = \rho_{-a}.$$

We have two equations:

$$\omega + \zeta^a\theta = (1 - \zeta^a)\eta_a\rho_a^p$$

$$\omega + \zeta^{-a}\theta = (1 - \zeta^{-a})\eta_a\bar{\rho}_a^p.$$

Multiplying, we obtain

$$\omega^2 + \theta^2 + (\zeta^a + \zeta^{-a})\omega\theta = \lambda_a\eta_a^2(\rho_a\bar{\rho}_a)^p,$$

where

$$\lambda_a = (1 - \zeta^a)(1 - \zeta^{-a}) = 2 - \zeta^a - \zeta^{-a}.$$

Also, from a previous formula for $\omega + \theta$, we find

$$\omega^2 + \theta^2 + 2\omega\theta = \eta_0^2\lambda^{2m-p+1}\rho_0^{2p}.$$

Subtract and divide by λ_a:

$$-\omega\theta = \eta_a^2(\rho_a\bar{\rho}_a)^p - \eta_0^2\lambda^{2m-p+1}\rho_0^{2p}\lambda_a^{-1}.$$

Now let $b \not\equiv 0 \bmod p$ be another index and assume $a \not\equiv \pm b \bmod p$. This is possible if $p > 3$. For the case $p = 3$, see the Exercises. We have

$$-\omega\theta = \eta_b^2(\rho_b\bar{\rho}_b)^p - \eta_0^2\lambda^{2m-p+1}\rho_0^{2p}\lambda_b^{-1}.$$

Subtract and rearrange:

$$\eta_a^2(\rho_a\bar{\rho}_a)^p - \eta_b^2(\rho_b\bar{\rho}_b)^p = \eta_0^2\lambda^{2m-p+1}\rho_0^{2p}(\lambda_a^{-1} - \lambda_b^{-1}).$$

An easy calculation shows that

$$\lambda_a^{-1} - \lambda_b^{-1} = \frac{(\zeta^{-b} - \zeta^{-a})(\zeta^{a+b} - 1)}{\lambda_a\lambda_b} = \frac{\delta'}{\lambda},$$

where δ' is a unit. In fact, δ' is real since λ, λ_a, and λ_b are real. Therefore

$$\left(\frac{\eta_a}{\eta_b}\right)^2(\rho_a\bar{\rho}_a)^p + (-\rho_b\bar{\rho}_b)^p = \delta\lambda^{2m-p}(\rho_0^2)^p,$$

where δ is a real unit. We now need the following.

Assumption II. *η_a/η_b is a pth power of a unit of $\mathbb{Q}(\zeta_p)^+$.*

Assuming this, we let

$$\omega_1 = \left(\frac{\eta_a}{\eta_b}\right)^{2/p} \rho_a \bar{\rho}_a,$$

$$\theta_1 = -\rho_b \bar{\rho}_b, \quad \text{and}$$

$$\xi_1 = \rho_0^2.$$

Then

$$\omega_1^p + \theta_1^p = \delta \lambda^{2m-p} \xi_1^p.$$

Note that δ is a real unit and

$$2m - p \geq p(p-1) - p = (p-2)p \geq p\frac{p-1}{2}.$$

Since the numbers

$$\frac{\omega + \zeta^a \theta}{1 - \zeta^a} = \eta_a \rho_a^p, \qquad 1 \leq a \leq p-1,$$

and

$$\omega + \theta = \eta_0 \lambda^{m-(p-1)/2} \rho_0^p \qquad (\text{with } \lambda \nmid \rho_0)$$

are pairwise relatively prime, it follows that ω_1, θ_1, ξ_1, λ are pairwise relatively prime. We are now in the situation in which we started.

Suppose now that ξ had the smallest possible number of distinct prime ideal factors (not counted with multiplicity). We know from above that

$$(\xi) = B_0 B_1 \ldots B_{p-1}$$

and that these factors are relatively prime. But

$$(\xi_1) = (\rho_0^2) = B_0^2.$$

Therefore

$$B_1 = \cdots = B_{p-1} \doteq (1),$$

so

$$\frac{\omega + \zeta^a \theta}{1 - \zeta^a} \text{ is a unit}, \qquad 1 \leq a \leq p-1.$$

Let $a = \pm 1$. We find that

$$\alpha = \left(\frac{\omega + \zeta\theta}{1 - \zeta}\right)\left(\frac{\omega + \zeta^{-1}\theta}{1 - \zeta^{-1}}\right)^{-1}$$

is a unit with $\alpha\bar{\alpha} = 1$. By Lemma 1.6, α is a root of unity: $\alpha = \pm \zeta^c$ for some c. But $\alpha \equiv 1 \bmod (1 - \zeta)^p$, hence $\bmod (1 - \zeta)^2$, by a previous calculation (formula preceding Lemma 9.1), so $\alpha = 1$. Consequently

$$\frac{\omega + \zeta\theta}{1 - \zeta} = \frac{\omega + \zeta^{-1}\theta}{1 - \zeta^{-1}}.$$

A short calculation yields

$$\zeta(\theta + \omega) = \zeta^{-1}(\theta + \omega).$$

Since $\theta + \omega \neq 0$ (otherwise $\xi = 0$; this is where the trivial solutions are excluded), we have $\zeta^2 = 1$, which is false. This contradiction completes the argument.

§9.2 The Theorems

There are various methods of satisfying Assumptions I and II. We give three ways in this section.

Theorem 9.3. *If p is regular then the second case of Fermat's Last Theorem has no solutions.*

Proof. If p is regular then $p \nmid h^+(\mathbb{Q}(\zeta_p))$, so Assumption I is satisfied.

From formulas in the previous section,

$$\begin{aligned}\eta_a &= \frac{\omega + \zeta^a\theta}{1 - \zeta^a}\rho_a^{-p} \\ &= \left(\omega + \zeta^a\frac{\omega + \theta}{1 - \zeta^a}\right)\rho_a^{-p} \\ &\equiv \omega\rho_a^{-p} \bmod (1 - \zeta)^{2m-p}.\end{aligned}$$

Since a similar equation holds with b, we obtain

$$\frac{\eta_a}{\eta_b} \equiv \left(\frac{\rho_b}{\rho_a}\right)^p \bmod (1 - \zeta)^{2m-p}.$$

But $2m - p \geq p - 1$ and $(\rho_b/\rho_a)^p$ is congruent to a rational integer mod p by Lemma 1.8. Therefore

$$\frac{\eta_a}{\eta_b} \equiv \text{rational integer} \pmod{p}.$$

By Theorem 5.36, η_a/η_b is a pth power. This proves Assumption II and completes the proof of Theorem 9.3. □

Theorem 9.4. *Suppose $p^3 \nmid B_{pi}$ for all even i, $2 \le i \le p-3$, and assume $p \nmid h^+(\mathbb{Q}(\zeta_p))$. Then the second case of Fermat's Last Theorem has no solutions.*

Remark. Since $B_{pi}/pi \equiv B_i/i \bmod p$, we have $p^3 \mid B_{pi}$ only if $p \mid B_i$ (but not conversely).

Proof. Assumption I holds by hypothesis, so it remains to check Assumption II. Since $p = 3$ is covered by Theorem 9.3 (or the Exercises), we assume $p > 3$. We know that

$$\rho_a^p = \eta_a^{-1}\frac{\omega + \zeta^a\theta}{1-\zeta^a},$$

$$\rho_{-a}^p = \eta_a^{-1}\frac{\omega + \zeta^{-a}\theta}{1-\zeta^{-a}} = -\eta_a^{-1}\frac{\zeta^a\omega + \theta}{1-\zeta^a}, \quad \text{and}$$

$$\omega + \theta = \eta_0\lambda^{m-(p-1)/2}\rho_0^p.$$

Therefore

$$\rho_a^p - \rho_{-a}^p = \eta_a^{-1}\frac{1+\zeta^a}{1-\zeta^a}\eta_0\lambda^{m-(p-1)/2}\rho_0^p,$$

hence

$$\prod_{i=0}^{p-1}(\rho_a - \zeta^i\rho_{-a}) = \tilde{\eta}(1-\zeta)^{2m-p}\rho_0^p,$$

where $\tilde{\eta}$ is a (nonreal) unit. Since ρ_a and ρ_{-a} are relatively prime, it follows as at the beginning of the previous section that the numbers

$$\frac{\rho_a - \zeta^i\rho_{-a}}{1-\zeta^i}\ (1 \le i \le p-1), \quad \text{and} \quad \frac{\rho_a - \rho_{-a}}{1-\zeta}$$

are relatively prime algebraic integers. Since $2m - p \ge (p-2)p > p$ (since $p > 3$), at least one (hence exactly one) of these numbers is divisible by $1-\zeta$. It follows that

$$(1-\zeta)^{2m-2p+1} \text{ divides } \rho_a - \zeta^i\rho_{-a} \text{ for some } i, \qquad 0 \le i \le p-1.$$

Consequently,

$$\zeta^{-i/2}\rho_a \equiv \zeta^{i/2}\rho_{-a} \bmod (1-\zeta)^{2m-2p+1}.$$

In the previous section, ρ_a and ρ_{-a} were determined up to roots of unity, subject to the restriction that $\bar{\rho}_a = \rho_{-a}$. Therefore, we may replace ρ_a by $\zeta^{-i/2}\rho_a$ and assume that

$$\rho_a \equiv \rho_{-a} \bmod (1-\zeta)^{2m-2p+1}.$$

As before, there exist ideals C_i, $0 \leq i \leq p-1$, of $\mathbb{Z}[\zeta]$ such that

$$\left(\frac{\rho_a - \zeta^i \rho_{-a}}{1-\zeta^i}\right) = C_i^p, \qquad 1 \leq i \leq p-1, \quad \text{and}$$

$$(\rho_a - \rho_{-a}) = (1-\zeta)^{2m-2p+1} C_0^p.$$

Since $(\rho_a - \zeta\rho_{-a})/(1-\zeta)$ is real, it follows as in the previous section, since $p \nmid h^+$, that C_1 is principal:

$$\frac{\rho_a - \zeta\rho_{-a}}{1-\zeta} = \tilde{\eta}_a \mu_a^p,$$

where $\tilde{\eta}_a$ is a real unit and $\mu_a \in \mathbb{Q}(\zeta)^+$. From the above congruence ($\rho_a \equiv \rho_{-a}$),

$$\rho_a \equiv \tilde{\eta}_a \mu_a^p \bmod (1-\zeta)^{2m-2p},$$

so

$$\frac{\omega + \zeta^a \theta}{1-\zeta^a} = \eta_a \rho_a^p \equiv \eta_a \tilde{\eta}_a^p \mu_a^{p^2} \bmod (1-\zeta)^{2m-2p}.$$

A similar formula holds with b in place of a. Therefore

$$\begin{aligned} \frac{\eta_a}{\eta_b}\frac{\tilde{\eta}_a^p}{\tilde{\eta}_b^p} &\equiv \frac{\omega + \zeta^a\theta}{1-\zeta^a}\,\frac{1-\zeta^b}{\omega+\zeta^b\theta}\left(\frac{\mu_b}{\mu_a}\right)^{p^2} \bmod (1-\zeta)^{2m-2p} \\ &\equiv \left(\frac{\mu_b}{\mu_a}\right)^{p^2} \bmod (1-\zeta)^{2m-2p}, \end{aligned}$$

since

$$\begin{aligned} \frac{\omega + \zeta^a\theta}{1-\zeta^a}\,\frac{1-\zeta^b}{\omega+\zeta^b\theta} &= \left(\omega + \zeta^a\frac{\theta+\omega}{1-\zeta^a}\right)\left(\omega + \zeta^b\frac{\theta+\omega}{1-\zeta^b}\right)^{-1} \\ &\equiv 1 \bmod (1-\zeta)^{2m-p}. \end{aligned}$$

Since $2m - 2p \geq p(p-1) - 2p = p(p-3) > 2(p-1)$, the above becomes a congruence mod p^2. From Lemma 1.8,

$$\left(\frac{\mu_b}{\mu_a}\right)^p \equiv \text{rational integer } (\bmod\ p),$$

from which it follows that

$$\left(\frac{\mu_b}{\mu_a}\right)^{p^2} \equiv \text{rational integer } (\bmod\ p^2).$$

Therefore

$$\frac{\eta_a}{\eta_b}\frac{\tilde{\eta}_a^p}{\tilde{\eta}_b^p} \text{ is a } p\text{th power},$$

by Corollary 8.23, hence η_a/η_b is a pth power. This verifies Assumption II and completes the proof of Theorem 9.4. □

The disadvantage of Theorem 9.4 is that it requires us to show that $p \nmid h^+(\mathbb{Q}(\zeta_p))$. The best way to do this is via Corollary 8.19. However, if the hypotheses of Corollary 8.17 are satisfied for a sufficiently small l, we are very fortunate, since not only does $p \nmid h^+$ but also the second case of Fermat's Last Theorem has no solutions, as the following result shows.

Theorem 9.5. *Let the notation be as in Proposition* 8.18 *and Corollary* 8.19. *If there exists a prime* $l \equiv 1 \bmod p$ *with* $l < p^2 - p$ *such that*

$$Q_i^k \not\equiv 1 \bmod l \quad \textit{for all } i \in \{i_1, \ldots, i_s\},$$

then the second case of Fermat's Last Theorem has no solutions.

Proof. By Corollary 8.19, $p \nmid h^+(\mathbb{Q}(\zeta_p))$, so Assumption I is satisfied. Suppose that

$$x^p + y^p = z^p, \qquad p \nmid xy, p \mid z, z \neq 0,$$

where x, y, $z \in \mathbb{Z}$ are relatively prime. Let l be as in the statement of the theorem.

Lemma 9.6. $l \nmid xy$.

Proof. Suppose $l \mid y$, hence $l \nmid xz$. Since

$$\prod_{a=0}^{p-1} (y - \zeta^a z) = -x^p,$$

the standard argument shows that the numbers

$$y - \zeta^a z, \qquad 0 \leq a \leq p - 1,$$

are relatively prime in $\mathbb{Z}[\zeta_p]$, so there exist ideals A_a, $0 \leq a \leq p - 1$, such that

$$(y - \zeta^a z) = A_a^p.$$

Let $a \not\equiv 0 \bmod p$, and let

$$\begin{aligned} \alpha &= (y - \zeta^a z)(y - \zeta^{-a} z)^{-1} \\ &= 1 - \frac{(\zeta^a - \zeta^{-a})z}{y - \zeta^{-a} z} \\ &\equiv 1 \bmod (1 - \zeta)^p, \quad \text{since } p \mid z. \end{aligned}$$

Since (α) is the pth power of an ideal, $\mathbb{Q}(\alpha^{1/p}, \zeta_p)/\mathbb{Q}(\zeta_p)$ is unramified except possibly at $(1 - \zeta)$. Lemma 9.1 implies that this extension is also unramified at $(1 - \zeta)$. Since $p \nmid h^+$, α is a pth power by Lemma 9.2. As in the previous section, the ideal

$$(y - \zeta^a z)(y - \zeta^{-a} z) = (A_a A_{-a})^p$$

is the pth power of a principal ideal in $\mathbb{Q}(\zeta_p)^+$ (since $p \nmid h^+$), and by the argument used there,

$$y - \zeta^a z = \gamma_a \sigma_a^p,$$

where γ_a is a real unit, $\sigma_a \in \mathbb{Z}[\zeta_p]$. Since we are assuming $l \mid y$,

$$-\zeta^a z \equiv \gamma_a \sigma_a^p \bmod l.$$

Taking complex conjugates and noting that $\gamma_a = \gamma_{-a}$, we find that

$$-\zeta^{-a} z \equiv \gamma_a \sigma_{-a}^p \bmod l.$$

Since $l \nmid z$, we may divide and obtain

$$\zeta^{2a} \equiv \left(\frac{\sigma_a}{\sigma_{-a}}\right)^p \bmod l.$$

Let $\tilde{l}$ be a prime of $\mathbb{Q}(\zeta_p)$ lying above l. Since $2a \not\equiv 0 \bmod p$, the equation $p = \prod (1 - \zeta^j)$ implies that $\zeta^{2a} \not\equiv 1 \bmod \tilde{l}$. Therefore σ_a/σ_{-a} has order $p^2 \bmod \tilde{l}$. Since $l \equiv 1 \bmod p$, $\mathbb{Z}[\zeta]\bmod \tilde{l}$ has l elements; hence $p^2 \mid l - 1$. Since $l < p^2 - p$, this is impossible, so $l \nmid y$. Similarly, $l \nmid x$. This proves Lemma 9.6. □

Lemma 9.7. $l \mid z$ (*this is where* $l < p^2 - p$ *is used most strongly*).

Proof. Write $l = 1 + kp$ with $k < p - 1$. By the equations obtained in Lemma 9.6 (we only needed $p \nmid x$),

$$(y - \zeta^a z)\sigma_a^{-p} = \gamma_a = \gamma_{-a} = (y - \zeta^{-a} z)\sigma_{-a}^{-p}, \qquad 1 \le a \le p - 1.$$

Let $\tilde{l}$ be a prime of $\mathbb{Z}[\zeta_p]$ above l. Since $\mathbb{Z}[\zeta]\bmod \tilde{l}$ has l elements,

$$\sigma_a^{kp} = \sigma_a^{l-1} \equiv 1 \bmod \tilde{l}$$

($l \nmid x$, so $\tilde{l} \nmid \sigma_a$). Therefore

$$(y - \zeta^a z)^k \equiv (y - \zeta^{-a} z)^k \bmod \tilde{l}.$$

Multiply each side by ζ^{-a} and expand to obtain

$$\zeta^{-a} y^k - kzy^{k-1} + \cdots + \zeta^{a(k-1)} z^k \equiv \zeta^{-a} y^k - k\zeta^{-2a} zy^{k-1} + \cdots + \zeta^{-a(k+1)} z^k.$$

Since $k < p - 1$, only the term $-kzy^{k-1}$ contains a trivial power of ζ (i.e., ζ^0). Note that the above congruence also holds for $a = 0$. Therefore we may sum for $0 \le a \le p - 1$. The powers of ζ sum to 0, so we obtain

$$-pkzy^{k-1} \equiv 0 \bmod \tilde{l}.$$

But $l = 1 + kp$, so $\tilde{l} \nmid pk$. Lemma 9.6 implies that $\tilde{l} \nmid y$. Therefore $\tilde{l} \mid z$, hence $l \mid z$. This completes the proof of Lemma 9.7. □

Now we may work with the "basic argument" of the previous section. From the above, we find that we may start with the equation

$$\omega^p + \theta^p = \eta\lambda^m\xi^p$$

with the added condition that $l \mid \xi$. Assuming that we can show that η_a/η_b is a pth power, we obtain

$$\omega_1^p + \theta_1^p = \delta\lambda^{2m-p}\xi_1^p,$$

where $\xi_1 = \rho_0^2$. We want to show that $l \mid \rho_0$, hence $l \mid \xi_1$. Then we may assume that ξ has the minimum number of distinct prime factors subject to the condition that $l \mid \xi$. The last part of the "basic argument" then yields the result.

Recall that

$$\omega + \theta = \eta_0\lambda^{m-(p-1)/2}\rho_0^p.$$

If we can prove that $l \mid (\omega + \theta)$, then every prime divisor of l divides ρ_0. Since l is unramified in $\mathbb{Q}(\zeta_p)$, $l \mid \rho_0$.

Lemma 9.8. $l \mid \omega + \theta$.

Proof. Let $\tilde{l}$ be a prime divisor of l in $\mathbb{Q}(\zeta_p)$. Since $l \mid \xi$,

$$\prod_{i=0}^{p-1}(\omega + \zeta^i\theta) \equiv 0 \bmod \tilde{l}.$$

Therefore $\omega + \zeta^j\theta \equiv 0 \bmod \tilde{l}$ for some j. Suppose $j \neq 0$. Since the numbers $(\omega + \zeta^a\theta)/(1 - \zeta^a)$ were pairwise relatively prime,

$$\tilde{l} \nmid \omega + \zeta^a\theta \quad \text{for } a \neq j, \qquad \text{hence } \tilde{l} \nmid \rho_a \quad \text{for } a \neq j.$$

Since η_a was real, so $\eta_a = \eta_{-a}$,

$$\rho_{-a}^p\frac{\omega + \zeta^a\theta}{1 - \zeta^a} = \rho_a^p\frac{\omega + \zeta^{-a}\theta}{1 - \zeta^{-a}}.$$

Recall that $l = 1 + kp$, hence $\rho_a^{kp} \equiv 1 \bmod \tilde{l}$ for $a \neq j$. Therefore, if $a \not\equiv \pm j \bmod p$,

$$\left(\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\right)^k \equiv \left(\frac{\omega + \zeta^{-a}\theta}{1 - \zeta^{-a}}\right)^k \equiv \left(\frac{\zeta^a\omega + \theta}{\zeta^a - 1}\right)^k \bmod \tilde{l}.$$

Since k is even, we obtain

$$(\omega + \zeta^a\theta)^k \equiv (\zeta^a\omega + \theta)^k \bmod \tilde{l}.$$

But $\omega \equiv -\zeta^j\theta \bmod \tilde{l}$, by the choice of j. Therefore

$$(\theta(\zeta^a - \zeta^j))^k \equiv (\theta(1 - \zeta^{a+j}))^k \bmod \tilde{l}.$$

Since ω, θ, ξ are relatively prime and $l \mid \xi$, we must have l and θ relatively prime, so

$$(\zeta^a - \zeta^j)^k \equiv (1 - \zeta^{a+j})^k \bmod \tilde{l}.$$

Lemma 9.9. *η_a/η_b is a pth power.*

PROOF. Let $\tilde{l}$ be a prime of $\mathbb{Q}(\zeta_p)$ lying above l. Then

$$\eta_a = \frac{\omega + \zeta^a\theta}{1 - \zeta^a}\rho_a^{-p} = \left(\omega + \zeta^a\frac{\omega + \theta}{1 - \zeta^a}\right)\rho_a^{-p}$$

$$\equiv \omega\rho_a^{-p} \bmod \tilde{l}, \quad \text{by Lemma 9.8.}$$

Therefore

$$\frac{\eta_a}{\eta_b} \equiv \left(\frac{\rho_b}{\rho_a}\right)^p \bmod \tilde{l}.$$

Consequently η_a/η_b is a pth power modulo every prime above l.

Since $p \nmid h^+(\mathbb{Q}(\zeta_p))$, Corollary 8.15 implies that $E^+ \bmod (E^+)^p$ is generated by the units E_i, $i = 2, 4, \ldots, p-3$. Therefore

$$\frac{\eta_a}{\eta_b} = \gamma^p \prod_i E_i^{d_i},$$

for some integers d_i. We want to show $p \mid d_i$ for all i. As in the proof of Theorem 9.3,

$$\frac{\eta_a}{\eta_b} \equiv \text{rational integer (mod } p).$$

By Exercises 8.11 and 8.10, we have $p \mid d_i$ if $p \nmid B_i$, so we only need to consider the "irregular" indices $i_1, \ldots, i_s$ for which $p \mid B_i$.

In Proposition 8.18, the integer t determines a prime ideal $\tilde{l}$ by $t \equiv \zeta \bmod \tilde{l}$. Henceforth, let $\tilde{l}$ denote this prime ideal. Fix a generator $\gamma_{\tilde{l}}$ for the multiplicative group $(\mathbb{Z}[\zeta_p] \bmod \tilde{l})^\times$. If $\tilde{l} \nmid x$, define $\text{ind}_{\tilde{l}}\, x$ by

$$\gamma_{\tilde{l}}^{\text{ind}_{\tilde{l}} x} \equiv x \bmod \tilde{l},$$

so $\text{ind}_{\tilde{l}}\, x$ is defined mod$(l-1)$, hence mod p.

Let $\sigma_\alpha \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Let $\gamma_{\sigma_\alpha(\tilde{l})} = \sigma_\alpha(\gamma_{\tilde{l}})$ be the multiplicative generator mod $\sigma_\alpha(\tilde{l})$. Then

$$\text{ind}_{\sigma_\alpha(\tilde{l})}\, x = \text{ind}_{\tilde{l}}\,\sigma_\alpha^{-1}(x).$$

Since

$$E_i = \prod_{b=1}^{p-1}\left(\zeta^{(b-bg)/2}\frac{1-\zeta^{bg}}{1-\zeta^b}\right)^{b^{p-1-i}} \cdot (p\text{th power}),$$

it follows easily that

$$\sigma_\alpha^{-1}(E_i) = E_i^{\alpha^{p-1-i}} \cdot (p\text{th power}).$$

Therefore

$$\text{ind}_{\tilde{l}}\,\sigma_\alpha^{-1}(E_i) \equiv \alpha^{-i}\,\text{ind}_{\tilde{l}}\,E_i \quad \bmod p.$$

From above, we obtain

$$\operatorname{ind}_{\sigma_\alpha(\tilde{l})} E_i \equiv \alpha^{-i} \operatorname{ind}_{\tilde{l}} E_i \mod p.$$

Since η_a/η_b was shown to be a pth power modulo each prir . above l,

$$0 \equiv \sum d_i \operatorname{ind}_{\sigma_\alpha(\tilde{l})} E_i \mod p,$$

hence

$$0 \equiv \sum d_i \alpha^{-i} \operatorname{ind}_{\tilde{l}} E_i \mod p, \quad \text{for all } \alpha \not\equiv 0 \mod p.$$

Since

$$\det(\alpha^{-i})_{\substack{i=2,4,\dots,p-3\\ \alpha=1,2,\dots,(p-3)/2}} = \left(\left(\frac{p-3}{2}\right)!\right)^{-2} \prod_{1 \le \beta < \alpha \le (p-3)/2} (\alpha^{-2} - \beta^{-2})$$
$$\not\equiv 0 \bmod p$$

(essentially a Vandermonde determinant), we must have

$$d_i \operatorname{ind}_{\tilde{l}} E_i \equiv 0 \bmod p.$$

As mentioned above, $d_i \equiv 0$ if $i \notin \{i_1, \dots, i_s\}$. But $Q_i^k \not\equiv 1 \bmod l$ implies, by Proposition 8.18, that $\operatorname{ind}_{\tilde{l}} E_i \not\equiv 0$. Therefore, for all $i, d_i \equiv 0 \bmod p$. It follows that η_a/η_b is a pth power. This completes Lemma 9.9. □

The proof of Theorem 9.5 is now complete. □

The verification of Fermat's Last Theorem is carried out on a computer as follows. First, the irregular indices are determined via congruences such as

$$(3^{p-2k} + 4^{p-2k} - 6^{p-2k} - 1)B_{2k}/4k \equiv \sum_{p/6 < s < p/4} s^{2k-1} \pmod{p}$$

(There are several such congruences; see (Wagstaff [1]) for details). This is the longest part of the computations. Then Theorem 9.5 is used to verify the second case of Fermat's Last Theorem. This has been done for $p < 125000$. For the first case it is possible to use Theorem 6.23 since $i(p) \le 5$ for all $p < 125000$. However, it is faster to use the Wieferich criterion: if $2^{p-1} \not\equiv 1 \bmod p^2$, then the first case of Fermat's Last Theorem has no solutions. In fact, if $a^{p-1} \not\equiv 1 \bmod p$ for some $a \le 31$ then there are no solutions. For $a = 2$, the only values of $p < 6 \times 10^9$ with $2^{p-1} \equiv 1 \bmod p^2$ are $p = 1093$ and 3511, and for both of these $3^{p-1} \not\equiv 1 \bmod p^2$. Therefore the first case holds up to 6×10^9. The fact that there are only two "bad" primes should not be very surprising: the probability that $2^{p-1} \equiv 1 \bmod p^2$ should be $1/p$. Therefore, the number of such p less than x should be approximately

$$\sum_{p<x} 1/p \sim \log\log x + 0.26.$$

Note that $\log\log(6 \times 10^9) = 3.1$; perhaps another example should be expected soon.

Notes

The criteria in this chapter were developed by Kummer and Vandiver. Theorem 9.5 has been extended to allow $p < \frac{3}{2}(p^2 - p)$ by Inkeri. For more on Fermat's Last Theorem, see Vandiver [1] and Ribenboim [1].

Exercises

9.1. Let K be a number field, $a \in K^\times$, and $n \in \mathbb{Z}$.

(a) Suppose $K(a^{1/n})$ is unramified. Show that $(a) = I^n$ for some ideal I of K.

(b) Suppose $(a) = I^n$ for some ideal I of K. Show that $K(a^{1/n})/K$ is unramified except possibly at the primes dividing n. (*Hint*: work locally. In a completion I is is principal, so the local extension can be obtained by adjoining $u^{1/n}$ with u a local unit.)

9.2. (This exercise proves part of Exercise 9.3(b)). Let p be prime and let K be a number field containing ζ_p. Let $\pi = \zeta_p - 1$ and let $\mathfrak{p}$ be a prime ideal of K dividing π. Let $\mathfrak{p}^a$ be the exact power of $\mathfrak{p}$ dividing π. Let $\alpha \in K^\times$ with $\mathfrak{p} \nmid \alpha$. Let c be maximal such that $x^p \equiv \alpha \bmod \mathfrak{p}^c$ has a solution. Assume that $c < pa$, so $x^p \not\equiv \alpha \bmod p\pi$, hence mod $\mathfrak{p}^{pa}$.

(a) Suppose $b < a$ and $x^p \equiv \alpha \bmod \mathfrak{p}^{pb}$. Let w have order 1 at $\mathfrak{p}$. Show that $(x + w^b y)^p \equiv \alpha \bmod \mathfrak{p}^{pb+1}$ for some $y \in K$. Conclude that $p \nmid c$, so

$$c = pd + r, \quad \text{with } 0 \leq d < a \quad \text{and} \quad 0 < r < p.$$

(b) Suppose $\mathfrak{p}$ is inert in the extension $K(\alpha^{1/p})/K$. Let $x \equiv \alpha^{1/p} \bmod \mathfrak{p}^g$, with g maximal. Show (i) $g > 0$; (ii) if $g \geq a$ then $x^p \equiv \alpha \bmod \mathfrak{p}^{pa}$, which is impossible; (iii) $g = d$, with d as in (*a*).

(c) Let notations and assumptions be as in (b). Let $z \in K$ be such that $(z)\mathfrak{p}^d$ is an integral ideal prime to $\mathfrak{p}$. Show that $z(x - \alpha^{1/p})$ is an integer in $K(\alpha^{1/p})$ which is prime to $\mathfrak{p}$ but whose norm to K is divisible by $\mathfrak{p}^r$, with r as in (*a*).

(d) Show that (c) contradicts the assumption that $\mathfrak{p}$ remains prime in $K(\alpha^{1/p})$. Conclude that $\mathfrak{p}$ must ramify or split completely (in fact, by Exercise 9.3(a), $\mathfrak{p}$ must ramify).

9.3. Let p be prime and let K be a number field containing ζ_p. Let $\pi = \zeta_p - 1$ and let $\mathscr{P} = \prod_{\mathfrak{p}|p} \mathfrak{p}$. Let $\alpha \in K^\times$ with $a \notin (K^\times)^p$, and assume α is relatively prime to p. The number α is called *primary* if $x^p \equiv \alpha \bmod p\pi$ has a solution in $K^\times$; *hyperprimary* if $x^p \equiv \alpha \bmod p\pi\mathscr{P}$ has a solution; and *singular primary* if α is primary and $(\alpha) = I^p$ for some ideal I of K.

(a) Show that α is hyperprimary if and only if all primes above p split completely in the extension $K(\alpha^{1/p})/K$.

(b) Show that α is primary if and only if $K(\alpha^{1/p})/K$ is unramified at all primes above p.

(c) Show that α is singular primary if and only if $K(\alpha^{1/p})/K$ is unramified at all primes of K (one exception: if $p = 2$ then K could be real and there might be ramification at the infinite primes). (*Hints*: Exercises 9.1 and 9.2; also look at the proof of Lemma 9.1 and the second proof of Theorem 5.36.)

9.4. (a) Let $f(X) = (((\zeta_p - 1)X + 1)^p - 1)/(\zeta_p - 1)^p$. Show that

$$f(X) \equiv X^p + \frac{p}{(\zeta_p - 1)^{p-1}} X \bmod(\zeta_p - 1)$$

and that $f(1) = 0$. Conclude that $p/(\zeta_p - 1)^{p-1} \equiv -1 \bmod(\zeta_p - 1)$.

(b) Look at the terms with lowest p-adic valuation in the expansion of

$$0 = \log_p(1 + (\zeta_p - 1))$$

to obtain the result of (a). This also works for ζ_{p^n}.

(c) (The easy way.) Find the minimal polynomial $g(X)$ for $\zeta_p - 1$, compute $g(\zeta_p - 1) \bmod(\zeta_p - 1)^p$, and obtain (a). This also works for ζ_{p^n}.

9.5. (The second case of Fermat's Last Theorem for $p = 3$). Recall that we needed $p > 3$ for part of the "basic argument." This exercise treats $p = 3$. Let $\zeta = \zeta_3$. It is well known that $Q(\zeta_3) = Q(\sqrt{-3})$ has class number 1. Suppose we have $x, y, z \in \mathbb{Z}$, with $3 \nmid xyz$, and $m \geq 1$ such that

$$x^3 + y^3 = (3^m z)^3.$$

We of course may assume that x, y, and z are pairwise relatively prime.

(a) Show that

$$x + y = \eta_0 3^{3m-1} \rho_0^3,$$
$$x + \zeta y = \eta_1(1 - \zeta)\rho_1^3,$$
$$x + \zeta^2 y = \eta_2(1 - \zeta^2)\rho_2^3,$$

with $\rho_1, \rho_2, \rho_3 \in \mathbb{Z}[\zeta]$ and pairwise relatively prime, and with η_1, η_2, η_3 units of $\mathbb{Z}[\zeta]$.

(b) Show that η_1 is congruent to a rational integer mod 3, hence $\eta_1 = \pm 1 = (\pm 1)^3$. Therefore we may assume $\eta_1 = 1$. Similarly, we may assume $\eta_2 = 1$.

(c) Show that $\eta_0/\bar{\eta}_0$ is a cube. Using the fact that η_0 has the form $\pm\zeta^r$, conclude that $\eta_0 = \pm 1$; hence we may assume $\eta_0 = 1$.

(d) Show that we may assume that $\rho_0 \in \mathbb{Z}$. (Hint: a straightforward calculation shows that $(s + t\zeta)^3 \in \mathbb{Q} \Rightarrow s = t$ or $st = 0$.)

(e) Write $\rho_1 = a + b\zeta$. Show that $(a, b) = 1$, hence $a, b, a - b$ are pairwise relatively prime.

(f) Show that $ab \neq 0$ and $a \neq b$ (in particular, $a = b = 1$ is excluded).

(g) Show that $x + y = 9ab(a - b)$.

(h) Use the equation $x + y = 3^{3m-1}\rho_0^3$ to show that there are nonzero rational integers a_1, b_1, c_1 such that some permutation of $(a, b, a - b)$ equals

$$(a_1^3, b_1^3, 3^{3m-3}c_1^3).$$

(i) Since $a_1^3 \pm b_1^3 = (\pm 3^{m-1}c_1)^3$ for some choice of signs, and since we know the first case has no solutions (by congruences mod 9), we are done by induction.

Chapter 10

Galois Groups Acting on Ideal Class Groups

Relatively recently, it has been observed, in particular by Iwasawa and Leopoldt, that the action of Galois groups on ideal class groups can be used to great advantage to reinterpret old results and to obtain new information on the structure of class groups. In this chapter we first give some results which are useful when working with class groups and class numbers. We then present the basic machinery, essentially Leopoldt's Spiegelungsatz, which underlies the rest of the chapter. As applications, Kummer's result "$p \mid h^+ \Rightarrow p \mid h^-$" is made more precise and a classical result of Scholz on class groups of quadratic fields is proved. Finally, we show that· Vandiver's conjecture implies that the ideal class group of $\mathbb{Q}(\zeta_{p^n})$ is isomorphic to the minus part of the group ring modulo the Stickelberger ideal.

§10.1 Some Theorems on Class Groups

Since it is useful, we repeat the following result.

Theorem 10.1. *Suppose the extension of number fields L/K contains no unramified abelian subextensions F/K with $F \neq K$. Then h_K divides h_L. In fact, the norm map from the class group of L to the class group of K is surjective.*

Proof. The first statement is Proposition 4.11. The second is proved in the appendix on class field theory. □

Theorem 10.2. *Let $n \not\equiv 2 \bmod 4$ be arbitrary and let $h_n = h(\mathbb{Q}(\zeta_n))$. If $2 \mid h_n^+$ then $2 \mid h_n^-$.*

PROOF. $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is totally ramified at infinity, so Theorem 10.1 implies that the norm map on the ideal class groups

$$N: C \to C^+$$

is surjective, so $h_n^- = h_n/h_n^+ = |\ker N|$. Suppose $2 | h_n^+$. Then there exists a nontrivial ideal class $\alpha \in C^+$ such that $\alpha^2 = 1$. Lift α to C. Since $N\alpha = \alpha^2 = 1$, $\alpha \in \ker N$. Since the map $C^+ \to C$ is injective by Theorem 4.14, $\alpha \neq 1$ in C, but $\alpha^2 = 1$. Therefore $\ker N$ has even order, so $2 | h_n^-$. □

Remark. Note that this proof works for any CM-field K such that the map $C^+ \to C$ is injective. This theorem is useful when one looks for cyclotomic fields whose real subfields have even class numbers. Such fields arise in topology (see, for example, Giffen [1]).

Theorem 10.3. *Let K be a CM-field. The kernel of the map $C^+ \to C$ from the ideal class group of K^+ to that of K has order* 1 *or* 2.

PROOF. Let I be an ideal of K^+ and suppose $I = (\alpha)$ in K. Then $(1) = \bar{I}/I = (\bar{\alpha}/\alpha)$, so $\bar{\alpha}/\alpha$ is a unit, hence a root of unity by Lemma 1.6. This root of unity does not depend on the class of I in K^+. Let W be the roots of unity in K. We obtain a homomorphism

$$\phi: \ker(C^+ \to C) \to W \to W/W^2.$$

If $\phi(I) = 1$, then $\bar{\alpha}/\alpha = \zeta^2$; so $\zeta\alpha = \overline{\zeta\alpha}$. This means $\zeta\alpha \in K^+$. Since $I = (\zeta\alpha)$ in K, unique factorization into primes implies $I = (\zeta\alpha)$ in K^+. Therefore ϕ is injective. Since W/W^2 has order 2, the proof is complete. □

Note that it is possible for the kernel to have order 2. See the example following Theorem 4.14.

Theorem 10.4. (a) *Suppose L/K is a Galois extension and* Gal(L/K) *is a p-group (p = any prime). Assume there is at most one prime (finite or infinite) which ramifies in L/K. If $p | h_L$ then $p | h_K$.*

(b) *If $L/\mathbb{Q}$ is Galois,* Gal$(L/\mathbb{Q})$ *is a p-group, and at most one finite prime ramifies, then $p \nmid h_L$.*

PROOF. Assume $p | h_L$. Let H be the Hilbert p-class field of L, so H is the maximal unramified abelian p-extension of L and Gal(H/L) is isomorphic to the p-Sylow subgroup of the ideal class group of L. Since L/K is Galois, the maximality of H implies that H/K is Galois. Let $G = \text{Gal}(H/K)$. Let $\mathfrak{p}$ be the prime (if it exists) of K which ramifies, let $\mathcal{P}$ be a prime of H above $\mathfrak{p}$, and let $I \subseteq G$ be the inertia group for $\mathcal{P}$. Since H/L is unramified,

$$|I| \leq \deg(L/K) < |G|.$$

By a well-known result in the theory of p-groups, there exists a normal subgroup G_1 of G, of index p, with $I \subseteq G_1 \subset G$ (proof: mod out by the subgroup generated by an element of order p in the center, then use induction on $|G|$). The inertia subgroups of the other primes of H above $\not{p}$ are conjugates of I, hence lie in G_1. Since $\not{p}$ is the only ramified prime, no prime ramifies from K to the fixed field of G_1. But the fixed field of G_1 is Galois of degree p over K, so K has an unramified abelian extension of degree p. Class field theory implies that $p \mid h_K$. This proves (a).

The case $K = \mathbb{Q}$ is treated similarly, except that we ignore ramification at infinity. Therefore, if $p \mid h_L$ we obtain an abelian extension of degree p which is unramified at all finite primes. But the Minkowski bound (see Lemma 14.3) implies that the discriminant of any nontrivial extension of $\mathbb{Q}$ is greater than 1, so at least one finite prime ramifies, contradiction (alternatively, if there is ramification at infinity then p must be even, and every quadratic extension of $\mathbb{Q}$ has ramification of at least one finite prime.) This completes the proof of Theorem 10.4. □

Corollary 10.5. *Let $n \geq 1$. Then $p \mid h(\mathbb{Q}(\zeta_p)) \Leftrightarrow p \mid h(\mathbb{Q}(\zeta_{p^n}))$.*

Proof. Theorems 10.1 and 10.4. □

Corollary 10.6. *If Vandiver's conjecture holds for p then $p \nmid h^+(\mathbb{Q}(\zeta_{p^n}))$ for all $n \geq 1$.* □

Corollary 10.7. *Let $p > 2$ and let $\mathbb{B}_n$ be the unique subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree p^n over $\mathbb{Q}$. Then $p \nmid h(\mathbb{B}_n)$ (note that $\mathbb{B}_\infty/\mathbb{B}_0$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. For $p = 2$, the corresponding result is contained in Corollary 10.6, since $\mathbb{B}_n = \mathbb{Q}(\zeta_{2^{n+2}})^+$).* □

If A is a finite abelian p-group, then

$$A \simeq \oplus \mathbb{Z}/p^{a_i}\mathbb{Z}$$

for some integers a_i. Let

$$n_a = \text{number of } i \text{ with } a_i = a,$$
$$r_a = \text{number of } i \text{ with } a_i \geq a.$$

Then

$$r_1 = p\text{-rank } A = \dim_{\mathbb{Z}/p\mathbb{Z}}(A/A^p)$$

and, more generally,

$$r_a = \dim_{\mathbb{Z}/p\mathbb{Z}}(A^{p^{a-1}}/A^{p^a}).$$

Theorem 10.8. *Let L/K be cyclic of degree n. Let p be prime, $p \nmid n$, and assume all fields E with $K \subseteq E \subsetneq L$ satisfy $p \nmid h_E$. Let A be the p-Sylow subgroup of the ideal class group of L, and let f be the order of p* mod n. *Then*

$$r_a(A) \equiv n_a(A) \equiv 0 \bmod f$$

for all a, where r_a and n_a are as above. In particular, if $p \mid h_L$ then the p-rank of A is at least f and $p^f \mid h_L$.

Proof. Let $V = A^{p^{a-1}}/A^{p^a}$, so V has p^{r_a} elements. Let σ generate $\mathrm{Gal}(L/K)$. Then σ acts on V. Let $v \in V$, $v \neq 0$, and suppose the orbit of v under the action of $\mathrm{Gal}(L/K)$ has less than n elements. Then $\sigma^i v = v$ for some $i < n$, $i \mid n$. Therefore

$$\begin{aligned}\frac{n}{i} v &= (1 + \sigma^i + \sigma^{2i} + \cdots + \sigma^{[(n/i)-1]i})v \\ &= \mathrm{Norm}(v),\end{aligned}$$

where the norm is induced by the norm from L to the subfield of degree i over K. Since p does not divide the class number of this subfield, by assumption, we have $(n/i)v = 0$. But $p \nmid n$, so $v = 0$, contradiction. It follows that the orbit of every $v \neq 0$ has n elements, so $p^{r_a} \equiv 1 \bmod n$. Therefore $f \mid r_a$. Since $n_a = r_a - r_{a+1}$, we obtain $f \mid n_a$. This completes the proof. □

Remark. It is easiest to apply this result when n is prime, so there are no nontrivial intermediate fields. In that case, we only need $p \nmid n$ and $p \nmid h_K$.

As an example for the theorem, consider $\mathbb{Q}(\zeta_{29})$. It can be shown (Exercises for Chapter 11) that its class number is 8. Therefore the class group in $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or $(\mathbb{Z}/2\mathbb{Z})^3$. Which is it? $\mathbb{Q}(\zeta_{29})$ is of degree 28 over $\mathbb{Q}$, hence has a subfield K of degree 4 over $\mathbb{Q}$. By Theorem 10.4, $2 \nmid h_K$. Since $2 \nmid n = 7$ and there are no nontrivial intermediate fields between K and $\mathbb{Q}(\zeta_{29})$, Theorem 10.8 applies. The order f of 2 mod 7 is 3, so the rank of the class group is at least 3. Therefore the class group is $(\mathbb{Z}/2\mathbb{Z})^3$.

§10.2 Reflection Theorems

Let p be an odd prime and let L/K be a Galois extension with $\mathrm{Gal}(L/K) = G$. We assume that $\zeta_p \in L$. Let L' be the maximal unramified elementary (i.e., isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$) abelian p-extension of L. Then $H = \mathrm{Gal}(L'/L) \simeq A/A^p$, where A is the p-Sylow subgroup of the ideal class group of L. Note that L'/K is Galois and H is a normal subgroup of $\mathrm{Gal}(L'/K)$, so G can act on H by conjugation (let $h \in H, h \in G$. Extend g to $\tilde{g} \in \mathrm{Gal}(L'/K)$. Then $h^g = \tilde{g}h\tilde{g}^{-1}$, which is independent of the choice of $\tilde{g}$ since H is abelian). H becomes a $\mathbb{Z}[G]$-module. $\mathbb{Z}[G]$ also acts on A/A^p, and in fact

$$H \simeq A/A^p \quad \text{as } \mathbb{Z}[G]\text{-modules}$$

(see the appendix on class field theory).

Since $\zeta_p \in L$, L'/L is a Kummer extension, so there is a subgroup

$$B \subseteq L^{\times}/(L^{\times})^p$$

such that $L' = L(\sqrt[p]{B})$, in the obvious notation. There is a pairing

$$H \times B \to W_p = p\text{th roots of unity}$$
$$\langle h, b \rangle = \frac{h(b^{1/p})}{b^{1/p}}.$$

It is easy to see that this pairing is nondegenerate ($\langle h, B \rangle = 1 \Leftrightarrow h = 1$, and $\langle H, b \rangle = 1 \Leftrightarrow b = 1$) and bilinear. By Lemma 3.1,

$$B \simeq \hat{H} \simeq H \simeq A/A^p,$$

though the second isomorphism is noncanonical and not G-linear. An easy calculation shows that

$$\langle h^g, b^g \rangle = \langle h, b \rangle^g, \qquad g \in G.$$

Let $b \in B$ (or more accurately $b \bmod (L^{\times})^p \in B$). Since $L(b^{1/p})/L$ is unramified, $(b) = I^p$ for some ideal I of L (Exercise 9.1). Changing b by an element of $(L^{\times})^p$ leaves the ideal class of I unchanged. We therefore have a map

$$\phi: B \to A_p = \{x \in A \mid x^p = 1\}.$$

Clearly $\phi(b^g) = \phi(b)^g$ for $g \in G$. Suppose $\phi(b) = 1$. Then $(b) = (a)^p$, so $b = \varepsilon a^p$ for some $\varepsilon \in E$ = units of L and $a \in L$. Therefore

$$\ker \phi \subseteq E(L^{\times})^p/(L^{\times})^p \simeq E/E^p$$

where the last isomorphism is G-linear.

To summarize, we have

$$B \simeq A/A^p, \quad \text{non-}G\text{-linearly,}$$
$$\phi: B \to A_p, \quad G\text{-linearly, and}$$
$$\ker \phi \simeq \text{subgroup of } E/E^p, \quad G\text{-linearly.}$$

It is precisely the non-G-linearity in the first isomorphism which will make things work (see Exercise 10.8). The basic machinery is now complete; we are ready for the applications.

Theorem 10.9. *Let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$ and let*

$$A = \bigoplus_{i=0}^{p-1} \varepsilon_i A$$

be the direct sum decomposition corresponding to the idempotents of the group ring $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$ (see Proposition 6.16). Let i be even and j odd with $i + j \equiv 1 \bmod (p-1)$. Then

$$p\text{-rank } \varepsilon_i A \le p\text{-rank } \varepsilon_j A \le 1 + p\text{-rank } \varepsilon_i A.$$

(this strengthens the result "$p \mid h^+ \Rightarrow p \mid h^-$").

PROOF. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ in the above. We have

$$H \simeq A/A^p \quad \text{as } G\text{-modules, so}$$
$$\varepsilon_i H \simeq \varepsilon_i(A/A^p) \quad \text{for all } i.$$

Let $h \in \varepsilon_i H$. Then $\sigma_a h = h^{\omega^i(a)}$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Let $b \in \varepsilon_k B$. Then

$$\begin{aligned}\langle h, b\rangle^{\omega(a)} &= \langle h, b\rangle^{\sigma_a} \quad (\text{since } \langle h, b\rangle \in W_p)\\ &= \langle h^{\sigma_a}, b^{\sigma_a}\rangle = \langle h^{\omega^i(a)}, b^{\omega^k(a)}\rangle\\ &= \langle h, b\rangle^{\omega^{i+k}(a)}, \quad \text{for all } a.\end{aligned}$$

If $i + k \not\equiv 1 \bmod (p-1)$ then $\langle h, b\rangle = 1$. Since the pairing between $B = \oplus\, \varepsilon_k B$ and $H = \oplus\, \varepsilon_i H$ is nondegenerate, it follows easily that the induced pairing

$$\varepsilon_i H \times \varepsilon_j B \to W_p, \qquad i + j \equiv 1 \bmod (p-1)$$

is nondegenerate. By Lemma 3.1,

$$\varepsilon_j B \simeq \varepsilon_i H \simeq \varepsilon_i(A/A^p), \quad \text{as abelian groups.}$$

Now, $\phi: B \to A_p$ is G-linear, so

$$\phi: \varepsilon_j B \to \varepsilon_j A_p.$$

We also have

$$(\ker \phi) \cap \varepsilon_j B \simeq \text{subgroup oi } \varepsilon_j(E/E^p).$$

From Propositions 8.10 and 8.13,

$$\varepsilon_j(E/E^p) \simeq \begin{cases} \mathbb{Z}/p\mathbb{Z}, & j \text{ even}, j \not\equiv 0 \bmod (p-1); \text{ or } j \equiv 1 \bmod (p-1);\\ 0, & \text{otherwise.}\end{cases}$$

Let dim denote dimension over $\mathbb{Z}/p\mathbb{Z}$. Note that

$$p\text{-rank } \varepsilon_i A = \dim \varepsilon_i(A/A^p) \quad \text{and} \quad p\text{-rank } \varepsilon_j A = \dim \varepsilon_j A_p.$$

From the above,

$$\dim(\varepsilon_i(A/A^p)) = \dim(\varepsilon_j B) \le \dim(\varepsilon_j(E/E^p)) + \dim(\varepsilon_j A_p).$$

If j is even and $j \not\equiv 0 \bmod (p-1)$, we obtain

$$p\text{-rank}(\varepsilon_i A) \le 1 + p\text{-rank}(\varepsilon_j A).$$

If j is odd and $j \not\equiv 1$, then

$$p\text{-rank}(\varepsilon_i A) \le p\text{-rank}(\varepsilon_j A).$$

If $j \equiv 1$, then we find

$$p\text{-rank}(\varepsilon_0 A) \le 1 + p\text{-rank}(\varepsilon_1 A).$$

However, we already know that $\varepsilon_0 A = \varepsilon_1 A = 0$. by Proposition 6.16. Putting everything together, we obtain the theorem. □

The next result is classical, due to Scholz. We proved a weak form of it in Chapter 5, using p-adic L-functions.

Theorem 10.10. *Let $d > 1$ be square-free. Let r be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$ and s the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3d})$ $(=\mathbb{Q}(\sqrt{-d/3})$ if $3\,|\,d)$. Then*

$$r \leq s \leq r + 1.$$

Proof. Let $L = \mathbb{Q}(\sqrt{d}, \sqrt{-3d})$ and $G = \operatorname{Gal}(L/\mathbb{Q})$. There are three quadratic subfields: $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{-3d})$, and $\mathbb{Q}(\sqrt{-3})$. Let

$$\begin{aligned} \{1, \tau\} &= \operatorname{Gal}(L/\mathbb{Q}(\sqrt{d})), \\ \{1, \sigma) &= \operatorname{Gal}(L/\mathbb{Q}(\sqrt{-3d})), \\ \{1, \sigma\tau\} &= \operatorname{Gal}(L/\mathbb{Q}(\sqrt{-3})). \end{aligned}$$

In $\mathbb{Z}_3[G]$ we may decompose the identity as a sum of idempotents:

$$\begin{aligned} 1 &= \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 \\ &= \left(\frac{1+\tau}{2}\right)\left(\frac{1+\sigma}{2}\right) + \left(\frac{1+\tau}{2}\right)\left(\frac{1-\sigma}{2}\right) + \left(\frac{1-\tau}{2}\right)\left(\frac{1+\sigma}{2}\right) \\ &\quad + \left(\frac{1-\tau}{2}\right)\left(\frac{1-\sigma}{2}\right). \end{aligned}$$

Let A be the 3-Sylow subgroup of the ideal class group of L. Then $A = \bigoplus \varepsilon_i A$. Since $\varepsilon_1 = (\text{Norm } L/\mathbb{Q})/4$, we have $\varepsilon_1 A = 0$. Also,

$$\varepsilon_4 = \tfrac{1}{4}(1 - \tau)(1 + \sigma\tau) = \tfrac{1}{4}(1 - \tau)(\text{Norm } L/\mathbb{Q}(\sqrt{-3})),$$

so $\varepsilon_4 A = 0$, since $h(\mathbb{Q}(\sqrt{-3})) = 1$. We now have

$$A = \varepsilon_2 A \oplus \varepsilon_3 A.$$

But

$$\varepsilon_2 = \tfrac{1}{4}(1 - \sigma)(\text{Norm } L/\mathbb{Q}(\sqrt{d})),$$

so

$$\varepsilon_2 A \subseteq A_{\mathbb{Q}(\sqrt{d})},$$

where the last group is the 3-Sylow subgroup of the class group of $\mathbb{Q}(\sqrt{d})$. Let $a \in A_{\mathbb{Q}(\sqrt{d})}$. Then $\tau a = a$. Since $1 + \sigma = \text{Norm}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, $(1 + \sigma)a = 0$, hence $\sigma a = -a$. It follows that $\varepsilon_2 a = a$, so

$$A_{\mathbb{Q}(\sqrt{d})} \subseteq \varepsilon_2 A.$$

Therefore

$$\varepsilon_2 A = A_{\mathbb{Q}(\sqrt{d})}.$$

Similarly

$$\varepsilon_3 A = A_{\mathbb{Q}(\sqrt{-3d})}.$$

We now use the machinery at the beginning of this section. We have $B = \bigoplus \varepsilon_j B$. A calculation similar to that in Theorem 10.9 shows that

$$\langle \varepsilon_i H, \varepsilon_j B \rangle = 1$$

unless $i = 2, j = 3$ or $i = 3, j = 2$. For example, if $h \in \varepsilon_2 H$ and $b \in \varepsilon_4 B$ then $\sigma h = h^{-1}$ and $\sigma b = b^{-1}$, so

$$\langle h, b \rangle = \langle h^{-1}, b^{-1} \rangle = \langle h^\sigma, b^\sigma \rangle = \langle h, b \rangle^\sigma.$$

But $\sigma \notin \mathrm{Gal}(L/\mathbb{Q}(\sqrt{-3}))$, so $\sigma(\zeta_3) \neq \zeta_3$. Therefore $\langle h, b \rangle = 1$.

Since $H \times B \to W_3$ is nondegenerate, we must have

$$\varepsilon_2 H \times \varepsilon_3 B \to W_3, \quad \text{and}$$
$$\varepsilon_3 H \times \varepsilon_2 B \to W_3$$

nondegenerate. Also,

$$\phi\colon \varepsilon_2 B \to \varepsilon_2 A_3,$$
$$\phi\colon \varepsilon_3 B \to \varepsilon_3 A_3,$$
$$(\ker \phi) \cap \varepsilon_2 B \simeq \text{subgroup of } \varepsilon_2(E/E^3), \text{ and}$$
$$(\ker \phi) \cap \varepsilon_3 B \simeq \text{subgroup of } \varepsilon_3(E/E^3).$$

Since $\varepsilon_2 = \frac{1}{4}(1 - \sigma)(\mathrm{Norm}\ L/\mathbb{Q}(\sqrt{d}))$, $\varepsilon_2(E/E^3)$ is contained in the units of $\mathbb{Q}(\sqrt{d})$ mod 3rd powers. Therefore

$$\varepsilon_2(E/E^3) \simeq 0 \quad \text{or} \quad \mathbb{Z}/3\mathbb{Z}.$$

Similarly,

$$\varepsilon_3 = \tfrac{1}{4}(1 - \tau)(\mathrm{Norm}\ L/\mathbb{Q}(\sqrt{-3d})).$$

Since $d \neq 1$, $\mathbb{Q}(\sqrt{-3d}) \neq \mathbb{Q}(\sqrt{-3})$, so the units of $\mathbb{Q}(\sqrt{-3d})$ are either $\{\pm 1\}$ or $\{\pm 1, \pm\sqrt{-1}\}$. Consequently

$$\varepsilon_3(E/E^3) = 0.$$

Putting everything together, we obtain,

$$\begin{aligned} r &= 3\text{-rank } A_{\mathbb{Q}(\sqrt{d})} = 3\text{-rank } \varepsilon_2 A \\ &= 3\text{-rank } \varepsilon_2 H = 3\text{-rank } \varepsilon_3 B \\ &\leq 3\text{-rank } \varepsilon_3(E/E^3) + 3\text{-rank } \varepsilon_3 A \\ &= 0 + 3\text{-rank } A_{\mathbb{Q}(\sqrt{-3d})} = s, \end{aligned}$$

and similarly,

$$s \leq 1 + r.$$

This completes the proof. □

Remark. The cases $r = s$ and $r + 1 = s$ both occur. For $d = 79$, $r = s = 1$, while for $d = 69$, $r = 0$, $s = 1$.

Theorem 10.11. *Let p be an odd prime. Let L be a CM-field with $\zeta_p \in L$, and let A be the p-Sylow subgroup of the ideal class group of L. Then*

$$p\text{-rank } A^+ \leq 1 + p\text{-rank } A^-.$$

Let W be the roots of unity in L. If $L(W^{1/p})/L$ is (totally) ramified, then

$$p\text{-rank } A^+ \leq p\text{-rank } A^-.$$

(As usual, $A^{\pm} = \{x \in A \,|\, \bar{x} = x^{\pm 1}\}$ and $A^+ \simeq A(L^+)$).

Proof. In the notation at the beginning of the section, let $K = L^+$, the maximal real subfield of L. Then $G = \mathrm{Gal}(L/K) = \{1, J\}$, where $J =$ complex conjugation, and

$$A^+ = \frac{1 + J}{2} A, \qquad A^- = \frac{1 - J}{2} A.$$

As in the above theorems $\langle H^+, B^+ \rangle = \langle H^-, B^- \rangle = 1$ (since $p \neq 2$), so

$$H^+ \times B^- \to W_p$$

is nondegenerate. Also,

$$\phi : B^- \to A_p^-,$$

and

$$(\ker \phi) \cap B^- \simeq \text{subgroup of } (E/E^p)^-.$$

Since $[E : WE^+] = 1$ or 2 (Theorem 4.12),

$$(E/E^p)^- = (W/W^p)^- \simeq \mathbb{Z}/p\mathbb{Z}.$$

Therefore

$$\begin{aligned} p\text{-rank } A^+ &= p\text{-rank } H^+ = p\text{-rank } B^- \\ &\leq 1 + p\text{-rank } A^-. \end{aligned}$$

If $L(W^{1/p})/L$ is ramified then $W \cap B = 1$, since $L(B^{1/p})/L$ is unramified. Therefore $(\mathrm{Ker}\, \phi) \cap B^- = 0$ and the "1" disappears from the above inequality. This completes the proof. □

If $p = 2$, the above result holds if we modify A^+. Note that

$$A^+ \cap A^- \subseteq \{x \in A \mid x^2 = 1\},$$

which does not allow us to conclude that the intersection is trivial for $p = 2$. In fact, for $\mathbb{Q}(\sqrt{-5})$, $A^+ = A^- = A \simeq \mathbb{Z}/2\mathbb{Z}$. Also, observe that if x is an ideal class of L^+ with $x^2 = 1$ then $x \in A^+ \cap A^-$. However, we actually want to be able to transfer information from h^- to h^+, so instead of A^+ we should be looking at the 2-Sylow subgroup of the class group of L^+, whose order is the 2-part of h^+. Instead of the decomposition $A = A^+ \oplus A^-$ obtained for odd p, we have an exact sequence

$$1 \to A_L^- \to A_L \to A_{L^+} \to 1,$$

which is induced by the norm (i.e., $1 + J$) from L to L^+ (cf. Theorem 10.1).

Proposition 10.12. *Let L be a CM-field and let A_L and A_{L^+} be the 2-Sylow subgroups of the ideal class groups of L and L^+, respectively. Then*

$$\text{2-rank } A_{L^+} \leq 1 + \text{2-rank } A_L^-.$$

Proof. Let $i(A_{L^+})$ denote the image in A_L and let $(A_{L^+})_2$ and $(A_L^-)_2$ denote the elements of order 2 in the respective groups. As noted above,

$$i((A_{L^+})_2) \subseteq (A_L^-)_2.$$

Therefore

$$\text{2-rank } i((A_{L^+})_2) \leq \text{2-rank } A_L^-.$$

But

$$\frac{|(A_{L^+})_2|}{|i((A_{L^+})_2)|} = 1 \text{ or } 2$$

by Theorem 10.3. Since the elements of order 2 determine the 2-rank,

$$-1 + \text{2-rank}(A_{L^+}) \leq \text{2-rank } i((A_{L^+})_2) \leq \text{2-rank } A_L^-.$$

This completes the proof. □

Finally, we use the Kummer pairing to give another characterization of irregular primes. □

Proposition 10.13. *Let p be odd. Then p divides $h(\mathbb{Q}(\zeta_p))$ if and only if there is an extension $K/\mathbb{Q}(\zeta_p)^+$, with $K \neq \mathbb{Q}(\zeta_{p^2})^+$ and* $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p)^+) \simeq \mathbb{Z}/p\mathbb{Z}$, *which is unramified at all primes not above p.*

Proof. First assume that such a K exists. Let F be the maximal elementary abelian p-extension of $\mathbb{Q}(\zeta_p)^+$ which is unramified outside p. Then $F/\mathbb{Q}$ is Galois and also $F(\zeta_p)/\mathbb{Q}$ is Galois. As before, $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on $H = \mathrm{Gal}(F(\zeta_p)/\mathbb{Q}(\zeta_p))$. Since F is real, complex conjugation acts trivially, so

$\varepsilon_i H = 1$ for all odd i (where ε_i is the usual idempotent for G). Suppose that $H = \varepsilon_0 H$. Then $h^g = h$ for all $g \in G$. Recall the definition $h^g = \tilde{g}h\tilde{g}^{-1}$, where $\tilde{g}$ is an extension of g to $F(\zeta_p)$. We find that $\tilde{g}h = h\tilde{g}$ for all $h \in H$, $g \in G$. Since G is cyclic, we may choose the $\tilde{g}$'s so they commute with each other. It follows that $\mathrm{Gal}(F(\zeta_p)/\mathbb{Q})$ is abelian. By the Kronecker–Weber theorem (14.1), and since $F(\zeta_p)/\mathbb{Q}$ is unramified outside p, $F(\zeta_p) \subseteq \mathbb{Q}(\zeta_{p^n})$ for some n. Therefore $F \subseteq \mathbb{Q}(\zeta_{p^n})^+$. By the choice of K, this is impossible, so $H \neq \varepsilon_0 H$, hence $\varepsilon_i H \neq 1$ for some even $i \neq 0$.

Since $F(\zeta_p)/\mathbb{Q}(\zeta_p)$ is a Kummer extension, there is a subgroup $B \subseteq \mathbb{Q}(\zeta_p)^\times/(\mathbb{Q}(\zeta_p)^\times)^p$ such that $F(\zeta_p) = \mathbb{Q}(\zeta_p)(B^{1/p})$. There is a nondegenerate bilinear pairing

$$H \times B \to W_p$$

such that

$$\langle h^g, b^g \rangle = \langle h, b \rangle^g, \qquad g \in G.$$

As before, the fact that $\varepsilon_i H \neq 1$ for some even $i \neq 0$ implies that $\varepsilon_j B \neq 1$ for some odd $j \neq 1$ $(i + j \equiv 1 \bmod p - 1)$. Choose $b \in \varepsilon_j B$, $b \neq 1$. Then $\mathbb{Q}(\zeta_p, b^{1/p})/\mathbb{Q}(\zeta_p)$ is unramified outside p, hence $(b) = I^p(\zeta_p - 1)^d$ for some ideal I and some integer d. Since $b \in \varepsilon_j B$, $b^{\sigma_a} = b^{a^j}c^p$, with $c \in \mathbb{Q}(\zeta_p)$; for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Also, $(\zeta_p - 1)^{\sigma_a} = (\zeta_p - 1)$. Therefore

$$(I^{\sigma_a})^p(\zeta_p - 1)^d = (b)^{\sigma_a} = (b)^{a^j}(c)^p = (I^{a^j})^p(\zeta_p - 1)^{da^j}(c)^p.$$

It follows that $d - da^j \equiv 0 \bmod p$, hence $d \equiv 0 \bmod p$. We therefore have $(b) = I^p$ for some ideal I of $\mathbb{Q}(\zeta_p)$.

Suppose now that I is principal, so $I = (\alpha)$. Then $\eta\alpha^p = b$ for some unit η. We may change b by a pth power, hence assume $b = \eta$. Write $b = \zeta_p^r\eta_1$ with η_1 real. Since ζ_p^r is in the ε_1 component and η_1 is real, it is impossible for $\zeta_p^r\eta_1$ to lie in the ε_j component with odd $j \neq 1$. This contradiction shows that I is nonprincipal. Since I^p is principal, we must have $p \mid h(\mathbb{Q}(\zeta_p))$.

Conversely, suppose $p \mid h(\mathbb{Q}(\zeta_p))$. Then $p \mid h^-(\mathbb{Q}(\zeta_p))$ so the ε_j component of the class group is nontrivial of some odd j. By Proposition 6.16, $j \neq 1$. Let I (nonprincipal) be an ideal representing a class of order p in the ε_j component: $I^p = (b)$ and $I^{\varepsilon_j} \equiv I$ mod principal ideals. Let

$$\beta \equiv b^{\varepsilon_j} \bmod (\mathbb{Q}(\zeta_p)^\times)^p.$$

Since (β) is the pth power of an ideal, Exercise 9.1 implies that $\mathbb{Q}(\zeta_p, \beta^{1/p})/\mathbb{Q}(\zeta_p)$ is unramified outside p. If B_1 denotes the subgroup of $\mathbb{Q}(\zeta_p)^\times/(\mathbb{Q}(\zeta_p)^\times)^p$ corresponding to the maximal elementary abelian p-extension of $\mathbb{Q}(\zeta_p)$ unramified outside p (call it F_1), then $\beta \in \varepsilon_j B_1$. We claim β is nontrivial. Suppose $\beta = \alpha^p$. Then, modulo pth powers of principal ideals,

$$1 \equiv (\alpha)^p = (\beta) \equiv (b)^{\varepsilon_j} = I^{p\varepsilon_j} \equiv I^p,$$

so I^p is the pth power of a principal ideal; hence I is principal, which is a contradiction. This proves the claim that β is nontrivial in $\varepsilon_j B$. Therefore

$\varepsilon_j B_1 \neq 1$. Let $H_1 = \mathrm{Gal}(F_1/\mathbb{Q}(\zeta_p))$. Via the Kummer pairing $H_1 \times B_1 \to W_p$, we find that $\varepsilon_i H_1$ is nontrivial for some even $i \neq 0$. Let K_1 be the corresponding extension of $\mathbb{Q}(\zeta_p)$; that is, $\mathrm{Gal}(K_1/\mathbb{Q}(\zeta_p)) = \varepsilon_i H_1$. It is clear that K_1 is Galois over $\mathbb{Q}$. Since i is even, complex conjugation J commutes with $\varepsilon_i H_1$. Therefore the group generated by J and $\varepsilon_i H_1$ has order $2|\varepsilon_i H_1|$, so the fixed field must be $\mathbb{Q}(\zeta_p)^+$. Since K_1^+ is the fixed field of J, we find that

$$\mathrm{Gal}(K_1^+/\mathbb{Q}(\zeta_p)^+) \simeq \varepsilon_i H_1 \neq 1.$$

Since $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})^+/\mathbb{Q}(\zeta_p)^+)$ is in the ε_0 component and since $i \neq 0$, we have $K_1^+ \cap \mathbb{Q}(\zeta_{p^2})^+ = \mathbb{Q}(\zeta_p)^+$. Clearly $K_1^+/\mathbb{Q}(\zeta_p)^+$ is unramified outside p. If we take a subfield $K \subseteq K_1^+$ such that $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p)^+) \simeq \mathbb{Z}/p\mathbb{Z}$, we obtain the desired field. This completes the proof. □

§10.3 Consequences of Vandiver's Conjecture

In this section we assume that Vandiver's conjecture holds, namely that p does not divide the class number of $\mathbb{Q}(\zeta_p)^+$. By Corollary 10.6, this implies that p also does not divide the class number of $\mathbb{Q}(\zeta_{p^n})^+$ for all $n \geq 1$. It is not clear whether or not Vandiver's conjecture should be true in general, but, as we mentioned in Chapter 9, it seems that it should hold for a large majority of primes (at present it is known to be true for all $p < 125000$). Hence the following results are possibly a good approximation to the truth in general.

Theorem 10.14. *Let p be odd and assume $p \nmid h(\mathbb{Q}(\zeta_p)^+)$. Let $A_n = A_n^-$ be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_{p^{n+1}})$, let*

$$R_{p,n} = \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})],$$

and let $I_{p,n}$ be the Stickelberger ideal (see Chapter 6). Then A_n^- is cyclic as a module over $R_{p,n}$ and

$$A_n^- \simeq R_{p,n}^-/I_{p,n}^-$$

as modules over $R_{p,n}$. In other words, the Stickelberger ideal gives all the relations in A_n^-.

Proof. The main part of the proof involves proving the cyclicity. The rest follows easily.

For $n = 0$ the result is an immediate consequence of Theorem 10.9, but in general we have to work a little more. We use the ideas of the previous section, but we must look more closely at the units. Recall that in the notation of the previous section, $\ker \phi \subset E/E^p$. Since the structure of E is fairly well understood, it is convenient to use all of E/E^p, rather than just a subgroup.

To do so, we must enlarge B. Therefore, let L'' be the maximal elementary abelian p-extension of $L = \mathbb{Q}(\zeta_{p^{n+1}})$ which is unramified at all primes except possibly $\not{p} = (1 - \zeta_{p^{n+1}})$, which is the prime above p. Then $L'' = L(\sqrt[p]{B'})$ for some subgroup $B' \subseteq L^\times/(L^\times)^p$. Let $H' = \mathrm{Gal}(L''/L)$. There is a nondegenerate bilinear pairing

$$H' \times B' \to W_p,$$

satisfying

$$\langle h^g, b^g \rangle = \langle h, b \rangle^g \quad \text{for } g \in G'' = \mathrm{Gal}(L''/\mathbb{Q}).$$

Let $b \in B'$. Then, as in the previous section,

$$(b) = I^p \not{p}^d$$

for some ideal I and some integer d. The $\not{p}$ must be singled out because of possible ramification at $\not{p}$. We obtain a map

$$\begin{aligned} \phi' \colon B' &\to A_p = \{x \in A \mid x^p = 1\} \\ b &\mapsto \text{class of } I. \end{aligned}$$

If $\phi'(b) = 1$ then $b = \varepsilon(1 - \zeta_{p^{n+1}})^d \cdot a^p$ for some unit ε and some $a \in \mathbb{Q}(\zeta_{p^{n+1}})$. Conversely, if b is of this form then $L(b^{1/p})/L$ is unramified outside $\not{p}$, so $b \in B'$ and clearly $\phi'(b) = 1$. Therefore $\ker \phi'$ is generated by E and $1 - \zeta_{p^{n+1}}$.

Since we are assuming $p \nmid h^+$, we have $p \nmid [E^+ : C^+]$ by Theorem 8.2, where C^+ denotes the real cyclotomic units. Since

$$E = \langle \zeta_{p^{n+1}} \rangle \times E^+ \quad \text{and} \quad C = \langle \zeta_{p^{n+1}} \rangle \times C^+,$$

we also have $p \nmid [E : C]$. Therefore C generates E/E^p. It follows from Lemma 8.1 that $\ker \phi'$ is generated over $R_{p,n}$ by $1 - \zeta_{p^{n+1}}$ (note that $\zeta = -(1-\zeta)/(1-\zeta^{-1})$). Consequently, $(\ker \phi')^+$ is generated by $(1 - \zeta_{p^{n+1}})(1 - \zeta_{p^{n+1}}^{-1})$. In fact,

$$\{((1 - \zeta_{p^{n+1}})(1 - \zeta_{p^{n+1}}^{-1}))^{\sigma_a} \mid 1 \le a < \tfrac{1}{2}p^n, (a, p) = 1\}$$

is a basis for $(\ker \phi')^+$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$. Note that $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ acts transitively on the elements of this basis.

If $p \nmid h^+$ then $A_p^+ = 1$. Therefore

$$(B')^+ = (\ker \phi')^+,$$

so $(B')^+$ is cyclic over $R_{p,n}$ (to obtain cyclicity is the reason we enlarged B). As before, the pairing

$$(H')^- \times (B')^+ \to W_p$$

is nondegenerate. We claim that $(H')^-$ is cyclic over $R_{p,n}$. Let $\{h_1, \ldots, h_r\}$ be the dual basis of $(H')^-$ corresponding to the basis of $(B')^+$ constructed above (call it $\{b_1, \ldots, b_r\}$). Then

$$\langle h_i, b_j \rangle = \begin{cases} \zeta_p, & i = j \\ 1, & i \neq j. \end{cases}$$

Let H_1 be the $R_{p,n}$-submodule of $(H')^-$ generated by h_1. Suppose $H_1 \neq (H')^-$. Then, by Proposition 3.3 or 3.4, there exists $b = \sum x_i b_i \neq 0$ in B $(x_i \in \mathbb{Z})$ such that $\langle H_1, b\rangle = 1$. In particular,

$$1 = \langle h_1^g, b\rangle = \langle h_1, b^{g^{-1}}\rangle^g,$$

so

$$\langle h_1, b^{g^{-1}}\rangle = 1, \quad \text{for all } g \in G.$$

Letting $g = 1$ we find

$$1 = \langle h_1, b\rangle = \zeta_p^{x_1}, \quad \text{hence } x_1 \equiv 0 \bmod p,$$

and since G acts transitively on $\{b_1, \ldots, b_r\}$, we may use other choices of g to obtain $x_i \equiv 0 \bmod p$ for all i. Therefore $b = 0$. It follows that $H_1 = (H')^-$, so $(H')^-$ is cyclic over $R_{p,n}$, as desired.

Returning to the beginning of the proof, we observe that $L' \subseteq L''$, so $H = \mathrm{Gal}(L'/L)$ is a quotient of $H' = \mathrm{Gal}(L''/L)$. Consequently, $H^- \simeq (A_n/A_n^p)^-$ is cyclic over $R_{p,n}$.

Let $x_0 \in A_n^-$ generate $(A_n/A_n^p)^-$. Let $x \in A_n^-$. Then

$$x = r_0 x_0 + p y_1, \quad \text{with } r_0 \in R_{p,n} \quad \text{and} \quad y_1 \in A_n^-.$$

But

$$y_1 = r_1 x_0 + p y_2, \quad \text{etc.}$$

Therefore

$$x = (r + pr_1 + \cdots)x_0,$$

so x_0 generates A_n^- over $R_{p,n}$. Therefore A_n^- is cyclic as an $R_{p,n}$-module.

Let x_0 be a generator for A_n^- over $R_{p,n}$, hence over $R_{p,n}^-$. Then we have a surjective $R_{p,n}$-homomorphism

$$R_{p,n}^- \to A_n^-,$$
$$r \mapsto r x_0.$$

By Stickelberger's theorem, $I_{p,n}^-$ is contained in the kernel. Since

$$[R_{p,n}^- : I_{p,n}^-] = |A_n^-|$$

by Theorem 6.21, the kernel is exactly $I_{p,n}^-$. This completes the proof. □

Corollary 10.15. *Let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$ and let*

$$A = \bigoplus_{i=0}^{p-2} \varepsilon_i A$$

be the decomposition according to idempotents. If $p \nmid h(\mathbb{Q}(\zeta_p)^+)$ then

$$\varepsilon_i A \simeq \mathbb{Z}_p / B_{1,\omega^{-i}} \mathbb{Z}_p \quad \text{for } i = 3, 5, \ldots, p-2.$$

Proof. By Theorem 10.14, each $\varepsilon_i A$ is a cyclic group. By Proposition 6.16, $B_{1,\omega^{-i}}$ annihilates $\varepsilon_i A$, so

$$|\varepsilon_i A| \leq p\text{-part of } B_{1,\omega^{-i}}.$$

Since

$$\begin{aligned}\prod_{\substack{i=3\\ i\,\text{odd}}}^{p-2} |\varepsilon_i A| = |A^-| &= p\text{-part of } h^- \\ &= p\text{-part of } 2p \prod_{\substack{i=1\\ i\,\text{odd}}}^{p-2} \left(-\tfrac{1}{2}B_{1,\omega^i}\right) \\ &= p\text{-part of } \prod_{i \neq p-2} (B_{1,\omega^i})\end{aligned}$$

(see the proof of Theorem 5.16), the inequalities must all be equalities. This completes the proof. □

Remark. It has recently been proved unconditionally by Mazur and Wiles that $|\varepsilon_i A| = p$-part of $B_{1,\omega^{-i}}$. It is a consequence of the "Main Conjecture" (see Chapter 13).

For the next result, recall that if $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p))$ and if γ_0 is a topological generator of Γ_0, then $\mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]]$, with γ_0 corresponding to $1 + T$. See Theorem 7.1. Hence a $\mathbb{Z}_p[[\Gamma]]$-module may be regarded as a $\mathbb{Z}_p[[T]]$-module. Let A_n be as above, so A_n is a $\mathbb{Z}_p[[\Gamma/\Gamma^{p^n}]]$-module. The norm map N_n from A_n to A_{n-1} commutes with the action of the group ring. Take the inverse limit $\varprojlim A_n$ with respect to the norm mappings. If

$$(\ldots, a_{n-1}, a_n, \ldots) \in \varprojlim A_n$$

and

$$(\ldots, y_{n-1}, y_n, \ldots) \in \varprojlim \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$$

then

$$N_n(y_n a_n) = y_n N_n(a_n) = y_{n-1} a_{n-1}$$

(since y_n restricts to y_{n-1}). Therefore

$$(\ldots, y_{n-1}a_{n-1}, y_n a_n, \ldots) \in \varprojlim A_n,$$

so $\varprojlim A$ is a $\mathbb{Z}_p[[\Gamma]]$-module.

We may also decompose each A_n according to the idempotents

$$\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1} \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})] \subseteq R_{p,n}.$$

Each component $\varprojlim \varepsilon_i A_n$ is also a $\mathbb{Z}_p[[\Gamma]]$-module.

Theorem 10.16. *Assume $p \nmid h(\mathbb{Q}(\zeta_p)^+)$. Let $P_n(T) = (1 + T)^{p^n} - 1$. Then, for $i = 3, 5, \ldots, p - 2$,*

$$\varepsilon_i A_n \simeq \mathbb{Z}_p[[T]]/(P_n(T), f(T, \omega^{1-i}))$$

and

$$\varprojlim \varepsilon_i A \simeq \mathbb{Z}_p[[T]]/(f(T, \omega^{1-i}))$$

as modules over $\mathbb{Z}_p[[T]]$, where $f(T, \omega^{1-i})$ is the power series satisfying

$$f((1 + p)^s - 1, \omega^{1-i}) = L_p(s, \omega^{1-i})$$

(see Theorem 7.10). For $i = 1$, $\varepsilon_1 A_n = 0$ for all n.

Proof. By Theorem 10.1, the norm map $A_n \to A_{n-1}$ is surjective, so $\varepsilon_i A_n \to \varepsilon_i A_{n-1}$ is also surjective. Since $p \nmid h^+$, each $\varepsilon_i A_n$ is cyclic as an $R_{p,n}$-module. If b_n generates $\varepsilon_i A_n$ over $R_{p,n}$, then the norm of b_n generates $\varepsilon_i A_{n-1}$ over $R_{p,n-1}$. This allows us to obtain arbitrarily long sequences $(b_0, \ldots, b_n)$ such that each b_j is a generator for $\varepsilon_i A_j$. Since $\varepsilon_i A_0$ is finite, there is some a_0 such that there are arbitrarily long sequences starting with a_0. Similarly, there is an $a_1 \in \varepsilon_i A_1$ whose norm is a_0 and such that there are arbitrarily long sequences starting with (a_0, a_1). Continuing, we obtain a sequence

$$(a_0, a_1, \ldots) \in \varprojlim \varepsilon_i A_n$$

such that a_n is a generator for $\varepsilon_i A_n$ for each n.

Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Let

$$\theta_{p^n} \in \mathbb{Q}_p[\Delta][\Gamma/\Gamma^{p^n}]$$

be the Stickelberger element. Then $I_{p,n}$ is generated by elements of the form $(c - \sigma_c)\theta_{p^{n+1}}$ (Lemma 6.9). Therefore $\varepsilon_i I_{p,n}$ is generated by elements of the form (recall $\gamma_c = \sigma_{\langle c \rangle}$; see Chapter 7)

$$(c - \omega^i(c)\gamma_c)\varepsilon_i \theta_{p^{n+1}}.$$

If we take $c = 1 + p$ and $i = 1$, then this corresponds to an invertible power series by Lemma 7.12. This yields $\varepsilon_1 A_n = 0$ for all n. If $i \neq 1$ and c is a primitive root mod p, then $c - \omega^i(c)\gamma_c$ corresponds to a power series with constant term $c - \omega^i(c) \not\equiv 0 \bmod p$, hence to an invertible power series which may be ignored. By Iwasawa's construction of p-adic L-functions (Chapter 7), $\varepsilon_i \theta_{p^{n+1}}$ corresponds to a polynomial

$$f_n(T, \omega^{1-i}) \in \mathbb{Z}_p[T]$$

such that

$$f(T, \omega^{1-i}) \equiv f_n(T, \omega^{1-i}) \bmod P_n(T),$$

where f is as in the statement of the theorem. From Theorem 10.14,

$$\mathbb{Z}_p[T]/(f_n(T, \omega^{1-i}), P_n(T)) \simeq \varepsilon_i A_n$$
$$g(T) \mapsto g(T)a_n,$$

where a_n is the generator obtained above. We claim this gives us an isomorphism

$$\varprojlim \mathbb{Z}_p[[T]]/(f, P_n) \simeq \varprojlim \varepsilon_i A_n.$$

Clearly an element on the left yields an element on the right side via the map defined above. Conversely, suppose $(y_0, y_1, \ldots) \in \varprojlim \varepsilon_i A_n$. Then $y_n = g_n(T)a_n$ for some g_n. Since $g_n(T)a_{n-1} = g_n(T)$ Norm$(a_n) =$ Norm$(g_n(T)a_n) = g_{n-1}(T)a_{n-1}$, we must have

$$g_n(T) - g_{n-1}(T) \in (f_{n-1}, P_{n-1}).$$

It follows that

$$(g_0, g_1, \ldots) \in \varprojlim \mathbb{Z}_p[[T]]/(f, P_n),$$

so $(y_0, y_1, \ldots)$ is in the image of the map. Since we have an injection at each level, we have an isomorphism as claimed.

It remains to evaluate the inverse limit. Clearly there is a map

$$\phi: \mathbb{Z}_p[[T]] \to \varprojlim \mathbb{Z}_p[[T]]/(f, P_n)$$

If $\phi(g) = 0$ then, for each n,

$$g = B_n f + B_n' P_n, \quad \text{with } B_n, B_n' \in \mathbb{Z}_p[[T]].$$

Since $P_n \to 0$ in $\mathbb{Z}_p[[T]]$, $\lim B_n = B$ exists. Therefore f divides g, so $\ker \phi = (f)$. Now suppose

$$(g_0, g_1, \ldots) \in \varprojlim \mathbb{Z}_p[[T]]/(f, P_n).$$

Then

$$g_{n+1} = g_n + C_n f + D_n P_n, \quad \text{with } C_n, D_n \in \mathbb{Z}_p[[T]].$$

Let

$$g_n' = g_n - \left(\sum_{j<n} C_j\right) f.$$

Then

$$g_{n+1}' = g_n' + D_n P_n,$$

so

$$(g_0', g_1', \ldots) \in \varprojlim \mathbb{Z}_p[[T]]/(P_n) = \mathbb{Z}_p[[T]]$$

(see the proof of Theorem 7.1). Therefore there is a power series g such that

$$g \equiv g_n' \bmod P_n,$$

where f is as in the statement of the theorem. From Theorem 10.14,

$$\mathbb{Z}_p[T]/(f_n(T, \omega^{1-i}), P_n(T)) \simeq \varepsilon_i A_n$$
$$g(T) \mapsto g(T)a_n,$$

where a_n is the generator obtained above. We claim this gives us an isomorphism

$$\varprojlim \mathbb{Z}_p[[T]]/(f, P_n) \simeq \varprojlim \varepsilon_i A_n.$$

Clearly an element on the left yields an element on the right side via the map defined above. Conversely, suppose $(y_0, y_1, \ldots) \in \varprojlim \varepsilon_i A_n$. Then $y_n = g_n(T)a_n$ for some g_n. Since $g_n(T)a_{n-1} = g_n(T) \operatorname{Norm}(a_n) = \operatorname{Norm}(g_n(T)a_n) = g_{n-1}(T)a_{n-1}$, we must have

$$g_n(T) - g_{n-1}(T) \in (f_{n-1}, P_{n-1}).$$

It follows that

$$(g_0, g_1, \ldots) \in \varprojlim \mathbb{Z}_p[[T]]/(f, P_n),$$

so $(y_0, y_1, \ldots)$ is in the image of the map. Since we have an injection at each level, we have an isomorphism as claimed.

It remains to evaluate the inverse limit. Clearly there is a map

$$\phi: \mathbb{Z}_p[[T]] \to \varprojlim \mathbb{Z}_p[[T]]/(f, P_n)$$

If $\phi(g) = 0$ then, for each n,

$$g = B_n f + B_n' P_n, \quad \text{with } B_n, B_n' \in \mathbb{Z}_p[[T]].$$

Since $P_n \to 0$ in $\mathbb{Z}_p[[T]]$, $\lim B_n = B$ exists. Therefore f divides g, so $\ker \phi = (f)$. Now suppose

$$(g_0, g_1, \ldots) \in \varprojlim \mathbb{Z}_p[[T]]/(f, P_n).$$

Then

$$g_{n+1} = g_n + C_n f + D_n P_n, \quad \text{with } C_n, D_n \in \mathbb{Z}_p[[T]].$$

Let

$$g_n' = g_n - \left(\sum_{j<n} C_j\right) f.$$

Then

$$g_{n+1}' = g_n' + D_n P_n,$$

so

$$(g_0', g_1', \ldots) \in \varprojlim \mathbb{Z}_p[[T]]/(P_n) = \mathbb{Z}_p[[T]]$$

(see the proof of Theorem 7.1). Therefore there is a power series g such that

$$g \equiv g_n' \bmod P_n,$$

hence

$$g \equiv g_n \bmod (f, P_n), \quad \text{for all } n.$$

This proves that ϕ is surjective. Therefore

$$\mathbb{Z}_p[[T]]/(f) \simeq \varprojlim \mathbb{Z}_p[[T]]/(f, P_n) \simeq \varprojlim \varepsilon_i A_n.$$

This completes the proof of Theorem 10.16. □

Remark. This result is rather amazing since it enables us to define an analytic object, namely the p-adic L-function, in terms of algebraic objects, namely ideal class groups. A similar situation exists for function fields (see Chapter 13).

A slightly weaker form of this theorem has been proved by Mazur and Wiles, without the assumption $p \nmid h^+$. See Section 13.6.

Corollary 10.17. *Suppose $p \nmid h(\mathbb{Q}(\zeta_p)^+)$. Let $i_1, \dots, i_s$ be the even indices i such that $2 \le i \le p - 3$ and $p \mid B_i$. If*

$$B_{1, \omega^{i-1}} \not\equiv 0 \bmod p^2$$

and

$$\frac{B_i}{i} \not\equiv \frac{B_{i+p-1}}{i+p-1} \bmod p^2 \quad \textit{for all } i \in \{i_1, \dots, i_s\}$$

then

$$A_n \simeq (\mathbb{Z}/p^{n+1}\mathbb{Z})^s$$

for all $n \ge 0$.

Remark. The above Bernoulli numbers are always divisible by p, but the above incongruences hold mod p^2 for all $p < 125000$. But there does not seem to be any reason to believe this in general. The above yields, for p as above,

$$\mu = 0, \quad \lambda = \nu = i(p)$$

where λ, μ, ν are the Iwasawa invariants (see Theorem 7.14 or Chapter 13) and $i(p) = s$ is the index of irregularity.

Proof. Let $f(T, \omega^i) = a_0 + a_1 T + \cdots$, with $a_j \in \mathbb{Z}_p$ for all p. Then, for $s \in \mathbb{Z}_p$,

$$L_p(s, \omega^i) = f((1+p)^s - 1, \omega^i) \equiv a_0 + a_1 sp \bmod p^2.$$

Since $B_2 = \frac{1}{6}$ we must have $i \ge 4$, so

$$\frac{B_i}{i} \equiv (1 - p^{i-1}) \frac{B_i}{i} = -L_p(1 - i, \omega^i) \equiv -a_0 - a_1(1 - i)p$$

and

$$\frac{B_{i+p-1}}{i+p-1} \equiv -a_0 - a_1(2 - p - i)p \equiv -a_0 - a_1(2 - i)p.$$

We obtain

$$a_1(1-i)p \not\equiv a_1(2-i)p \bmod p^2.$$

Therefore $p \nmid a_1$. Since $p \mid B_i$, we must have $p \mid a_0$, so $\lambda_i = 1$ for the power series $f(T, \omega^i)$. This means that

$$f(T, \omega^i) = (T - \alpha_i)U_i(T)$$

with $\alpha_i \in p\mathbb{Z}_p$ and $U_i \in \mathbb{Z}_p[[T]]^\times$ (see Theorem 7.3). It follows that

$$\varepsilon_{p-i}A_n \simeq \mathbb{Z}_p[[T]]/(P_n(T), T-\alpha_i) \simeq \mathbb{Z}_p/P_n(\alpha_i)\mathbb{Z}_p.$$

But $P_n(\alpha_i) = (1+\alpha_i)^{p^n} - 1 \equiv p^n\alpha_i \bmod p^n\alpha_i^2$, so we already have the result

$$\varepsilon_{p-i}A_n \simeq \mathbb{Z}_p/p^{n+f_i}\mathbb{Z}_p, \quad \text{where } f_i = v_p(\alpha_i).$$

Since

$$-B_{1,\omega^{i-1}} = f(0, \omega^i) = -\alpha_i U_i(0)$$

we find that

$$v_p(\alpha_i) = v_p(B_{1,\omega^{i-1}}) = 1.$$

This completes the proof. □

Notes

For results related to the first section, see the papers of Masley. Corollary 10.5 was first proved by Furtwängler.

For the general statement of Leopoldt's Spiegelungsatz, see Leopoldt [4]. For generalizations, see Oriat [2], Oriat–Satgé [1], and Kuroda [1].

There is some interest in class groups of cyclotomic fields because of their relations with class groups of group rings. See Kervaire–Murthy [1], Ullom [1], and McCulloh [2].

For divisibility properties of h_n^- see Metsänkylä [1], [2], [3] and Lehmer [3]. For parity questions, see the notes on Chapter 8, plus Cohn [1] and Uchida [4].

Proposition 10.13 has an elliptic analogue (Coates–Wiles [2]).

Exercises

10.1. Suppose L/K is an extension of degree n. Show:

(a) If $m \mid h_K$ and $(m, n) = 1$, then $m \mid h_L$.

(b) If $(n, h_K) = 1$ then the map $C_K \to C_L$ of ideal class groups is injective (this does not use class field theory or Theorem 10.1).

10.2. Suppose L/K is an abelian extension of odd degree. Show that if h_K is odd and h_L is even, then 4 divides h_L (it follows easily that the result is true for solvable extensions of odd degree; by the Feit–Thompson theorem, it is therefore true for all Galois extensions of odd degree).

10.3. (a) It is known (for example, Kummer's *Collected Papers*, vol. I, p. 944) that the cubic subfield of $\mathbb{Q}(\zeta_{163})^+$ has class number 4. Show that $\mathbb{Q}(\zeta_{163})^+$ has even class number.

(b) Let $p \equiv 1 \bmod 4$ be prime. Show that the quadratic subfield of $\mathbb{Q}(\zeta_p)^+$ has odd class number; so the technique of (a) will not produce even class numbers via quadratic subfields. This makes the computations more difficult.

10.4. Suppose p and q are distinct primes with $p \equiv q \equiv 1 \bmod 4$ and $(p/q) = -1$. Let K_{pq}^+ be the maximal real subextension of $\mathbb{Q}(\zeta_{pq})$ such that $[K_{pq}^+ : \mathbb{Q}]$ is a power of 2, and let K_p^+ be the similarly defined subfield of $\mathbb{Q}(\zeta_p)$.

(a) Show that K_p^+ has odd class number and that there is only one prime above q (*Hint*: $K_p^+/\mathbb{Q}$ is cyclic of prime power order. What is the decomposition group for q?).

(b) Show that K_{pq}^+ has odd class number.

10.5. Consider $\mathbb{Q}(\zeta_p)$. Show that if i is even and $\varepsilon_i A \neq 0$ then $p \mid B_i$. Is the converse true?

10.6. Let $d > 0$ be square-free. Let r be the 2-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$ and let s be the 2-rank of the ideal class group of $\mathbb{Q}(\sqrt{-d})$. Show that

$$r \leq s \leq r + 1$$

(this was known to Gauss; it does not require the techniques of this chapter).

10.7. Let K be a CM-field and suppose $[E : WE^+] = 2$. Show that the map $C^+ \to C$ of ideal class groups is injective.

10.8. Let L, B, H be as in the section on reflection theorems.

(a) Show that $H \simeq \operatorname{Hom}_{\mathbb{Z}}(B, W_p)$ as G-modules, where the action of G on a homomorphism f is defined by $(gf)(b) = g(f(g^{-1}b))$.

(b) Let χ be a 1-dimensional character of G such that the idempotent $\varepsilon_\chi \in \mathbb{Z}_p[G]$. Show that

$$\operatorname{Hom}_{\mathbb{Z}}(\varepsilon_\chi B, W_p) \simeq \varepsilon_{\omega\chi^{-1}} \operatorname{Hom}_{\mathbb{Z}}(B, W_p).$$

This explains the condition $i + j \equiv 1 \pmod{p-1}$ of Theorem 10.9. The 1-dimensional character χ may be replaced by a higher dimensional character Φ which is irreducible over $\mathbb{Q}_p$. The idempotent $\varepsilon_{\omega\chi^{-1}}$ must be replaced by $\varepsilon_{\omega\Phi^*}$, where Φ^* is the character of the contragredient representation, and $\Phi^*(\sigma) = \Phi(\sigma^{-1})$.

Chapter 11

Cyclotomic Fields of Class Number One

In this chapter we determine those m for which $\mathbb{Q}(\zeta_m)$ has class number one. In Chapter 4, the Brauer–Siegel theorem was used to show that there are only finitely many such fields, but the result was noneffective: there was no computable bound on m. So we need other techniques. Since h_n divides h_m if n divides m, it is reasonable to start with m prime. In 1964 Siegel showed that $h_p = 1$ implies $p \leq C$, where C is a computable constant, but the constant was presumably too large to make computations feasible. In 1971, Montgomery and Uchida independently obtained much better values of C, from which it followed that $h_p = 1 \Leftrightarrow p \leq 19$. Masley was then able to use this information, plus a table of h_m^- for $\phi(m) \leq 256$, to explicitly determine all m with $h_m = 1$.

Montgomery's original argument was for h_p^-, but Masley pointed out to me that the proof could be extended to composite indices. In the following, we use an adaption of Montgomery's method, though some of the less important estimates have been weakened. We obtain a finite list of prime powers for which $h^- = 1$, and the estimates are also good enough to handle some composite cases, in particular $m = 17 \times 19$, for which h_m^- has not been calculated. This information suffices for finding a finite list of possibilities for $h_m = 1$. But we still must calculate h_m^+, which is generally rather difficult. The original argument of Masley used some calculations plus some algebraic techniques. However, Odlyzko subsequently obtained rather precise lower bounds for discriminants, which allowed Masley to simplify the argument for h_m^+. It turns out that $h_m^+ = 1$ for all those m with $h_m^- = 1$. So we obtain all m with $h_m = 1$.

Theorem 11.1. *Let* $m \not\equiv 2 \bmod 4$. *Then* $h(\mathbb{Q}(\zeta_m)) = 1$ *if and only if* m *is one of the following*:

1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.

§11.1 The Estimate For Even Characters

We need to estimate h_m^- from below, which will involve estimating L-series. It will be convenient to use imprimitive characters; so let χ be a Dirichlet character of conductor f, with $f \mid m$, and define

$$\chi_m(n) = \begin{cases} \chi(n), & \text{if } (n, m) = 1 \\ 0, & \text{if } (n, m) > 1. \end{cases}$$

We have

$$L(s, \chi_m) = \sum_{n=1}^{\infty} \frac{\chi_m(n)}{n^s} = L(s, \chi) \prod_{p \mid m} \left(1 - \frac{\chi(p)}{p^s}\right).$$

If $\chi \neq 1$,

$$L(1, \chi_m) = \sum_{n=1}^{\infty} \frac{\chi_m(n)}{n} = L(1, \chi) \prod_{p \mid m} \left(1 - \frac{\chi(p)}{p}\right).$$

The advantage of using these characters is that

$$\sum_{\chi \bmod m} \chi_m(n) = 0 \quad \text{if } n \not\equiv 1 \bmod m$$

and

$$\sum_{\chi \text{ even}} \chi_m(n) = 0 \quad \text{if } n \not\equiv \pm 1 \bmod m.$$

This is not true if we use χ (see Exercise 3.6). By using imprimitive characters we can take a sum involving $L(s, \chi_m)$ for all χ and cancel many terms, and consequently obtain a better estimate than if we worked with each character separately.

We know that h_m^- can be expressed in terms of the product of $L(1, \chi)$ for odd characters χ. But it works better to obtain a lower bound for the product over all nontrivial characters, and an upper bound for the product over the nontrivial even characters, then divide. The latter is perhaps a more delicate estimate in our case and we do it first.

Let $\prod_+$ and $\sum_+$ denote respectively the product and sum over the nontrivial even characters χ mod m. By the arithmetic-geometric mean inequality,

$$\left| \prod_+ L(1, \chi_m)^2 \right|^{2/(\phi(m) - 2)} \leq \frac{2}{\phi(m) - 2} \sum_+ |L(1, \chi_m)|^2.$$

We shall estimate the right-hand side. Note that

$$L(1, \chi_m) = \lim_{N \to \infty} \sum_{n=1}^{Nm} \frac{\chi_m(n)}{n}.$$

We shall make estimates with the finite sum, then let $N \to \infty$. Let χ_0 denote the trivial imprimitive character mod m ($\chi_0(n) = 1$ if $(m, n) = 1$; 0 otherwise). We have

$$\sum_{+}\left|\sum_{n=1}^{Nm}\frac{\chi_m(n)}{n}\right|^2 = \sum_{\text{all even }\chi}\left|\sum_{n=1}^{Nm}\frac{\chi_m(n)}{n}\right|^2 - \left|\sum_{n=1}^{Nm}\frac{\chi_0(n)}{n}\right|^2$$
$$\stackrel{\text{def}}{=} T(N) - T_0(N).$$

First, we estimate $T(N)$:

$$\begin{aligned} T(N) &= \sum_{\chi\text{ even}}\sum_{n=1}^{Nm}\sum_{n'=1}^{Nm}\frac{\chi_m(n)\chi_m(n')}{nn'} \\ &= \frac{\phi(m)}{2}\sum_{\substack{n\equiv\pm n'(m)\\(n,m)=1}}\frac{1}{nn'} \\ &= \frac{\phi(m)}{2}\sum_{\substack{n=1\\(n,m)=1}}^{Nm}\frac{1}{n^2} + \phi(m)\sum_{j=1}^{N-1}\sum_{\substack{n=1\\(n,m)=1}}^{(N-j)m}\frac{1}{n(n+jm)} \\ &\quad + \frac{\phi(m)}{2}\sum_{j=1}^{N}\sum_{\substack{n=1\\(n,m)=1}}^{jm}\frac{1}{n(jm-n)} + \frac{\phi(m)}{2}\sum_{j=1}^{N-1}\sum_{\substack{n=jm\\(n,m)=1}}^{Nm}\frac{1}{n(Nm+jm-n)} \end{aligned}$$

(the first sum is for $n = n'$; the second, $n \equiv n'$, $n \neq n'$; the third and fourth, $n \equiv -n'$)

$$\begin{aligned} &\leq \frac{\phi(m)}{2}\frac{\pi^2}{6} + \phi(m)\sum_{j=1}^{N-1}\sum_{\substack{n=1\\(n,m)=1}}^{(N-j)m}\frac{1}{jm}\left(\frac{1}{n} - \frac{1}{n+jm}\right) \\ &\quad + \frac{\phi(m)}{2}\sum_{j=1}^{N}\sum_{\substack{n=1\\(n,m)=1}}^{jm}\frac{1}{jm}\left(\frac{1}{n} + \frac{1}{jm-n}\right) \\ &\quad + \frac{\phi(m)}{2}\sum_{j=1}^{N-1}\frac{1}{Nm+jm}\sum_{\substack{n=jm\\(n,m)=1}}^{Nm}\left(\frac{1}{n} + \frac{1}{Nm+jm-n}\right) \\ &\leq \frac{\phi(m)\pi^2}{12} + \phi(m)\sum_{j=1}^{N-1}\frac{1}{jm}\left(\sum_{\substack{n=1\\(n,m)=1}}^{Nm}\frac{1}{n} - \sum_{\substack{n=jm+1\\(n,m)=1}}^{Nm}\frac{1}{n}\right) \\ &\quad + \phi(m)\sum_{j=1}^{N}\frac{1}{jm}\sum_{\substack{n=1\\(n,m)=1}}^{jm}\frac{1}{n} + \phi(m)\sum_{j=1}^{N-1}\frac{1}{Nm+jm}\sum_{\substack{n=jm\\(n,m)=1}}^{Nm}\frac{1}{n} \end{aligned}$$

(in the second expression, we added some positive terms corresponding to $(N - j)m < n \leq Nm$)

$$\leq \frac{\phi(m)\pi^2}{12} + \frac{2\phi(m)}{m}\sum_{j=1}^{N}\frac{1}{j}\sum_{\substack{n=1\\(n,m)=1}}^{jm}\frac{1}{n} + \frac{\phi(m)}{m}\sum_{j=1}^{N-1}\frac{1}{N+j}\sum_{n=jm+1}^{Nm}\frac{1}{n}.$$

Lemma 11.2. *Let $\gamma = 0.577\ldots$ be the Euler–Mascheroni constant and let A be a positive integer. Then*

$$\gamma + \log A \le \sum_{a=1}^{A} \frac{1}{a} \le \frac{1}{A} + \gamma + \log A.$$

Proof. Since

$$\log\left(\frac{A+1}{A}\right) = \frac{1}{A} - \frac{1}{2A^2} + \frac{1}{3A^3} \cdots$$

has alternating signs and decreasing terms, we have

$$\frac{1}{A} - \frac{1}{2A^2} < \log\left(\frac{A+1}{A}\right) < \frac{1}{A}.$$

Therefore

$$\frac{1}{A+1} - \log\left(\frac{A+1}{A}\right) < \frac{1}{A+1} - \frac{1}{A} + \frac{1}{2A^2} \le 0.$$

It follows that

$$\sum_{a=1}^{A} \frac{1}{a} - \log A$$

decreases monotonically to γ. This proves the first inequality. Since

$$\begin{aligned}\gamma - \sum_{a=1}^{A} \frac{1}{a} + \log A &= \sum_{a=A}^{\infty} \left(\frac{1}{a+1} - \log\left(\frac{a+1}{a}\right)\right)\\ &> \sum_{a=A}^{\infty} \left(\frac{1}{a+1} - \frac{1}{a}\right) = -\frac{1}{A},\end{aligned}$$

the second inequality follows. □

Lemma 11.3. *Let $\pi(m)$ be the number of distinct prime divisors of m. Then*

$$\sum_{\substack{n=1\\(n,m)=1}}^{jm} \frac{1}{n} = \left(\gamma + \log(jm) + \sum_{p\mid m} \frac{\log p}{p-1}\right) \prod_{p\mid m} \left(1 - \frac{1}{p}\right) + \frac{2^{\pi(m)}\theta}{jm},$$

where $-1 \le \theta \le 1$.

PROOF. We shall use induction on $\pi(m)$. By Lemma 11.2, the lemma is true for $\pi(m) = 0$. Assume it is true for $\pi(m)$ and then replace m by mq, with q prime, $(q, m) = 1$ (the cases mq^2, etc., are obtained by varying j). We have

$$\sum_{\substack{n=1 \\ (n,mq)=1}}^{jmq} \frac{1}{n} = \sum_{\substack{n=1 \\ (n,m)=1}}^{jmq} \frac{1}{n} - \frac{1}{q} \sum_{\substack{n=1 \\ (n,m)=1}}^{jm} \frac{1}{n}$$

$$= \left(\gamma + \log(jmq) + \sum_{p \mid m} \frac{\log p}{p-1}\right) \prod_{p \mid m} \left(1 - \frac{1}{p}\right) + \frac{2^{\pi(m)}\theta}{jmq},$$

$$- \frac{1}{q}\left(\gamma + \log(jm) + \sum_{p \mid m} \frac{\log p}{p-1}\right) \prod_{p \mid m} \left(1 - \frac{1}{p}\right) - \frac{2^{\pi(m)}\theta'}{jmq}$$

$$= \left(\gamma + \log(jmq) + \frac{\log q}{q-1} + \sum_{p \mid m} \frac{\log p}{p-1}\right)\left(1 - \frac{1}{q}\right) \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$

$$+ \frac{2^{\pi(m)}(\theta - \theta')}{jmq}.$$

Since $-2 \leq \theta - \theta' \leq 2$, the result follows. □

Lemma 11.4.

$$\sum_{j=1}^{N} \frac{\log j}{j} < 0.11 + \tfrac{1}{2}(\log N)^2 \quad \textit{for } N \geq 1,$$

and

$$\sum_{j=1}^{N} \frac{\log j}{j} < \tfrac{1}{2}(\log N)^2 \quad \textit{for } N \geq 21.$$

PROOF. A calculation shows that

$$\sum_{j=1}^{21} \frac{\log j}{j} < \tfrac{1}{2}(\log 21)^2.$$

Since $(\log x)/x$ is decreasing for $x > e$,

$$\sum_{j=22}^{N} \frac{\log j}{j} < \int_{21}^{N} \frac{\log x}{x}\, dx = \tfrac{1}{2}(\log N)^2 - \tfrac{1}{2}(\log 21)^2.$$

The second part of the lemma follows easily. The first part follows from a calculation of the cases $N < 21$ (the worst case is $N = 3$). □

We now return to the estimation of $T(N)$. For $N \geq 21$,

$$\begin{aligned}
T(N) &\leq \frac{\phi(m)\pi^2}{12} + \frac{2\phi(m)}{m}\sum_{j=1}^{N}\frac{1}{j}\left(\gamma + \log(jm) + \sum_{p\mid m}\frac{\log p}{p-1}\right)\prod_{p\mid m}\left(1-\frac{1}{p}\right)\\
&\quad + \frac{2\phi(m)}{m}\sum_{j=1}^{N}\frac{2^{\pi(m)}}{mj^2} + \frac{\phi(m)}{m}\sum_{j=1}^{N-1}\frac{-\log(j/N)}{1+j/N}\frac{1}{N} + O\left(\frac{1}{N}\right)\\
&\leq \frac{\phi(m)\pi^2}{12} + \frac{\phi(m)}{m}(\log N)^2\prod_{p\mid m}\left(1-\frac{1}{p}\right)\\
&\quad + \frac{2\phi(m)}{m}\left(\gamma + \log m + \sum_{p\mid m}\frac{\log p}{p-1}\right)\left(\gamma + \log N + \frac{1}{N}\right)\prod_{p\mid m}\left(1-\frac{1}{p}\right)\\
&\quad + \frac{\phi(m)\pi^2}{3m} + \frac{\phi(m)}{m}\int_0^1\frac{-\log x}{1+x}\,dx + o(1)
\end{aligned}$$

(use Lemma 11.2 for the third term; use $2^{\pi(m)} \leq m$ and $\sum j^{-2} \leq \pi^2/6$ for the fourth term)

$$\begin{aligned}
&\leq \frac{\phi(m)\pi^2}{12} + \left[(\log N)^2 + 2\left(\gamma + \log m + \sum_{p\mid m}\frac{\log p}{p-1}\right)(\gamma + \log N)\right]\\
&\quad \times \prod_{p\mid m}\left(1-\frac{1}{p}\right)^2 + \frac{\phi(m)\pi^2}{3m} + \frac{\phi(m)}{m}\frac{\pi^2}{12} + o(1)
\end{aligned}$$

(use $\phi(m) = m\prod(1 - 1/p)$. Also, the integral is easily seen to equal $1 - \frac{1}{4} + \frac{1}{9} - \cdots = \pi^2/6 - \frac{1}{2}(\pi^2(6))$. This is our estimate for $T(N)$.

We now estimate $T_0(N)$:

$$\begin{aligned}
T_0(N) &= \left|\sum_{\substack{n=1\\(n,m)=1}}^{Nm}\frac{1}{n}\right|^2\\
&= \left(\left(\gamma + \log N + \log m + \sum_{p\mid m}\frac{\log p}{p-1}\right)\prod_{p\mid m}\left(1-\frac{1}{p}\right) + \frac{2^{\pi(m)}\theta}{Nm}\right)^2\\
&= \left(\gamma + \log N + \log m + \sum_{p\mid m}\frac{\log p}{p-1}\right)^2\prod_{p\mid m}\left(1-\frac{1}{p}\right)^2 + O\left(\frac{\log N}{N}\right).
\end{aligned}$$

Therefore

$$\begin{aligned}
T(N) - T_0(N) &\leq \frac{\phi(m)\pi^2}{12} + \frac{\phi(m)\pi^2}{3m}\\
&\quad + \left(\gamma^2 - \left(\log m + \sum_{p\mid m}\frac{\log p}{p-1}\right)^2\right)\prod_{p\mid m}\left(1-\frac{1}{p}\right)^2\\
&\quad + \frac{5\phi(m)\pi^2}{12m} + o(1)\\
&\leq \frac{\phi(m)\pi^2}{12} + \frac{5\pi^2}{12} + o(1)
\end{aligned}$$

(it is rather amazing that the coefficients of both $(\log N)^2$ and $\log N$ disappear. It would have been easy to get rid of just the $(\log N)^2$ term, but that would not suffice. This is why we called this estimate "delicate" at the beginning of this section).

We now obtain

$$\begin{aligned}\sum_{+} |L(1, \chi_m)|^2 &= \lim_{N\to\infty} (T(N) - T_0(N)) \\ &\le \frac{\phi(m)\pi^2}{12} + \frac{5\pi^2}{12} \\ &\le \left(\frac{\phi(m) - 2}{2}\right)(1.7) \quad \text{if } \phi(m) \ge 220.\end{aligned}$$

By an inequality at the beginning of this section,

$$\left|\prod_{+} L(1, \chi_m)\right| \le (1.7)^{(\phi(m)-2)/4}.$$

We record this for future reference.

Lemma 11.5. *If* $\phi(m) \ge 220$ *then*

$$\left|\prod_{\substack{\chi\,\text{even}\\ \chi\ne 1}} L(1, \chi_m)\right| \le (1.7)^{(\phi(m)-2)/4}. \qquad \square$$

§11.2 The Estimate For All Characters

We now need to estimate $\prod L(s, \chi_m)$ from below, where χ runs through all nontrivial characters mod m. We continue to use imprimitive characters. Surprisingly, we first need an upper bound.

Lemma 11.6. *If* $\phi(m) \ge 20$ *and* $|s - 2| \le \frac{4}{3}$ *then*

$$\left|\prod_{\chi\ne 1} L(s, \chi_m)\right| < \phi(m)^{\phi(m)/2}.$$

PROOF. By the arithmetic–geometric mean inequality,

$$\left|\prod_{\chi\ne 1} L(s, \chi_m)^2\right|^{1/(\phi(m)-1)} \le \frac{1}{\phi(m) - 1} \sum_{\chi\ne 1} |L(s, \chi_m)|^2.$$

Let $S(u, \chi_m) = \sum_{1 \leq n < u} \chi_m(n)$ ($= \sum_{m \leq n < u} \chi_m(n)$ if $u > m$ and $\chi \neq 1$). Then, for $\chi \neq 1$,

$$\begin{aligned} L(s, \chi_m) &= \sum_{n=1}^{\infty} \frac{\chi_m(n)}{n^s} \\ &= \sum_{n=1}^{m-1} \frac{\chi_m(n)}{n^s} + \chi_m(m)(m^{-s} - (m+1)^{-s}) \\ &\quad + (\chi_m(m) + \chi_m(m+1))((m+1)^{-s} - (m+2)^{-s}) + \cdots \end{aligned}$$

(this is just partial summation)

$$= \sum_{n=1}^{m-1} \frac{\chi_m(n)}{n^s} + s \int_m^{\infty} S(u, \chi_m) u^{-s-1}\, du.$$

Since $|S(u, \chi_m)| \leq \phi(m)/2$ (but see Lemma 11.8), the integral converges for $\sigma = \operatorname{Re}(s) > 0$, so by analytic continuation the above holds for $\sigma > 0$. Also,

$$\begin{aligned} |L(s, \chi_m)| &\leq \left| \sum_{n=1}^{m-1} \frac{\chi_m(n)}{n^s} \right| + |s| \frac{\phi(m)}{2} \int_m^{\infty} u^{-\sigma-1}\, du \\ &\leq \left| \sum_{n=1}^{m-1} \frac{\chi_m(n)}{n^s} \right| + \frac{|s|}{\sigma} \frac{\phi(m)}{2} m^{-\sigma}. \end{aligned}$$

Since $|s - 2| \leq \frac{4}{3}$, we have $\sigma \geq \frac{2}{3}$ and $|s|/\sigma \leq \sqrt{2}$. Therefore

$$|L(s, \chi_m)| \leq \left| \sum_{n=1}^{m-1} \frac{\chi_m(n)}{n^s} \right| + \frac{\phi(m)}{\sqrt{2}} m^{-2/3}.$$

The triangle inequality says that for real a_i, b_i,

$$((a_1 + b_1)^2 + (a_2 + b_2)^2 + \cdots)^{1/2} \leq (a_1^2 + a_2^2 + \cdots)^{1/2} + (b_1^2 + b_2^2 + \cdots)^{1/2}.$$

In the present case this yields

$$\begin{aligned} \left(\sum_{\chi \neq 1} |L(s, \chi_m)|^2 \right)^{1/2} &\leq \left(\sum_{\chi \neq 1} \left| \sum_{n=1}^{m-1} \chi_m(n) n^{-s} \right|^2 \right)^{1/2} + \left(\sum_{\chi \neq 1} \left(\frac{\phi(m)}{\sqrt{2}} m^{-2/3} \right)^2 \right)^{1/2} \\ &\leq \left(\sum_{\text{all } \chi} \left| \sum_{n=1}^{m-1} \chi_m(n) n^{-s} \right|^2 \right)^{1/2} + (\phi(m) - 1)^{1/2} \frac{\phi(m)}{\sqrt{2}} m^{-2/3}. \end{aligned}$$

The first term is the square root of

$$\sum_{\text{all } \chi} \sum_{n=1}^{m-1} \sum_{n'=1}^{m-1} \chi_m(n) \bar{\chi}_m(n') n^{-s} (n')^{-\bar{s}} = \phi(m) \sum_{\substack{n=1 \\ (n,m)=1}}^{m-1} n^{-2\sigma}$$

($\sum \chi_m(n) \bar{\chi}_m(n') = 0$ if $n \not\equiv n' \bmod m$, since we are using imprimitive characters). Since $\sigma \geq \frac{2}{3}$,

$$\sum_{\substack{n=1 \\ (n,m)=1}}^{m-1} n^{-2\sigma} \leq \zeta(\tfrac{4}{3}) \leq 1 + \int_1^{\infty} u^{-4/3}\, du = 4.$$

Putting everything together, we obtain

$$\left|\prod_{\chi\neq 1} L(s,\chi_m)^2\right|^{1/(\phi(m)-1)}$$

$$\le \frac{1}{\phi(m)-1}\left((4\phi(m))^{1/2} + (\phi(m)-1)^{1/2}\frac{\phi(m)}{\sqrt{2}}m^{-2/3}\right)^2$$

$$\le \left(\left(\frac{4\phi(m)}{\phi(m)-1}\right)^{1/2} + \frac{\phi(m)}{\sqrt{2}}\phi(m)^{-2/3}\right)^2$$

$$\le \phi(m) \quad \text{if } \phi(m) \ge 20.$$

The lemma follows easily. □

The next result uses the upper bound to get a lower bound.

Lemma 11.7. *Suppose*

(a) $f(s)$ *is regular and satisfies* $|f(s)| \le M$ *in the disc* $|s-2| \le \frac{4}{3}$,

(b) $f(s)\zeta(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ *for* $\text{Re}(s) > 1$, *with* $a_1 \ge 1$ *and* $a_n \ge 0$ *for* $n \ge 2$,

(c) $26/27 \le \alpha < 1$, *and*

(d) $f(\alpha) \ge 0$.

Then

$$f(1) \ge \tfrac{1}{4}(1-\alpha)M^{-4(1-\alpha)}.$$

Proof. Let $F(s) = f(s)\zeta(s)$. Then $F(2) \ge a_1 \ge 1$ and

$$(-1)^j F^j(2) = \sum_{n=1}^{\infty} a_n(\log n)^j n^{-2} \ge 0,$$

so

$$F(s) = \sum_{j=0}^{\infty} b_j(2-s)^j \quad (\text{for } |s-2| < 1)$$

with

$$b_0 \ge 1 \quad \text{and} \quad b_j \ge 0 \quad \text{for } j \ge 1.$$

Also,

$$F(s) - \frac{f(1)}{s-1} = \sum_{j=0}^{\infty}(b_j - f(1))(2-s)^j \quad \text{for } |s-2| < 1.$$

Since the left-hand side is regular throughout the whole disc $|s-2| \le \frac{4}{3}$, the right-hand side must converge in this disc (and equal the left-hand side). A short calculation shows that for $\text{Re}(s) > 1$,

$$\frac{1}{s-1} + 1 - s\int_1^{\infty}\frac{u-[u]}{u^{s+1}}\,du \quad ([u] = \text{greatest integer} \le u)$$

$$= \sum_{m=1}^{\infty} m\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) = (1^{-s} - 2^{-s}) + 2(2^{-s} - 3^{-s}) + \cdots$$

$$= \zeta(s).$$

Since both sides are regular for $\operatorname{Re}(s) > 0$, $s \neq 1$, the equality holds for these s. On the circle $|s - 2| = \frac{4}{3}$,

$$|\zeta(s)| \leq \frac{1}{|s - 1|} + 1 + |s| \int_1^\infty \frac{1}{u^{\sigma+1}}\,du$$
$$\leq 3 + 1 + \frac{|s|}{\sigma} \leq 6.$$

Consequently, for $|s - 2| = \frac{4}{3}$ (hence for $|s - 2| \leq \frac{4}{3}$),

$$\left|F(s) - \frac{f(1)}{s - 1}\right| \leq 6M + \frac{f(1)}{|s - 1|} \leq 9M.$$

Therefore

$$|b_j - f(1)| = \left|\frac{(-1)^j}{2\pi i}\int_{|s-2|=4/3}\left(F(s) - \frac{f(1)}{s - 1}\right)\frac{ds}{(s - 2)^{j+1}}\right|$$
$$\leq 9M\left(\frac{3}{4}\right)^j.$$

With α as in the statement of the lemma, and for $A > 0$, we obtain

$$F(\alpha) - \frac{f(1)}{\alpha - 1} \geq \sum_{j=0}^{A}(b_j - f(1))(2 - \alpha)^j - \sum_{j=A+1}^{\infty} 9M(\tfrac{3}{4})^j(2 - \alpha)^j$$
$$\geq \sum_{j=0}^{A}(b_j - f(1))(2 - \alpha)^j - 9M\frac{(\frac{3}{4}(2 - \alpha))^{A+1}}{1 - \frac{3}{4}(2 - \alpha)}$$
$$\geq b_0 - \sum_{j=0}^{A} f(1)(2 - \alpha)^j - 32M(\tfrac{7}{9})^A$$

(since $b_j \geq 0$)

$$\geq 1 - \frac{f(1)}{\alpha - 1}(1 - (2 - \alpha)^{A+1}) - 32M(\tfrac{7}{9})^A.$$

Since $f(\alpha) \geq 0$ and $\zeta(\alpha) < 0$, $F(\alpha) \leq 0$. Therefore, after some rearranging, we have

$$f(1)\frac{(2 - \alpha)^{A+1}}{1 - \alpha} \geq 1 - 32M(\tfrac{7}{9})^A.$$

Let

$$A = \left[\frac{(\log 64M)}{\log(\frac{9}{7})}\right] + 1$$

(note that $M \geq f(2) = F(2)/\zeta(2) \geq 6/\pi^2$, so $A > 0$). Then

$$f(1)\frac{(2 - \alpha)^{A+1}}{1 - \alpha} \geq \frac{1}{2}.$$

Since $\log(\frac{9}{7}) > \frac{1}{4}$, $A < 1 + 4\log(64M)$. Therefore

$$(2-\alpha)^{A-1} \le (e^{1-\alpha})^{A-1} \le (64M)^{4(1-\alpha)}.$$

Also,

$$2(2-\alpha)^2(64)^{4(1-\alpha)} \le 2\left(\frac{28}{27}\right)^2 64^{4/27} < 4.$$

Putting everything together, we obtain the lemma. □

Lemma 11.8 (Polya–Vinogradov). *Let $\chi \neq 1$ be primitive with conductor f. Let $S(u,\chi) = \sum_{0\le n<u}\chi(n)$. Then*

$$|S(u,\chi)| < f^{1/2}\log f.$$

(If $\chi \neq 1$ is imprimitive mod *m, the result holds with $2m^{1/2}\log m$ on the right. See Ellison* [1], *p.* 344.)

Proof. Let $\zeta = e^{2\pi i/f}$ and let $\tau(\chi) = \sum_{c=1}^{f-1}\chi(c)\zeta^c$. By Lemma 4.7,

$$\overline{\chi(n)}\tau(\chi) = \sum_c \chi(c)\zeta^{cn}.$$

We may assume u is a positive integer, so

$$\tau(\chi)\overline{S(u,\chi)} = \sum_c \chi(c)\sum_{0\le n<u}\zeta^{cn}$$

$$= \sum_c \chi(c)\frac{\zeta^{uc}-1}{\zeta^c-1}.$$

Note that if $f/2 \in \mathbb{Z}$ then $\chi(f/2) = 0$. Therefore

$$|\tau(\chi)||S(u,\chi)| \le \sum_{\substack{c=1\\ c\neq f/2}}^{f-1}\left|\frac{\zeta^{uc}-1}{\zeta^c-1}\right|$$

$$\le \sum_{\substack{c=1\\ c\neq f/2}}^{f-1}\left|\frac{\sin(\pi uc/f)}{\sin(\pi c/f)}\right| \le 2\sum_{c=1}^{[(f-1)/2]}\frac{1}{\sin(\pi c/f)}.$$

But $\sin x \ge 2x/\pi$ for $0 \le x \le \pi/2$. Therefore

$$|\tau(\chi)||S(u,\chi)| \le 2\sum_{c=1}^{[(f-1)/2]}\frac{f}{2c} = f\sum_c\frac{1}{c}.$$

We claim that

$$\sum_{c=1}^{[(f-1)/2]}\frac{1}{c} < \log f, \quad \text{for } f \ge 3.$$

It clearly suffices to prove the claim for odd f. The inequality holds for $f = 3$. Suppose it is true for $f = 2n - 1$. To change to $f = 2n + 1$, we add $1/n$ to the left and $\log(2n + 1) - \log(2n - 1)$ to the right. Since

$$\begin{aligned}\log(2n + 1) - \log(2n - 1) &= \log\left(1 + \frac{1}{2n}\right) - \log\left(1 - \frac{1}{2n}\right)\\ &= 2\left(\frac{1}{2n} + \frac{1}{3}\left(\frac{1}{2n}\right)^3 + \frac{1}{5}\left(\frac{1}{2n}\right)^5 + \cdots\right)\\ &> \frac{1}{n},\end{aligned}$$

the inequality still holds. This proves the claim.

Therefore

$$|\tau(\chi)||S(u, \chi)| < f \log f.$$

By Lemma 4.8, $|\tau(\chi)| = f^{1/2}$, since χ is primitive. This proves the lemma. □

Lemma 11.9. *If χ is a primitive nontrivial character of conductor f and $1 \geq \sigma \geq 1 - 1/4f$, then*

$$|L'(\sigma, \chi)| \leq (1.3)(\log f)^2.$$

Proof. As in the proof of Lemma 11.6, we have for $\sigma = \operatorname{Re}(s) > 0$,

$$L(s, \chi) = \sum_{n=1}^{f-1} \chi(n)n^{-s} + s\int_f^\infty S(u, \chi)u^{-s-1}\,du.$$

Differentiate:

$$L'(s, \chi) = -\sum_{n=1}^{f-1} \chi(n)(\log n)n^{-s} + \int_f^\infty S(u, \chi)u^{-s-1}(1 - s\log u)\,du.$$

By Lemma 11.8,

$$|L'(\sigma, \chi)| \leq \sum_{n=1}^{f-1} (\log n)n^{-\sigma} + f^{1/2}\log f \int_f^\infty u^{-\sigma-1}(\sigma \log u - 1)\,du$$

($\sigma \log u - 1 \geq \sigma \log f - 1 \geq \frac{11}{12}\log 3 - 1 > 0$). Therefore

$$\begin{aligned}|L'(\sigma, \chi)| &\leq f^{1-\sigma}\sum_{n=1}^{f-1} \frac{\log n}{n} + f^{1/2-\sigma}(\log f)^2\\ &\leq f^{1/4f}(0.11 + \tfrac{1}{2}(\log f)^2 + f^{-1/2}(\log f)^2)\end{aligned}$$

(by Lemma 11.4)

$$< (1.3)(\log f)^2.$$

This proves Lemma 11.9. □

Lemma 11.10. *If χ is a primitive quadratic character of conductor f, then*

$$L(\sigma, \chi) \geq 0 \quad \textit{for } \sigma \geq 1 - \frac{1}{4f}.$$

Proof. By the analytic class number formula (see the discussion following Theorem 4.9),

$$L(1, \chi) = \begin{cases} \dfrac{2h \log \varepsilon}{\sqrt{f}}, & \chi \text{ even}, \\ \dfrac{2\pi h}{w\sqrt{f}}, & \chi \text{ odd}, \end{cases}$$

where h and ε are the class number and fundamental unit of the corresponding quadratic field; and $w = 2$ if $f \neq 3, 4$; $w = 6$ if $f = 3$; $w = 4$ if $f = 4$.

If χ is real, $f \geq 5$, so

$$\varepsilon = \frac{a + b\sqrt{f}}{2} \geq \frac{1 + \sqrt{5}}{2}.$$

Since $h \geq 1$, we obtain, for all f,

$$L(1, \chi) \geq (0.96) f^{-1/2}.$$

If $1 \geq \sigma \geq 1 - 1/4f$,

$$\begin{aligned} L(\sigma, \chi) &\geq L(1, \chi) - (1 - \sigma) \operatorname*{Max}_{1 \geq \sigma' \geq \sigma} |L'(\sigma', \chi)| \\ &\geq (0.96) f^{-1/2} - \frac{1}{4f}(1.3)(\log f)^2 > 0. \end{aligned}$$

This completes the proof of Lemma 11.10. □

Lemma 11.11. *If χ is a quadratic character* mod m, *then*

$$L(\sigma, \chi_m) \geq 0 \quad \text{for } \sigma \geq 1 - 1/4m.$$

Proof.
$$L(\sigma, \chi_m) = L(\sigma, \chi) \prod_{p \mid m} \left(1 - \frac{\chi(p)}{p^\sigma}\right) \geq 0$$

since $1 - 1/4m \geq 1 - 1/4f$. □

Lemma 11.12. *If $\phi(m) \geq 20$, then*

$$\prod_{\chi \neq 1} L(1, \chi_m) \geq \frac{1}{16m\phi(m)^{1/2}}.$$

Proof. We shall use Lemma 11.7 with $f(s) = \prod_{\chi \neq 1} L(s, \chi_m)$ and $\alpha = 1 - 1/4m$. M is given by Lemma 11.6. Clearly (a) and (c) are satisfied. Since $f(s)\zeta(s)$ is the Dedekind zeta function of $\mathbb{Q}(\zeta_m)$, with the terms removed which have a factor in common with m, we find that (b) holds. If χ is real-valued, hence quadratic, Lemma 11.11 implies that $L(\alpha, \chi_m) \geq 0$. If χ is complex then

$$L(\alpha, \chi_m)L(\alpha, \bar{\chi}_m) = |L(\alpha, \chi_m)|^2 \geq 0.$$

Therefore $f(\alpha) \geq 0$, so Lemma 11.7 applies. We obtain

$$\prod_{\chi \neq 1} L(1, \chi_m) \geq \frac{1}{4}\left(\frac{1}{4m}\right)\phi(m)^{-\phi(m)/2m}.$$

The lemma follows easily. □

§11.3 The Estimate for h_m^-

Lemma 11.13. *If* $\phi(m) \geq 220$ *then*

$$\left|\prod_{\chi\,\text{odd}} L(1, \chi_m)\right| \geq \frac{1}{16m\phi(m)^{1/2}}(1.7)^{(2-\phi(m))/4}.$$

Proof. Lemmas 11.5 and 11.12. □

The following lets us return to primitive characters. However, the estimate is not good enough to be of use for our purposes.

Lemma 11.14 $$\prod_{\chi\,\text{odd}} \prod_{p|m} \left(1 - \frac{\chi(p)}{p}\right)^{-1} \geq e^{-7\phi(m)/24}.$$

Proof. Write $m = m_p m_p'$, where m_p is a power of p and $p \nmid m_p'$. Then $\chi(p) \neq 0 \Leftrightarrow f_\chi | m_p'$. There are at most $\frac{1}{2}\phi(m_p')$ such odd characters. Therefore the product is at least

$$\prod_{p|m}\left(1 + \frac{1}{p}\right)^{-(1/2)\phi(m_p')}.$$

Take the logarithm (the minus sign reverses all the inequalities):

$$\begin{aligned} -\frac{1}{2}\sum_{p|m} \phi(m_p')\log\left(1 + \frac{1}{p}\right) &\geq -\frac{1}{2}\sum_{p|m}\phi(m_p')\frac{1}{p} \\ &\geq -\frac{\phi(m)}{2}\left(\frac{1}{\phi(4)}\frac{1}{2} + \sum_{\substack{p|m \\ p>2}} \frac{1}{(p-1)p}\right) \\ &\geq -\frac{\phi(m)}{2}\left(\frac{1}{4} + \sum_{p>2}\frac{1}{(p-1)p}\right) \\ &\geq -\frac{\phi(m)}{2}\left(\frac{1}{4} + \frac{1}{3}\right) = -\frac{7\phi(m)}{24}. \end{aligned}$$

This completes the proof. □

Proposition 11.15. *If $\phi(m) \geq 220$ then*

$$\log h_m^- \geq \tfrac{1}{4}\log d_m - (1.37)\phi(m).$$

where d_m is the absolute value of the discriminant of $\mathbb{Q}(\zeta_m)$.

PROOF. From the class number formula (in particular, see the discussion preceding Theorem 4.17),

$$\log h_m^- = \tfrac{1}{2}\log\left(\frac{d_m}{d_m^+}\right) + \log \prod_{\chi\,\text{odd}} L(1,\chi) + \log w$$
$$+ \log Q - \frac{\phi(m)}{2}\log(2\pi),$$

where d_m^+ is the discriminant of $\mathbb{Q}(\zeta_m)^+$, $w = m$ or $2m$, and $Q = 1$ or 2. By Lemma 4.19,

$$d_m \geq (d_m^+)^2, \quad \text{so } \frac{d_m}{d_m^+} \geq \sqrt{d_m}.$$

Using Lemmas 11.13 and 11.14, we obtain

$$\log h_m^- \geq \tfrac{1}{4}\log d_m - \log(16m\phi(m)^{1/2}) + \frac{2-\phi(m)}{4}\log(1.7)$$
$$- \tfrac{7}{24}\phi(m) + \log m - \frac{\phi(m)}{2}\log(2\pi)$$
$$\geq \tfrac{1}{4}\log d_m - (1.37)\phi(m), \quad \text{if } \phi(m) \geq 220.$$

This proves the proposition. □

Since $\log d_m \sim \phi(m)\log m$ (Lemma 4.17), it is clear that we are almost done. Also, note that we find that $\log h_m^-$ grows at least as fast as predicted by the Brauer–Siegel theorem (see Theorem 3.20). It remains to estimate the discriminant. If m is a prime power, this is easy, but for composite m the estimates are harder. By Proposition 2.7,

$$\frac{\log d_m}{\phi(m)} = \log m - \sum_{p \mid m} \frac{\log p}{p-1}.$$

We can obtain an easy estimate as follows: If $2 \mid m$ then the right-hand side is at least

$$\log m - \log 2 - \frac{1}{2}\sum_{p \mid (m/2)} \log p \geq \log m - \log 2 - \frac{1}{2}\log\left(\frac{m}{2}\right)$$
$$\geq \frac{1}{2}\log\left(\frac{m}{2}\right).$$

If m is odd, we obtain $\tfrac{1}{2}\log m$. Therefore

$$\log h_m^- \geq \left(\frac{1}{8}\log\left(\frac{m}{2}\right) - 1.37\right)\phi(m) > 0 \quad \text{if } m > 116000.$$

So, in principle (i.e., with unlimited computer time), we are done. However, with a little work we can improve the situation. Of course, we could make some progress by estimating d_m more carefully. But let's look back at the proof. The major terms are $\frac{1}{4}\log(d_m)$, which cannot be changed; $\frac{1}{4}\phi(m)\log(1.7)$, which comes from Lemma 11.5; $\frac{7}{24}\phi(m)$, from Lemma 11.14; and $\frac{1}{2}\phi(m)\log(2\pi)$, which cannot be changed. If m is a prime power, then the estimate of Lemma 11.14 is very bad, since the left side is 1. Therefore, we bypass Lemma 11.14 and replace Proposition 11.15 with the following.

Proposition 11.16. *Assume $\phi(m) \geq 220$. If m is a prime power then*

$$\log h_m^- \geq \tfrac{1}{4}d_m - (1.08)\phi(m).$$

If m is arbitrary then

$$\log h_m^- \geq \tfrac{1}{4}d_m - (1.08)\phi(m) - \tfrac{1}{2}\phi(m) \sum_{p \mid m} \frac{1}{\phi(2p^2)}.$$

Proof. In Lemma 11.14, all the factors are 1 if m is a prime power. If m is arbitrary, we have, as in the proof of the lemma,

$$\log \prod_{\chi\,\text{odd}} \prod_{p \mid m} \left(1 - \frac{\chi(p)}{p}\right)^{-1} \geq -\frac{\phi(m)}{2}\left(\underbrace{\frac{1}{\phi(4)}\frac{1}{2}}_{\text{if } 2 \mid m} + \sum_{\substack{p \mid m \\ p > 2}} \frac{1}{(p-1)p}\right)$$

(omit the term for 2 if m is odd)

$$= -\tfrac{1}{2}\phi(m) \sum_{p \mid m} \frac{1}{\phi(2p^2)}.$$

Using these estimates in the proof of Proposition 11.15, we obtain the result. □

Corollary 11.17. *If $\phi(p^a) \geq 220$, then $h_{p^a}^- > 1$.*

Proof. We have

$$\frac{\log(d_{p^a})}{\phi(p^a)} = \log(p^a) - \frac{\log p}{p-1} \geq \log(p^a) - \log 2$$
$$\geq \log(220) - \log(2) \geq 4.7.$$

Therefore

$$\log(h_{p^a}^-) \geq (\tfrac{1}{4}(4.7) - 1.08)\phi(p^a) > 0.$$

This proves Corollary 11.17 (in fact, we obtain $h_{p^a}^- > 10^9$). □

Corollary 11.18. *$h_{p^a}^- = 1$ if and only if p^a is one of the following: an odd prime $p \leq 19$, or 4, 8, 9, 16, 25, 27, 32 (one could also include $p^a = 1$).*

Proof. We know that $\phi(p^a) < 220$. The table in the appendix yields the answer. □

Our strategy is now as follows: We know that $h_{p^a} = 1$ for at most those values listed in Corollary 11.18. By Exercise 4.4, or by Lemma 6.15 plus Theorem 10.1, $h_n | h_m$ if n divides m. Therefore, if $h_m = 1$, all the prime factors of m are less than or equal to 19. In fact, if p^a divides m, then p^a is on the above list. This gives us finitely many possibilities, each of which can be checked individually. We give some of the details:

19. The table in the appendix shows that $h_m^- > 1$, hence $h_m > 1$, for $m = 4 \times 19$, 3×19, $5 \times 19, \ldots, 13 \times 19$. Corollary 11.18 takes care of 19^2. However $\phi(17 \times 19) = 288 > 256$, so is not listed in the table. But Proposition 11.16 applies. We have

$$\begin{aligned}\frac{\log d_m}{\phi(m)} &= \log(323) - \frac{\log 17}{16} - \frac{\log 19}{18} \\ &\geq 5.4.\end{aligned}$$

Also

$$\frac{1}{2}\sum_{p|m}\frac{1}{\phi(2p^2)} = \frac{1}{2}\left(\frac{1}{16 \times 17} + \frac{1}{18 \times 19}\right) < 0.004.$$

Therefore

$$\log h_{323}^- \geq (\tfrac{1}{4}(5.4) - 1.08 - 0.004)\phi(323) > 0.$$

Consequently, $h_{19n} > 1$ for $2 \neq n > 1$, so we may henceforth ignore 19.

17. From the table, $h_{17n}^- > 1$ for $1 < n < 17$ ($n \neq 2$). Corollary 11.17 implies $h_{289}^- > 1$. Therefore $h_{17n} > 1$ for $n > 1$.

13. From the table, $h_{13n}^- > 1$ for $1 < n \leq 13$, so $h_{13n} > 1$ for $n > 1$.

11. We obtain $h_{33}^- = 1$ and $h_{44}^- = 1$, but $h_{11p}^- > 1$ for $3 < p \leq 11$. So if m is a multiple of 11, $m = 11 \cdot 2^a \cdot 3^b$. Since $h_{99}^- > 1$, $h_{132}^- > 1$, and $h_{88}^- > 1$, we must have $m = 33$ or 44.

7. We have $h_{28}^- = 1$, $h_{21}^- = 1$, and $h_{35}^- = 1$, so we have only eliminated multiples of 49. Next, consider 56, 84, 140, 63, 105, and 175. Only 84 gives $h^- = 1$. Since 2×84, 3×84, and 5×84 are multiples of numbers already eliminated, we may stop here.

2,3,5: These are treated similarly.

We have proved the following.

Proposition 11.19. *If $h_m = 1$ then m is one of the numbers given in the statement of Theorem* 11.1. *All these values have $h_m^- = 1$.* □

Remark. We have not yet calculated h_m^+, so we have not proved the converse of Proposition 11.19.

Masley proved that $n | m \Rightarrow h_n^- | h_m^-$. Hence he was able to work exclusively with h_m^- in the above and show that Theorem 11.1 lists exactly those m with $h_m^- = 1$.

§11.4 Odlyzko's Bounds On Discriminants

The results of this section will be used in the next section to compute h_m^+. However, as we shall see, they are also useful in other situations.

Let K be a number field of (absolute value of) discriminant D and degree $n = r_1 + 2r_2$. Let

$$\zeta_K(s) = \prod_{\mathscr{P}} (1 - N\mathscr{P}^{-s})^{-1} \quad \text{(Dedekind zeta function of } K\text{)},$$

$$Z(s) = -\frac{\zeta_K'(s)}{\zeta_K(s)} = -\frac{d}{ds} \log \zeta_K(s),$$

$$Z_1(s) = -\frac{d}{ds} Z(s),$$

$$\psi(s) = \frac{\Gamma'(s)}{\Gamma(s)} \quad (\Gamma = \text{gamma function}).$$

For $\sigma > 1$,

$$Z(\sigma) = \sum_{\mathscr{P}} \frac{\log N\mathscr{P}}{N\mathscr{P}^{\sigma} - 1} > 0$$

and since $N\mathscr{P}^{\sigma}$ increases with σ,

$$Z_1(\sigma) > 0.$$

The estimates we need will arise from the following.

Theorem 11.20. *Let* $\alpha = \sqrt{\dfrac{7 - \sqrt{32}}{17}} = 0.28108\ldots$. *Suppose* $\tilde{\sigma}, \sigma > 1$ *satisfy*

$$\tilde{\sigma} \geq \frac{5 + \sqrt{12\sigma^2 - 5}}{6} \quad \textit{and} \quad \tilde{\sigma} \geq 1 + \alpha\sigma.$$

Then

$$\begin{aligned}\log D \geq\ & r_1\left(\log \pi - \psi\left(\frac{\sigma}{2}\right)\right) + 2r_2(\log 2\pi - \psi(\sigma)) \\ &+ (2\sigma - 1)\left\{\frac{r_1}{4}\psi'\left(\frac{\tilde{\sigma}}{2}\right) + r_2\psi'(\tilde{\sigma})\right\} + 2Z(\sigma) \\ &+ (2\sigma - 1)Z_1(\tilde{\sigma}) - \frac{2}{\sigma} - \frac{2}{\sigma - 1} - \frac{2\sigma - 1}{\tilde{\sigma}^2} - \frac{2\sigma - 1}{(\tilde{\sigma} - 1)^2}.\end{aligned}$$

We postpone the proof in order to show how to use the theorem. The idea is to fix n, r_1, and r_2, and find optimal choices for σ and $\tilde{\sigma}$. For small n it is best to take

$$\tilde{\sigma} = \frac{5 + \sqrt{12\sigma^2 - 5}}{6}.$$

The best choice for σ will satisfy $\tilde{\sigma} \geq 1 + \alpha\sigma$ for these cases. Fortunately, Odlyzko has determined in many cases the best value of σ. We shall give the results below.

For any σ, $\tilde{\sigma}$ we obtain an estimate of the form

$$\log(D^{1/n}) \geq \frac{r_1}{n} A + \frac{2r_2}{n} B - \frac{C}{n}$$

with $A, B, C \geq 0$. Therefore, estimates for $D^{1/n}$ for K of a given degree n are also valid for fields of higher degree, provided the ratios r_1/n and r_2/n are held constant (e.g., K is totally real, or totally complex). We also have, for any $\sigma > 1$ and for any admissible $\tilde{\sigma}$,

$$\log(D^{1/n}) \geq \frac{r_1}{n} A + \frac{2r_2}{n} B + O\left(\frac{1}{n}\right)$$

where

$$A = \log \pi - \psi\left(\frac{\sigma}{2}\right) + \frac{2\sigma - 1}{4} \psi'\left(\frac{\tilde{\sigma}}{2}\right)$$

$$B = \log 2\pi - \psi(\sigma) + (2\sigma - 1)\psi'(\tilde{\sigma}).$$

We may let σ be arbitrarily close to 1 and let $\tilde{\sigma} = 1 + \alpha$ (this satisfies the other inequality). We find

$$D^{1/n} \geq (50.66)^{r_1/n}(19.96)^{2r_2/n}\left(1 + O\left(\frac{1}{n}\right)\right).$$

We give an application. Let $H_0 = \mathbb{Q}(\sqrt{d})$ be a real quadratic field. Let H_1 be the Hilbert class field of $\mathbb{Q}(\sqrt{d})$ and inductively let H_{i+1} be the Hilbert class field of H_i. Does this class field tower stop (i.e., $H_i = H_{i+1} = \cdots$ for some i)? Equivalently, can $\mathbb{Q}(\sqrt{d})$ be embedded in a field of class number 1? (Exercise 11.4). Golod and Shafarevich have shown that for $d = 3 \times 4 \times 7 \times 11 \times 13 \times 19 \times 23$, the tower does not stop.

Suppose that d is the discriminant (not $\frac{1}{4}$ disc.) of $\mathbb{Q}(\sqrt{d})$ and $d < 2500$. Since $H_i/\mathbb{Q}(\sqrt{d})$ is unramified,

$$D_i = d^{[H_i : \mathbb{Q}(\sqrt{d})]}$$

(see Lemma 11.22). Therefore, if $n_i = [H_i : \mathbb{Q}]$,

$$D_i^{1/n_i} = d^{1/2} < 50.$$

If $n_i \to \infty$ then

$$\liminf D_i^{1/n_i} \geq 50.66,$$

contradiction. So the class field tower stops.

It can be shown that

$$\frac{1}{n}\log D \geq \gamma + \log(4\pi) + 1 - 8.317302n^{-2/3} \quad (K \text{ totally real}),$$

$$\frac{1}{n}\log D \geq \gamma + \log(4\pi) - 6.860404n^{-2/3} \quad (K \text{ totally complex}).$$

(See Poitou[1]; also see Poitou[2]). These yield

$$D^{1/n} \geq 60.83 - o(1) \quad (K \text{ totally real}),$$

$$D^{1/n} \geq 22.38 - o(1) \quad (K \text{ totally complex}).$$

Even better estimates are available if one assumes the generalized Riemann Hypothesis.

We now give the table we promised. Keep in mind that an estimate for a given n works for a larger n; so for $n = 18$, for example, use the estimate for $n = 15$.

Lower bounds for $D_K^{1/n}$ for $[K:\mathbb{Q}] \geq n$

	K totally real		K totally complex	
n	σ	$D^{1/n}$	σ	$D^{1/n}$
10	1.84	10.00	2.26	5.53
15	1.57	13.58	1.85	7.06
20	1.44	16.40	1.66	8.11
30	1.32	20.57	1.46	9.68
40	1.26	23.55	1.37	10.77
60	1.19	27.61	1.27	12.23
100	1.14	32.25	1.19	13.86
120	1.12	33.75	1.165	14.38
180	1.095	36.76	1.13	15.40
240	1.08	38.62	1.11	16.03

This table is copied from Odlyzko [1]. For a more comprehensive table, see Odlyzko [4] and Diaz y Diaz [1].

To show how the various terms contribute to the estimates, we give the calculation of the lower bound for $n = 10$ and K totally real. It is hard to estimate $Z(\sigma)$ and $Z_1(\sigma)$; but recall that they are positive, hence may be ignored. We have $\sigma = 1.84$ and $\tilde{\sigma} = 1.828\ldots$. Writing the terms in the same order as in Theorem 11.20 (leaving out terms with $r_2 = 0$, and leaving out Z and Z_1), we have

$$\begin{aligned}\log D &\geq 10(1.14 - (-0.72)) \\ &\quad + (2.68)(\tfrac{10}{4}\, 1.88) \\ &\quad - 1.09 - 2.38 - 0.80 - 3.91 \\ &= 23.02.\end{aligned}$$

Therefore

$$D^{1/10} \geq e^{2.302} = 9.99$$

(we lost a little to rounding errors). As one can see, most of the terms make significant contributions to the final answer.

Proof of Theorem 11.20. Let

$$g(s) = \left(\frac{D}{\pi^{r_1}(2\pi)^{2r_2}}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2}\zeta_K(s)s(1-s).$$

Then $g(s)$ is an entire function of order 1 (see Lang [1], p. 332) and satisfies

$$g(s) = g(1-s)$$

(see the discussion preceding Corollary 4.6). By the Hadamard Product Theorem (see, for example, Lang [7], p. 253), there exist constants A and B such that

$$g(s) = e^{A+Bs} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho},$$

where ρ runs through the zeros of $g(s)$ ($=$ zeros of $\zeta_K(s)$ with $0 < \mathrm{Re}(s) < 1$) counted with multiplicity. If $g(\rho) = 0$ then $g(1-\rho) = 0$ (if $g(\frac{1}{2}) = 0$ then it has even multiplicity), so we pair ρ and $1-\rho$ to obtain

$$\begin{aligned} g(s) &= e^{A+Bs} \prod_{\rho,\, 1-\rho} \left(1 - \frac{s}{\rho}\right)\left(1 - \frac{s}{1-\rho}\right) e^{s/\rho(1-\rho)} \\ &= \exp\left(A + Bs + s\sum \frac{1}{\rho(1-\rho)}\right) \prod_{\rho,\, 1-\rho} \left(1 - \frac{s}{\rho}\right)\left(1 - \frac{s}{1-\rho}\right) \end{aligned}$$

(since $g(s)$ is of order 1, $\sum 1/\rho(1-\rho)$ converges; therefore the product converges also; hence the rearrangement is easily justified). Since, for any ρ and s,

$$\left(1 - \frac{s}{\rho}\right)\left(1 - \frac{s}{1-\rho}\right) = \left(1 - \frac{1-s}{\rho}\right)\left(1 - \frac{1-s}{1-\rho}\right),$$

we have

$$1 = \frac{g(s)}{g(1-s)} = \exp\left(B(2s-1) + (2s-1)\sum \frac{1}{\rho(1-\rho)}\right).$$

Therefore $B = -\sum 1/\rho(1-\rho)$, hence

$$g(s) = e^A \prod_{\rho,1-\rho} \left(1 - \frac{s}{\rho}\right)\left(1 - \frac{s}{1-\rho}\right).$$

Recalling the definition of $g(s)$ and taking the logarithmic derivative, we obtain

$$\tfrac{1}{2}\log D - \tfrac{1}{2}r_1 \log \pi - r_2 \log 2\pi + \frac{r_1}{2}\psi\left(\frac{s}{2}\right) + r_2\psi(s) - Z(s) + \frac{1}{s} + \frac{1}{s-1}$$
$$= \sum_{\rho,1-\rho}\left(\frac{1}{s-\rho} + \frac{1}{s-1+\rho}\right).$$

This may be rearranged to yield

$$\log D = r_1\left(\log \pi - \psi\left(\frac{s}{2}\right)\right) + 2r_2(\log 2\pi - \psi(s))$$
$$+ 2Z(s) - \frac{2}{s} - \frac{2}{s-1} + 2\sum_{\rho,1-\rho}\left(\frac{1}{s-\rho} + \frac{1}{s-1+\rho}\right).$$

This is valid for all s (except $s = \rho, 1-\rho, 0, 1$).

Differentiate with respect to s and let $s = \tilde{\sigma}$ to obtain

$$\frac{r_1}{2}\psi'\left(\frac{\tilde{\sigma}}{2}\right) + 2r_2\psi'(\tilde{\sigma}) + 2Z_1(\tilde{\sigma}) - \frac{2}{\tilde{\sigma}^2} - \frac{2}{(\tilde{\sigma}-1)^2}$$
$$-2\sum_{\rho,1-\rho}\left(\frac{-1}{(\tilde{\sigma}-\rho)^2} + \frac{-1}{(\tilde{\sigma}-1+\rho)^2}\right) = 0.$$

Multiply by $(2\sigma - 1)/2$ and add the result to the previous equation, with $s = \sigma$:

$$\log D = r_1\left(\log \pi - \psi\left(\frac{\sigma}{2}\right)\right) + 2r_2(\log 2\pi - \psi(\sigma))$$
$$+ (2\sigma - 1)\left\{\frac{r_1}{4}\psi'\left(\frac{\tilde{\sigma}}{2}\right) + r_2\psi'(\tilde{\sigma})\right\}$$
$$+ 2Z(\sigma) + (2\sigma - 1)Z_1(\tilde{\sigma}) - \frac{2}{\sigma} - \frac{2}{\sigma - 1}$$
$$-\frac{2\sigma-1}{\tilde{\sigma}^2} - \frac{2\sigma-1}{(\tilde{\sigma}-1)^2} + 2\sum_{\rho,1-\rho}\left(\frac{1}{\sigma-\rho} + \frac{1}{\sigma-1+\rho}\right)$$
$$-(2\sigma-1)\sum_{\rho,1-\rho}\left(\frac{-1}{(\tilde{\sigma}-\rho)^2} + \frac{-1}{(\tilde{\sigma}-1+\rho)^2}\right).$$

It therefore remains to show that

$$\sum\left(\frac{1}{\sigma-\rho}+\frac{1}{\sigma-1+\rho}\right)\geq\left(\sigma-\frac{1}{2}\right)\sum\left(\frac{-1}{(\tilde{\sigma}-\rho)^2}+\frac{-1}{(\tilde{\sigma}-1+\rho)^2}\right).$$

Since $g(\rho)=0\Leftrightarrow g(\bar{\rho})=0$, we may pair the terms for ρ and $\bar{\rho}$, which amounts to taking the real part of each side of the above inequality. Let $\rho=x+iy$. It suffices to prove the following.

Lemma 11.21. *Let* $\alpha=\sqrt{\dfrac{7-\sqrt{32}}{17}}$. *Suppose* $\tilde{\sigma}, \sigma>1$ *satisfy*

$$\tilde{\sigma}\geq\frac{5+\sqrt{12\sigma^2-5}}{6}\quad\textit{and}\quad\tilde{\sigma}\geq 1+\alpha\sigma.$$

If $0\leq x\leq 1$ *and* y *is real, then*

$$\frac{\sigma-x}{(\sigma-x)^2+y^2}+\frac{\sigma-1+x}{(\sigma-1+x)^2+y^2}$$
$$\geq\left(\sigma-\frac{1}{2}\right)\left\{\frac{y^2-(\tilde{\sigma}-x)^2}{(y^2+(\tilde{\sigma}-x)^2)^2}+\frac{y^2-(\tilde{\sigma}-1+x)^2}{(y^2+(\tilde{\sigma}-1+x)^2)^2}\right\}.$$

Proof. Both sides are invariant under $x\mapsto 1-x$ and under $y\mapsto -y$, so it suffices to prove the inequality for $\frac{1}{2}\leq x\leq 1$ and $y\geq 0$. A lower bound for the left-hand side is

$$\frac{\sigma-x}{(\sigma-1+x)^2+y^2}+\frac{\sigma-1+x}{(\sigma-1+x)^2+y^2}=\frac{2(\sigma-\frac{1}{2})}{(\sigma-1+x)^2+y^2}.$$

Therefore, it suffices to show

$$\frac{2}{(\sigma-1+x)^2+y^2}\geq\frac{y^2-(\tilde{\sigma}-x)^2}{(y^2+(\tilde{\sigma}-x)^2)^2}+\frac{y^2-(\tilde{\sigma}-1+x)^2}{(y^2+(\tilde{\sigma}-1+x)^2)^2}\qquad(*)$$

for $\frac{1}{2}\leq x\leq 1$ and $y\geq 0$.

Case I. $y\leq\tilde{\sigma}-x$ $(\leq\tilde{\sigma}-1+x)$.

In this case the right-hand side of $(*)$ is negative, so the inequality is trivial.

Case II. $\tilde{\sigma}-x<y<\tilde{\sigma}-1+x$.

The second term on the right-hand side is negative, so we ignore it. Let

$$A=(\sigma-1+x)^2-5(\tilde{\sigma}-x)^2,$$
$$B=\tfrac{1}{4}\{17(\tilde{\sigma}-x)^4-14(\tilde{\sigma}-x)^2(\sigma-1+x)^2+(\sigma-1+x)^4\}$$
$$=\tfrac{17}{4}(\sigma-1+x)^4\left\{\frac{(\tilde{\sigma}-x)^2}{(\sigma-1+x)^2}-\alpha^2\right\}\left\{\frac{(\tilde{\sigma}-x)^2}{(\sigma-1+x)^2}-\frac{1}{17\alpha^2}\right\},$$
$$C=(y^2-\tfrac{1}{2}A)^2-B$$
$$=y^4-Ay^2+(\tilde{\sigma}-x)^2(\sigma-1+x)^2+2(\tilde{\sigma}-x)^4.$$

A calculation shows that

$$\frac{2}{(\sigma-1+x)^2+y^2}-\frac{y^2-(\tilde{\sigma}-x)^2}{(y^2+(\tilde{\sigma}-x)^2)^2}$$
$$=\frac{C}{((\sigma-1+x)^2+y^2)(y^2+(\tilde{\sigma}-x)^2)^2}.$$

We must show $C \geq 0$. If $A \leq 0$, the second expression for C yields $C \geq 0$. Suppose now that $A > 0$, which means that

$$(\tilde{\sigma}-x)^2 < \tfrac{1}{5}(\sigma-1+x)^2.$$

Since $17\alpha^2 < 5$,

$$(\tilde{\sigma}-x)^2 < \frac{1}{17\alpha^2}(\sigma-1+x)^2.$$

Since $\tilde{\sigma} \geq 1+\alpha\sigma$ by assumption,

$$\tilde{\sigma}-x \geq \alpha\sigma+1-x \geq \alpha\sigma-\alpha(1-x) > 0,$$

hence

$$(\tilde{\sigma}-x)^2 \geq \alpha^2(\sigma-1+x)^2.$$

The second expression for B yields $B \leq 0$. The first formula for C shows that $C \geq 0$, as desired.

Case III. $\tilde{\sigma}-1+x \leq y$.

The right-hand side of (*) is bounded above by

$$\frac{2y^2-(\tilde{\sigma}-x)^2-(\tilde{\sigma}-1+x)^2}{(y^2+(\tilde{\sigma}-x)^2)^2}.$$

A short calculation yields

$$\frac{2}{(\sigma-1+x)^2+y^2}-\frac{2y^2-(\tilde{\sigma}-x)^2-(\tilde{\sigma}-1+x)^2}{(y^2+(\tilde{\sigma}-x)^2)^2}$$
$$\geq\frac{y^2(5(\tilde{\sigma}-x)^2+(\tilde{\sigma}-1+x)^2-2(\sigma-1+x)^2)}{((\sigma-1+x)^2+y^2)(y^2+(\tilde{\sigma}-x)^2)^2}.$$

We must show the numerator is nonnegative. Let

$$f(x)=5(\tilde{\sigma}-x)^2+(\tilde{\sigma}-1+x)^2-2(\sigma-1+x)^2.$$

Then

$$f'(x)=8(x-\tilde{\sigma})+(2-4\sigma)<0,$$

for $x \leq 1$. Therefore

$$f(x) \geq f(1) = 5(\tilde{\sigma}-1)^2+\tilde{\sigma}^2-2\sigma^2 \geq 0,$$

since $\tilde{\sigma} \geq (5 + \sqrt{12\sigma^2 - 5})/6$. This completes the proof of Case III, hence of Lemma 11.21. □

The proof of Theorem 11.20 is now complete. □

§11.5 Calculation of h_m^+

The estimates given in the table of the previous section may be used to calculate h_m^+ for small m, in particular for those m listed in Theorem 11.1. The main tools we need are the following two lemmas.

Lemma 11.22. *If L/K is an extension of degree n in which no finite primes ramify, then*

$$D_L = D_K^n,$$

where D_L and D_K are the absolute values of the discriminants of L and K, respectively.

Proof. A well-known formula (see Lang [1], pp. 60, 66) states that

$$D_L = D_K^n N\mathscr{D}_{L/K}$$

where $N\mathscr{D}_{L/K}$ is the norm of the relative different. Since no primes ramify, $\mathscr{D}_{L/K} = (1)$. The result follows. □

Lemma 11.23. *Let $B(n)$ be the lower bound for $D^{1/n}$ for totally real fields of degree $\geq n$ (as given in the table of the previous section). Let d_m^+ and h_m^+ be the discriminant and class number of $\mathbb{Q}(\zeta_m)^+$. If*

$$(d_m^+)^{2/\phi(m)} < B\left(\frac{h\phi(m)}{2}\right)$$

then

$$h_m^+ < h.$$

Proof. Let H be the Hilbert class field of $\mathbb{Q}(\zeta_m)^+$, so $H/\mathbb{Q}(\zeta_m)^+$ is an unramified extension of degree h_m^+, and

$$n_H = [H:\mathbb{Q}] = \tfrac{1}{2}\phi(m)h_m^+.$$

By Lemma 11.22,

$$D_H^{1/n_H} = (d_m^+)^{2/\phi(m)} < B\left(\frac{h\phi(m)}{2}\right).$$

Therefore

$$\tfrac{1}{2}\phi(m)h_m^+ = n_H < \frac{h\phi(m)}{2}.$$

The lemma follows. □

Since $2|h_m^+ \Rightarrow 2|h_m^-$ by Theorem 10.2, h_m^+ must be odd whenever $h_m^- = 1$. Consequently, we only need to show $h_m^+ < 3$. This may be done via Lemma 11.23. The value of d_m^+ may be calculated by Lemma 4.18 and Proposition 2.7, or by the conductor–discriminant formula. We give a few examples:

$\boldsymbol{m = 3, 4.}$ $\mathbb{Q}(\zeta_m)^+ = \mathbb{Q}$, so $h_m^+ = 1$.

$\boldsymbol{m = 5, 8, 12.}$ $\mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\sqrt{m})$, so these class numbers may be calculated directly (via the analytic class number formula).

$\boldsymbol{m = 7, 9.}$ $[\mathbb{Q}(\zeta_m)^+ : \mathbb{Q}] = 3$ and only one prime ramifies, so $3 \nmid h_m^+$ by Theorem 10.4. Since h_m^+ is odd, $h_m^+ = 1$ or $h_m^+ \geq 5$. The discriminants are 7^2 and 9^2. Both satisfy

$$(d_m^+)^{1/3} < 10 = B(10) = B((\tfrac{10}{3})3).$$

By Lemma 11.23, $h_m^+ < \frac{10}{3}$, hence $h_m^+ = 1$.

$\boldsymbol{m = 15, 16, 20, 24.}$ These all have degree 4. The discriminants are $3^2 \cdot 5^3$, $2^{11}, 2^4 \cdot 5^3, 2^8 \cdot 3^2$, respectively. The largest of these is $d_{24}^+ = 2^8 \cdot 3^2$. Therefore

$$(d_m^+)^{1/4} \leq (2^8 \cdot 3^2)^{1/4} = 4\sqrt{3} < B(10) = B(\tfrac{5}{2} \cdot 4),$$

so $h_m^+ < \frac{5}{2}$. Therefore $h_m^+ = 1$.

$\boldsymbol{m = 35, 45, 84.}$ These all have degree 12. The discriminants are $5^9 \cdot 7^{10}$, $3^{18} \cdot 5^9$, $2^{12} \cdot 3^6 \cdot 7^{10}$, respectively. The largest of these is $2^{12} \cdot 3^6 \cdot 7^{10}$. As before,

$$(d_m^+)^{1/2} \leq (2^{12} \cdot 3^6 \cdot 7^{10})^{1/12} = 2\sqrt{3} \cdot 7^{5/6} < 18 < B(30) = B(\tfrac{5}{2} \cdot 12).$$

Therefore $h_m^+ < 5/2$, so $h_m^+ = 1$.

The other values of m are treated similarly. So all the values of m listed in Theorem 11.1 have $h_m^+ = 1$. Since all of these have $h_m^- = 1$, and since Proposition 11.19 says that these are the only possibilities for $h_m = 1$, the proof of Theorem 11.1 is complete. □

Remark. It is not always true that if $h^- = 1$ for a CM-field, then $h^+ = 1$. See Exercise 11.6.

Notes

The papers of Masley contain several discussions of the results in this chapter.

The estimation of h_m^- follows the method used in Masley [1]. For other methods, see Masley–Montgomery [1], Uchida [1], and Hoffstein [1]. The last paper applies to many CM-fields and does not rely on the factorization of the zeta function into L-series.

For analytic estimates of h_p^- and $h_{p^n}^-$, see Ankeny–Chowla [1], Lepistö [1], and Metsänkylä [4]. For a simple but accurate upper bound, see Carlitz [2].

For the calculation of h_m^+, see van der Linden [1] and the papers of Masley. For examples of $h_m^+ > 1$, see Ankeny–Chowla–Hasse [1], S.-D. Lang [1], Cornell–Washington [1], and Takeuchi [1].

For Euclidean cyclotomic fields, see Masley [3], Ojala [1], and several papers of Lenstra.

For more on Odlyzko's results, see his papers, plus Martinet [1], [2], Diaz y Diaz [1], and Poitou [1], [2].

Exercises

11.1. Use the Minkowski bound (Exercise 2.5) to show that

$$D^{1/n} \geq (e^2)^{r_1/n}\left(\frac{e^2\pi}{4}\right)^{2r_2/n}(1 + o(1)).$$

This is much weaker than Theorem 11.20.

11.2. Show that none of the fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$ has any nontrivial unramified extension. These are precisely the imaginary quadratic fields with class number 1, so we know that there are no such abelian extensions. The problem is therefore the other (not necessarily Galois) extensions.

11.3. (a) Show that if $2 \mid h_{29}^+$ then $8 \mid h_{29}^+$ (see the example following Theorem 10.8).

(b) Show that $h_{29}^+ = 1$ (hence the class group of $\mathbb{Q}(\zeta_{29})$ is $(\mathbb{Z}/2\mathbb{Z})^3$ by the example of Chapter 10).

11.4. Let $K = H_0$ and let H_{i+1} be the Hilbert class field of H_i. Show that the class field tower stops ($H_i = H_{i+1} = \cdots$ for some i) $\Leftrightarrow K$ is contained in a field of class number 1.

11.5. Let n divide m, so $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$. Let p be odd and let A_n and A_m be the p-Sylow subgroups of the ideal class groups. Show that the norm maps A_m^- onto A_n^-. Conclude that h_n^- divides h_m^-, except for possibly a power of 2 (Masley has shown that h_n^- divides h_m^-).

11.6. Let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{10})$.

(a) Show that $K \subset \mathbb{Q}(\zeta_8, \sqrt{5}) \subset \mathbb{Q}(\zeta_{40})$.

(b) Show that $\mathbb{Q}(\zeta_{40})/\mathbb{Q}(\zeta_8, \sqrt{5})$ is totally ramified at the primes above 5.

(c) Use Theorem 11.1 to show that $\mathbb{Q}(\zeta_8, \sqrt{5})$ has class number 1.

(d) Show that K has class number at most 2. In fact, use Theorem 3.5 to show that the extension $\mathbb{Q}(\zeta_8, \sqrt{5})/K$ is unramified, so the class number is 2 and $\mathbb{Q}(\zeta_8, \sqrt{5})$ is the Hilbert class field.

(e) Show $K^+ = \mathbb{Q}(\sqrt{10})$, which has class number 2.

(f) Conclude that $h^- = 1$ but $h^+ = 2$ for K.

Chapter 12

Measures and Distributions

The concept of a distribution, as given in this chapter, is one that occurs repeatedly in mathematics, especially in the theory of cyclotomic fields. As we shall see, many ideas from Chapters 4, 5, 7, and 8 fit into this general framework. The related concept of a measure yields a p-adic integration theory which allows us to interpret the p-adic L-function as a Mellin transform, as in the classical case.

Many of the extensions of the cyclotomic theory have used measures and distributions; see for example the work of Kubert and Lang on modular curves. For an approach to cyclotomic fields that is much more measure-theoretic than the present exposition, the reader should consult Lang [4] and [5].

In this chapter, we first introduce distributions and give some examples. We then define measures and give a p-adic integration theory, including the Γ-transform and Mellin transform. We also give the relations between the present theory and the power series of Chapter 7. Finally we determine the ranks of some universal distributions, and consequently obtain a proof of Bass' theorem on generators and relations for cyclotomic units (Theorem 8.9). The second and third sections of this chapter are independent and may be read in either order.

§12.1 Distributions

Let I be a partially ordered set. For technical reasons we assume that for each $i, j \in I$, there is a $k \in I$ such that $k \geq i$, $k \geq j$. Such sets I are called "directed." Let

$$\{X_i \mid i \in I\}$$

be a collection of finite sets. If $i \geq j$ we assume there is a surjective map

$$\pi_{ij}: X_i \to X_j.$$

such that $\pi_{ij} \circ \pi_{jk} = \pi_{ik}$ whenever $i \geq j \geq k$. Suppose that for each i we have a function ϕ_i on X_i, with values in some fixed abelian group, such that if $i \geq j$,

$$\phi_j(x) = \sum_{\pi_{ij}(y)=x} \phi_i(y).$$

The collection of maps $\{\phi_i\}$ is called a *distribution.*

Examples. (1) Let I be the positive integers with the usual ordering and let $X_i = \mathbb{Z}/p^i\mathbb{Z}$, with π_{ij} the obvious map. Fix $a \in \mathbb{Z}_p$. Let

$$\phi_i(y) = \begin{cases} 1, & \text{if } y \equiv a \bmod p^i, \\ 0, & \text{otherwise.} \end{cases}$$

Then $\{\phi_i\}$ forms a distribution, called the delta distribution.

(2) Let I be the positive integers ordered by divisibility: $i \geq j$ if $j \mid i$. Let

$$X_i = \mathbb{Z}/i\mathbb{Z}$$

and

$$\pi_{ij}: \mathbb{Z}/i\mathbb{Z} \to \mathbb{Z}/j\mathbb{Z}$$

$$y \bmod i \mapsto y \bmod j.$$

Let

$$\zeta_i(a, s) = \sum_{\substack{n \equiv a \bmod i \\ n > 0}} n^{-s}$$

be the partial zeta function, as in Chapter 4. Then $\{\phi_i\}$, where $\phi_i(a) = \zeta_i(a, s)$ is a distribution (with values in the additive group of meromorphic functions on $\mathbb{C}$).

(3) Let I be the positive integers ordered as in Example 2. Let

$$X_i = \frac{1}{i}\mathbb{Z}/\mathbb{Z}$$

and let π_{ij} be multiplication by i/j. For $k > 0$, let $B_k(X)$ be the kth Bernoulli polynomial, as defined in Chapter 4. Let

$$\phi_i\left(\frac{a}{i}\right) = i^{k-1}B_k\left(\left\{\frac{a}{i}\right\}\right)$$

where $\{\ \}$ denotes the fractional part. To get an odd distribution for odd k, it is convenient to let

$$\phi_i\left(\frac{0}{i}\right) = 0 \quad \text{if } k = 1.$$

Then $\{\phi_i\}$ forms a distribution, called the kth Bernoulli distribution. This follows from properties of Bernoulli polynomials. Even better, we know that

$$\zeta_i(a, 1-k) = -\frac{i^{k-1}}{k} B_k\left(\left\{\frac{a}{i}\right\}\right),$$

so the distribution relation follows from that of Example 2.

One easily sees that the sets X_i and maps π_{ij} of Examples 2 and 3 are essentially equivalent: We have a commutative diagram

$$\begin{tikzcd}
\frac{1}{i}\mathbb{Z}/\mathbb{Z} \arrow[r, "i/j"] \arrow[d, "i"'] & \frac{1}{j}\mathbb{Z}/\mathbb{Z} \arrow[d, "j"'] \\
\mathbb{Z}/i\mathbb{Z} \arrow[r] & \mathbb{Z}/j\mathbb{Z}.
\end{tikzcd}$$

(4) Let I and X_i be as in Example 3. Let ζ_i be a primitive ith root of 1; we assume $(\zeta_i)^{i/j} = \zeta_j$ (for example, with terrible notation, $\zeta_i = e^{2\pi i/i}$). Let

$$\phi_i\left(\frac{a}{i}\right) = \zeta_i^a - 1.$$

Since

$$\prod_{b=0}^{(i/j)-1} (\zeta_i^{a+bj} - 1) = \zeta_j^a - 1 \quad (\text{if } j \mid i),$$

the (multiplicative) distribution relations are satisfied. But there is a problem. The function ϕ_i takes values in $\mathbb{C}^\times \cup \{0\}$, which is not a multiplicative group. We could allow monoid-valued distributions, but this causes problems with Theorem 12.18. It is more convenient to define a *punctured distribution* by omitting the relations with $x = 0$ in the defining relations for a distribution. The value $\phi_i(0)$ may then be ignored.

We could also let $\phi_i(a/i) = |\zeta_i^a - 1|$ or $\phi_i(a/i) = \log|\zeta_i^a - 1|$. We then obtain punctured distributions (one multiplicative, the other additive) which satisfy

$$\phi_i\left(-\frac{a}{i}\right) = \phi_i\left(\frac{a}{i}\right).$$

In other words, ϕ_i is even. Since

$$B_k(1 - X) = (-1)^k B_k(X),$$

the kth Bernoulli distribution is even or odd, depending on k (technical point: Since $\{-0\} \neq 1 - \{0\}$, we also need the fact that $B_k(0) = 0$ for odd $k > 1$).

There is a special type of distribution, which will be studied in the third section of this chapter. Assume ϕ is a function defined on $\mathbb{Q}/\mathbb{Z}$ such that

$$\phi\left(\frac{a}{j}\right) = \sum_{b=0}^{(i/j)-1} \phi\left(\frac{a+bj}{i}\right)$$

whenever $a \in \mathbb{Z}$ and $j \mid i$. Equivalently, if $m \in \mathbb{Z}$, $m > 0$, and $y \in \mathbb{Q}/\mathbb{Z}$, then

$$\phi(y) = \sum_{mx=y} \phi(x)$$

(let $m = i/j$, $y = a/j$). We call ϕ an *ordinary distribution.* The distribution of Example 4 and the first Bernoulli distribution fit into this category if we let

$$\phi\left(\frac{a}{i}\right) = \phi_i(a).$$

The main point is that if $a/i = b/j$ then $\phi_i(a) = \phi_j(b)$, so ϕ is well-defined as a function on $\mathbb{Q}/\mathbb{Z}$. The delta distribution of Example 1 does not arise from an ordinary distribution, even on $\mathbb{Q}_p/\mathbb{Z}_p$: $\phi_i(a) = 1$ but $\phi_{i+1}(pa) = 0$ (unless $a \equiv 0 \bmod p^{i+1}$). Also, if $k \neq 1$, the kth Bernoulli distribution is not ordinary.

There is a second, equivalent definition of distributions. Consider the situation at the beginning of this section and let

$$X = \varprojlim X_i$$

(see the appendix for inverse limits). Since each X_i is finite, X is compact. Let ϕ be a finitely additive function on the collection of compact-open subsets of X. We shall show that ϕ gives rise to a distribution. For each i there is a surjective (since each π_{ij} is surjective) map

$$\pi_i : X \to X_i.$$

If $a \in X_i$ then $\pi_i^{-1}(a)$ is a compact-open subset of X. All compact-open sets are obtained as finite unions of such $\pi_i^{-1}(a)$, as i and a vary (these sets form a basis for the topology of X). Suppose $b \in X_j$. For $i \geq j$,

$$\pi_j^{-1}(b) = \bigcup_{\substack{a \in X_i \\ \pi_{ij}(a) = b}} \pi_i^{-1}(a),$$

and this is a disjoint union. Therefore

$$\phi(\pi_j^{-1}(b)) = \sum_{\pi_{ij}(a)=b} \phi(\pi_i^{-1}(a)),$$

so $b \mapsto \phi(\pi_j^{-1}(b))$ satisfies the distribution relation. Conversely, any distribution $\{\phi_i\}$ on $\{X_i\}$ gives a finitely additive function on compact-open sets of X.

Finally, we give a third formulation of distributions. A function f on X is called locally constant (or a step function) if for each $x \in X$, there is a neighborhood U of x such that f is constant on U. Since X is compact, this means that f is a finite linear combination of characteristic functions of disjoint compact-open sets. In fact, f is a finite linear combination of characteristic functions of sets of the form $\pi_i^{-1}(a)$. Call these characteristic functions $\chi_{i,a}$.

Let Step (X) be the set of locally constant functions on X. If ϕ is a finitely additive function on compact-opens with values in a group W, then we may extend ϕ by linearity to obtain a map

$$\phi\colon \text{Step}\,(X) \to W.$$

If $\{\phi_i\}$ is the associated distribution, then

$$\phi(\chi_{i,a}) = \phi_i(a).$$

Conversely, a linear function on Step (X) may be restricted to characteristic functions to yield a finitely additive function on compact-opens.

In summary, we have the following one-one correspondences:

$$\begin{aligned}\text{distributions} &\leftrightarrow \text{finitely additive functions on compact-opens}\\ &\leftrightarrow \text{linear functionals on Step}\,(X).\end{aligned}$$

We now reinterpret the delta distribution of Example 1. Let $U \subset \mathbb{Z}_p$ be compact and open, and let $a \in \mathbb{Z}_p$. Let

$$\delta_a(U) = \begin{cases} 1, & \text{if } a \in U \\ 0, & \text{if } a \notin U. \end{cases}$$

Since

$$\pi_i^{-1}(y \bmod p^i) = y + p^i\mathbb{Z}_p,$$

we see that δ_a corresponds to the delta distribution. If $f \in$ Step (X), we have

$$\delta_a(f) = f(a),$$

which is exactly how the classical delta function acts.

There is a natural function on compact-opens of $\mathbb{Z}_p$, namely

$$\phi(U) = \text{meas}(U),$$

where meas is the Haar measure normalized by $\text{meas}(\mathbb{Z}_p) = 1$. We have

$$\phi(y + p^i\mathbb{Z}_p) = \frac{1}{p^i}$$

so the associated distribution satisfies

$$\phi_i(y \bmod p^i) = \frac{1}{p^i}.$$

More generally, consider the spaces $X_i = \mathbb{Z}/i\mathbb{Z}$ and maps π_{ij} of Example 2. In this case,

$$X = \varprojlim \mathbb{Z}/i\mathbb{Z} \overset{\text{def}}{=} \hat{\mathbb{Z}} \simeq \prod_{\text{all } p} \mathbb{Z}_p,$$

where the isomorphism is obtained via the Chinese Remainder Theorem ($\mathbb{Z}/i\mathbb{Z} \simeq \prod_p \mathbb{Z}_p/i\mathbb{Z}_p$). Again, we have a compact group, so we can let $\phi(U) = \text{meas}(U)$. This yields the distribution defined by $\phi_i(y \bmod i) = 1/i$.

The Haar distributions will not be very useful to us when we develop p-adic integration in the next section. Consider the case of $\mathbb{Z}_p$. As the sets $y + p^i\mathbb{Z}_p$ become smaller ($i \to \infty$), their Haar measures become p-adically larger. Clearly this is not desirable since a small change in a function could produce a large change in its integral. The distributions that will be of use will be those with bounded denominators, which we shall call measures. These will be studied in the next section.

§12.2 Measures

Let the notations be as in the first section. Consider a distribution $\{\phi_i\}$. Let ϕ be the corresponding functional on Step (X). For $f \in$ Step (X), denote

$$\phi(f) = \int_X f\, d\phi.$$

Assume that ϕ takes values in $\mathbb{C}_p$ (= completion of the algebraic closure of $\mathbb{Q}_p$). We say that ϕ (or $d\phi$) is a *measure* if there exists a constant K such that

$$|\phi_i(a)| \leq K$$

for all i and all $a \in X_i$. Let $C(X, \mathbb{C}_p)$ be the $\mathbb{C}_p$-Banach space of continuous $\mathbb{C}_p$-valued functions on X, where

$$\|f\| = \sup_{x \in X} |f(x)|.$$

Then Step (X) (with values in $\mathbb{C}_p$) is dense in $C(X, \mathbb{C}_p)$.

Proposition 12.1. *If ϕ is a measure, then*

$$\int_X f\, d\phi\colon \text{Step }(X) \to \mathbb{C}_p$$

extends uniquely to a continuous $\mathbb{C}_p$-linear map

$$\int_X f\, d\phi\colon C(X, \mathbb{C}_p) \to \mathbb{C}_p.$$

Proof. Since the step functions are dense, the map must be unique if it exists.

Observe that if K is the constant used above and $\chi_{i,a}$ is the characteristic function of the previous section,

$$\left|\int_X \chi_{i,a}\, d\phi\right| = |\phi_i(a)| \leq K.$$

Since the absolute value is non-archimedean,

$$\left|\int_X f\, d\phi\right| \leq K\|f\|, \qquad f \in \text{Step}\,(X).$$

If $g \in C(X, \mathbb{C}_p)$ and $\{f_n\}$ is a Cauchy sequence in Step (X) converging to g, then

$$\left|\int_X f_n\, d\phi - \int_X f_m\, d\phi\right| \leq K\|f_n - f_m\| \to 0$$

as $m, n \to \infty$. Therefore, let

$$\int_X g\, d\phi = \lim \int_X f_n\, d\phi.$$

This has the desired properties, so the proof is complete. □

Examples. (1) Let $a \in \mathbb{Z}_p$ and let δ_a be the delta distribution. Then

$$\int f\, d\delta_a = f(a)$$

for $f \in$ Step (X), hence for $f \in C(X, \mathbb{C}_p)$.

(2) Let ϕ be the Haar distribution on $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Then ϕ is not a measure. What happens if we try to integrate anyway? Let $f(x) = x$ be defined on $\mathbb{Z}_p$. Recall that $\chi_{n,a}$ is the characteristic function of $a + p^n\mathbb{Z}_p$. Hence

$$\left|f(x) - \sum_{a=0}^{p^n-1} a\chi_{n,a}(x)\right| \leq |p^n| \to 0 \quad \text{as } n \to \infty.$$

also

$$\left|f(x) - \sum_{a=1}^{p^n} a\chi_{n,a}(x)\right| \to 0.$$

But

$$\sum_{a=0}^{p^n-1} a \operatorname{meas}(a + p^n\mathbb{Z}_p) = \sum_{a=0}^{p^n-1} \frac{a}{p^n} = \frac{p^n-1}{2} \to -\frac{1}{2},$$

while

$$\sum_{a=1}^{p^n} a \operatorname{meas}(a + p^n\mathbb{Z}_p) \to +\frac{1}{2}.$$

Therefore $\int x\,d\phi$ is not well defined. This is why we require ϕ to be bounded. However, it is possible to weaken this condition slightly (see Koblitz [1], p. 41).

(3) If $g \in C(X, \mathbb{C}_p)$ and $d\phi$ is a measure on X, we may define a new measure

$$d\psi = g\,d\phi$$

by

$$\int_X f\,d\psi = \int_X fg\,d\phi.$$

Clearly this gives a finitely additive linear functional on Step (X). Since X is compact, g is bounded. It follows that $d\psi$ is a measure. Often we shall take g to be the characteristic function of a subset $X' \subseteq X$. We then write $\int_{X'} f\,d\phi$ for $\int_X fg\,d\phi$.

(4) If $h\colon X \to Y$ is continuous and $d\phi$ is a measure on X, then we obtain a measure $d\psi$ on Y by defining

$$\int_Y f\,d\psi = \int_X f(h(x))\,d\phi.$$

This will allow us to obtain measures on $\mathbb{Z}_p$ from measures on $1 + p\mathbb{Z}_p$, via the logarithm mapping.

The Bernoulli distributions are not measures. However it is possible to modify them. We treat only the case $k = 1$; the cases $k \geq 2$ are similar.

Let $(d, p) = 1$ and let

$$X_n = (\mathbb{Z}/d_p^{n+1}\mathbb{Z})^\times.$$

Then

$$X = \varprojlim X_n \simeq (\mathbb{Z}/dp\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$$

(if $p \neq 2$; the modifications for $p = 2$ are left to the reader). We could also work with $\mathbb{Z}/dp^{n+1}\mathbb{Z}$, but the present situation fits into the framework of later results. Let $c \in \mathbb{Z}$, $(c, dp) = 1$. For $n \geq 0$, let c^{-1} denote an integer such that $cc^{-1} \equiv 1 \bmod dp^{2(n+1)}$ (the 2 in the exponent is for technical reasons: it is used to obtain (**) below; probably it can be avoided). Alternatively, $c \in X$ in a natural way, so let c^{-1} be the inverse of c in X and then reduce mod $dp^{2(n+1)}$ when needed. For $x_n \in X_n$, define

$$\begin{aligned} E_c(x_n) &= B_1\left(\left\{\frac{x_n}{dp^{n+1}}\right\}\right) - cB_1\left(\left\{\frac{c^{-1}x_n}{dp^{n+1}}\right\}\right) \\ &= \left\{\frac{x_n}{dp^{n+1}}\right\} - c\left\{\frac{c^{-1}x_n}{dp^{n+1}}\right\} + \frac{c-1}{2}. \end{aligned}$$

It is easily seen that E_c is a distribution. Since

$$\left\{\frac{x_n}{dp^{n+1}}\right\} - c\left\{\frac{c^{-1}x_n}{dp^{n+1}}\right\} \in \mathbb{Z},$$

$E_c(x_n) \in \mathbb{Z}_p$, so E_c is a measure.

If χ is a Dirichlet character of conductor dp^m for some $m \geq 0$, we may write $\chi\omega^{-1} = \theta\psi$, where θ is of the first kind, and ψ is of the second kind (see Chapter 7). Then θ is a function on $(\mathbb{Z}/dp\,\mathbb{Z})^\times$ and ψ is a function on $1 + p\mathbb{Z}_p$. Therefore we may regard $\chi\omega^{-1} = \theta\psi$ as a function on X. Also, $\langle x\rangle$ may be regarded as a function on X; it is just the projection onto $1 + p\mathbb{Z}_p$.

Theorem 12.2. *Let χ have conductor dp^m with $(d, p) = 1$ and $m \geq 0$. For $s \in \mathbb{Z}_p$,*

$$\int_{(\mathbb{Z}/dp\,\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)} \chi\omega^{-1}(a)\langle a\rangle^s\, dE_c = -(1 - \chi(c)\langle c\rangle^{s+1})L_p(-s, \chi)$$

Proof. We shall show later (Corollary 12.5) that the left-hand side is analytic in s, so it suffices to let $s = k - 1$, with k a positive integer. We may estimate a by $b \in \mathbb{Z}$ on $\{x \in X \,|\, x \equiv b \bmod dp^n\}$. We obtain the sum

$$\sum_{\substack{b=0\\ p\nmid b}}^{dp^n-1} \chi\omega^{-k}(b)b^{k-1}\left(\frac{b}{dp^n} - c\left\{\frac{c^{-1}b}{dp^n}\right\} + \frac{c-1}{2}\right).$$

By Lemma 7.11, the term with $(c - 1)/2$ tends to 0 as $n \to \infty$, so we may ignore it. By the same lemma,

$$\frac{1}{dp^n}\sum_b \chi\omega^{-k}(b)b^k \to (1 - \chi\omega^{-k}(p)p^{k-1})B_{k,\chi\omega^{-k}} \overset{\text{def}}{=} U.$$

The remaining term is the hardest to evaluate. Let

$$c^{-1}b = b_1 + dp^n b_2, \quad \text{with} \quad 0 \leq b_1 < dp^n.$$

Note that

$$\chi\omega^{-k}(b) = \chi\omega^{-k}(c)\chi\omega^{-k}(b_1) \quad (\text{if } n \geq m) \tag{$*$}$$

and

$$b^k \equiv c^k(b_1 + dp^n b_2)^k \equiv c^k(b_1^k + k\, dp^n b_2 b_1^{k-1}) \pmod{p^{2n}}. \tag{$**$}$$

Therefore

$$\sum_b \chi\omega^{-k}(b)b^k \equiv \chi\omega^{-k}(c)c^k \sum_b \chi\omega^{-k}(b_1)b_1^k$$
$$+ k\, dp^n\chi\omega^{-k}(c)c^k \sum_b \chi\omega^{-k}(b_1)b_2 b_1^{k-1}.$$

But b_1 runs through the same values as b, in a different order. Consequently, we obtain

$$\begin{aligned}&\chi\omega^{-k}(c)c^k \sum \chi\omega^{-k}(b_1)b_2 b_1^{k-1}\\ &\qquad \equiv (1 - \chi\omega^{-k}(c)c^k)\frac{1}{k\,dp^n}\sum \chi\omega^{-k}(b)b^k \left(\operatorname{mod} \frac{1}{k}p^n\right).\end{aligned}$$

The remaining term in the original sum involves $c\{c^{-1}b/dp^n\} = cb_1/dp^n$. We have

$$\begin{aligned}&-\frac{c}{dp^n}\sum_b \chi\omega^{-k}(b)b^{k-1}b_1\\ &\qquad \equiv -\frac{c}{dp^n}\sum_b \chi\omega^{-k}(b)c^{k-1}(b_1^k + (k-1)\,dp^n b_2 b_1^{k-1})\end{aligned}$$

(by (**) with k replaced by $k - 1$)

$$\begin{aligned}&\equiv -\frac{c^k}{dp^n}\chi\omega^{-k}(c)\sum_b \chi\omega^{-k}(b_1)b_1^k\\ &\qquad -(k-1)c^k\chi\omega^{-k}(c)\sum_b \chi\omega^{-k}(b_1)b_2 b_1^{k-1} \pmod{p^n} \text{ (by (*))}.\end{aligned}$$

By Lemma 7.11, the first term yields

$$-\chi\omega^{-k}(c)c^k(1 - \chi\omega^{-k}(p)p^{k-1})B_{k,\chi\omega^{-k}} \overset{\text{def}}{=} V.$$

By the above calculations, the second term is congruent mod $(1/k)p^n$ to

$$\begin{aligned}&-(k-1)(1 - \chi\omega^{-k}(c)c^k)\frac{1}{k\,dp^n}\sum_b \chi\omega^{-k}(b)b^k\\ &\qquad \to -\frac{k-1}{k}(1 - \chi\omega^{-k}(c)c^k)(1 - \chi\omega^{-k}(p)p^{k-1})B_{k,\chi\omega^{-k}} \overset{\text{def}}{=} W,\end{aligned}$$

as $n \to \infty$. Addition of the relevant terms shows that the original sum approximating the integral becomes, as $n \to \infty$,

$$\begin{aligned}U + V + W &= (1 - \chi\omega^{-k}(c)c^k)(1 - \chi\omega^{-k}(p)p^{k-1})\frac{B_{k,\chi\omega^{-k}}}{k}\\ &= -(1 - \chi\omega^{-k}(c)c^k)L_p(1 - k, \chi)\\ &= -(1 - \chi(c)\langle c\rangle^k)L_p(1 - k, \chi).\end{aligned}$$

This completes the proof. □

The reader probably noticed that there is a great similarity between this proof and that of Theorem 7.10. This is not a coincidence, as we shall see later. First, however, we note some consequences. If $\chi \neq 1$, choose c so that $\chi(c) \neq 1$. Then $\chi(c)\langle c\rangle^s \neq 1$. Otherwise $\langle c\rangle^{sN} = 1$ for some $N > 0$, which implies $s = 0$. Since $\chi(c) \neq 1$, we have $\chi(c)\langle c\rangle^0 \neq 1$, so the claim holds for all s. Consequently, we may divide by $(1 - \chi(c)\langle c\rangle^s)$. Assuming that the integral is holomorphic, we find that $L_p(s, \chi)$ is holomorphic. If $\chi = 1$, then $1 - \langle c\rangle^s = 0$ for $s = 0$. So $L_p(s, \chi)$ is holomorphic except possibly for $s = 1$.

Corollary 12.3. *If* $m \equiv n \bmod p^{b-1}(p - 1)$, *and* $m \not\equiv 0 \bmod p - 1$, *then*

$$(1 - p^{m-1})\frac{B_m}{m} \equiv (1 - p^{n-1})\frac{B_n}{n} \pmod{p^b}.$$

PROOF. Let $d = 1$, $\chi = \omega^m$, and $s = m - 1$. Then

$$(1 - c^m)(1 - p^{m-1})\frac{B_m}{m} = -(1 - c^m)L_p(1 - m, \omega^m) = \int_{\mathbb{Z}_p^\times} a^{m-1}\, dE_c.$$

Since E_c is $\mathbb{Z}_p$-valued, and $a^{m-1} \equiv a^{n-1} \bmod p^b$,

$$\int_{\mathbb{Z}_p^\times} a^{m-1}\, dE_c \equiv \int_{\mathbb{Z}_p^\times} a^{n-1}\, dE_c \bmod p^b.$$

Also, $1 - c^m \equiv 1 - c^n$. Choose c so that $c^m \not\equiv 1 \bmod p$. The result now follows easily, since m and n are interchangeable. □

Theorem 12.2 has an analogue for the complex L-series. In the proof of Theorem 4.2 we showed that for a certain function $F_b(t)$,

$$\Gamma(s)\zeta(s, b) = \int_0^\infty F_b(t)t^{s-2}\, dt,$$

so

$$\Gamma(s)L(s, \chi) = \int_0^\infty G(t)t^{s-1}\, dt,$$

for some function $G(t)$. The Mellin transform of a function $f(t)$ is defined to be

$$\int_0^\infty t^s f(t)\frac{dt}{t}.$$

We write dt/t since this is the Haar measure on the multiplicative group of positive real numbers.

Let Δ be a finite group and let (for simplicity, $p \neq 2$)

$$X = \Delta \times (1 + p\mathbb{Z}_p) = \varprojlim \Delta \times (1 + p\mathbb{Z}_p)/(1 + p^{n+1}\mathbb{Z}_p).$$

For $a \in X$, $\langle a\rangle$ represents the projection onto $1 + p\mathbb{Z}_p$. Let ϕ be a measure on X. Define the *gamma transform* of ϕ by

$$(\Gamma_p\phi)(s) = \int_X \langle a\rangle^s\, d\phi.$$

If $\Delta = (\mathbb{Z}/dp\,\mathbb{Z})^\times$ with $(d, p) = 1$, then

$$X \simeq (\mathbb{Z}/d\mathbb{Z})^\times \times \mathbb{Z}_p^\times.$$

For $a \in X$, write $a = a_d a_p$, corresponding to this decomposition. We may define the *Mellin transform* of ϕ by

$$(M_p\phi)(s) = \int_X \langle a\rangle^s \frac{1}{a_p}\, d\phi.$$

Of course, the gamma and Mellin transforms are almost the same:

$$M_p(\phi) = \Gamma_p\left(\frac{1}{a_p}\phi\right).$$

From Theorem 12.2, we have

$$\begin{aligned} -(1 - \chi(c)\langle c\rangle^{s+1})L_p(-s, \chi) &= \Gamma_p(\chi\omega^{-1}E_c)(s) \\ &= M_p(\chi E_c)(s + 1). \end{aligned}$$

The gamma transform receives its name by analogy with the classical equation

$$\Gamma(s) = \int_0^\infty t^s e^{-t} \frac{dt}{t}.$$

Of course, this just the Mellin transform of e^{-t}.

We now investigate the relation between measures and power series. Suppose

$$X_n = \Delta \times \Gamma_n$$

where Δ is a finite group and $\Gamma_n \simeq \mathbb{Z}/p^n\mathbb{Z}$. We assume $X_n \to X_m$ corresponds to $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$. Then

$$X = \Delta \times \Gamma, \quad \text{with } \Gamma \simeq \mathbb{Z}_p.$$

Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Then

$$\mathcal{O}[[\Delta \times \Gamma]] = \varprojlim \mathcal{O}[\Delta \times \Gamma_n] = \varprojlim \mathcal{O}[\Delta][\Gamma_n].$$

Choose a generator γ_0 of Γ. Since

$$\varprojlim \mathcal{O}[\Gamma_n] \simeq \mathcal{O}[[T]]$$

by Theorem 7.1, with $\gamma_0 \mapsto 1 + T$, we obtain

$$\mathcal{O}[[\Delta \times \Gamma]] \simeq \mathcal{O}[\Delta][[T]].$$

Let

$$(\ldots, x_n, \ldots) \in \varprojlim \mathcal{O}[\Delta \times \Gamma_n].$$

Write

$$x_n = \sum_{g \in \Delta \times \Gamma_n} \phi_n(g) g.$$

It follows easily from the fact that $x_n \mapsto x_m$ if $n \geq m$ that $\{\phi_n\}$ defines an $\mathcal{O}$-valued distribution, hence an $\mathcal{O}$-valued measure. Conversely, if $\{\phi_n\}$ defines an $\mathcal{O}$-valued distribution on $\Delta \times \Gamma$, we obtain a corresponding element of $\mathcal{O}[[\Delta \times \Gamma]]$. We therefore have the following one-one correspondences:

$$\begin{tikzcd}
\mathcal{O}\text{-valued distributions} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \mathcal{O}[[\Delta \times \Gamma]] \arrow[d, leftrightarrow] \\
\mathcal{O}\text{-valued measures on } \Delta \times \Gamma & \mathcal{O}[\Delta][[T]]
\end{tikzcd}$$

Therefore, measures correspond to power series. We shall investigate this correspondence.

Assume the order of $\hat{\Delta}$ is prime to p. Let $\theta \in \hat{\Delta}$ and let

$$\varepsilon_\theta = \frac{1}{|\Delta|} \sum_{\alpha \in \Delta} \theta(\alpha)\alpha^{-1}$$

be the idempotent. Henceforth, we assume $\mathcal{O}$ contains the values of all such θ, so $\varepsilon_\theta \in \mathcal{O}[\Delta]$. We have

$$\mathcal{O}[\Delta] \xrightarrow{\sim} \bigoplus_\theta \mathcal{O}\varepsilon_\theta \xrightarrow{\sim} \bigoplus_\theta \mathcal{O}$$

$$\alpha \mapsto (\ldots, \theta(\alpha), \ldots).$$

Therefore

$$\mathcal{O}[\Delta][[T]] \xrightarrow{\sim} \bigoplus_\theta \mathcal{O}[[T]]$$

$$\sum_\theta f_\theta(T)\varepsilon_\theta \mapsto (\ldots, f_\theta(T), \ldots).$$

Consequently,

$\mathcal{O}$-valued measures on $\Delta \times \Gamma \leftrightarrow \bigoplus_{\theta \in \hat{\Delta}} \mathcal{O}[[T]] = |\Delta|$-tuples of power series.

Examples. (1) Let $\Delta = 1$ and let $\gamma \in \Gamma$. Then $\gamma \in \mathcal{O}[[\Gamma]]$. The corresponding distribution is the delta distribution, the measure is δ_γ. If $\gamma = \gamma_0^s$ with $s \in \mathbb{Z}_p$, then the power series is

$$(1 + T)^s = \sum_{j=0}^{\infty} \binom{s}{j} T^j \in \mathbb{Z}_p[[T]].$$

(2) Let $\Delta = (\mathbb{Z}/dp\,\mathbb{Z})^\times$ with $(d, p) = 1$, and

$$\Gamma_n = (1 + p\mathbb{Z}_p)/(1 + p^{n+1}\mathbb{Z}_p)$$

(assume $p \neq 2$; otherwise the theory needs a slight modification). Then

$$\Delta \times \Gamma_n \simeq (\mathbb{Z}/dp^{n+1}\mathbb{Z})^\times,$$

which we identify with $\mathrm{Gal}(\mathbb{Q}(\zeta_{dp^{n+1}})/\mathbb{Q})$. Let $q_0 = dp$, so $\gamma_0 = \sigma_{1+q_0}$ generates $\Gamma = \varprojlim \Gamma_n$. Let $c = 1 + q_0$. Consider the measure E_c of Theorem 12.2. The corresponding element in $\mathcal{O}[[\Delta \times \Gamma]]$ is

$$\lim \sum_{\substack{a=0\\(a,dp)=1}}^{dp^{n+1}-1} \left(\frac{a}{dp^{n+1}} - c\left\{\frac{c^{-1}a}{dp^{n+1}}\right\} + \frac{c-1}{2}\right)\sigma_a$$

$$= \lim(1 - c\sigma_c)\sum\left(\frac{a}{dp^{n+1}} - \frac{1}{2}\right)\sigma_a,$$

which is essentially the Stickelberger element. We map this to $\bigoplus \mathcal{O}[[T]]$. Let θ be even of conductor d or dp, so $\theta^* = \omega\theta^{-1}$ is odd. In the θ^*th component we have ($\sigma_c = \sigma_{1+q_0} = \gamma_0$)

$$\lim(1 - (1 + q_0)\gamma_0)\frac{1}{q_n}\sum a\,\omega\theta^{-1}(a)\gamma_n(a)$$

in the notation of Chapter 7. This is just $-\eta(\omega^2\theta^{-1})$ in that notation, except that $\gamma_n(a)$ replaces $\gamma_n(a)^{-1}$. Observe that γ_0^{-1} corresponds to $1/(1 + T)$, so when we change to power series we obtain

$$-g\left(\frac{1}{1+T} - 1, \omega^2\theta^{-1}\right) \stackrel{\text{def}}{=} g_{\theta^*}(T)$$

with g as in Chapter 7 (before Theorem 7.10). Note that

$$\begin{aligned} g_{\theta^*}((1 + q_0)^s - 1) &= -g((1 + q_0)^{-s} - 1, \omega^2\theta^{-1}) \\ &= -(1 - (1 + q_0)^{1+s})L_p(-s, \omega\theta^*). \end{aligned}$$

So the modified Bernoulli distribution E_c corresponds to the vector of power series which give the p-adic L-functions (one technicality: the above calculations assumed that the character θ had conductor exactly d or pd. The characters with smaller conductors yield slightly modified p-adic L-functions).

These last two examples are special cases of a general phenomenon. Fix a generator γ_0 of Γ. Let κ_0 correspond to γ_0 under the isomorphism $1 + p\mathbb{Z}_p \simeq \Gamma$ (again, assume $p \neq 2$ for simplicity), so

$$X = \Delta \times \Gamma \simeq \Delta \times (1 + p\mathbb{Z}_p)$$

$$(\alpha, \gamma_0^s) \mapsto (\alpha, \kappa_0^s).$$

For instance, in Example 2 above, $\gamma_0 = \sigma_{1+q_0}$ and $\kappa_0 = 1 + q_0$. Recall that a character ψ of the second kind is one of conductor p^n, $n \geq 2$, such that $\psi(a) = \psi(\langle a \rangle)$. Such a character may be regarded as a character on $1 + p\mathbb{Z}_p$.

Theorem 12.4. *Let $d\phi$ be an $\mathcal{O}$-valued measure on $\Delta \times \Gamma$ and let*

$$(\ldots, g_\theta(T), \ldots) \in \bigoplus_{\theta \in \hat{\Delta}} \mathcal{O}[[T]]$$

be the corresponding power series. Let $\theta \in \hat{\Delta}$ and let ψ be a character of the second kind. Then

$$\Gamma_p(\theta\psi\, d\phi)(s) = \int_{\Delta\times(1+p\mathbb{Z}_p)} \theta(a)\psi(a)\langle a\rangle^s\, d\phi = g_\theta(\psi(\kappa_0)\kappa_0^s - 1).$$

PROOF. First consider

$$(\ldots, a_{\theta'}(1+T)^n, \ldots) \in \bigoplus_{\theta'} \mathcal{O}[[T]].$$

By the above, this corresponds to

$$\sum_{\theta'} a_{\theta'}\varepsilon_{\theta'}\gamma_0^n = \frac{1}{|\Delta|}\sum_{\alpha\in\Delta}\sum_{\theta'} a_{\theta'}\theta'(\alpha^{-1})\alpha\gamma_0^n \in \mathcal{O}[[\Delta\times\Gamma]].$$

This yields a sum of delta distributions:

$$d\phi = \frac{1}{|\Delta|}\sum_{\alpha}\sum_{\theta'} a_{\theta'}\theta'(\alpha^{-1})\delta_{\alpha\gamma_0^n}.$$

On $1 + p\mathbb{Z}_p$, $\delta_{\alpha\gamma_0^n}$ is replaced by $\delta_{\alpha\kappa_0^n}$. We obtain

$$\int \theta(a)\psi(a)\langle a\rangle^s\, d\phi = \frac{1}{|\Delta|}\sum_{\alpha}\sum_{\theta'} a_{\theta'}\theta(\alpha)\theta'(\alpha^{-1})\psi(\kappa_0)^n\kappa_0^{ns}$$
$$= a_\theta(\psi(\kappa_0)\kappa_0^s)^n = a_\theta(1+T)^n \quad \text{at} \quad T = \psi(\kappa_0)\kappa_0^s - 1$$

(by orthogonality of characters, the sum over α vanishes for $\theta \neq \theta'$). By linearity, the theorem is true for polynomials. Since the polynomials are dense in $\mathcal{O}[[T]]$, we need a continuity statement. For any fixed $s \in \mathbb{Z}_p$, the function $f(a) = \theta(a)\psi(a)\langle a\rangle^s$ is continuous on X. Let $\varepsilon > 0$, There exists a step function $S(a)$ such that

$$|f(a) - S(a)| < \varepsilon \quad \text{for all } a \in X.$$

Suppose we are given a vector

$$(\ldots, g_\theta(T), \ldots) \in \bigoplus_{\theta} \mathcal{O}[[T]].$$

Recall that integration of step functions was accomplished by evaluation at sufficiently large finite levels. Let N be large and let

$$g_\theta(T) = P_N(T)q_N^\theta(T) + r_N^\theta(T),$$

where $P_N(T) = (1+T)^{p^N} - 1$ and $\deg r_N^\theta < p^N$ (Proposition 7.2). If $d\phi$ corresponds to g and $d\phi_N$ corresponds to $r_N = (\ldots, r_N^\theta, \ldots)$, then

$$\int_X S(a)\, d\phi = \int_X S(a)\, d\phi_N \quad \text{for large } N.$$

Therefore

$$\left|\int_X f(a)\, d\phi - \int_X f(a)\, d\phi_N\right| \leq \text{Max}\left\{\left|\int_X (f-S)\, d\phi\right|, \left|\int_X (S-f)\, d\phi_N\right|\right\} < \varepsilon,$$

since $|f - S| < \varepsilon$ and ϕ and ϕ_N are $\mathcal{O}$-valued. But $d\phi_N$ corresponds to a polynomial, for which the theorem is true. Also

$$\begin{aligned}|g_\theta(\psi(\kappa_0)\kappa_0^s - 1) &- r_N^\theta(\psi(\kappa_0)\kappa_0^s - 1)|\\ &\le |P_N(\psi(\kappa_0)\kappa_0^s - 1)| = |\psi(\kappa_0)^{p^N}\kappa_0^{p^N s} - 1)| < \varepsilon\end{aligned}$$

for large N (note $\psi(\kappa_0)$ is a p-power root of 1). Therefore

$$\left|\int_X f\, d\phi - g_\theta(\psi(\kappa_0)\kappa_0^s - 1)\right| < \varepsilon.$$

Since ε was arbitrary, the proof is complete. □

Corollary 12.5. *Let ϕ be a measure. Then $(\Gamma_p\phi)(s)$ is an analytic function of s.*

Proof. Let $\theta = \psi = 1$. Clearly any function of the form $g(\kappa_0^s - 1)$ is analytic.

Theorem 12.4 gives us something stronger than analyticity. Functions of the form

$$f(s) = g(\kappa^s - 1)$$

with $g(T) \in \mathcal{O}[[T]]$ and $\kappa \in 1 + p\mathbb{Z}_p$ ($1 + 4\mathbb{Z}_2$ if $p = 2$) are called *Iwasawa functions*. They satisfy

$$f(s) \equiv f(0) \bmod p\mathcal{O}$$

for all $s \in \mathbb{Z}_p$. This was the basis for Exercises 7.5–7.7. Not all analytic functions have this property, for example $f(s) = s$.

Corollary 12.6. *If $\int_{\Delta\times(1+p\mathbb{Z}_p)}\theta\psi\, d\phi = 0$ for all $\theta \in \hat{\Delta}$ and all ψ of the second kind, then $\phi = 0$. (In other words, a measure is determined by its values on characters of finite order. Note that $\theta(a)\psi(a)\langle a\rangle^s$ is a character of infinite order if $s \neq 0$).*

Proof. Let g_θ be one of the corresponding power series. Then

$$g_\theta(\psi(\kappa_0) - 1) = 0 \quad \text{for all } \psi,$$

hence

$$g_\theta(\zeta_{p^n} - 1) = 0 \quad \text{for all } n.$$

By the p-adic Weierstrass Preparation Theorem (see Corollary 7.4), a nonzero power series in $\mathcal{O}[[T]]$ has only finitely many zeros. Therefore $g_\theta = 0$ for all θ, so $\phi = 0$, as desired. □

For $f(T) \in \mathcal{O}[[T]]$, let

$$Df(T) = (1 + T)f'(T).$$

Observe that when $f(T) = (1 + T)^n$, $D^k f(0) = n^k$, which is a continuous p-adic function of k, if $p \nmid n$ and if we restrict k to a fixed congruence class mod $p - 1$. The next results will show that this holds more generally.

We assume $\Delta = 1$. Then

$$X = 1 + p\mathbb{Z}_p.$$

Let

$$\tilde{X} = \mathbb{Z}_p.$$

There is an isomorphism

$$\rho \colon X \xrightarrow{\sim} \tilde{X}$$

$$x \mapsto \frac{\log_p x}{\log_p \kappa_0},$$

Alternatively,

$$\kappa_0^y \mapsto y$$

If $d\phi$ is a measure on X, define the measure $d\tilde{\phi}$ on $\tilde{X}$ by

$$\int_{y \in \tilde{X}} f(y)\, d\tilde{\phi} = \int_{x \in X} f(\rho(x))\, d\phi$$

(see Example 4 at the beginning of this section).

Suppose $g(T) = \sum a_n(1 + T)^n$ is a polynomial. Then the corresponding measure $d\phi$ is a sum of delta measures

$$d\phi = \sum a_n \delta_{\kappa_0^n} \quad (\text{on } 1 + p\mathbb{Z}_p)$$

and

$$d\tilde{\phi} = \sum a_n \delta_n \quad (\text{on } \mathbb{Z}_p).$$

Proposition 12.7. *Let $g \in \mathcal{O}[[T]]$ and let $d\tilde{\phi}_g$ be the corresponding measure on $\tilde{X} = \mathbb{Z}_p$. For $k \geq 0$,*

$$(D^k g)(0) = \int_{y \in \tilde{X}} y^k\, d\tilde{\phi}_g.$$

Proof. First let $g = (1 + T)^n$. As mentioned above, the left-hand side is n^k. The measure $d\tilde{\phi}$ is the delta measure δ_n, so

$$\int y^k\, d\tilde{\phi} = n^k.$$

By linearity, the result holds for polynomials.

Let $g(T) \in \mathcal{O}[[T]]$ be arbitrary. Let $\varepsilon > 0$ and choose N so that $p^{-N} < \varepsilon$. As in the proof of Theorem 12.4,

$$g(T) = P_N(T)q_N(T) + r_N(T).$$

Therefore

$$D^k g(T) = a_0(T)P_N(T) + \cdots + a_k(T)P_N^{(k)}(T) + D^k r_N(T),$$

where $a_i(T) \in \mathcal{O}[[T]]$. But

$$P_N(0) = 0 \quad \text{and} \quad P_N^{(i)}(0) \equiv 0 \bmod p^N.$$

Therefore

$$|D^k g(0) - D^k r_N(0)| < \varepsilon.$$

As in the proof of Theorem 12.4, we may approximate $\rho(x)^k = (\log x/\log \kappa_0)^k$ on X by a step function $S(x)$, say within ε. Then

$$\left|\int_{\tilde{X}} y^k \, d\phi - \int_{\tilde{X}} y^k \, d\tilde{\phi}_{r_N}\right| = \left|\int_X \rho(x)^k \, d\phi - \int_X \rho(x)^k \, d\phi_{r_N}\right|$$

$$\leq \operatorname{Max}\left\{\left|\int_X (\rho(x)^k - S(x)) \, d\phi\right|,\right.$$

$$\left.\left|\int_X S(x) \, d\phi - \int_X S(x) \, d\phi_{r_N}\right|, \left|\int_X (S(x) - \rho(x)^k) \, d\phi_{r_N}\right|\right\}.$$

For large N, the second expression vanishes (this would not necessarily have happened if we worked on $\tilde{X}$ with $d\tilde{\phi}$ and $d\phi_{r_N}$ since the latter is not necessarily a finite sum of delta distributions; see Exercise 12.2). The first and third expressions are less than ε. Since we know the theorem is true for the polynomial r_N, we obtain

$$\left|\int_{\tilde{X}} y^k \, d\tilde{\phi} - D^k g(0)\right| < \varepsilon.$$

This completes the proof. □

To match the set-up of Theorem 12.4, we need an integral over $\mathbb{Z}_p^\times$ instead of $\mathbb{Z}_p$. To obtain this we do the following. Let $g(T) \in \mathcal{O}[[T]]$. Define

$$Ug(T) = g(T) - \frac{1}{p} \sum_{\zeta^p = 1} g(\zeta(1 + T) - 1).$$

One easily sees that

$$U \sum_{n=0}^{N} a_n(1 + T)^n = \sum_{\substack{n=0 \\ p \nmid n}}^{N} a_n(1 + T)^n.$$

Proposition 12.8. *Let $g \in \mathcal{O}[[T]]$ and let $d\phi_g$ and $d\tilde{\phi}_g$ be the corresponding measures on $X = 1 + p\mathbb{Z}_p$ and $\tilde{X} = \mathbb{Z}_p$. Let $\chi_{\tilde{X}^\times}(y)$ be the characteristic function of $\tilde{X}^\times = \mathbb{Z}_p^\times \subset \tilde{X}$. Then*

$$d\tilde{\phi}_{Ug} = \chi_{\tilde{X}^\times} \, d\tilde{\phi}_g,$$

so

$$(D^k Ug)(0) = \int_{y \in \mathbb{Z}_p^\times} y^k \, d\tilde{\phi}_g.$$

Proof. By Proposition 12.7, it suffices to prove the first equality. As usual, let $N \geq 1$ be large and write

$$g(T) = P_N(T)q_N(T) + r_N(T).$$

Then

$$Ug = U(P_N q_N) + Ur_N.$$

But

$$P_N(\zeta(1 + T) - 1) = P_N(T), \qquad N \geq 1,$$

So

$$Ug = P_N U q_N + Ur_N.$$

Let

$$r_N(T) = \sum_n a_n(1 + T)^n,$$

hence

$$Ur_N(T) = \sum_{p \nmid n} a_n(1 + T)^n.$$

On $\tilde{X}$, r_N corresponds to the measure

$$\sum_n a_n \delta_n$$

and Ur_N corresponds to

$$\sum_{p \nmid n} a_n \delta_n = \chi_{\tilde{X}^\times} \sum_n a_n \delta_n.$$

The same argument as was used at the end of the proof of Proposition 12.7, with y^k replaced by $f\chi_{\tilde{X}^\times}$ for any continuous function f on $\tilde{X}$, shows that

$$\int_{\tilde{X}} f \, d\tilde{\phi}_{Ur_N} = \int_{\tilde{X}} f\chi_{\tilde{X}^\times} \, d\tilde{\phi}_{r_N} \to \int_{\tilde{X}} f\chi_{\tilde{X}^\times} \, d\tilde{\phi}_g \quad \text{as } N \to \infty,$$

and since $Ug \equiv Ur_N \bmod P_N$, we similarly have

$$\int_{\tilde{X}} f \, d\tilde{\phi}_{Ur_N} \to \int_{\tilde{X}} f \, d\tilde{\phi}_{Ug}.$$

Therefore

$$d\tilde{\phi}_{Ug} = \chi_{\tilde{X}^\times} \, d\tilde{\phi}_g.$$

This completes the proof. □

Corollary 12.9. *Let $g \in \mathcal{O}[[T]]$. Fix a congruence class α mod $p - 1$. Then there exists $h(T) \in \mathcal{O}[[T]]$ such that*

$$(D^k Ug)(0) = h(\kappa_0^k - 1) \quad \textit{for } k \equiv \alpha \bmod p - 1, k \geq 0.$$

PROOF. Decompose

$$\tilde{X}^{\times} = (\mathbb{Z}/p\mathbb{Z})^{\times} \times (1 + p\mathbb{Z}_p).$$

Then

$$\begin{aligned}(D^k U g)(0) &= \int_{\tilde{X}^{\times}} \omega^{\alpha}(y)\langle y\rangle^k \, d\tilde{\phi}_g \\ &= \Gamma_p(\omega^{\alpha} \, d\tilde{\phi}_g)(k) \\ &= h(\kappa_0^k - 1)\end{aligned}$$

for some $h \in \mathcal{O}[[T]]$, by Theorem 12.4. □

We give an application. Let $c \in \mathbb{Z}$, $(c, p) = 1$, and let

$$g(T) = \frac{1}{(1+T)-1} - \frac{c}{(1+T)^c - 1}.$$

Since

$$\frac{c}{(1+T)^c - 1} = \frac{1}{T\left(1 + \frac{1}{c}\binom{c}{2}T + \cdots\right)} = \frac{1}{T} + \cdots,$$

we have

$$g(T) \in \mathbb{Z}_p[[T]].$$

Using the relation

$$\frac{1}{Y^p - 1} = \frac{1}{p} \sum_{\zeta^p = 1} \frac{1}{\zeta Y - 1},$$

we easily find that

$$Ug(T) = g(T) - g((1+T)^p - 1).$$

Observe that

$$Dg((1+T)^p - 1) = p(1+T)^p g'((1+T)^p - 1),$$

which is just p times Dg, with $1 + T$ replaced by $(1 + T)^p$. It follows by induction that

$$(D^k U g)(0) = (1 - p^k)(D^k g)(0).$$

To calculate $D^k g(0)$ we change variables. Let

$$T = e^Z - 1 = Z + \tfrac{1}{2}Z^2 + \tfrac{1}{6}Z^3 + \cdots \in \mathbb{Q}_p[[Z]].$$

Let

$$f(Z) = g(e^Z - 1) \in \mathbb{Q}_p[[Z]].$$

Then

$$\frac{d}{dZ} f(Z) = e^Z g'(e^Z - 1) = (1 + T)g'(T) = Dg(T).$$

Therefore,

$$\left(\frac{d}{dZ}\right)^k f(0) = D^k g(0).$$

But

$$\begin{aligned} g(e^Z - 1) &= \frac{1}{e^Z - 1} - \frac{c}{e^{cZ} - 1} \\ &= \frac{1}{Z} \sum_{n=0}^{\infty} (1 - c^n) B_n \frac{Z^n}{n!} \\ &= \sum_{n=0}^{\infty} (1 - c^{n+1}) \frac{B_{n+1}}{n+1} \frac{Z^n}{n!} \end{aligned}$$

Therefore

$$D^k g(0) = \left(\frac{d}{dZ}\right)^k f(0) = (1 - c^{k+1}) \frac{B_{k+1}}{k+1},$$

so

$$\begin{aligned} (D^k Ug)(0) &= (1 - c^{k+1})(1 - p^k) \frac{B_{k+1}}{k+1} \\ &= -(1 - \omega^{k+1}(c)\langle c \rangle^{k+1}) L_p(-k, \omega^{k+1}). \end{aligned}$$

By Corollary 12.9, we find that for $k \equiv \alpha \pmod{p-1}$, this extends to an analytic function, in fact to an Iwasawa function.

The reader might find it interesting to start with Theorem 12.2 and deduce that $g(T)$ is the power series we should use to obtain the above.

The use of differentiation to obtain values of L-functions was also implicitly used in the proof of Theorem 5.18 (evaluation of $L_p(1, \omega^k)$). This technique was probably first used by Euler, later by Kummer, and more recently by Coates and Wiles.

§12.3 Universal Distributions

The main purpose of this section is to prove Bass' theorem on generators and relations for cyclotomic units. But to do so, we consider the general question of universal ordinary distributions (sometimes punctured, even, or odd) on

$\mathbb{Q}/\mathbb{Z}$. We restrict to the subset $(1/n)\mathbb{Z}/\mathbb{Z}$. Let A_n be the abelian group with generators

$$\left\{ g\left(\frac{a}{n}\right) \,\middle|\, \frac{a}{n} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} \right\}$$

and relations

$$g\left(\frac{a}{r}\right) = g\left(\frac{(n/r)a}{n}\right) = \sum_{k=0}^{(n/r)-1} g\left(\frac{a+rk}{n}\right), \quad \text{for } r \mid n.$$

Then A_n is called the *universal ordinary distribution* on $(1/n)\mathbb{Z}/\mathbb{Z}$. The map

$$g: \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to A_n$$

$$\frac{a}{n} \mapsto g\left(\frac{a}{n}\right)$$

defines an ordinary distribution on $(1/n)\mathbb{Z}/\mathbb{Z}$. If ϕ is another ordinary distribution on $(1/n)\mathbb{Z}/\mathbb{Z}$, then there is a map

$$A_n \to \text{group generated by } \left\{ \phi\left(\frac{a}{n}\right) \right\}$$

$$g\left(\frac{a}{n}\right) \mapsto \phi\left(\frac{a}{n}\right),$$

so A_n is universal in the sense of category theory. We shall show that A_n is a free abelian group of rank $\phi(n)$. We start with an upper bound.

Proposition 12.10. *There is a set of $\phi(n)$ elements which generates A_n.*

PROOF. Let $n = \prod p_i^{e_i}$. We may write, for any $a \in \mathbb{Z}$,

$$\frac{a}{n} \equiv \sum \frac{a_i}{p_i^{e_i}} \bmod \mathbb{Z},$$

with $0 \le a_i < p_i^{e_i}$. We first show that

$$B_n = \left\{ g\left(\frac{a}{n}\right) \,\middle|\, \text{for each } i, \text{ either } a_i = 0 \text{ or } (a_i, p_i) = 1 \right\}$$

generates A_n. This is not yet a minimal set of generators, but it gets things started. Note that if $a_i = 0$ then p_i does not appear in the denominator of a/n, while if $(a_i, p_i) = 1$ then the full power $p_i^{e_i}$ is in the denominator.

Consider an arbitrary a/n. If $a_i = 0$ for some i then by induction we may conclude that $g(a/n)$ is in the group generated by $B_{n/p_i^{e_i}} \subseteq B_n$ (This induction starts with the case $n = 1$, which is trivial). Therefore assume $a_i \ne 0$ for all i. Write $a = ct$ with $t \mid n$ and $(c, n) = 1$. This is possible since $a_i \ne 0$ implies $p_i^{e_i} \nmid a$, so t divides $\prod p_i^{e_i - 1}$, which divides n. If $t = 1$ then $a/n = c/n$ has denominator exactly n, so $(a_i, p_i) = 1$ for all i. Hence $g(a/n) \in B_n$ and we are done. Therefore assume $t > 1$. As mentioned above, t divides $\prod p_i^{e_i - 1}$, so $p_i | (n/t)$ for each i. By the distribution relation,

$$g\left(\frac{a}{n}\right) = g\left(\frac{ct}{n}\right) = \sum_{k=0}^{t-1} g\left(\frac{c + (n/t)k}{n}\right).$$

Since $(c, n) = 1$ and since $p_i | (n/t)$ for each i, we must have

$$\left(c + \left(\frac{n}{t}\right)k, n\right) = 1,$$

for all k. Therefore all fractions involved in the last sum have denominator exactly n, so $g(a/n)$ is in the group generated by B_n. Therefore B_n generates A_n.

But there are relations among the elements of B_n. Let

$$C_n = \left\{ g\left(\frac{a}{n}\right) \middle| \text{for each } i,\ a_i \neq 1 \text{ and either } a_i = 0 \text{ or } (a_i, p) = 1 \right\}.$$

We claim that C_n generates A_n. By induction, we may assume $C_{n/p_i^{e_i}}$ generates $A_{n/p_i^{e_i}}$ for each i. Note that $C_{n/p_i^{e_i}} \subseteq C_n$.

Let $g(a/n) \in B_n$. Suppose $b_1 = 1$. Let

$$y = \sum_{i \neq 1} \frac{a_i}{p_i^{e_i}}.$$

Then

$$\sum_{k=0}^{p_1^{e_1} - 1} g\left(y + \frac{k}{p_1^{e_1}}\right) = g(p_1^{e_1} y),$$

and

$$\sum_{k=0}^{p_1^{e_1 - 1} - 1} g\left(y + \frac{p_1 k}{p_1^{e_1}}\right) = g(p_1^{e_1 - 1} y).$$

Since $p_1^{e_1} y$ and $p_1^{e_1 - 1} y$ do not have p_1 in their denominators, $g(p_1^{e_1} y)$ and $g(p_1^{e_1 - 1} y)$ lie in $\langle C_{n/p_1^{e_1}} \rangle =$ the group generated by $C_{n/p_1^{e_1}}$. Subtraction yields

$$\sum_{\substack{k=0 \\ p_1 \nmid k}}^{p_1^{e_1} - 1} g\left(y + \frac{k}{p_1^{e_1}}\right) \in \langle C_{n/p_1^{e_1}} \rangle,$$

hence

$$g\left(y + \frac{1}{p_1^{e_1}}\right) \equiv - \sum_{\substack{p_1 \nmid k \\ k \neq 1}} g\left(y + \frac{k}{p_1^{e_1}}\right) \bmod \langle C_{n/p_1^{e_1}} \rangle.$$

Note that $a_1 = 1$ is changed to a sum with $a_1 = k \neq 1$ and $(a_1, p_1) = 1$, but y is left unchanged (this is important). Now consider

$$g\left(y + \frac{k}{p_1^{e_1}}\right) = g\left(\frac{k}{p_1^{e_1}} + \sum_{i \neq 1} \frac{a_i}{p_i^{e_i}}\right).$$

If another $a_i = 1$ then we may perform the above operations again. Note that a_j for $j \neq i$ is left unchanged (in particular no such a_j is changed to 1). Continuing, we eventually get $a_i \neq 1$ for all i, and also $(a_i, p) = 1$ or $a_i = 0$. Therefore all $g(a/n)$ in B_n are expressible in terms of C_n, so C_n generates A_n. Since C_n contains

$$\prod \phi(p_i^{e_i}) = \phi(n)$$

elements, the proof of Proposition 12.10 is complete. □

Proposition 12.11. *The universal punctured ordinary distribution A_n^0 on $(1/n)\mathbb{Z}/\mathbb{Z}$ requires at most $\phi(n) + \pi(n) - 1$ generators, where $\pi(n)$ equals the number of distinct prime factors of n.*

Proof. A_n^0 is generated by

$$\left\{ g\left(\frac{a}{n}\right) \middle| \frac{a}{n} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}, \frac{a}{n} \neq 0 \right\}$$

with relations

$$g\left(\frac{a}{r}\right) = \sum_{k=0}^{(n/r)-1} g\left(\frac{a+rk}{n}\right) \quad \text{whenever } r|n \quad \text{and} \quad \frac{a}{r} \neq 0.$$

So we have taken the distribution A_n and removed $g(0)$ and also eliminated the relations

$$g(0) = \sum_{(n/r)x \equiv 0(\mathbb{Z})} g(x) = g(0) + \sum_{\substack{(n/r)x \equiv 0 \\ x \neq 0}} g(x).$$

We see that whenever $g(0)$ appears in a relation for a nonpunctured distribution, it appears equally on both sides. So we really have the relations

$$\sum_{\substack{(n/r)x \equiv 0 \\ x \neq 0}} g(x) = 0, \qquad r|n.$$

We claim that such relations follow from those with n/r prime. Let $m = n/r$ and let $p|m$. Then

$$\begin{aligned} \sum_{\substack{mx \equiv 0 \\ x \neq 0}} g(x) &= \sum_{\substack{py \equiv 0 \\ y \neq 0}} \sum_{(m/p)x \equiv y} g(x) + \sum_{\substack{(m/p)x \equiv 0 \\ x \neq 0}} g(x) \\ &= \sum_{\substack{py \equiv 0 \\ y \neq 0}} g(y) + \sum_{\substack{(m/p)x \equiv 0 \\ x \neq 0}} g(x). \end{aligned}$$

Choose a prime dividing m/p and continue. Eventually $\sum_{mx \equiv 0, x \neq 0} g(x)$ is expressed as a sum of expressions of the form $\sum_{py \equiv 0, y \neq 0} g(y)$ with p prime. This proves the claim.

We now see that to obtain A_n from A_n^0 it suffices to add a generator $g(0)$ and add the relations

$$\sum_{\substack{py\equiv 0\\ y\neq 0}} g(y) = 0$$

for each $p|n$. Let

$$R = \left\{\sum_{a=1}^{p-1} g\left(\frac{a}{p}\right) \middle| p \text{ divides } n, p \text{ prime}\right\}.$$

We have just shown that we have a natural isomorphism

$$(A_n^0 \oplus \mathbb{Z}g(0)) \bmod\langle R\rangle \simeq A_n.$$

We already have the set of generators C_n for A_n. Let

$$D_n = C_n \cup R - \{g(0)\}.$$

Clearly D_n generates A_n^0. Since D_n has $\phi(n) + \pi(n) - 1$ elements, Proposition 12.11 is proved. □

To show that the sets of generators in Propositions 12.10 and 12.11 are minimal, we shall produce concrete examples of the desired ranks. By the *rank* of a distribution ϕ we mean the $\mathbb{Z}$-rank ($=$number of summands isomorphic to $\mathbb{Z}$, in the usual decomposition) of the abelian group generated by $\{\phi(a/n)|0 \le a < n\}$. (Omit $\phi(0)$ if ϕ is punctured).

From now on, we assume $n > 2$ ($n = 1$ and $n = 2$ are trivial, of course). Assume first that $n \not\equiv 2 \bmod 4$. Let ζ_n be a primitive nth root of unity. Consider the punctured even distribution defined by

$$h\left(\frac{a}{n}\right) = (\ldots, \log|\zeta_n^{ar} - 1|, \ldots) \in \mathbb{C}^{\phi(n)}$$

where r runs through the integers with $(r, n) = 1$, $1 \le r \le n$ (we could have used half of these r's). Various combinations, call them v_i, of the vectors $h(a/n)$ give the logarithms of the $\frac{1}{2}\phi(n) - 1$ independent units of Theorem 8.3 (in the first component; the other components are the Galois conjugates). We may also take $a/n = 1/p$ for p dividing n and obtain a generator for the ideal of $\mathbb{Q}(\zeta_p)$ lying above p. We claim that the group generated by the $h(a/n)$ has rank at least $\frac{1}{2}\phi(n) + \pi(n) - 1$. In fact the vectors $h(1/p)$ for $p|n$ and the v_i are independent over $\mathbb{Z}$: Suppose

$$\sum a_p h\left(\frac{1}{p}\right) + \sum a_i v_i = 0.$$

Add the components of the vectors. For each v_i, we get the logarithm of the norm of a unit, hence 0. For $h(1/p)$ we get the logarithm of a nontrivial power of p. But the logarithms of primes are linearly independent over $\mathbb{Z}$, so $a_p = 0$ for all p. Since the v_i's are independent over $\mathbb{Z}$, $a_i = 0$ for all i. This proves the claim.

If $n \equiv 2 \bmod 4$, then we may use the same distribution $h(a/n)$ defined above. We know that the group generated by $\{h(2a/n)\}$ has rank at least

$$\tfrac{1}{2}\phi\left(\frac{n}{2}\right) + \pi\left(\frac{n}{2}\right) - 1 = \tfrac{1}{2}\phi(n) + \pi(n) - 2.$$

But

$$h(\tfrac{1}{2}) = (\log 2, \ldots, \log 2),$$

which is independent of the vectors used to get this estimate on the rank. Therefore the rank is at least $\frac{1}{2}\phi(n) + \pi(n) - 1$.

Therefore, for all $n(> 1)$, we have a punctured even distribution of rank at least $\frac{1}{2}\phi(n) + \pi(n) - 1$.

We now produce an odd distribution of rank $\frac{1}{2}\phi(n)$. As in the case just completed, the construction will depend on the fact that $L(1, \chi) \neq 0$; but this time it will be in the form $B_{1,\chi} \neq 0$ for odd χ. We shall be using the first Bernoulli distribution, but our preliminary calculations will be valid more generally.

Let h be an ordinary distribution on $(1/n)\mathbb{Z}/\mathbb{Z}$, and let $\chi \neq 1$ be a Dirichlet character of conductor f_χ. The proofs of the following lemmas are essentially the same as the arguments given for Lemmas 8.4–8.7. Simply replace $\log|1 - \zeta_n^a|$ by $h(a/n)$. The fact that $\zeta_n^{m'} = \zeta_m$ when $n = mm'$ corresponds to the fact that h is ordinary. We also use the fact that h is periodic mod 1. (Of course, assuming Bass' theorem, essentially any relation satisfied by $\log|1 - \zeta_n^a|$ is also satisfied by $h(a/n)$, with the possible exception of evenness).

Lemma 12.12. *Suppose $m|n$. If $f_\chi \nmid (n/m)$ then*

$$\sum_{\substack{a=1\\(a,n)=1}}^{n} \chi(a)h\left(\frac{am}{n}\right) = 0 \qquad \square$$

Lemma 12.13. *Let $n = mm'$ with $(m, m') = 1$, and suppose $f_\chi|m$. Then*

$$\sum_{\substack{a=1\\(a,n)=1}}^{n} \chi(a)h\left(\frac{am'}{n}\right) = \phi(m') \sum_{\substack{b=1\\(b,m)=1}}^{m} \chi(b)h\left(\frac{b}{m}\right). \qquad \square$$

Lemma 12.14. *Suppose F, g, t are positive integers with $f_\chi|F$, $g|F$, and $Ft|n$. Then*

$$\sum_{\substack{a=1\\(a,g)=1}}^{Ft} \chi(a)h\left(\frac{a}{Ft}\right) = \sum_{\substack{b=1\\(b,g)=1}}^{F} \chi(b)h\left(\frac{b}{F}\right)$$

(we require $Ft|n$ since h is not defined for larger denominators). □

Lemma 12.15. *Assume $f_\chi | m$ and $m | n$. Then*

$$\sum_{\substack{b=1\\(b,m)=1}}^{m} \chi(b)h\left(\frac{b}{m}\right) = \left(\prod_{p|m}(1-\chi(p))\right)\sum_{b=1}^{m}\chi(b)h\left(\frac{b}{m}\right).$$ □

Lemma 12.16. *Let $n = mm'$ with $f_\chi | m$. Then*

$$\sum_{\substack{a=1\\(a,n)=1}}^{n} \chi(a)h\left(\frac{am'}{n}\right) = \phi(m')\left(\prod_{p|m}(1-\chi(p))\right)\sum_{a=1}^{f_\chi}\chi(a)h\left(\frac{a}{f_\chi}\right).$$

PROOF. See the calculations following the proof of Lemma 8.7. □

Proposition 12.17. *Let $n = \prod_{i=1}^{s} p_i^{e_i}$. Let I run through all subsets of $\{1, \ldots, s\}$, except $\{1, \ldots, s\}$, and let $n_I = \prod_{i \in I} p_i^{e_i}$. Then*

$$\sum_I \sum_{\substack{a=1\\(a,n)=1}}^{n} \chi(a)h\left(\frac{an_I}{n}\right) = \left(\prod_{p_i \nmid f_\chi}(\phi(p_i^{e_i}) + 1 - \chi(p_i))\right)\sum_{a=1}^{f_\chi}\chi(a)h\left(\frac{a}{f_\chi}\right).$$

PROOF. See the end of the proof of Theorem 8.3. This is where we need $\chi \neq 1$ (if $\chi = 1$, include $I = \{1, \ldots, s\}$ and the result holds). □

As in the case of even distributions, it is this last formula which will prove useful.

Consider

$$G = (\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

(we allow $n \equiv 2 \bmod 4$). Let σ_a be the automorphism corresponding to a mod n. Let $b(a/n)$ be a complex-valued ordinary distribution on $(1/n)\mathbb{Z}/\mathbb{Z}$. Define

$$H\left(\frac{c}{n}\right) = \sum_{\substack{a=1\\(a,n)=1}}^{n} b\left(\frac{ac}{n}\right)\sigma_a^{-1} \in \mathbb{C}[G].$$

We claim that H is an ordinary distribution on $(1/n)\mathbb{Z}/\mathbb{Z}$. It suffices to prove this for $b(ac/n)$ for each a. Let $r | n$. Since $(a, n) = 1$,

$$\left\{\frac{rj}{n} \bmod 1 \,\middle|\, 0 \le j < \frac{n}{r}\right\} = \left\{\frac{ark}{n} \bmod 1 \,\middle|\, 0 \le k < \frac{n}{r}\right\}.$$

Therefore,

$$\sum_{k=0}^{(n/r)-1} b\left(\frac{a(c+rk)}{n}\right) = \sum_{j=0}^{(n/r)-1} b\left(\frac{ac+rj}{n}\right)$$
$$= b\left(\frac{ac}{r}\right), \quad \text{as desired.}$$

This proves the claim.

Let $\chi \in \hat{G}$ be a Dirichlet character mod n of conductor f_χ. Let

$$\varepsilon_\chi = \frac{1}{\phi(n)} \sum_{(a,n)=1} \chi(a)\sigma_a^{-1}$$

be the corresponding idempotent. Since $\varepsilon_\chi \sigma_a^{-1} = \bar{\chi}(a)\varepsilon_\chi$,

$$H_\chi\left(\frac{c}{n}\right) \overset{\text{def}}{=} \varepsilon_\chi H\left(\frac{c}{n}\right) = \frac{1}{\phi(n)} \sum_{\substack{a=1\\(a,n)=1}}^{n} \bar{\chi}(a) b\left(\frac{ac}{n}\right)\varepsilon_\chi.$$

Of course, H_χ is a distribution. Let H be the abelian group generated by $\{H(c/n) | 0 \le c < n\}$ and let $H_{\mathbb{C}}$ be the $\mathbb{C}$-subspace of $\mathbb{C}[G]$ spanned by H. Then

$$\operatorname{rank} H \geq \dim H_{\mathbb{C}}$$

(we have an inequality since elements which are independent over $\mathbb{Z}$ could become dependent over $\mathbb{C}$ (e.g., 1, $\sqrt{2}$)). Since

$$\sigma_a H\left(\frac{c}{n}\right) = H\left(\frac{ac}{n}\right),$$

$H_{\mathbb{C}}$ is stable under G, so

$$H_{\mathbb{C}} = \bigoplus_\chi \varepsilon_\chi H_{\mathbb{C}},$$

hence

$$\dim H_{\mathbb{C}} = \sum_\chi \dim \varepsilon_\chi H_{\mathbb{C}}.$$

Observe that $H_\chi(c/n) \in \varepsilon_\chi H_{\mathbb{C}}$ for each c.

We now choose the distribution b. Let $B_1(X) = X - \frac{1}{2}$ be the first Bernoulli polynomial, so

$$B\left(\frac{c}{n}\right) = B_1\left(\left\{\frac{c}{n}\right\}\right) = \left\{\frac{c}{n}\right\} - \frac{1}{2}, \qquad c \neq 0;\ B(0) = 0,$$

is the corresponding distribution. Let $n = \prod p_i^{e_i}$ and I be as in Proposition 12.17. Then we let

$$b\left(\frac{c}{n}\right) = \sum_I B\left(\frac{cn_I}{n}\right).$$

Clearly $b(c/n)$ is odd, hence so is $H(c/n)$. By Proposition 12.17,

$$\begin{aligned} H_\chi\left(\frac{1}{n}\right) &= \frac{1}{\phi(n)} \sum_{(a,n)=1} \bar{\chi}(a) b\left(\frac{a}{n}\right)\varepsilon_\chi \\ &= \frac{1}{\phi(n)}\left(\prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \bar{\chi}(p_i))\right) \sum_{a=1}^{f_\chi} \bar{\chi}(a) B\left(\frac{a}{f_\chi}\right)\varepsilon_\chi. \end{aligned}$$

If χ is even, the sum vanishes. If χ is odd,

$$\sum \bar{\chi}(a)B\left(\left\{\frac{a}{f_\chi}\right\}\right) = B_{1,\bar{\chi}} \neq 0.$$

Since the product over p_i does not vanish (each factor has positive real part),

$$0 \neq H_\chi\left(\frac{1}{n}\right) \in \varepsilon_\chi H_{\mathbb{C}},$$

so $\varepsilon_x H_{\mathbb{C}}$ is non-trivial. Since there are $\frac{1}{2}\phi(n)$ odd characters,

$$\text{rank } H \geq \dim H_{\mathbb{C}} \geq \tfrac{1}{2}\phi(n).$$

We now have an odd distribution of rank at least $\frac{1}{2}\phi(n)$. Note that $H(0) = 0$, which does not affect the rank. If we ignore $H(0)$ and some of the relations (e.g., $\sum_{py \equiv 0} H(y) = 0$), then we may consider H as a punctured odd distribution, which still has the same rank.

Therefore we have a punctured even distribution of rank at least $\frac{1}{2}\phi(n) + \pi(n) - 1$ and an odd one of rank at least $\frac{1}{2}\phi(n)$. We want to put them together. Suppose h^+ and h^- are any two punctured distributions, with h^+ even and h^- odd. Let $H^\pm$ be the groups generated by $h^\pm$ and define

$$h\left(\frac{a}{n}\right) = \left(h^+\left(\frac{a}{n}\right), h^-\left(\frac{a}{n}\right)\right) \in H^+ \oplus H^-.$$

Let $H \subseteq H^+ \oplus H^-$ be the group generated by h. Then

$$h\left(\frac{a}{n}\right) + h\left(-\frac{a}{n}\right) = \left(2h^+\left(\frac{a}{n}\right), 0\right) \in H$$

and

$$h\left(\frac{a}{n}\right) - h\left(-\frac{a}{n}\right) = \left(0, 2h^-\left(\frac{a}{n}\right)\right) \in H.$$

Consequently

$$2H^+ \oplus 2H^- \subseteq H \subseteq H^+ \oplus H^-,$$

so

$$\text{rank } h = \text{rank } h^+ + \text{rank } h^-.$$

Using the distributions obtained above, we obtain a punctured distribution of rank at least $\phi(n) + \pi(n) - 1$. Since the universal punctured ordinary distribution A_n^0 is generated by $\phi(n) + \pi(n) - 1$ elements (Proposition 12.11), and maps surjectively onto the group generated by the values of this distribution A_n^0 is generated by $\phi(n) + \pi(n) - 1$ elements (Proposition If we had an even punctured distribution of rank greater than $\frac{1}{2}\phi(n) + \pi(n) - 1$, or an odd one of rank greater than $\frac{1}{2}\phi(n)$, we could obtain a punctured distribution of too large a rank. Therefore the universal punctured even distribution $(A_n^0)^+$ has rank $\frac{1}{2}\phi(n) + \pi(n) - 1$, and the odd distribution $(A_n^0)^-$ has rank $\frac{1}{2}\phi(n)$. However, we cannot conclude that $(A_n^0)^\pm$ are free abelian. We know from the above that

$$2(A_n^0)^+ + 2(A_n^0)^- \subseteq A_n^0,$$

so $2(A_n^0)^\pm$ have no torsion. But there is the possibility of 2-torsion. In fact,

$$(A_n^0)^+ \simeq \mathbb{Z}^{(1/2)\phi(n)+\pi(n)-1} \oplus (\mathbb{Z}/2\mathbb{Z})^{2^{r-1}-r},$$

and

$$(A_n^0)^- \simeq \mathbb{Z}^{(1/2)\phi(n)} \oplus (\mathbb{Z}/2\mathbb{Z})^{2^{r-1}-1}$$

where $r = \pi(n)$ if $n \not\equiv 2 \bmod 4$, $r = \pi(n/2)$ if $n \equiv 2 \pmod 4$. (See C.-G. Schmidt [4], K. Yamamoto [2]).

We now consider nonpunctured distributions. A_n is a quotient of $A_n^0 \oplus \mathbb{Z}g(0)$ by a subgroup $\langle R \rangle$ of rank at most $\pi(n)$, hence

$$A_n \simeq \mathbb{Z}^e \oplus \text{torsion}$$

with $e \geq \phi(n)$. By Proposition 12.10,

$$A_n \simeq \mathbb{Z}^{\phi(n)}.$$

Since $(A_n^0)^+ \oplus \mathbb{Z}g(0)$ modulo $\langle R \rangle$ yields an even distribution,

$$\text{rank } A_n^+ \geq \tfrac{1}{2}\phi(n).$$

Also, we already have an odd distribution (constructed via $B_{1,\bar{\chi}} \neq 0$) of rank at least $\frac{1}{2}\phi(n)$. As in the case of punctured distributions, we must have

$$A_n^\pm \simeq \mathbb{Z}^{(1/2)\phi(n)} \oplus (\mathbb{Z}/2\mathbb{Z})^{C^\pm},$$

for some integers $C^\pm$. In this case it is easy to see that the 2-torsion actually occurs (Exercise 12.4).

We summarize what we have proved:

Theorem 12.18. *Let $n > 2$. For some integers a, b, c, d, we have*

Universal punctured $= A_n^0 \simeq \mathbb{Z}^{\phi(n)+\pi(n)-1}$,

Universal even punctured $= (A_n^0)^+ \simeq \mathbb{Z}^{(1/2)\phi(n)+\pi(n)-1} \oplus (\mathbb{Z}/2\mathbb{Z})^a$,

Universal odd punctured $= (A_n^0)^- \simeq \mathbb{Z}^{(1/2)\phi(n)} \oplus (\mathbb{Z}/2\mathbb{Z})^b$,

Universal $= A_n \simeq \mathbb{Z}^{\phi(n)}$,

Universal even $= A_n^+ \simeq \mathbb{Z}^{(1/2)\phi(n)} \oplus (\mathbb{Z}/2\mathbb{Z})^c$,

Universal odd $= A_n^- \simeq \mathbb{Z}^{(1/2)\phi(n)} \oplus (\mathbb{Z}/2\mathbb{Z})^d$. □

The proof of Bass' theorem is now immediate. Since

$$(A_n^0)^+ \to \text{group generated by } \{\log|\zeta_n^a - 1|, 0 < a < n\}$$

is surjective, and the latter is free abelian of rank (at least, hence exactly) $\frac{1}{2}\phi(n) + \pi(n) - 1$, we must have

$$(A_n^0)^+/(\mathbb{Z}/2\mathbb{Z})^a \simeq \langle\{\log|\zeta_n^a - 1|\}\rangle.$$

This is Bass' theorem (8.9). □

Notes

For more on measures, see Koblitz [1], Mazur–Swinnerton-Dyer [1], and Lang [4], [5]. For the concept of pseudo-measures, which can handle denominators, see Serre [3].

For other versions of the Γ-transform, see Leopoldt [10], Iwasawa [23], and Lichtenbaum [4].

For more on Iwasawa functions, see Serre [2].

The theory of universal distributions was developed by Kubert-Lang. Theorem 12.18 was proved, in more generality, by Kubert. The fact that 2-torsion must be considered in Bass' theorem was first recognized by Ennola [1], [2].

Exercises

12.1. Give another proof of Corollary 12.6 by showing that the characters ψ of the second kind and the $\theta \in \hat{\Delta}$ span Step (X).

12.2. In the second section, we started with a power series $g \in \mathcal{O}[[T]]$, obtained a measure $d\phi_g$ on $1 + p\mathbb{Z}_p$ (assume $\Delta = 1$), then a measure $d\tilde{\phi}_g$ on $\mathbb{Z}_p$, which restricted to $d\tilde{\phi}_g$ on $(\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$. Therefore $d\tilde{\phi}_g$ corresponds to a vector of power series

$$(\ldots, \tilde{g}_{\omega^\alpha}(T), \ldots), \qquad 0 \leq \alpha \leq p - 2.$$

Show that if $g(T) = \sum_{n=0}^{N} a_n(1 + T)^n$ is a polynomial, then

$$\tilde{g}_{\omega^\alpha}(T) = \sum_{p \nmid n} a_n \omega^\alpha(n)(1 + T)^{(\log_p n/\log_p \kappa_0)}.$$

12.3. Let κ_0 be as in the chapter.

(a) Let $u \in 1 + p\mathbb{Z}_p$ (or $1 + 4\mathbb{Z}_2$). Show that there exists $h(T) \in \mathbb{Z}_p[[T]]$ such that $u^s = h(\kappa_0^s - 1)$.

(b) Suppose $h_n(\kappa_0^s - 1)$ is a Cauchy sequence (in the sup norm on continuous functions on $\mathbb{Z}_p$) of Iwasawa functions, with $h_n(T) \in \mathcal{O}[[T]]$. Show that there exists $h(T) \in \mathcal{O}[[T]]$ such that

$$\lim h_n(\kappa_0^s - 1) = h(\kappa_0^s - 1).$$

(*Hint*: let s be close to 0. Show successively that each coefficient converges mod p^n for all n).

(c) Show that the Iwasawa functions are the closure of the span of the functions of the form $f(s) = u^s$, with $u \in 1 + p\mathbb{Z}_p$.

12.4. (a) Let p be an odd prime and let A_p^+ be the universal even ordinary distribution on $(1/p)\mathbb{Z}/\mathbb{Z}$. Show that

$$\chi = \sum_{a=1}^{(p-1)/2} g\left(\frac{a}{p}\right) \neq 0 \quad \text{but } 2\chi = 0.$$

Therefore A_p^+ has 2-torsion. (This idea may be extended to arbitrary $n > 2$).

(b) Let A_n^- be the universal odd ordinary distribution on $(1/n)\mathbb{Z}/\mathbb{Z}$. Show that $g(0) \neq 0$ but $2g(0) = 0$, hence A_n^- has 2-torsion.

12.5. ([Ennola 2]) Let $n = 105$. Let

$$a_x = g\left(\frac{x}{105}\right) \in (A_{105}^0)^+.$$

(a) Show that all relations among the a_x are generated by the relations

$$\begin{aligned} a_x &= a_{-x} \\ a_{3x} &= a_x + a_{x+35} + a_{x+70} \\ a_{5x} &= a_x + a_{x+21} + \cdots + a_{x+84} \\ a_{7x} &= a_x + a_{x+15} + \cdots + a_{x+90}. \end{aligned}$$

(b) Show that in all such relations, the number of x with $x \not\equiv 0 \bmod 3$ is even (count both sides of the equation).

(c) Show that $r = 0$, where

$$r = a_1 + a_2 + a_{17} + a_{43} + a_{44} + a_{46} - a_3 + a_9 + a_{36} + a_{25} + a_{40} + a_{28},$$

is not a relation in $(A_{105}^0)^+$.

(d) Show that $2r = 0$ is a relation. This shows that 2-torsion must be considered in Bass' theorem.

Chapter 13

Iwasawa's Theory of $\mathbb{Z}_p$-extensions

The theory of $\mathbb{Z}_p$-extensions has turned out to be one of the most fruitful areas of research in number theory in recent years. The subject receives its motivation from the theory of curves over finite fields, which is known to have a strong analogy with the theory of number fields. In the case of curves, it is convenient to extend the field of constants to its algebraic closure, which amounts to adding on roots of unity. There is a natural generator of the Galois group, namely the Frobenius, and its action on various modules yields zeta functions and L-functions. In the number field case, it turns out to be too unwieldy, at least at present, to use all roots of unity. Instead, it is possible to obtain a satisfactory theory by just adjoining the p-power roots of unity for a fixed prime p. This yields a $\mathbb{Z}_p$-extension. The action of a generator of the Galois group on a certain module yields, at least conjecturally, the p-adic L-functions.

In the present chapter, we first prove some preliminary results on $\mathbb{Z}_p$-extensions. We then determine the structure of modules over the ring $\Lambda = \mathbb{Z}_p[[T]]$. As a result, we obtain the beautiful theorem of Iwasawa which describes the behavior of the p-part of the class number in a $\mathbb{Z}_p$-extension. We then discuss the Main Conjecture, relating certain Galois actions to p-adic L-functions. Finally, we use logarithmic derivatives to prove a result of Iwasawa, which could be considered as a local version of the Main Conjecture, which describes local units modulo cyclotomic units in terms of p-adic L-functions. Extensions of this theorem to elliptic curves have proved very useful in the work of Coates and Wiles on the conjecture of Birch and Swinnerton-Dyer.

In this chapter we use more class field theory than in previous chapters. A summary of the necessary facts is given in an appendix.

§13.1 Basic Facts

A $\mathbb{Z}_p$-extension of a number field K is an extension K_∞/K with $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, the additive group of p-adic integers. As Proposition 13.1 below shows, it is also possible to regard a $\mathbb{Z}_p$-extension as a sequence of fields

$$K = K_0 \subset K_1 \subset \cdots \subset K_\infty = \bigcup K_n$$

with

$$\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z},$$

In Chapter 7 we showed that every number field has at least one $\mathbb{Z}_p$-extension, namely the cyclotomic $\mathbb{Z}_p$-extension. It is obtained by letting K_∞ be an appropriate subfield of $K(\zeta_{p^\infty})$.

Proposition 13.1. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then, for each $n \geq 0$, there is a unique field K_n of degree p^n over K, and these K_n, plus K_∞, are the only fields between K and K_∞.*

Proof. The intermediate fields correspond to the closed subgroups of $\mathbb{Z}_p$. Let $S \neq 0$ be a closed subgroup and let $x \in S$ be such that $v_p(x)$ is minimal. Then $x\mathbb{Z}$, hence $x\mathbb{Z}_p$, is in S. By the choice of x, we must have $S = x\mathbb{Z}_p = p^n\mathbb{Z}_p$ for some n. The result follows. □

Proposition 13.2. *Let K_∞/K be a $\mathbb{Z}_p$-extension and let $\tilde{l}$ be a prime (possibly archimedean) of K which does not lie above p. Then K_∞/K is unramified at $\tilde{l}$. In other words, $\mathbb{Z}_p$-extensions are "unramified outside p."*

Proof. Let $I \subseteq \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$ be the inertia group for $\tilde{l}$. Since I is closed, $I = 0$ or $I = p^n\mathbb{Z}_p$ for some n. If $I = 0$ we are done, so assume $I = p^n\mathbb{Z}_p$. In particular, I is infinite. Since I must have order 1 or 2 for infinite primes, we may assume $\tilde{l}$ is non-archimedean. For each n, choose inductively a place $\tilde{l}_n$ of K_n lying above $\tilde{l}_{n-1}$, with $\tilde{l}_0 = \tilde{l}$. Let $\bar{K}_n$ be the completion, and let $\bar{K}_\infty = \bigcup \bar{K}_n$. Then

$$I \subseteq \mathrm{Gal}(\bar{K}_\infty/\bar{K}).$$

Let U be the units of $\bar{K}$. Local class field theory says that there is a continuous surjective homomorphism

$$U \to I \simeq p^n\mathbb{Z}_p.$$

But

$$U \simeq (\text{finite group}) \times \mathbb{Z}_l^a, \qquad a \in \mathbb{Z},$$

where l is the rational prime divisible by $\tilde{l}$ (proof: $\log_l\colon U \to l^{-N}\mathcal{O}$ for some N; the kernel is finite and $\mathcal{O}(=\text{local integers})$ is a finitely generated free $\mathbb{Z}_l$-module). Since $p^n\mathbb{Z}_p$ has no torsion, we must have a surjective and continuous map

$$\mathbb{Z}_l^a \to p^n\mathbb{Z}_p \to p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p.$$

However, $\mathbb{Z}_l^a$ has no closed subgroups of index p, so we have a contradiction. This completes the proof. □

The proposition may also be proved without class field theory. See Long [1], p. 94.

Lemma 13.3. *Let K_∞/K be a $\mathbb{Z}_p$-extension. At least one prime ramifies in this extension, and there exists $n \geq 0$ such that every prime which ramifies in K_∞/K_n is totally ramified.*

Proof. Since the class number of K is finite, the maximal abelian unramified extension of K is finite, so some prime must ramify in K_∞/K. We know that only finitely many primes of K ramify in K_∞/K by Proposition 13.2. Call them $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, and let $I_1, \ldots, I_s$ be the corresponding inertia groups. Then

$$\bigcap I_j = p^n\mathbb{Z}_p$$

for some n. The fixed field of $p^n\mathbb{Z}_p$ is K_n and $\mathrm{Gal}(K_\infty/K_n)$ is contained in each I_j. Therefore all primes above each $\mathfrak{p}_j$ are totally ramified in K_∞/K_n. This completes the proof. □

However, it is possible to have K_n/K unramified for some n (see Exercises 13.3 and 13.4).

We already know that every number field K has at least one $\mathbb{Z}_p$-extension, namely the cyclotomic $\mathbb{Z}_p$-extension defined in Chapter 7. However, there could be more. Let E_1 be those units of K which are congruent to 1 modulo every prime $\mathfrak{p}$ of K lying above p. Let $U_{1,\mathfrak{p}}$ denote the local units congruent to 1 mod $\mathfrak{p}$. There is an embedding

$$E_1 \to U_1 = \prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}$$

$$\varepsilon \mapsto (\varepsilon, \ldots, \varepsilon).$$

The closure $\bar{E}_1$ is a $\mathbb{Z}_p$-module. Leopoldt's conjecture predicts that the $\mathbb{Z}_p$-rank is $r_1 + r_2 - 1$, where r_1, r_2 have the usual meanings. We know this is true for abelian number fields (Corollary 5.32).

Theorem 13.4. *Suppose the $\mathbb{Z}_p$-rank of $\bar{E}_1$ is $r_1 + r_2 - 1 - \delta$, with $\delta \geq 0$. Then there are $r_2 + 1 + \delta$ independent $\mathbb{Z}_p$-extensions of K. In other words, if $\tilde{K}$ is the compositum of all $\mathbb{Z}_p$-extensions of K, then $\mathrm{Gal}(\tilde{K}/K) \simeq \mathbb{Z}_p^{r_2+1+\delta}$.*

Proof. Let $\tilde{K}$ be as above and F the maximal abelian extension of K which is unramified outside p. Then $\tilde{K} \subseteq F$. Let J denote the idèles of K. By class field theory, there is a closed subgroup H with

$$K^\times \subseteq H \subseteq J$$

such that

$$J/H \simeq \mathrm{Gal}(F/K).$$

Let $U_{\mathfrak{l}}$ denote the local unit group at a finite prime $\mathfrak{l}$ of K, and $U_{\mathfrak{l}} = K_{\mathfrak{l}}^{\times}$ if $\mathfrak{l}$ is archimedean. Let

$$U' = \prod_{\not{p} \mid p} U_{\not{p}}, \qquad U'' = \prod_{\mathfrak{l} \nmid p} U_{\mathfrak{l}}, \qquad U = U' \times U''.$$

All of these may be regarded as subgroups of J by putting a 1 in all the remaining components for U' and U''. U is an open subgroup. Since F/K is unramified outside p, $U'' \subseteq H$. Since F is maximal, we must have

$$H = \overline{K^{\times} U''}$$

(technical point: we need $J/\overline{K^{\times} U''}$ to be totally disconnected; but this will follow from the fact that this is true for U_1). Let

$$J' = J/H,$$

and

$$J'' = K^{\times} U/H = U'H/H \simeq U'/U' \cap H.$$

Let $U_1 = \prod_{\not{p} \mid p} U_{1,\not{p}}$ be as in the discussion preceding the statement of the theorem. Then

$$U' = U_1 \times (\text{finite group}).$$

Therefore

$$\begin{aligned} J'' \simeq U'/U' \cap H &= (\text{finite}) \times U_1(U' \cap H)/(U' \cap H) \\ &\simeq (\text{finite}) \times U_1/U_1 \cap H. \end{aligned}$$

We have a map

$$\psi \colon E_1 \to U_1 \subset J$$

as above, but note that $\psi(\varepsilon)$ has component 1 at all $\mathfrak{l} \not\mid p$. So this is not the same as $K^{\times} \hookrightarrow J$.

Lemma 13.5. $U_1 \cap H = U_1 \cap \overline{K^{\times} U''} = \overline{\psi(E_1)}$.

Proof. Let $\varepsilon \in E_1$. Then $\psi(\varepsilon) \in U_1$. Also

$$\psi(\varepsilon) = (\varepsilon)\left(\frac{\psi(\varepsilon)}{\varepsilon}\right) \in K^{\times} U''$$

since $\psi(\varepsilon)/\varepsilon$ has component 1 at all $\not{p} \mid p$. Taking closures, we obtain one inclusion.

The reverse inclusion is more difficult. Since U has a "nice" topology, we may obtain the closure of an arbitrary subset S by taking the intersection of (a cofinal subset of) the closed neighborhoods of S. If $U_{n,\not{p}}$ denotes those units congruent to 1 mod $\not{p}^n$ and $U_n = \prod_{\not{p} \mid p} U_{n,\not{p}}$ (put 1 in all components for $\not{p} \not\mid p$) then

$$\overline{K^{\times} U''} = \bigcap_n K^{\times} U'' U_n.$$

Also, we have

$$\overline{\psi(E_1)} = \bigcap_n \psi(E_1)U_n.$$

It suffices to show that

$$U_1 \cap K^\times U''U_n \subseteq \psi(E_1)U_n.$$

Let $x \in K^\times$, $u'' \in U''$, $u \in U_n$. Suppose

$$xu''u \in U_1.$$

Then $xu'' \in U_1$. Since u'' has component 1 at all $\mathfrak{p}|p$, x must be a principal unit at these primes. Since U_1 has component 1 at $\mathfrak{l} \nmid p$, and u'' is a unit at these places, x must also be a unit at these places. Therefore x is a unit everywhere, so x is a global unit, in fact $x \in E_1$. To summarize, at $\mathfrak{p}|p$ we have $xu'' = x \in E_1$. At $\mathfrak{l} \nmid p$, $xu'' = 1$. This is exactly what it means for xu'' to be in $\psi(E_1)$. Consequently

$$xu''u \in \psi(E_1)U_n.$$

This completes the proof of Lemma 13.5. □

The logarithm maps $U_{n,\mathfrak{p}} \simeq \mathfrak{p}^n \simeq \mathcal{O}_\mathfrak{p}$ for large enough n, by Proposition 5.7. But $\mathcal{O}_\mathfrak{p} \simeq \mathbb{Z}_p^{e_\mathfrak{p} f_\mathfrak{p}}$ where $e_\mathfrak{p}, f_\mathfrak{p}$ denote the ramification and residue class degrees. Also, $[K:\mathbb{Q}] = \sum e_\mathfrak{p} f_\mathfrak{p}$. We obtain

$$U_1 \simeq (\text{finite}) \times \mathbb{Z}_p^{[K:\mathbb{Q}]}.$$

Therefore

$$U_1/U_1 \cap H = U_1/\overline{\psi(E_1)} \simeq (\text{finite}) \times \mathbb{Z}_p^{r_2+1+\delta}$$

A similar statement holds for J''.

We want information about J'. But

$$J'/J'' \simeq J/K^\times U \simeq \text{ideal class group of } K$$

(see the appendix on class field theory; better: prove it yourself). Consequently

$$J'/\mathbb{Z}_p^{r_2+1+\delta} \simeq \text{finite group}.$$

This is approximately what we want. However, we need the quotient of J' by a finite group to be $\mathbb{Z}_p^{r_2+1+\delta}$, since then the fixed field of the finite group is L. Let N be the order of the finite group in the last equation above. Then

$$N\mathbb{Z}_p^{r_2+1+\delta} \subseteq NJ' \subseteq \mathbb{Z}_p^{r_2+1+\delta},$$

so

$$NJ' \simeq \mathbb{Z}_p^{r_2+1+\delta}, \quad \text{as a } \mathbb{Z}_p\text{-module}$$

(we are writing J' additively). Let $J'_N = \{x \in J' \mid Nx = 0\}$. Then J'_N is closed and

$$J'/J'_N \simeq NJ' \simeq \mathbb{Z}_p^{r_2+1+\delta}.$$

It is easy to see that J'_N is finite: if it had order larger than N, then two elements of J'_N would have the same representative in the finite group above. Hence their difference, which is killed by N, would be a nontrivial element of finite order in $\mathbb{Z}_p^{r_2+1+\delta}$. This is impossible, so J'_N is finite.

The fixed field of $J'_N \subset J' = \mathrm{Gal}(F/K)$ must be $\tilde{K}$, so the proof is complete. □

Corollary 13.6. *Let H be the Hilbert class field of K and let F be the maximal abelian extension of K unramified outside p. Then*

$$\mathrm{Gal}(F/H) \simeq \left(\prod_{\not{p} \mid p} U_{\not{p}}\right) \Big/ \bar{E},$$

where $\bar{E}$ is the closure of E, embedded in $\prod U_{\not{p}}$ diagonally.

Proof. $\mathrm{Gal}(F/K) \simeq J'$, and the closed subgroup J'' corresponds to H. Hence $\mathrm{Gal}(F/H) \simeq J'' \simeq U'/U' \cap H$. The same proof as for Lemma 13.5 shows that $U' \cap H = \overline{\psi(E)}$. The result follows. □

§13.2 The Structure of Λ-modules

Let $\Lambda = \mathbb{Z}_p[[T]]$. Recall that a nonconstant polynomial $P(T) \in \Lambda$ is called distinguished if

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0, \qquad p \mid a_i, \qquad 0 \le i \le n-1.$$

By the p-adic Weierstrass Preparation Theorem (7.3), if $f(T) \in \Lambda$ is nonzero, then we may uniquely write

$$f(T) = p^\mu P(T) U(T)$$

with $\mu \ge 0$, $P(T)$ distinguished, and $U(T) \in \Lambda^\times$. By Lemma 7.5, if f is a polynomial so is U. Also, there is a division algorithm (Proposition 7.2) for distinguished polynomials: if $f(T) \in \Lambda$ and $P(T)$ is distinguished then (uniquely)

$$f(T) = q(T)P(T) + r(T)$$

with $r(T) \in \mathbb{Z}_p[T]$, $\deg r(T) < \deg P(T)$ (let $\deg 0 = -\infty$, for convenience).

It follows from the above that Λ is a unique factorization domain, whose irreducible elements are p and the irreducible distinguished polynomials. The units are the power series with constant term in $\mathbb{Z}_p^\times$.

Lemma 13.7. *Suppose $f, g \in \Lambda$ are relatively prime. Then the ideal (f, g) is of finite index in Λ.*

Proof. Let $h \in (f, g)$ be of minimal degree. Then $h = p^s H$ with $H = 1$ or H distinguished. Suppose $H \neq 1$. Since f and g are relatively prime, we may assume H does not divide f. But

$$f = Hq + r, \qquad \deg r < \deg H = \deg h,$$

so

$$p^s f = hq + p^s r.$$

Since $\deg(p^s r) < \deg h$ and $p^s r \in (f, g)$, we have a contradiction. Therefore $H = 1$ and $h = p^s$. Without loss of generality, we may assume f is not divisible by p and is distinguished. Otherwise, use g or divide by a unit. We have

$$(f, g) \supseteq (p^s, f).$$

By the division algorithm, any element of Λ is congruent $\operatorname{mod} f$ to a polynomial of degree less than $\deg f$. Since there are only finitely many such polynomials mod p^s, the ideal (p^s, f) has finite index. This completes the proof. □

Lemma 13.8. *Suppose $f, g \in \Lambda$ are relatively prime. Then*

(1) *the natural map*

$$\Lambda/(fg) \to \Lambda/(f) \oplus \Lambda/(g)$$

is an injection with finite cokernel;

(2) *there is an injection*

$$\Lambda/(f) \oplus \Lambda/(g) \to \Lambda/(fg)$$

with finite cokernel.

Proof. (1) Since Λ is a unique factorization domain, the map is an injection. Consider $(a \bmod f, b \bmod g)$. If $a - b \in (f, g)$, then $a - b = fA + gB$, for some A, B. Let

$$c = a - fA = b + gB.$$

Then

$$c \equiv a \bmod f, \qquad c \equiv b \bmod g,$$

so (a, b) is in the image. Now let $r_1, \dots, r_n \in \Lambda$ be representatives for $\Lambda/(f, g)$. It follows that

$$\{(0 \bmod f, r_j \bmod g) \mid 1 \leq j \leq n\}$$

is a set of representatives for the cokernel of the above map. This proves (1).

(2) From (1),

$$\Lambda/(fg) \simeq M \subseteq \Lambda/(f) \oplus \Lambda/(g) \overset{\text{def}}{=} N$$

with M of finite index in N. Let P be any distinguished polynomial in Λ which is relatively prime to fg. If $(x, y) \in N$, then

$$(P^i)(x, y) \equiv (P^j)(x, y) \bmod M$$

for some $i < j$. Since

$$1 - P^{j-i} \in \Lambda^\times,$$

we have

$$P^i(x, y) \in M.$$

It follows that $P^k N \subseteq M$ for some k. (Alternatively, this follows from the fact that $P^k \to 0$ in Λ). Suppose $P^k(x, y) = 0$ in N, so $f \mid P^k x$, $g \mid P^k y$. Since $gcd(P, fg) = 1$, $f \mid x$ and $g \mid y$; so $(x, y) = 0$ in N. Therefore

$$N \xrightarrow{P^k} M \simeq \Lambda/(fg)$$

is injective. The image contains the ideal (P^k, fg), which is of finite index by Lemma 13.7. This completes the proof. □

Proposition 13.9. *The prime ideals of* Λ *are* 0, (p, T), (p), *and the ideals* $(P(T))$ *where* $P(T)$ *is irreducible and distinguished. The ideal* (p, T) *is the unique maximal ideal.*

Proof. All the above are easily seen to be prime ideals. Let $\mathfrak{p} \neq 0$ be prime. Let $h \in \mathfrak{p}$ be of minimal degree. Then $h = p^s H$ with $H = 1$ or H distinguished. Since $\mathfrak{p}$ is prime, $p \in \mathfrak{p}$ or $H \in \mathfrak{p}$. If $1 \neq H \in \mathfrak{p}$ then H must be irreducible by the minimality of the degree of h. Therefore, in both cases, $(f) \subseteq \mathfrak{p}$ where $f = p$ or f is irreducible and distinguished. If $(f) = \mathfrak{p}$, then $\mathfrak{p}$ is on the above list so we are done. Therefore assume $(f) \neq \mathfrak{p}$, so there is a $g \in \mathfrak{p}$ with $f \nmid g$. Since f is irreducible, f and g are relatively prime. Lemma 13.7 implies that $\mathfrak{p}$ is of finite index in Λ. Since $\Lambda/\mathfrak{p}$ is a finite $\mathbb{Z}_p$-module, $p^N \in \mathfrak{p}$ for large N, hence $p \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Also, $T^i \equiv T^j \bmod \mathfrak{p}$ for some $i < j$. But $1 - T^{j-i} \in \Lambda^\times$, so $T^i \in \mathfrak{p}$. Therefore $T \in \mathfrak{p}$, so $(p, T) \subseteq \mathfrak{p}$. But $\Lambda/(p, T) \simeq \mathbb{Z}/p\mathbb{Z}$, so (p, T) is maximal and $\mathfrak{p} = (p, T)$.

Since all the prime ideals are contained in (p, T), this is the only maximal ideal. This completes the proof. □

Lemma 13.10. *Let* $f \in \Lambda$ *then* $\Lambda/(f)$ *is infinite.*

Proof. We may assume $f \neq 0$. It suffices to consider $f = p$ and $f =$ distinguished. If $f = p$, $\Lambda/(f) \simeq \mathbb{Z}/p\mathbb{Z}[[T]]$. If f is distinguished, use the division algorithm. □

Lemma 13.11. Λ *is a Noetherian ring.*

Proof. It is known (Lang's *Algebra*) that if A is Noetherian then so is $A[[T]]$. One could also use the Hilbert basis theorem (A Noetherian $\Rightarrow A[T]$ Noetherian) since the generators of an ideal may always be assumed to be polynomials. □

Definition. Two Λ-modules M and M' are said to be *pseudo-isomorphic*, written

$$M \sim M',$$

if there is a homomorphism $M \to M'$ with finite kernel and co-kernel. In other words, there is an exact sequence of Λ-modules

$$0 \to A \to M \to M' \to B \to 0$$

with A and B finite Λ-modules.

Warning. $M \sim M'$ does not imply $M' \sim M$. For example, $(p, T) \sim \Lambda$, obviously. But suppose $\Lambda \to (p, T)$. Let $f(T)$ be the image of $1 \in \Lambda$. Then the image of Λ is $(f) \subseteq (p, T)$. But $\Lambda/(f)$ is infinite, so $(p, T)/(f)$ is infinite. Hence, the cokernel is infinite. However, it can be shown that for finitely generated Λ-torsion Λ-modules, $M \sim M' \Leftrightarrow M' \sim M$.

Lemma 13.8 says that if $(f, g) = 1$ then

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g) \quad \text{and} \quad \Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg).$$

We shall need to know the structure of finitely generated Λ-modules. The following theorem was first proved by Iwasawa in terms of the group ring $\mathbb{Z}_p[[\Gamma]]$. Serre observed that the group ring is isomorphic to Λ and deduced the structure theorem from some general results in commutative algebra. Paul Cohen showed that one could give a proof via row and column operations, just as is done for modules over principal ideal domains. In the following, we follow Lang's treatment [4] of Cohen's proof.

Theorem 13.12. *Let M be a finitely generated Λ-module. Then*

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\right),$$

where $r, s, t, n_i, m_j \in \mathbb{Z}$, and f_j is distinguished and irreducible.

Proof. Note that the result is the same as for modules over principal ideal domains, except that there is only a pseudo-isomorphism. The proof will use an extension of the techniques employed in that theorem (the reader who has not seen the p.i.d. theorem proved via row and column operations should immediately consult an algebra text).

Suppose M has generators $u_1, \ldots, u_n$, with various relations

$$\lambda_1 u_1 + \cdots + \lambda_n u_n = 0, \qquad \lambda_i \in \Lambda.$$

Since the relations R are a submodule of Λ^n, and Λ is Noetherian, the relations are finitely generated. So we can represent M by a matrix whose rows are of the form $(\lambda_1, \ldots, \lambda_n)$, where $\sum \lambda_i u_i = 0$ is a relation. By abuse of notation, we call this matrix R.

We first review the basic row and column operations, which correspond to changing the generators of R and M.

Operation A. *We may permute the rows or permute the columns.*

Operation B. *We may add a multiple of a row (or column) to another row (column). Special case: if* $\lambda' = q\lambda + r$ *then*

$$\begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & \lambda' & \cdots \\ \vdots & & \vdots & \end{pmatrix} \to \begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & r & \cdots \\ \vdots & & \vdots & \end{pmatrix}$$

Operation C. *We may multiply a row or column by an element of* $\Lambda^{\times}$.

The above operations are used for principal ideal domains. However, we have three additional operations, which are where the pseudo-isomorphisms enter.

Operation 1. *If R contains a row $(\lambda_1, p\lambda_2, \ldots, p\lambda_n)$ with $p \nmid \lambda_1$, then we may change R to the matrix R' whose first row is $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and the remaining rows are the rows of R with the first elements multiplied by p. In pictures:*

$$\begin{pmatrix} \lambda_1 & p\lambda_2 & \cdots \\ \alpha_1 & \alpha_2 & \cdots \\ \beta_1 & \beta_2 & \cdots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p\alpha_1 & \alpha_2 & \cdots \\ p\beta_1 & \beta_2 & \cdots \end{pmatrix}.$$

As a special case, if $\lambda_2 = \cdots = \lambda_n = 0$ then we may multiply $\alpha_1, \beta_1, \ldots$ by an arbitrary power of p.

Proof. In R we have the relation

$$\lambda_1 u_1 + p(\lambda_2 u_2 + \cdots + \lambda_n u_n) = 0.$$

Let $M' = M \oplus v\Lambda$, with a new generator v, modulo the additional relations

$$(-u_1, pv) = 0, \qquad (\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v) = 0.$$

There is a natural map $M \to M'$. Suppose $m \mapsto 0$. Then m lies in the module of relations, so

$$(m, 0) = a(-u_1, pv) + b(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v)$$

with $a, b \in \Lambda$. Therefore

$$ap = -b\lambda_1.$$

Since $p \nmid \lambda_1$ by assumption, $p \mid b$. Also, $\lambda_1 \mid a$. In the M-component,

$$\begin{aligned} m &= -\frac{a}{\lambda_1}(\lambda_1 u_1) - \frac{a}{\lambda_1} p(\lambda_2 u_2 + \cdots + \lambda_n u_n) \\ &= -\frac{a}{\lambda_1}(0) = 0. \end{aligned}$$

Since the images of pv and $\lambda_1 v$ in M' are in the image of M, the ideal (p, λ_1) annihilates M'/M. Since $\Lambda/(p, \lambda_1)$ is finite and M' is finitely generated, M'/M is finite. Therefore

$$M \sim M'.$$

The new module M' has generators $v, u_2, \ldots, u_n$. Any relation $\alpha_1 u_1 + \cdots + \alpha_n u_n = 0$ becomes $p\alpha_1 v + \cdots + \alpha_n u_n = 0$, so the first column is multiplied by p, as claimed. We also have the relation $\lambda_1 v + \cdots + \lambda_n u_n$. So the new matrix R' has the form stated above (we removed the redundant row $(p\lambda_1, \ldots, p\lambda_n)$). □

Operation 2. *If all elements in the first column of R are divisible by p^k and if there is a row $(p^k\lambda_1, \ldots, p^k\lambda_n)$ with $p \nmid \lambda_1$, then we may change to the matrix R' which is the same as R except that $(p^k\lambda_1, \ldots, p^k\lambda_n)$ is replaced by $(\lambda_1, \ldots, \lambda_n)$. In pictures:*

$$\begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \end{pmatrix}$$

Proof. Let $M' = M \oplus \Lambda v$ modulo the relations

$$(p^k u_1, -p^k v) = 0, \qquad (\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v) = 0.$$

As before, the fact that $p \nmid \lambda_1$ allows us to conclude that M embeds in M'. Also, the ideal (p^k, λ_1) annihilates M'/M, so the quotient is finite. Consequently $M \sim M'$.

Using the fact that $p^k(u_1 - v) = 0$ and the fact that p^k divides the first coefficient of all relations involving u_1, we find that

$$M' = M'' \oplus (u_1 - v)\Lambda,$$

where M'' is generated by $v, u_2, \ldots, u_n$ and has relations generated by $(\lambda_1, \ldots, \lambda_n)$ and R. Therefore M'' has R' for its relations. Note that

$$(u_1 - v)\Lambda \simeq \Lambda/(p^k),$$

which is already of the desired form. So it suffices to work with M'' and R' □

Operation 3. *If R contains a row $(p^k\lambda_1, \ldots, p^k\lambda_n)$, and for some Λ with $p \nmid \lambda$, $(\lambda\lambda_1, \ldots, \lambda\lambda_n)$ is also a relation (not necessarily explicitly contained in R), then we may change R to R', where R' is the same as R except that $(p^k\lambda_1, \ldots, p^k\lambda_n)$ is replaced by $(\lambda_1, \ldots, \lambda_n)$.*

Proof. Consider the surjection

$$M \to M' = M/(\lambda_1 u_1 + \cdots + \lambda_n u_n)\Lambda.$$

The kernel is annihilated by the ideal (λ, p^k). Since M, hence the kernel, is finitely generated, and since $\Lambda/(\lambda, p)$ is finite, the kernel must be finite; so $M \sim M'$. Clearly M' has R' as its relation matrix. □

This completes our list of operations. We call A, B, C, 1, 2, 3 admissible operations. Note that all of them preserve the size of the matrix.

We are now ready to begin. If $0 \neq f \in \Lambda$, then

$$f(T) = p^{\mu} P(T) U(T),$$

with P distinguished and $U \in \Lambda^{\times}$. Let

$$\deg_w f = \begin{cases} \infty, & \mu > 0 \\ \deg P(T), & \mu = 0; \end{cases}$$

this is called the Weierstrass degree of f. Given a matrix R, define

$$\deg^{(k)}(R) = \min \deg_w(a'_{ij}) \quad \text{for } i, j \geq k,$$

where (a'_{ij}) ranges over all relation matrices obtained from R via admissible operations which leave the first $(k-1)$ rows unchanged (we allow a_{ij} for $i \geq k$ and all j to change; we also allow operations such as B which use, but do not change, the first $(k-1)$ rows).

If the matrix R has the form

$$\begin{pmatrix} \lambda_{11} & & 0 & 0 & \cdots & 0 \\ & \ddots & & & & \\ 0 & & \lambda_{r-1,r-1} & 0 & \cdots & 0 \\ * & \cdots & * & * & \cdots & * \\ * & \cdots & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} D_{r-1} & 0 \\ A & B \end{pmatrix}$$

with λ_{kk} distinguished and

$$\deg \lambda_{kk} = \deg_w \lambda_{kk} = \deg^{(k)}(R), \quad \text{for } 1 \leq k \leq r-1,$$

then we say that T is in $(r-1)$-normal form.

Claim. *If the submatrix $B \neq 0$ then R may be transformed, via admissible operations, into R' which is in r-normal form and has the same first $(r-1)$ diagonal elements.*

Proof. The "special case" of Operation 1 allows us to assume, when necessary, that a large power of p divides each λ_{ij} with $i \geq r$ and $j \leq r-1$. That is, $p^N \mid A$, with N large (large enough that $p^N \nmid B$). Using Operation 2, we may assume that $p \nmid B$. We may also assume that B contains an entry λ_{ij} such that

$$\deg_w \lambda_{ij} = \deg^{(r)}(R) < \infty.$$

If $\lambda_{ij} = P(T)U(T)$, then multiply the jth column by U^{-1}. Therefore we may assume λ_{ij} is distinguished. (Since the first $r-1$ rows have 0 in the jth column, they do not change). Operation A lets us assume $\lambda_{ij} = \lambda_{rr}$ (again, the 0's help us).

By the division algorithm (special case of B), we may assume that λ_{rj} is a polynomial with

$$\deg \lambda_{rj} < \deg \lambda_{rr}, \qquad j \neq r,$$

and

$$\deg \lambda_{rj} < \deg \lambda_{jj}, \qquad j < r.$$

Since λ_{rr} has minimal Weierstrass degree in B, we must have $p \mid \lambda_{rj}$ for $j > r$. By 1, we may assume $p^N \mid \lambda_{rj}$, $j < r$, for some large N. Suppose $\lambda_{rj} \neq 0$ for some $j > r$. Operation 1 lets us remove the power of p from some nonzero λ_{rj} with $j > r$ (the 0's above are left unchanged). Then

$$\deg_w \lambda_{rj} = \deg \lambda_{rj} < \deg \lambda_{rr} = \deg_w \lambda_{rr},$$

which is impossible. Consequently, $\lambda_{rj} = 0$ for $j > r$.

If some $\lambda_{rj} \neq 0$ for $j < r$, use Operation 1 to obtain $p \nmid \lambda_{rj}$ for some j. But then

$$\deg_w \lambda_{rj} \leq \deg \lambda_{rj} < \deg \lambda_{jj} = \deg_w \lambda_{jj}.$$

Since

$$\deg_w \lambda_{jj} = \deg^{(j)}(R),$$

this contradicts the definition of $\deg^{(j)}(R)$. Therefore $\lambda_{rj} = 0$ for all $j \neq r$. This proves the claim. □

If we start with a matrix R and $r = 1$, we may successively change R until we obtain a matrix

$$\begin{pmatrix} \lambda_{11} & & 0 \\ & \ddots & \\ & & \lambda_{rr} \\ A & & 0 \end{pmatrix}$$

with each λ_{jj} distinguished and $\deg \lambda_{jj} = \deg^{(j)}(R)$ for $j \leq r$. By the division algorithm, we may assume that λ_{ij} is a polynomial and

$$\deg \lambda_{ij} < \deg \lambda_{jj}, \quad \text{for } i \neq j.$$

Suppose $\lambda_{ij} \neq 0$ for some $i \neq j$. Since $\deg_w \lambda_{jj}$ is minimal, $p \mid \lambda_{ij}$; so we have a nonzero relation $(\lambda_{i1}, \ldots, \lambda_{ir}, 0, \ldots, 0)$ which is divisible by p. Let $\lambda = \lambda_{11} \cdots \lambda_{rr}$. Then $p \nmid \lambda$, since the λ_{jj}'s are distinguished; and

$$\left(\lambda \frac{1}{p} \lambda_{i1}, \ldots, \lambda \frac{1}{p} \lambda_{ir}, 0, \ldots, 0\right)$$

is also a relation, since $\lambda_{jj} u_j = 0$. By Operation 3 we may assume p does not divide λ_{ij} for some j, so

$$\deg_w \lambda_{ij} \leq \deg \lambda_{ij} < \deg \lambda_{jj} = \deg^{(j)}(R).$$

This is impossible. Therefore $\lambda_{ij} = 0$ for all i and j with $i \neq j$. This means $A = 0$. In terms of Λ-modules, we have

$$\Lambda/(\lambda_{11}) \oplus \cdots \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r}.$$

Putting back in the factors $\Lambda/(p^k)$ which were discarded in Operation 2, we obtain the desired result, except that the λ_{ii} are not necessarily irreducible. Lemma 13.8 takes care of this problem. This completes the proof of Theorem 13.12. □

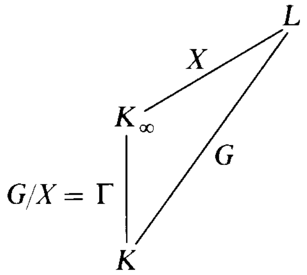
§13.3 Iwasawa's Theorem

The purpose of this section is to prove the following result.

Theorem 13.13. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there exist integers $\lambda \geq 0$, $\mu \geq 0$, and ν, all independent of n, and an integer n_0 such that*

$$e_n = \lambda n + \mu p^n + \nu \quad \textit{for all } n \geq n_0.$$

Proof. Let $\Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, and let γ_0 be a topological generator of Γ, as in Chapter 7. Let L_n be the maximal unramified abelian p-extension of K_n, so $X_n = \mathrm{Gal}(L_n/K_n) \simeq A_n = p$-Sylow of the ideal class group of K_n. Let $L = \bigcup_{n \geq 0} L_n$ and $X = \mathrm{Gal}(L/K_\infty)$. Each L_n is Galois over K since L_n is maximal, so L/K is also Galois. Let $G = \mathrm{Gal}(L/K)$. We have the following diagram.



The idea will be to make X into a Γ-module, hence a Λ-module. It will be shown to be finitely generated and Λ-torsion, hence pseudo-isomorphic to a direct sum of modules of the form $\Lambda/(p^k)$ and $\Lambda/(P(T)^k)$. It is easy to calculate what happens at the nth level for these modules. We then transfer the result back to X to obtain the theorem.

We start with the following special case.

Assumption. *All primes which are ramified in K_∞/K are totally ramified.*

By Lemma 13.3, this may be accomplished by replacing K by K_m for some m. By our assumption,

$$K_{n+1} \cap L_n = K_n,$$

so

$$\mathrm{Gal}(L_n/K_n) \simeq \mathrm{Gal}(L_n K_{n+1}/K_{n+1}),$$

which is a quotient of X_{n+1}. We have a map

$$X_{n+1} \to X_n.$$

This corresponds to the norm map $A_{n+1} \to A_n$ on ideal class groups (see the appendix on class field theory). Observe that

$$X_n \simeq \mathrm{Gal}(L_n K_\infty/K_\infty),$$

so

$$\varprojlim X_n \simeq \varprojlim \mathrm{Gal}((\bigcup L_n K_\infty)/K_\infty) = \mathrm{Gal}(L/K_\infty) = X.$$

Let $\gamma \in \Gamma_n = \Gamma/\Gamma^{p^n}$. Extend γ to $\tilde{\gamma} \in \mathrm{Gal}(L_n/K)$. Let $x \in X_n$. Then γ acts on x by

$$x^\gamma = \tilde{\gamma}x(\tilde{\gamma})^{-1}.$$

Since $\mathrm{Gal}(L_n/K_n)$ is abelian, x^γ is well-defined. (This action corresponds to the action on A_n). Therefore X_n becomes a $\mathbb{Z}_p[\Gamma_n]$-module. Representing an element of $X \simeq \varprojlim X_n$ as a vector $(x_0, x_1, \ldots)$, and letting $\mathbb{Z}_p[\Gamma_n]$ act on the nth component, we easily find that X becomes a module over $\Lambda \simeq \varprojlim \mathbb{Z}_p[\Gamma_n]$. (The only thing to be checked is that $x^\gamma \in X$, and this is easy to do). The polynomial $1 + T \in \Lambda$ acts as $\gamma_0 \in \Gamma$. We have

$$x^\gamma = \tilde{\gamma}x\tilde{\gamma}^{-1}, \quad \text{for } \gamma \in \Gamma, x \in X,$$

where $\tilde{\gamma}$ is an extension of γ to G.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the primes which ramify in K_∞/K, and fix a prime $\tilde{\mathfrak{p}}_i$ of L lying above $\mathfrak{p}_i$. Let $I_i \subseteq G$ be the inertia group. Since L/K_∞ is unramified,

$$I_i \cap X = 1.$$

Since K_∞/K is totally ramified at $\mathfrak{p}_i$,

$$I_i \hookrightarrow G/X = \Gamma$$

is surjective, hence bijective. So

$$G = I_i X = X I_i, \qquad i = 1, \ldots, s.$$

Let $\sigma_i \in I_i$ map to γ_0. Then σ_i must be a topological generator of I_i. Since

$$I_i \subseteq X I_1,$$

we have

$$\sigma_i = a_i \sigma_1$$

for some $a_i \in X$. Note that $a_1 = 1$.

Lemma 13.14 (Assuming the above "Assumption"). *Let G' be the closure of the commutator subgroup of G. Then*

$$G' = X^{\gamma_0 - 1} = TX.$$

Proof. Since $\Gamma \simeq I_1 \subseteq G$ maps onto $\Gamma = G/X$, we may lift $\gamma \in \Gamma$ to the corresponding element in I_1 in order to define the action of Γ on X. For simplicity, we identify Γ and I_1, so $x^\gamma = \gamma x \gamma^{-1}$. Let

$$a = \alpha x, b = \beta y, \quad \text{with } \alpha, \beta \in \Gamma, \quad x, y \in X,$$

be arbitrary elements of $G = \Gamma X$. Then

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} = x^\alpha (yx^{-1})^{\alpha\beta} (\alpha\beta) \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha (yx^{-1})^{\alpha\beta} (y^{-1})^\beta \quad \text{(since } \Gamma \text{ is abelian)} \\ &= (x^\alpha)^{1-\beta} (y^\beta)^{\alpha - 1}. \end{aligned}$$

Let $\beta = 1, \alpha = \gamma_0$. We find that $y^{\gamma_0 - 1} \in G'$, so

$$X^{\gamma_0 - 1} \subseteq G'.$$

For β arbitrary, there exists $c \in \mathbb{Z}_p$ with $\beta = \gamma_0^c$, so

$$1 - \beta = 1 - \gamma_0^c = 1 - (1 + T)^c = 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n \in T\Lambda.$$

Since $\gamma_0 - 1 = T$, $(x^\alpha)^{1-\beta} \in X^{\gamma_0 - 1}$. Similarly, $(y^\beta)^{1-\alpha} \in X^{\gamma_0 - 1}$. Since $X^{\gamma_0 - 1} = TX$ is closed (it is the image of the compact set X), $G' \subseteq X^{\gamma_0 - 1}$. This proves the lemma. □

Lemma 13.15. (Assuming the "Assumption"). *Let Y_0 be the $\mathbb{Z}_p$-submodule of X generated by $\{a_i | 2 \le i \le s\}$ and by $X^{\gamma_0 - 1} = TX$. Let $Y_n = \nu_n Y_0$, where*

$$\nu_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1} = \frac{(1 + T)^{p^n} - 1}{T}.$$

Then

$$X_n \simeq X/Y_n \quad \textit{for } n \ge 0.$$

Proof. First, consider $n = 0$. We have $K \subseteq L_0 \subseteq L$. Since L_0 is the maximal abelian unramified p-extension of K, and since L/K is a p-extension, L_0/K is the maximal unramified abelian subextension of L/K. Therefore $\mathrm{Gal}(L/L_0)$ must be the closed subgroup of G generated by G' and all the inertia groups

I_i, $1 \leq i \leq s$. Therefore $\mathrm{Gal}(L/L_0)$ is the closure of the group generated by $X^{\gamma_0 - 1}$, I_1, and $a_2, \ldots, a_s$, so

$$\begin{aligned} X_0 = \mathrm{Gal}(L_0/K) &= G/\mathrm{Gal}(L/L_0) = XI_1/\mathrm{Gal}(L/L_0) \\ &\simeq X/\overline{\langle X^{\gamma_0 - 1}, a_2, \ldots, a_s \rangle} = X/Y_0. \end{aligned}$$

Now, suppose $n \geq 1$. Replace K by K_n and γ_0 by $\gamma_0^{p^n}$. Then σ_i becomes $\sigma_i^{p^n}$. Observe that

$$\begin{aligned} \sigma_i^{k+1} &= (a_i \sigma_1)^{k+1} = a_i \sigma_1 a_i \sigma_1^{-1} \sigma_1^2 a_i \sigma_1^{-2} \cdots \sigma_1^k a_i \sigma_1^{-k} \sigma_1^{k+1} \\ &= a_i^{1 + \sigma_1 + \cdots + \sigma_1^k} \sigma_1^{k+1}. \end{aligned}$$

Therefore

$$\sigma_i^{p^n} = (v_n a_i) \sigma_1^{p^n},$$

so a_i is replaced by $v_n a_i$. Finally, $X^{\gamma_0 - 1}$ is replaced by $(\gamma_0^{p^n} - 1)X = v_n X^{\gamma_0 - 1}$. Therefore Y_0 becomes $v_n Y_0$, which yields the desired result. This completes the proof of Lemma 13.15. □

The above result is a very crucial step since it allows us to retrieve information about X_n from information about X.

Lemma 13.16 (Nakayama's Lemma). *Let X be a compact Λ-module. Then*

$$X \text{ is finitely generated over } \Lambda \Leftrightarrow X/(p, T)X \text{ is finite.}$$

If $x_1, \ldots, x_n$ generate $X/(p, T)X$ over $\mathbb{Z}$, then they also generate X as a Λ-module. A special case:

$$X/(p, T)X = 0 \Leftrightarrow X = 0.$$

Proof. Consider a small neighborhood U of 0 in X. Since $(p, T)^n \to 0$ in Λ, each $z \in X$ has a neighborhood U_z such that $(p, T)^n U_z \subseteq U$ for large n. Since X is compact, finitely many U_z cover X. Therefore $(p, T)^n X \subseteq U$ for large n, so $\bigcap ((p, T)^n X) = 0$ for any compact Λ-module X.

Now assume $x_1, \ldots, x_n$ generate $X/(p, T)X$. Let $Y = \Lambda x_1 + \cdots + \Lambda x_n \subseteq X$. Then Y is compact (image of Λ^n), hence closed, so X/Y is a compact Λ-module. By assumption, $Y + (p, T)X = X$. Therefore

$$(p, T)(X/Y) = (Y + (p, T)X)/Y = X/Y,$$

hence

$$(p, T)^n(X/Y) = X/Y \quad \text{for all } n \geq 0.$$

It follows from the above that $X/Y = 0$, so $X = Y$ and $\{x_i\}$ generates X (this could also be proved more explicitly by successively considering $x \in X \bmod (p, T)$, then $\bmod (p, T)^2$, etc.). The other parts of the lemma follow easily. □

Lemma 13.17 (With the "Assumption," but see Lemma 13.18). *$X = \mathrm{Gal}(L/K_\infty)$ is a finitely generated Λ-module.*

PROOF. Clearly $v_1 \in (p, T)$, so $Y_0/(p, T)Y_0$ is a quotient of $Y_0/v_1 Y_0 = Y_0/Y_1 \subseteq X/Y_1 = X_1$, which is finite. Therefore Y_0 is finitely generated. Since $X/Y_0 = X_0$ is finite, X must also be finitely generated. This proves the lemma. □

Arbitrary *K*. We now remove the Assumption. Let K_∞/K be a $\mathbb{Z}_p$-extension and choose $e \geq 0$ such that in K_∞/K_e all ramified primes are totally ramified. Then Lemmas 13.15 and 13.17 apply to K_∞/K_e. In particular, X, which is the same for K_e and K, is a finitely generated Λ-module. For $n \geq e$,

$$1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \cdots + \gamma_0^{p^n - p^e} = \frac{v_n}{v_e} \overset{\text{def}}{=} v_{n,e}.$$

This replaces v_n for K_∞/K_e, since $\gamma_0^{p^e}$ generates $\mathrm{Gal}(K_\infty/K_e)$. Let Y_e be "Y_0 for K_e," as defined in Lemma 13.15. Then

$$Y_n = v_{n,e} Y_e, \quad \text{and} \quad X_n \simeq X/Y_n, \quad \text{for } n \geq e.$$

We have proved the following.

Lemma 13.18. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then X is a finitely generated Λ-module, and there exists $e \geq 0$ such that*

$$X_n \simeq X/v_{n,e} Y_e, \quad \textit{for all } n \geq e. \qquad □$$

We can now apply Theorem 13.12 to X. We can also apply it to Y_e with the same answer, since X/Y_e is finite. So we have

$$Y_e \sim X \sim \Lambda^r \oplus \left(\bigoplus \Lambda/(p^{k_i})\right) \oplus \left(\bigoplus \Lambda/(f_j(T)^{m_j})\right).$$

We shall calculate $V/v_{n,e}V$ for each of the summands V on the right side.

(1) $V = \Lambda$. By Lemma 13.10, $\Lambda/(v_{n,e})$ is infinite. Since $Y_e/v_{n,e}Y_e$ is finite, it follows easily that Λ does not occur as a summand.

(2) $V = \Lambda/(p^k)$. In this case,

$$V/v_{n,e}V \simeq \Lambda/(p^k, v_{n,e}).$$

It is easy to show that if the quotient of two distinguished polynomials is a polynomial, then it is distinguished (or constant). Therefore

$$v_{n,e} = \frac{v_n}{v_e} = \frac{((1+T)^{p^n} - 1)/T}{((1+T)^{p^e} - 1)/T}$$

is distinguished. By the division algorithm, every element of $\Lambda/(p^k, v_{n,e})$ is represented uniquely by a polynomial mod p^k of degree less than deg $v_{n,e} = p^n - p^e$. Therefore

$$|V/v_{n,e}V| = p^{k(p^n - p^e)} = p^{kp^n + c},$$

for some constant c.

(3) $V = \Lambda/(f(T)^m)$. Let $g(T) = f(T)^m$. Then g is also distinguished, say of degree d. Hence

$$T^d \equiv pQ(T) \bmod g$$

for some polynomial $Q(T)$, so

$$T^k \equiv (p)(\text{polynomial}) \bmod g \quad \text{for } k \geq d.$$

If $p^n \geq d$ then

$$\begin{aligned}(1 + T)^{p^n} &= 1 + (p)(\text{poly.}) + T^{p^n} \\ &\equiv 1 + (p)(\text{poly.}) \bmod g.\end{aligned}$$

Therefore

$$(1 + T)^{p^{n+1}} \equiv 1 + p^2(\text{poly.}) \bmod g.$$

It follows that

$$\begin{aligned}P_{n+2}(T) &= (1 + T)^{p^{n+2}} - 1 \\ &= ((1 + T)^{(p-1)p^{n+1}} + \cdots + (1 + T)^{p^{n+1}} + 1)((1 + T)^{p^{n+1}} - 1) \\ &\equiv (1 + \cdots + 1 + (p^2)(\text{poly.}))(P_{n+1}(T)) \\ &\equiv p(1 + (p)(\text{poly.}))P_{n+1}(T) \bmod g.\end{aligned}$$

Since $1 + (p)(\text{poly.}) \in \Lambda^\times$,

$$\frac{P_{n+2}}{P_{n+1}} \text{ acts as } (p)(\text{unit}) \text{ on } V = \Lambda/(g),$$

for $p^n \geq d$. Assume $n_0 > e$, $p^{n_0} \geq d$, and $n \geq n_0$. Then

$$\frac{v_{n+2,e}}{v_{n+1,e}} = \frac{v_{n+2}}{v_{n+1}} = \frac{P_{n+2}}{P_{n+1}},$$

and

$$v_{n+2,e}V = \frac{P_{n+2}}{P_{n+1}}(v_{n+1,e}V) = pv_{n+1,e}V.$$

Therefore

$$|V/v_{n+2,e}V| = |V/pV||pV/pv_{n+1,e}V|$$

for $n \geq n_0$. Since $(g, p) = 1$, multiplication by p is injective, so

$$|pV/pv_{n+1,e}V| = |V/v_{n+1,e}V|.$$

Since

$$V/pV \simeq \Lambda/(p, g) = \Lambda/(p, T^d),$$

we have

$$|V/pV| = p^d.$$

By induction,

$$|V/v_{n,e}V| = p^{d(n-n_0-1)}|V/v_{n_0+1,e}V|$$

for $n \geq n_0 + 1$. If $V/v_{n,e}V$ is finite for all n, then

$$|V/v_{n,e}V| = p^{dn+c}, \qquad n \geq n_0 + 1$$

for some constant c. If $V/\nu_{n,e}V$ is infinite then V cannot occur in our case. This happens only when $(\nu_{n,e}, f) \neq 1$, by Lemma 13.7.

Putting everything together, we obtain the following.

Proposition 13.19. *Suppose*

$$E = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(g_j(T))\right),$$

where each $g_j(T)$ is distinguished (not necessarily irreducible). Let $m = \sum k_i$ and $l = \sum \deg g_j$. If $E/\nu_{n,e}E$ is finite for all n, then $r = 0$ and there exist n_0 and c such that

$$|E/\nu_{n,e}E| = p^{mp^n + ln + c}, \quad \textit{for all } n > n_0. \qquad \square$$

We interrupt the proof of Theorem 13.13 to give the following, which will be used in the next section.

Lemma 13.20. *Assume E is as in Proposition 13.19, with $r = 0$. Then*

$$m = 0 \Leftrightarrow p\text{-rank } (E/\nu_{n,e}E) \textit{ is bounded as } n \to \infty.$$

Proof. Recall that the p-rank of a finite abelian group A is the number of direct summands of p-power order when A is decomposed into cyclic groups of prime power order. It is also equal to

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA).$$

Recall that $\nu_{n,e}$ is distinguished of degree $p^n - p^e$, so if $\deg \nu_{n,e} \geq \max \deg g_j$,

$$\begin{aligned} E/(p, \nu_{n,e})E &= \left(\bigoplus_{i=1}^{s} \Lambda/(p, \nu_{n,e})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(p, g_j, \nu_{n,e})\right) \\ &= \left(\bigoplus_{i=1}^{s} \Lambda/(p, T^{p^n - p^e})\right) \oplus \left(\bigoplus_{j} \Lambda/(p, T^{\deg g_j})\right) \\ &\simeq (\mathbb{Z}/p\mathbb{Z})^{s(p^n - p^e) + l}. \end{aligned}$$

Therefore the rank is bounded $\Leftrightarrow s = 0$. This proves Lemma 13.20. $\square$

We now return to the proof of Theorem 13.13. We have an exact sequence

$$0 \to A \to Y_e \to E \to B \to 0$$

where A and B are finite and E is as in Proposition 13.19. We know the order of $E/\nu_{n,e}E$ for all $n > n_0$. It remains to obtain similar information about Y_e. At the moment, all we can conclude is that $e_n = mp^n + ln + c_n$, where c_n is bounded. The following lemma solves our problem.

Lemma 13.21. *Suppose Y and E are Λ-modules with $Y \sim E$ such that $Y/\nu_{n,e}Y$ is finite for all $n \geq e$. Then, for some constant c and some n_0,*

$$|Y/\nu_{n,e}Y| = p^c|E/\nu_{n,e}E| \quad \textit{for all } n \geq n_0.$$

Proof. We have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & v_{n,e}Y \arrow[r] \arrow[d, "\phi_n'"] & Y \arrow[r] \arrow[d, "\phi"] & Y/v_{n,e}Y \arrow[r] \arrow[d, "\phi_n''"] & 0 \\
0 \arrow[r] & v_{n,e}E \arrow[r] & E \arrow[r] & E/v_{n,e}E \arrow[r] & 0
\end{tikzcd}$$

There are the following inequalities.

(i) $|\mathrm{Ker}\ \phi_n'| \leq |\mathrm{Ker}\ \phi|$
(ii) $|\mathrm{Coker}\ \phi_n'| \leq |\mathrm{Coker}\ \phi|$
(iii) $|\mathrm{Coker}\ \phi_n''| \leq |\mathrm{Coker}\ \phi|$
(iv) $|\mathrm{Ker}\ \phi_n''| \leq |\mathrm{Ker}\ \phi| \cdot |\mathrm{Coker}\ \phi|$.

Inequality (i) is obvious. (iii) holds because representatives of Coker ϕ give representatives for Coker ϕ_n''. For (ii), multiply the representatives of Coker ϕ by $v_{n,e}$.

By the Snake Lemma (see Clayburgh [1], or any book on homological algebra), there is a long exact sequence

$$0 \to \mathrm{Ker}\ \phi_n' \to \mathrm{Ker}\ \phi \to \mathrm{Ker}\ \phi_n'' \to \mathrm{Coker}\ \phi_n' \to \mathrm{Coker}\ \phi \to \mathrm{Coker}\ \phi_n'' \to 0.$$

Everything is straightforward except the map $\mathrm{Ker}\ \phi_n'' \to \mathrm{Coker}\ \phi_n'$. Let $x \in \mathrm{Ker}\ \phi_n''$. There exists $y \in Y$ which maps to x. Since $\phi(y)$ maps to 0 in $E/v_{n,e}E$ by the commutativity of the diagram, we must have $\phi(y) \in v_{n,e}E$. One checks that $\phi(y)$ mod $\phi_n'(v_{n,e}Y)$ depends only on x. The map $x \mapsto \phi(y)$ is the desired one. It remains to check exactness. This is left to the reader.

It follows that

$$|\mathrm{Ker}\ \phi_n''| \leq |\mathrm{Ker}\ \phi||\mathrm{Coker}\ \phi_n'| \leq |\mathrm{Ker}\ \phi||\mathrm{Coker}\ \phi|,$$

by (ii). This proves (iv).

Now suppose $m \geq n \geq 0$. We have the following inequalities.

(a) $|\mathrm{Ker}\ \phi_n'| \geq |\mathrm{Ker}\ \phi_m'|$
(b) $|\mathrm{Coker}\ \phi_n'| \geq |\mathrm{Coker}\ \phi_m'|$
(c) $|\mathrm{Coker}\ \phi_n''| \leq |\mathrm{Coker}\ \phi_m''|$.

For (a), observe that $v_{m,e} = (v_{m,e}/v_{n,e})v_{n,e}$. Therefore $v_{m,e}Y \subseteq v_{n,e}Y$, so $\ker \phi_m' \subseteq \mathrm{Ker}\ \phi_n'$. For (b), let $v_{m,e}y \in v_{m,e}E$. Let $z \in v_{n,e}E$ be a representative for $v_{n,e}y$ in Coker ϕ_n'. Then

$$v_{n,e}y - z = \phi(v_{n,e}x) \quad \text{for some } x \in Y.$$

Multiply by $v_{m,e}/v_{n,e}$ to obtain

$$v_{m,e}y - \left(\frac{v_{m,e}}{v_{n,e}}\right)z = \phi(v_{m,e}x) = \phi_m'(v_{m,e}x).$$

So $(v_{m,e}/v_{n,e})$ times representatives for Coker ϕ'_n gives representatives for Coker ϕ'_m. This proves (b). Since $v_{m,e}E \subseteq v_{n,e}E$, inequality (c) follows easily.

By (i), (ii), (iii), (a), (b), (c), the orders of Ker ϕ'_n, Coker ϕ'_n, and Coker ϕ''_n are constant for $n \geq n_0$, for some n_0. It remains to treat Ker ϕ''_n. By the Snake Lemma,

$$|\text{Ker } \phi'_n||\text{Ker } \phi''_n||\text{Coker } \phi| = |\text{Ker } \phi||\text{Coker } \phi'_n||\text{Coker } \phi''_n|.$$

(In any exact sequence, the alternating product of the orders is 1; proof: replace $0 \to A \to B \to \cdots$ by $0 \to B/A \to \cdots$ and use induction on the length of the sequence). It follows that $|\text{Ker } \phi''_n|$ must be constant for $n \geq n_0$. Lemma 13.21 follows easily. □

We therefore have E as in Proposition 13.19, integers $\lambda \geq 0$, $\mu \geq 0$, and v, and an integer n_0 such that

$$\begin{aligned} p^{e_n} = |X_n| &= |X/Y_e||Y_e/v_{n,e}Y_e| \\ &= (\text{const.})|E/v_{n,e}E| \\ &= p^{\lambda n + \mu p^n + v}, \quad \text{for all } n > n_0. \end{aligned}$$

This completes the proof of Theorem 13.13. □

§13.4 Consequences

Proposition 13.22. *Suppose K_∞/K is a $\mathbb{Z}_p$-extension in which exactly one prime is ramified, and assume it is totally ramified. Then*

$$A_n \simeq X_n \simeq X/((1 + T)^{p^n} - 1)X$$

and

$$p \nmid h_0 \Leftrightarrow p \nmid h_n \quad \textit{for all } n \geq 0.$$

Proof. Since K_∞/K satisfies the "assumption" in the proof of Theorem 13.13, we may use Lemma 13.15. We have $s = 1$, so $Y_0 = TX$ and $Y_n = ((1 + T)^{p^n} - 1)X$. This proves the first part. If $p \nmid h_0$, then $X/TX = 0$, so $X/(p, T)X = 0$. By Lemma 13.16, $X = 0$. This completes the proof. □

Of course, the last statement of the proposition also follows from Theorems 10.1 and 10.4, and, in a special case, from Exercise 7.4.

Proposition 13.23. $\mu = 0 \Leftrightarrow p$-rank$(A_n)$ *is bounded as* $n \to \infty$.

Proof. We have $Y_e \sim E$ with E as in Lemma 13.20. By the lemma, $\mu = 0 \Leftrightarrow$ p-rank$(E/v_{n,e}E)$ is bounded. From the proof of Lemma 13.21, we have an exact sequence

$$0 \to C_n \to Y_e/v_{n,e}Y \to E/v_{n,e}E \to B_n \to 0$$

with $|C_n|$ and $|B_n|$ bounded independent of n. It follows that

$$\mu = 0 \Leftrightarrow p\text{-rank}(Y_e/\nu_{n,e}Y_e) \text{ is bounded.}$$

But

$$A_n \simeq X_n = X/\nu_{n,e}Y_e$$

and X/Y_e is finite. The result follows easily. □

Suppose each K_n is a CM-field. Then K_∞^+/K^+ is a $\mathbb{Z}_p$-extension (cyclotomic if Leopoldt's conjecture is true, by Theorem 13.4). If p is odd we may decompose the p-Sylow subgroup A_n of the class group of K_n as

$$A_n = A_n^+ \oplus A_n^-.$$

Also,

$$X_n = X_n^+ \oplus X_n^-,$$

hence

$$X = X^+ \oplus X^-.$$

We obtain, as in the proof of Theorem 13.13,

$$A_n^\pm \simeq X_n^\pm \simeq X^\pm/\nu_{n,e}Y^\pm.$$

If $p^{e_n^\pm}$ is the exact power of p dividing $h_n^\pm$, then

$$e_n = e_n^+ + e_n^-.$$

We obtain

$$e_n^\pm = \lambda^\pm n + \mu^\pm p^n + \nu^\pm \quad \text{for } n \geq n_0^\pm,$$

with

$$\lambda = \lambda^+ + \lambda^-, \qquad \mu = \mu^+ + \mu^-, \qquad \nu = \nu^+ + \nu^-.$$

The analogue of Proposition 13.23 applies, so

$$\mu^\pm = 0 \Leftrightarrow p\text{-rank}(A_n^\pm) \text{ is bounded.}$$

If $p = 2$, we cannot decompose $A_n^\pm$. However, if

$$A_n^- = \{a \mid Ja = -a\} \quad (J = \text{complex conjugation})$$

then everything in the proof of Theorem 13.13 works for A_n^-, X_n^-, etc. We may obtain e_n^+ by looking at the class group $A_n(K_n^+)$ of K_n^+, rather than A_n^+ (cf. Proposition 10.12). We again obtain

$$e_n^\pm = \lambda^\pm n + \mu^\pm 2^n + \nu^\pm.$$

From the exact sequence

$$0 \to A_n^- \to A_n \xrightarrow{1+J} A(K_n^+) \to 0$$

we have $\mu = \mu^+ + \mu^-$, etc. We also have, as above,

$$\mu^+ = 0 \Leftrightarrow \text{2-rank } A(K_n^+) \text{ is bounded,}$$
$$\mu^- = 0 \Leftrightarrow \text{2-rank } A_n^- \text{ is bounded.}$$

Proposition 13.24. *Let p be prime. Suppose K is a CM-field with $\zeta_p \in K$ and let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension. Then*

$$\mu = 0 \Leftrightarrow \mu^- = 0.$$

PROOF. "$\Rightarrow$" is trivial. For "$\Leftarrow$", we know that $\mu^- = 0 \Rightarrow p$-rank A_n^- is bounded. By Theorem 10.11 and Proposition 10.12, p-rank A_n^+ (or 2-rank $A(K_n^+)$) is bounded, which implies $\mu^+ = 0$. This completes the proof. □

This result also completes the proof that $\mu = 0$ for abelian number fields (Theorem 7.15), since in Chapter 7 we showed that $\mu^- = 0$ for all such fields.

Proposition 13.25. *Suppose K_∞/K is a $\mathbb{Z}_p$-extension and assume $\mu = 0$. Then*

$$X \simeq \varprojlim A_n \simeq \mathbb{Z}_p^\lambda \oplus (\textit{finite p-group})$$

as $\mathbb{Z}_p$-modules.

PROOF. We have

$$X \sim E = \bigoplus_j \Lambda/(g_j(T))$$

where each g_j is distinguished and $\sum \deg g_j = \lambda$. By the division algorithm,

$$\Lambda/(g_j(T)) \simeq \mathbb{Z}_p^{\deg g_j}.$$

Therefore

$$E \simeq \mathbb{Z}_p^\lambda.$$

Since X is a $\mathbb{Z}_p$-module, which is finitely generated since E is finitely generated, the result follows from the structure theorem for modules over principal ideal domains. □

Proposition 13.26. *Let p be odd. Suppose K is a CM-field and K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension of K. Then the map*

$$A_n^- \to A_{n+1}^-$$

is injective.

Remarks. The map $A_n^+ \to A_{n+1}^+$ is not necessarily injective (Exercise 13.4). If $p = 2$, $A_n^- \to A_{n+1}^-$ is not necessarily injective (Exercise 13.3). Since the map of ideal class groups $C_n \to C_{n+1}$ followed by the norm is the pth power map, the kernel is always in the p-Sylow subgroup.

PROOF. Suppose I is an ideal in A_n which becomes principal in K_{n+1}, so

$$I = (\alpha) \quad \text{with } \alpha \in K_{n+1}.$$

Let σ be a generator for $\mathrm{Gal}(K_{n+1}/K_n)$. Then

$$(\alpha^{\sigma-1}) = \frac{I^\sigma}{I} = (1).$$

Consequently

$$\alpha^{\sigma-1} = \varepsilon \in E_{n+1} = \text{units of } K_{n+1}.$$

Let N be the norm for K_{n+1}/K_n. Then

$$N\varepsilon = (N\alpha)^{\sigma-1} = 1.$$

For those who know cohomology of groups: we easily obtain an injection

$$\mathrm{Ker}(A_n \to A_{n+1}) \to H^1(\mathrm{Gal}(K_{n+1}/K_n), E_{n+1}).$$

Now suppose I represents a class in A_n^-. Let J denote complex conjugation. Then

$$I^{1+J} = (\beta), \quad \text{with } \beta \in K_n \quad (\text{so } \beta^\sigma = \beta),$$

hence

$$\alpha^{1+J} = \beta\eta \quad \text{with } \eta \in E_{n+1}.$$

Let

$$\alpha_1 = \frac{\alpha^2}{\eta},$$

and

$$\varepsilon_1 = \alpha_1^{\sigma-1} = \frac{\varepsilon^2}{\eta^{\sigma-1}} \in E_{n+1}.$$

Then

$$\varepsilon_1^{1+J} = (\alpha_1^{1+J})^{\sigma-1} = (\beta^2)^{\sigma-1}(\eta^{\sigma-1})^{1-J} = (\eta^{\sigma-1})^{1-J} \in E_{n+1}^-.$$

But

$$E_{n+1}^- = W_{n+1} = \text{roots of 1 in } K_{n+1}$$

by Lemma 1.6. Therefore some power of ε_1 is killed by $1 + J$, hence is a root of 1, again by Lemma 1.6. Consequently

$$\varepsilon_1 \in W_{n+1}.$$

(Alternatively, since $p \neq 2$ we may assume $\beta \in K_n^+$ (see Theorem 10.3) and consequently $\eta = \alpha^{1+J}/\beta$ is real. Therefore $\eta^{1-J} = 1$, so Lemma 1.6 applies directly to ε_1). Also, observe that

$$N\varepsilon_1 = (N\alpha_1)^{\sigma-1} = 1.$$

Lemma 13.27. *If $\varepsilon_1 \in W_{n+1}$ and $N\varepsilon_1 = 1$ then $\varepsilon_1 = \varepsilon_2^{\sigma-1}$ with $\varepsilon_2 \in W_{n+1}$ (so $H^1(\mathrm{Gal}(K_{n+1}/K_n), W_{n+1}) = 0$).*

PROOF. Hilbert's Theorem 90 tells us that $\varepsilon_1 = y^{\sigma-1}$ with $y \in K_{n+1}$, but we already know this with $y = \alpha_1$. We want $y \in W_{n+1}$. Consider the following two sequences:

$$1 \to W_n \to W_{n+1} \xrightarrow{\sigma-1} W_{n+1}^{\sigma-1} \to 1$$

$$1 \to W_{n+1} \cap \operatorname{Ker} N \to W_{n+1} \xrightarrow{N} W_n \to 1.$$

The first is obviously exact. The second is slightly more difficult. If $\zeta_p \notin K_0$ then $\zeta_p \notin K_m$ for all m. Otherwise, a nontrivial subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ would be in $\operatorname{Gal}(K_\infty/K_0)$, which is impossible. Since N: $W_n \to W_n$ is the pth power map, it is surjective in this case, hence N: $W_{n+1} \to W_n$ is surjective (in fact, $W_{n+1} = W_n$). If $\zeta_p \in K_0$ then $K_{n+1} = K_n(\zeta)$, where $\zeta = \zeta_{p^m}$ for some $m \geq n+1$. Also, $W_{n+1} = \langle\zeta\rangle \times \langle\zeta_t\rangle$ for some t with $(p, t) = 1$, and $W_n = \langle\zeta^p\rangle \times \langle\zeta_t\rangle$. A trivial calculation shows that $N\zeta = \zeta^p$ and $N\zeta_t = \zeta_t^p$, hence $\langle N\zeta_t\rangle = \langle\zeta_t\rangle$. Therefore N is surjective in this case, so the second sequence is exact.

We obtain

$$|W_{n+1}^{\sigma-1}| = \frac{|W_{n+1}|}{|W_n|} = |W_{n+1} \cap \operatorname{Ker} N|.$$

Since

$$W_{n+1}^{\sigma-1} \subseteq W_{n+1} \cap \operatorname{Ker} N,$$

we have equality. This proves Lemma 13.27. □

We can now complete the proof of Proposition 13.26. We have

$$\alpha_1^{\sigma-1} = \varepsilon_1 = \varepsilon_2^{\sigma-1} \quad \text{with } \varepsilon_2 \in W_{n+1}.$$

Therefore

$$\left(\frac{\alpha_1}{\varepsilon_2}\right)^\sigma = \frac{\alpha_1}{\varepsilon_2},$$

so

$$\frac{\alpha_1}{\varepsilon_2} \in K_n.$$

But

$$\left(\frac{\alpha_1}{\varepsilon_2}\right) = (\alpha_1) = (\alpha^2) = I^2 \quad \text{in } K_{n+1}.$$

By unique factorization of ideals, we must have

$$\left(\frac{\alpha_1}{\varepsilon_2}\right) = I^2 \quad \text{in } K_n.$$

Since p is odd and I has p-power order in A_n^-, we must have I principal in K_n. This completes the proof of Proposition 13.26. □

Proposition 13.28. *Let p be odd, let K be a CM-field, and let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension. Then $X^- = \varprojlim A_n^-$ contains no finite Λ-submodules. Therefore there is an injection, with finite cokernel,*

$$X^- \hookrightarrow \bigoplus_i \Lambda/(p^{k_i}) \oplus \bigoplus_j \Lambda/(g_j(T)).$$

Proof. Suppose $F \subseteq X^-$ is a finite Λ-module. Let γ_0 be a generator of $\mathrm{Gal}(K_\infty/K)$. Since F is finite, $\gamma_0^{p^n}$ acts trivially on F for all sufficiently large n, say $n \geq n_0$. Suppose

$$0 \neq x = (\ldots, x_m, x_{m+1}, \ldots) \in F \subseteq \varprojlim A_n^-.$$

Then $x_{m+1} \mapsto x_m$ under the appropriate norm map, and $x_m \neq 0$ for all sufficiently large m, say $m \geq m_0$. Let m be larger than m_0 and n_0. By Proposition 13.26, $x_m \neq 0$ when lifted to A_{m+1}^-. Apply the map

$$1 + \gamma_0^{p^m} + \gamma_0^{2p^m} + \cdots + \gamma_0^{(p-1)p^m}$$

to x. Since $m \geq n_0$, it acts as p on x. Also, it is the norm from K_{m+1} to K_m, so it maps x_{m+1} to x_m. Therefore

$$px_{m+1} = x_m \neq 0, \quad \text{in } A_{m+1}^-,$$

so

$$px \neq 0.$$

It follows that multiplication by p is injective on the finite p-group F, so $F = 0$. This completes the proof. □

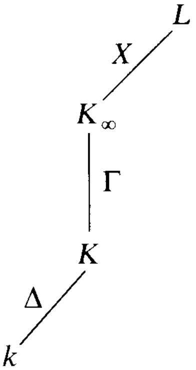
Corollary 13.29. *Let p be odd. Let K be a CM-field and let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension. If $\mu^- = 0$ then*

$$X^- \simeq \mathbb{Z}_p^{\lambda^-}.$$

Proof. Proposition 13.28 plus the analogue of Proposition 13.25 for X^-. □

Usually the finite kernel and cokernel in the pseudo-isomorphism make it difficult to obtain much information at finite levels of the $\mathbb{Z}_p$-extension. Proposition 13.28 is useful since it eliminates half the problem. For a situation where there is also a trivial cokernel, see Theorem 10.16.

In the above we have used the decomposition $X = X^+ \oplus X^-$ for odd primes. More generally, suppose we have the following situation



where Δ is a finite abelian group and $\mathrm{Gal}(K_\infty/K) \simeq \Delta \times \Gamma$. For example, $K = \mathbb{Q}(\zeta_p)$, $K_\infty = \mathbb{Q}(\zeta_{p^\infty})$, $k = \mathbb{Q}$, and $\Delta = (\mathbb{Z}/p\mathbb{Z})^\times$. Then Δ acts on X, since $\Delta \times \Gamma$ acts on X by conjugation in the same way as the action of Γ on X was defined. If p does not divide the order of Δ and if the values of the characters $\chi \in \hat{\Delta}$ are in $\mathbb{Z}_p$ (rather than an extension), then we may decompose X according to the idempotents ε_χ of $\mathbb{Z}_p[\Delta]$:

$$X = \bigoplus_\chi \varepsilon_\chi X.$$

For example, in the above we used $\Delta = \mathrm{Gal}(K/K^+)$ and $\varepsilon_\pm = (1 \pm J)/2$. In the present case we obtain

$$\varepsilon_\chi X \sim \bigoplus_i \Lambda/(p^{k_i^\chi}) \oplus \bigoplus_j \Lambda/(g_j^\chi(T))$$

for some integers k_i^χ and distinguished polynomials $g_j^\chi(T)$. We also have $\mu = \sum \mu_\chi$, etc.

Returning to the general case, we consider the $\mathbb{C}_p$-vector space

$$V = X \otimes_{\mathbb{Z}_p} \mathbb{C}_p.$$

If

$$X \sim \bigoplus \Lambda/(p^{k_i}) \oplus \bigoplus \Lambda/(g_j(T))$$

then it is easy to see that

$$V \simeq \bigoplus_j \mathbb{C}_p[T]/(g_j(T)),$$

which is a finite-dimensional vector space. The group Γ acts on V; the generator γ_0 acts as $1 + T$. So

$$g(T) = \prod g_j(T)$$

is the characteristic polynomial for $\gamma_0 - 1$.

If $\Delta = \mathrm{Gal}(K/k)$ is as above, with no assumption on $|\Delta|$ or the values of $\chi \in \hat{\Delta}$, then we may decompose

$$V = \sum_\chi \varepsilon_\chi V.$$

Then

$$g(T) = \prod_\chi g_\chi(T),$$

where $g_\chi(T)$ is the characteristic polynomial of $\gamma_0 - 1$ on $\varepsilon_\chi V$. We shall discuss the significance of these polynomials when we treat the main conjecture.

§13.5 The Maximal Abelian p-extension Unramified Outside p

Often it is more convenient to work with an extension larger than the p-class field and allow ramification above p. This is what we did in the proof of Theorem 10.13. In many respects, the theory is more natural in this context, especially from the point of view of Kummer theory. In this section we sketch the basic set-up, leaving the details to the reader. The proofs are very similar to those in Chapter 10.

We start with a totally real field F. Let p be odd, let $K_0 = F(\zeta_p)$, and let K_∞/K_0 be the cyclotomic $\mathbb{Z}_p$-extension. Let M_∞ be the maximal abelian p-extension of K_∞ which is unramified outside p, and let

$$\mathscr{X}_\infty = \operatorname{Gal}(M_\infty/K_\infty).$$

Then $\mathscr{X}_\infty$ is a Λ-module in the natural way (just as for $X = \operatorname{Gal}(L_\infty/K_\infty)$). Let M_n be the maximal abelian p-extension of K_n which is unramified outside p. Clearly $M_n \supseteq K_\infty$. We have

$$\operatorname{Gal}(M_n/K_\infty) \simeq \mathscr{X}_\infty/\omega_n\mathscr{X}_\infty,$$

where $\omega_n = \gamma_0^{p^n} - 1 = (1 + T)^{p^n} - 1$. The proof is essentially the same as for Lemma 13.15, namely computing commutator subgroups, but in the present case we do not have to consider inertia groups. From Corollary 13.6 we know that

$$\operatorname{Gal}(M_n/K_0) \simeq \mathbb{Z}_p^{r_2p^n+1+\delta_n} \times \text{(finite group)},$$

where $r_2 = r_2(K_0)$ and δ_n is the defect in Leopoldt's Conjecture (see Theorem 13.4). Therefore

$$\mathscr{X}_\infty/\omega_n\mathscr{X}_\infty \simeq \mathbb{Z}_p^{r_2p^n+\delta_n} \times \text{(finite group)}.$$

By Lemma 13.16, $\mathscr{X}_\infty$ is a finitely generated Λ-module, so

$$\mathscr{X}_\infty \sim \Lambda^a \oplus (\Lambda\text{-torsion})$$

for some $a \geq 0$.

Lemma 13.30. *δ_n is bounded, independent of n.*

Proof. Suppose $\delta_n > 0$ for some n. Let $\varepsilon_1, \ldots, \varepsilon_r$ be a basis for $E_1 = E_1(K_n)$. We may assume $\varepsilon_{\delta_n+1}, \ldots, \varepsilon_r$ are independent and generate $\bar{E}_1$ over $\mathbb{Z}_p$. Then

$$\varepsilon_i = \prod_{j>\delta_n} \varepsilon_j^{a_{ij}}, \quad \text{with } a_{ij} \in \mathbb{Z}_p,$$

for $1 \leq i \leq \delta_n$. Let a'_{ij} be the nth partial sum of the p-adic expansion of a_{ij}. Let

$$\eta_i = \varepsilon_i \prod_j \varepsilon_j^{-a'_{ij}} \in E_1, \qquad 1 \leq i \leq \delta_n.$$

Then η_i is a p^nth power in $\bar{E}_1 \subseteq \prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}$, and $\eta_1, \ldots, \eta_{\delta_n}$ generate a subgroup $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$ of $K_n^\times/(K_n^\times)^{p^n}$. Since $\zeta_p \in K_0$ by assumption, $\zeta_{p^n} \in K_n$. Therefore the extension

$$K_n(\{\eta_i^{1/p^n}\})/K_n$$

has Galois group $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$. Clearly this extension is unramified outside p. Since each η_i is a p^nth power in $U_{1,\mathfrak{p}}$ for each $\mathfrak{p}|p$, these primes split completely hence do not ramify. Therefore the Galois group X_n of the Hilbert p-class field of K_n has a quotient isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$. In the decomposition of

X, the terms of the form $\Lambda/(p^k)$ cannot account for this for large n. The term of the form $\bigoplus_j \Lambda/(g_j(T))$ can only yield $(\mathbb{Z}/p^n\mathbb{Z})^\lambda$, where $\lambda = \sum \deg g_j$. Therefore $\delta_n \leq \lambda$. This completes the proof. □

If $\zeta_p \notin K_0$, the lemma is still true. Simply adjoin ζ_p and use the easily proved fact that if $K \subseteq L$ then $\delta(K) \leq \delta(L)$.

The above result perhaps could have been conjectured from Theorem 7.10 (although we already know $\delta_n = 0$ in that situation). Intuitively, the number δ_n should be approximately the number of occurrences of $L_p(1, \chi) = 0$ for K_n^+. Since each series $f(T, \theta)$ has only finitely many zeros,

$$L_p(1, \theta\psi) = f(\zeta_\psi(1 + q_0) - 1, \theta) \neq 0$$

when ψ has large enough conductor. So the number of χ with $L_p(1, \chi) = 0$ is bounded.

By the lemma,

$$\mathbb{Z}_p\text{-rank } \mathscr{X}_\infty/\omega_n\mathscr{X}_\infty = r_2 p^n + O(1).$$

By the structure theorem for $\mathscr{X}_\infty$, we see that the Λ-torsion contributes only bounded $\mathbb{Z}_p$-rank (at most λ) and $\Lambda^a/\omega_n\Lambda^a$ yields ap^n. Therefore we have proved the following.

Theorem 13.31. *$\mathscr{X}_\infty \sim \Lambda^{r_2} \oplus$ (Λ-torsion).* □

One advantage of using $\mathscr{X}_\infty$ rather than X is that it is easier to describe how L_∞ is generated. Since all p-power roots of unity are in K_∞, M_∞/K_∞ is a Kummer extension. There is a subgroup

$$V \subseteq K_\infty^\times \otimes_\mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p$$

$$V = \{a \otimes p^{-n} \mid \text{various } n \geq 0 \text{ and } a \in K_\infty^\times\}$$

(it is not hard to see that all elements of $K_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ are of the form $a \otimes p^{-n}$) such that

$$M_\infty = K_\infty(\{a^{1/p^n}\}).$$

There is a Kummer pairing

$$\mathscr{X}_\infty \times V \to W_{p^\infty} = p\text{-power roots of unity},$$

just as in Chapter 10. In particular,

$$(\sigma x, \sigma v) = (x, v)^\sigma, \qquad \sigma \in \mathrm{Gal}(K_\infty/F).$$

Let I_m be the group of fractional ideals of K_m and let $I_\infty = \bigcup I_m$. Since $a \otimes p^{-n}$ gives an extension unramified outside p, and since $a \in K_m$ for some m, it follows that

$$(a) = B_1^{p^n} \cdot B_2 \text{ in some } I_m,$$

where $B_1 \in I_m$ and B_2 is a product of primes above p. Since all primes above p are infinitely ramified in a cyclotomic $\mathbb{Z}_p$-extension, B_2 is a p^nth power in I_∞. Hence we may assume

$$(a) = B_1^{p^n}.$$

We obtain a map

$$V \to A_\infty = \varinjlim A_n$$
$$a \otimes p^{-n} \mapsto \text{class of } B_1.$$

It is not hard to see that this map is well-defined, i.e., independent of m and the representation $a \otimes p^{-n}$. It is also surjective, since $A \in A_\infty \Rightarrow A^{p^n} = 1$ for some n (see Exercise 9.1). As in Chapter 10, the kernel is contained in

$$E_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p,$$

where $E_\infty = \bigcup E(K_n)$. Since we are allowing ramification above p,

$$E_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \subseteq V,$$

so it follows that this gives the kernel (cf. Theorem 10.13, where the situation is essentially the same). We now have an exact sequence

$$1 \to E_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to V \to A_\infty \to 1.$$

Let $\Delta = \mathrm{Gal}(K_0/F)$, which is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. For $i \in \mathbb{Z}$, ω^i is a character of Δ ($i \equiv j \bmod |\Delta| \Leftrightarrow \omega^i = \omega^j$ on Δ). Let

$$\varepsilon_i = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \omega^{-i}(\delta)\delta.$$

Everything decomposes via these idempotents. W_{p^∞} is in the ε_1 component. If i is odd and $i \not\equiv 1 \bmod |\Delta|$, then $\varepsilon_i(E_\infty \otimes \mathbb{Q}_p/\mathbb{Z}_p) = 0$, since $[E : WE^+] = 1$ or 2 for each K_n. We obtain

$$\varepsilon_i V \simeq \varepsilon_i A_\infty, \qquad i \text{ odd}, i \not\equiv 1 \bmod |\Delta|.$$

Note that by Proposition 13.26, $\varepsilon_i A_\infty = \bigcup \varepsilon_i A_n$. As in Chapter 10,

$$\varepsilon_j \mathscr{X}_\infty \times \varepsilon_i V \to W_{p^\infty},$$

is nondegenerate, hence

$$\varepsilon_j \mathscr{X}_\infty \times \varepsilon_i A_\infty \to W_{p^\infty}, \qquad \begin{array}{l} i + j \equiv 1 \bmod |\Delta| \\ i \text{ odd}, i \not\equiv 1 \bmod |\Delta|, \end{array}$$

is nondegenerate. Therefore

$$\varepsilon_j \mathscr{X}_\infty \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\varepsilon_i A_\infty, W_{p^\infty}),$$

where $\mathrm{Gal}(K_\infty/F)$ acts via $(\sigma f)(a) = \sigma(f(\sigma^{-1}a)$ (cf. Exercise 10.8).

This last equation is often written in another form. Let

$$T = \varprojlim W_{p^{n+1}}$$

where the inverse limit is taken with respect to the pth power map (which is the same as the norm map from $\mathbb{Q}(\zeta_{p^{n+1}})$ to $\mathbb{Q}(\zeta_{p^n})$). Then

$$T \simeq \mathbb{Z}_p, \text{ as abelian groups,}$$

but the Galois group acts via

$$\sigma_a(t) = at \quad \text{for } a \in \Delta \times (1 + p\mathbb{Z}_p) \subseteq \mathbb{Z}_p^\times,$$

where we are writing T additively. Let

$$T^{(-1)} = \operatorname{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p)$$

with the Galois action on Hom as above. Then

$$T^{(-1)} \simeq \mathbb{Z}_p, \text{ as abelian groups.}$$

If $f \in T^{(-1)}$ and $t \in T$ then, since σ_a acts trivially on $\mathbb{Z}_p$,

$$(\sigma_a f)(t) = \sigma_a(f(\sigma_a^{-1}t)) = f(a^{-1}t) = a^{-1}f(t),$$

so

$$\sigma_a f = a^{-1}f.$$

It follows that

$$T \otimes_{\mathbb{Z}_p} T^{(-1)} \simeq \mathbb{Z}_p, \text{ with trivial Galois action.}$$

Define the "twist" $\varepsilon_j \mathscr{X}_\infty(-1)$ by

$$\varepsilon_j \mathscr{X}_\infty(-1) = \varepsilon_j \mathscr{X}_\infty \otimes_{\mathbb{Z}_p} T^{(-1)}.$$

This is the same as $\varepsilon_j \mathscr{X}_\infty$ as a $\mathbb{Z}_p$-module but the Galois action has been changed:

$$\sigma_a(x \otimes f) = \sigma_a(x) \otimes a^{-1}f = \omega^j(a)a^{-1}(x \otimes f).$$

Proposition 13.32. $\varepsilon_j \mathscr{X}_\infty(-1) \simeq \operatorname{Hom}_{\mathbb{Z}_p}(\varepsilon_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ *as* Λ-*modules, where* $i + j \equiv 1 \bmod |\Delta|$, *i is odd, and* $i \not\equiv 1 \bmod |\Delta|$.

Proof. We shall show more generally that

$$\operatorname{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \operatorname{Hom}_{\mathbb{Z}_p}(B, W_{p^\infty}) \otimes_{\mathbb{Z}_p} T^{(-1)}$$

for any Λ-module B. There is an isomorphism of abelian groups

$$\mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\phi} W_{p^\infty}$$

$$\frac{a}{p^n} \mapsto \zeta_{p^n}^a.$$

Choose a generator t_0 for $T^{(-1)}$ as a $\mathbb{Z}_p$-module. If we ignore the Galois action, we obtain an isomorphism by mapping

$$h \mapsto (\phi h) \otimes t_0,$$

for $h \in \operatorname{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$. Let $\sigma = \sigma_a \in \Gamma$. Then

$$(\sigma h)(b) = \sigma(h(\sigma^{-1}b)) = h(\sigma^{-1}b),$$

and

$$\begin{aligned}\sigma(\phi h \otimes t_0) &= \sigma\phi h\sigma^{-1} \otimes \sigma t_0\\ &= a\phi h\sigma^{-1} \otimes a^{-1}t_0\\ &= \phi h\sigma^{-1} \otimes t_0.\end{aligned}$$

Therefore

$$\sigma h \mapsto \sigma(\phi h \otimes t_0)$$

under the above isomorphism, so the Galois actions are compatible. This completes the proof. □

The proposition says that the discrete group $\varepsilon_i A_\infty$ and the compact group $\varepsilon_j \mathscr{X}_\infty(-1)$ are dual in the sense of Pontryagin.

§13.6 The Main Conjecture

For simplicity, we assume $p \neq 2$ in this section. Consider the $\mathbb{Z}_p$-extension $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}(\zeta_p)$. In Theorem 10.16 we showed that if Vandiver's Conjecture holds for p then

$$\varepsilon_i X \simeq \Lambda/(f(T, \omega^{1-i}))$$

for $i = 3, 5, \ldots, p-2$, where

$$f((1+p)^s - 1, \omega^{1-i}) = L_p(s, \omega^{1-i}).$$

Factor $f(T, \omega^{1-i}) = p^{\mu_i} g_i(T) U_i(T)$ with g_i distinguished and $U_i \in \Lambda^\times$. We know that $\mu_i = 0$ by Theorem 7.15. Therefore

$$\varepsilon_i X \simeq \Lambda/(g_i(T)),$$

which is in the form of Theorem 13.12. So in this case the distinguished polynomial in the decomposition of $\varepsilon_i X$ is essentially the p-adic L-function. This is conjectured to happen more generally.

Let F be totally real and let $K_0 = F(\zeta_p)$, $K_\infty = F(\zeta_{p^\infty})$. Let

$$\Delta = \operatorname{Gal}(K_0/F) \subseteq (\mathbb{Z}/p\mathbb{Z})^\times.$$

Let $\chi \in \hat{\Delta}$ be odd (i.e., $\chi(J) = -1$). Then

$$\varepsilon_\chi X \hookrightarrow \bigoplus_i \Lambda/(p^{k_i^\chi}) \oplus \bigoplus_j \Lambda/(g_j^\chi(T))$$

with finite cokernel. Let $\mu_\chi = \sum k_i^\chi$ and let

$$g^\chi(T) = p^{\mu_\chi} \prod_j g_j^\chi(T).$$

It has been shown (see Barsky [4], Cassou-Noguès [4], Deligne–Ribet [1]) that there exists a p-adic L-function $L_p(s, \omega\chi^{-1})$ for the even character $\omega\chi^{-1}$. If $F = \mathbb{Q}$, this is the usual p-adic L-function. For larger F, the existence is more difficult to establish. Let γ_0 be the generator of $\mathrm{Gal}(K_\infty/K_0)$ corresponding to $1 + T$. Define $\kappa_0 \in 1 + p\mathbb{Z}_p$ by $\gamma_0 \zeta_{p^n} = \zeta_{p^n}^{\kappa_0}$ for all $n \geq 1$. It has been shown that there is a power series $f_\chi \in \Lambda$ such that

$$L_p(s, \omega\chi^{-1}) = f_\chi(\kappa_0^s - 1), \qquad \chi \neq \omega.$$

The Main Conjecture (First Form). *$f_\chi(T) = g^\chi(T)U_\chi(T)$ with $U_\chi(T) \in \Lambda^\times$.*

We may also state a slightly different form. For simplicity, assume $F = \mathbb{Q}$, though any totally real field F could be used. Let $\chi \neq \omega$ be an odd Dirichlet character of the first kind (see Chapter 7, let K_χ be the associated field (see Chapter 3), and let $K_0 = K_\chi(\zeta_p)$, $K_\infty = (\zeta_{p^\infty})$. Let $\mathcal{O} \supseteq \mathbb{Z}_p$ contain the values of χ and let $f_\chi \in \mathcal{O}[[T]]$ satisfy

$$f_\chi(\kappa_0^s - 1) = L_p(s, \omega\chi^{-1}),$$

as in Theorem 7.10. Then

$$f_\chi(T) = p^{\mu_\chi} \tilde{f}_\chi(T) U_\chi(T)$$

with $U_\chi \in \mathcal{O}[[T]]^\times$, $\tilde{f}_\chi$ distinguished, and $\mu_\chi \geq 0$ (in the present case, $\mu_\chi = 0$ by Theorem 7.15).

Consider the $\mathbb{C}_p$-vector space

$$V = X \otimes_{\mathbb{Z}_p} \mathbb{C}_p$$

as at the end of Section 13.4, and let $g_\chi(T)$ be the characteristic polynomial for $\gamma_0 - 1$ acting on $V_\chi = \varepsilon_\chi V$.

The Main Conjecture (Second Form). $\tilde{f}_\chi(T) = g_\chi(T)$.

The advantage of this form is that we may consider a larger class of characters χ. The disadvantage is that we are no longer requiring the μ obtained from $\varepsilon_\chi X$ (when this module is defined) to equal the μ_χ obtained from f_χ. For abelian extensions of $\mathbb{Q}$ this makes no difference since both are 0.

The motivation for the main conjecture comes from the theory of curves over finite fields (or, function fields over finite fields). Let C be a curve (complete, nonsingular) of genus g over a field k of characteristic $l \neq p$ and let J be its Jacobian variety (if we were working over $\mathbb{C}$, J would be $\mathbb{C}^g$ modulo a lattice). Let J_p be the points on J of p-power order defined over the algebraic closure $\bar{k}$ of k. This is essentially the analogue of $A_\infty = \varinjlim A_n$ (or of $A_\infty^- = \bigcup A_n^-$) for cyclotomic $\mathbb{Z}_p$-extensions. Then

$$J_p \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{2g}, \text{ as abelian groups.}$$

Therefore (compare Corollary 13.29)

$$\mathrm{Hom}_{\mathbb{Z}_p}(J_p, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \mathbb{Z}_p^{2g}$$

and

$$\mathrm{Hom}_{\mathbb{Z}_p}(J_p, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^{2g}.$$

The Frobenius automorphism of $\bar{k}$ over k acts on this last space, and a classical theorem of Weil states that the characteristic polynomial is the numerator of the zeta function of C (see Weil [5]). Therefore, the Main Conjecture is an attempt to extend the analogy between number fields and function fields to this important situation.

The Main Conjecture (first form) has been proved by Mazur and Wiles for $F = \mathbb{Q}$, $K_0 = \mathbb{Q}(\zeta_p)$. In fact, they proved a slightly stronger statement, which we now briefly describe.

Let R be a commutative ring and let M be a finitely generated R-module. For some $r \in \mathbb{Z}$ and $B \subseteq R^r$, there is an exact sequence

$$0 \to B \xrightarrow{\phi} R^r \xrightarrow{\psi} M \to 0.$$

Consider the $r \times r$ matrices of the form

$$\Phi = \begin{pmatrix} \phi(b_1) \\ \vdots \\ \phi(b_r) \end{pmatrix}$$

where $(b_1, \ldots, b_r)$ runs through all r-tuples of elements of B. The *Fitting ideal* $F_R(M)$ (see Fitting [1], Mazur–Wiles [1] or Northcott [1]), is defined to be the ideal in R generated by the elements $\det(\Phi)$ for all such Φ. It may be shown that $F_R(M)$ is independent of the choices of r and ψ, hence depends only on M. It is not hard to show that if

$$\mathrm{Ann}(M) = \{a \in R \mid aM = 0\}$$

then

$$(\mathrm{Ann}(M))^r \subseteq F_R(M) \subseteq \mathrm{Ann}(M).$$

Examples. (1) $R = \mathbb{Z}$, $M =$ a finite abelian group. Then $F_R(M) = |M|\mathbb{Z}$.

(2) $M = R/I$, where I is an ideal of R. Then $F_R(M) = I$.

(3) $R = \Lambda$ and M satisfies

$$0 \to M \to \bigoplus_j \Lambda/(g_j(T)) \to (\text{finite}) \to 0.$$

Then it can be shown that

$$F_\Lambda(M) = \left(\prod g_j\right)\Lambda.$$

(4) If $M \to N$ is a surjective map of R-modules then $F_R(M) \subseteq F_R(N)$.

(5) If I is an ideal of R then

$$F_{R/I}(M/IM) = F_R(M) \bmod I.$$

(6) If $R = \mathbb{Z}_p[G]$ with $G \simeq \mathbb{Z}/p^n\mathbb{Z}$, then

$$F_R(M) = F_R(\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)),$$

where Hom is an R-module via

$$(\sigma f)(m) = \sigma(f(\sigma^{-1}m)) = f(\sigma^{-1}m) \quad \text{for } \sigma \in G.$$

Let $i \not\equiv 1 \bmod p-1$ be odd. Then there exists $f_{\omega^i}(T) \in \Lambda$ such that

$$f_{\omega^i}((1+p)^s - 1) = L_p(-s, \omega^{1-i}).$$

Let ε_i be the idempotent and recall that

$$\varepsilon_i A_\infty = \varinjlim \varepsilon_i A_n = \bigcup \varepsilon_i A_n.$$

Define

$$X_\infty^{(i)} = \mathrm{Hom}_{\mathbb{Z}_p}(\varepsilon_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p).$$

It can be shown that if $\varepsilon_i X \sim \bigoplus \Lambda/(g_j(T))$ then $X_\infty^{(i)} \sim \bigoplus \Lambda/(\tilde{g}_j(T))$, where

$$\tilde{g}_j(T) = g_j((1+T)^{-1} - 1)$$

(i.e., γ_0 is replaced by γ_0^{-1}). See Iwasawa [25, p. 250], where a slightly different Galois action is used.

Theorem (Mazur–Wiles). *Let $i \not\equiv 1 \bmod p-1$ be odd. Then*

(i) $F_\Lambda X_\infty^{(i)} = (f_{\omega^i}(T))$,

(ii) $F_{\Lambda/(P_n(T))}(\varepsilon_i A_n) = F_{\Lambda/(P_n(T))}(X_\infty^{(i)}/P_n(T)X_\infty^{(i)})$

$$= (f_{\omega^i}(T) \bmod P_n(T)),$$

where $P_n(T) = (1+T)^{p^n} - 1$.

By Example 3, part (i) yields the main conjecture. Note that $(f_{\omega^i}(T) \bmod P_n(T))$ is essentially part of the Stickelberger ideal (see Chapters 6 and 7; the difference is that γ_0 is replaced by γ_0^{-1}). So this result identifies the Stickelberger ideal. If we assume Vandiver's conjecture, then we are in the situation of Example 2 above. But there are often many noncyclic modules which give the same fitting ideal as a cyclic module gives, as shown by Example 1. So the theorem does not imply Vandiver's conjecture or the cyclicity of the class group as a module over the group ring.

The proof uses delicate techniques from algebraic geometry and the theory of modular curves to construct unramified extensions of $\mathbb{Q}(\zeta_{p^{n+1}})$ for each n. This makes $X_\infty^{(i)}$ big enough that $F_\Lambda(X_\infty^{(i)}) \subseteq (f_{\omega^i}(T))$ for each i. If

$$X_\infty^{(i)} \hookrightarrow \bigoplus \Lambda/(\tilde{g}_j(T))$$

with finite cokernel, then

$$F_\Lambda(X_\infty^{(i)}) = \left(\prod \tilde{g}_j(T)\right) \overset{\text{def}}{=} (\tilde{g}_{\omega^i}(T)).$$

Hence

$$f_{\omega^i}(T) \mid \tilde{g}_{\omega^i}(T).$$

Therefore $\deg_w f_{\omega^i} \leq \deg_w \tilde{g}_{\omega^i}$, where $\deg_w$ denotes the Weierstrass degree, which is the degree of the distinguished polynomial in the Weierstrass decomposition. But $\lambda^- = \sum_i \deg_w f_{\omega^i}$ by Theorem 7.14. Also

$$\lambda^- = \sum_i \deg_w \tilde{g}_{\omega^i},$$

as in the proof of Theorem 13.13. Therefore

$$\deg_w f_{\omega^i} = \deg_w \tilde{g}_{\omega^i},$$

so

$$f_{\omega^i} = (\tilde{g}_{\omega^i})(\text{unit}).$$

This yields (i). Of course, the main part of the proof is the construction of sufficiently many unramified extensions. The techniques are an extension of those used to prove Ribet's converse to Herbrand's theorem (Theorem 6.18). For further details we must refer the reader to the paper of Mazur–Wiles [1] or to Coates' Bourbaki talk [8].

One application is the following result (compare Proposition 6.16):

$$|\varepsilon_i A_0| = p\text{-part of } B_{1,\omega^{-i}} (i \not\equiv 1 \bmod p-1, i \text{ odd}).$$

This follows from (ii). Since $\Lambda/(P_0(T)) = \mathbb{Z}_p$, the Fitting ideal gives the order, as in Example 1. But

$$f_{\omega^i}(T) \equiv f_{\omega^i}(0) = L_p(0, \omega^{1-i}) = -B_{1,\omega^{-i}} \bmod P_0(T),$$

which yields the result.

§13.7 Logarithmic Derivatives

This section provides the machinery needed for the next section. We first give a classical homomorphism, due to Kummer, and then present its generalization, due to Coates and Wiles.

Let p be odd and let U_1 be the local units of $\mathbb{Q}_p(\zeta_p)$ which are congruent to $1 \bmod (\zeta_p - 1)$. If $u \in U_1$ (or U), we may write

$$u = f(\zeta_p - 1), \quad \text{with} f(T) \in \Lambda^\times.$$

Let

$$D = (1 + T)\frac{d}{dT}$$

as in Chapter 12, and define

$$\phi_k(u) = D^{k-1}(1 + T)\frac{f'}{f}\bigg|_{T=0} \bmod p, \quad \text{for } 1 \le k \le p - 2.$$

If $g \in \Lambda^\times$ is another such power series, then $(f/g) - 1 \in \Lambda$ and has $\zeta_p - 1$ as a zero. Write

$$\frac{f}{g} - 1 = p^\mu P(T)A(T)$$

with $P(T)$ distinguished and $A \in \Lambda^\times$. Then $P(\zeta_p - 1) = 0$, so

$$h(T) = \frac{1}{T}((1 + T)^p - 1)$$

divides $P(T)$. Therefore

$$f(T) = g(T)(1 + h(T)B(T))$$

for some $B \in \Lambda$. We obtain

$$\frac{f'}{f} = \frac{g'}{g} + \frac{h'B + hB'}{(1 + hB)}.$$

Since $h \equiv T^{p-1} \bmod p\Lambda$,

$$\frac{f'}{f} \equiv \frac{g'}{g} \bmod(T^{p-2}, p).$$

It follows that $\phi_k(u)$ is well-defined for $1 \le k \le p - 2$, so we obtain a homomorphism

$$\phi_k : U_1 \to \mathbb{Z}/p\mathbb{Z}.$$

These maps were first defined by Kummer. However, he worked with polynomials, let $T = e^z - 1$, and considered $f(e^z - 1)$. Then $D = (1 + T)(d/dT)$ corresponds to d/dz, so

$$\phi_k(u) = \left(\frac{d}{dz}\right)^k \log f(e^z - 1)|_{z=0} \bmod p.$$

For an application due to Kummer, see Exercise 13.9.

Lemma 13.33. *Let $u \in U_1$ and let $1 \le n \le p - 2$. Then $\phi_k(u) = 0$ for $1 \le k \le n \Leftrightarrow u \equiv 1 \bmod(\zeta_p - 1)^{n+1}$.*

Proof. If $u \equiv 1 \bmod(\zeta_p - 1)^{n+1}$ we may take $f(T) = 1 + T^{n+1}g(T)$ with $g \in \Lambda$. Since $f'(T) \in T^n\Lambda$, $\phi_k(u) = 0$ for all $k \le n$.

Conversely, suppose $\phi_k(u) = 0$ for all $k \le n$. Let $u = f(\zeta_p - 1)$. Write

$$(1 + T)\frac{f'}{f} \equiv a_0 + a_1(1 + T) + \cdots + a_{n-1}(1 + T)^{n-1} \bmod T^n\Lambda.$$

Then $\phi_1(u) \equiv a_0 + a_1 + \cdots + a_{n-1}$ and

$$\phi_k(u) \equiv a_1 + 2^{k-1}a_2 + \cdots + (n-1)^{k-1}a_{n-1},$$

for $2 \leq k \leq n$. The determinant

$$\det(j^{k-1}), \qquad 0 \leq j \leq n-1, \quad 1 \leq k \leq n,$$

with $0^0 = 1$, is a Vandermonde determinant and is nonzero mod p. Therefore $a_i \equiv 0$ for $0 \leq i \leq n-1$. It follows that $f'(T) \in (T^n, p)$. Since $f \in \Lambda$ (so T^p/p does not occur), integration yields $f(T) \equiv a \bmod(T^{n+1}, p)$ with $a \in \mathbb{Z}_p$. Since $a \equiv u \equiv 1 \bmod(\zeta_p - 1)$, we have $a \equiv 1 \bmod p$. Therefore

$$\begin{aligned} u = f(\zeta_p - 1) &\equiv a \bmod(\zeta_p - 1)^{n+1} \\ &\equiv 1 \bmod(\zeta_p - 1)^{n+1}. \end{aligned}$$

This completes the proof. □

Lemma 13.34. *Let* $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. *Then*

$$\phi_k(\sigma_a u) = a^k \phi_k(u).$$

Proof. Let $u = f(\zeta_p - 1)$. Define

$$g(T) = f((1+T)^a - 1).$$

Then $\sigma_a u = g(\zeta_p - 1)$, and

$$(1+T)\frac{g'}{g} = a(1+T)^a \frac{f'}{f}((1+T)^a - 1).$$

By induction,

$$D^{k-1}(1+T)\frac{g'}{g} = a^k D^{k-1}(1+X)\frac{f'}{f}\bigg|_{X=(1+T)^a-1}.$$

The lemma follows easily. □

Lemma 13.35. *Let* ε_i, $0 \leq i \leq p-2$, *be the idempotents of* $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$. *If* $u \in U_1$ *then*

$$\phi_k(\varepsilon_i u) = \begin{cases} 0 & \text{if } k \neq i \\ \phi_i(u), & \text{if } k = i. \end{cases}$$

Proof. By Lemma 13.34,

$$\phi_k(\varepsilon_i u) = \frac{1}{p-1}\sum_{a=1}^{p-1} \omega^{-i}(a) a^k \phi_k(u) \equiv \begin{cases} 0 \bmod p, & \text{if } k \neq i, \\ \phi_k(u) \bmod p, & \text{if } k = i. \end{cases}$$ □

Lemma 13.36. *If* $i \not\equiv 1 \bmod p-1$ *then* $\varepsilon_i U_1$ *is cyclic as a* $\mathbb{Z}_p$*-module. For* $i = 1$, $\varepsilon_1 U_1 \simeq \langle \zeta_p \rangle \times$ *(cyclic* $\mathbb{Z}_p$*-module). If* $2 \leq i \leq p-2$ *and* $u \in \varepsilon_i U_1$ *then* u *generates* $\varepsilon_i U_1 \Leftrightarrow \phi_i(u) \neq 0$.

PROOF. First, let $i \geq 1$ be arbitrary. Since $(\zeta_p^a - 1)/(\zeta_p - 1) \equiv a \bmod(\zeta_p - 1)$,

$$\begin{aligned}\eta_i \overset{\text{def}}{=} (1 - (\zeta_p - 1)^i)^{\varepsilon_i} &= \prod_{a=1}^{p-1} (1 - (\zeta_p^a - 1)^i)^{\omega^{-i}(a)/(p-1)}\\ &\equiv 1 - \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^{-i}(a) a^i (\zeta_p - 1)^i\\ &\equiv 1 - (\zeta_p - 1)^i \bmod(\zeta_p - 1)^{i+1}.\end{aligned}$$

From the p-adic expansions, we easily see that $\eta_1, \ldots, \eta_p$ generate $U_1 \bmod(\zeta_p - 1)^{p+1}$, which is easily seen to be U_1/U_1^p. By Nakayama's Lemma (see Lemma 13.16), they generate U_1 over $\mathbb{Z}_p$. Since $\eta_i \in \varepsilon_i U_1$ for each i, η_i must generate $\varepsilon_i U_1$ for $i \neq 1, p$, and $\eta_1 = \zeta_p$ and η_p together generate $\varepsilon_1 U_1$.

Now suppose $2 \leq i \leq p - 2$ and let $u \in \varepsilon_i U_1$. Then $u = \eta_i^b$ for some $b \in \mathbb{Z}_p$, and u is a generator $\Leftrightarrow (p, b) = 1$. By Lemmas 13.33 and 13.35, $\phi_i(\eta_i) \neq 0$. Therefore

$$\phi_i(u) = b\phi_i(\eta_i) \neq 0 \Leftrightarrow (p, b) = 1 \Leftrightarrow u \text{ is a generator.}$$

This completes the proof. □

Corollary 13.37. *Let $2 \leq i \leq p - 2$. There exists $\lambda = \lambda_i \neq 1$ with $\lambda^{p-1} = 1$ such that*

$$\xi_i = \varepsilon_i\left(\frac{\lambda - \zeta_p}{\omega(\lambda - 1)}\right)$$

generates $\varepsilon_i U_1$. (We divide by $\omega(\lambda - 1)$ to get an element of U_1).

PROOF. By Lemma 13.36, it suffices to find λ such that $\phi_i(\xi_i) \neq 0$, and by Lemma 13.35, we can work with $(\lambda - \zeta_p)/\omega(\lambda - 1)$. Let

$$f(T) = \frac{\lambda - 1 - T}{\omega(\lambda - 1)}.$$

Then

$$f(\zeta_p - 1) = \frac{\lambda - \zeta_p}{\omega(\lambda - 1)},$$

and

$$\begin{aligned}(1 + T)\frac{f'}{f} &= 1 + \frac{\lambda}{1 + T - \lambda}\\ &= -\left(\frac{1 + T}{\lambda}\right) - \cdots - \left(\frac{1 + T}{\lambda}\right)^{p-1} + \frac{\lambda}{1 + T - \lambda}\left(\frac{1 + T}{\lambda}\right)^p.\end{aligned}$$

It follows that

$$D^{i-1}(1+T)\frac{f'}{f} \equiv$$

$$-\sum_{j=1}^{p-1} j^{i-1}\left(\frac{1+T}{\lambda}\right)^j + \left(\frac{1+T}{\lambda}\right)^p D^{i-1}\left(\frac{\lambda}{1+T-\lambda}\right) \bmod p\Lambda.$$

For $2 \le i \le p-2$, we obtain, since $\lambda^{p-1} = 1$,

$$\left(1-\frac{1}{\lambda}\right)\phi_i\left(\frac{\lambda-\zeta_p}{\omega(\lambda-1)}\right) \equiv -\sum_{j=1}^{p-1} j^{i-1}\lambda^{p-1-j} = -P(\lambda),$$

where

$$P(X) = X^{p-2} + 2^{i-1}X^{p-3} + \cdots + (p-1)^{i-1}.$$

Since $P(X)$ has degree $p-2$, and since

$$P(1) \equiv \sum_{j=1}^{p-1} \omega(j)^{i-1} \equiv 0 \pmod p$$

(in fact, 1 is a multiple root), at least one $\lambda \ne 1$ satisfies $P(\lambda) \not\equiv 0 \bmod p$. Then $\phi_i((\lambda-\zeta_p)/\omega(\lambda-1)) \ne 0$, so ξ_i generates $\varepsilon_i U_1$. This completes the proof. □

We now consider the generalization to higher levels. Let $U_1^{(n)}$ be the local units of $\mathbb{Q}_p(\zeta_{p^{n+1}})$ which are congruent to $1 \bmod(\zeta_{p^{n+1}}-1)$. The norm $N_{n,n-1}$ from $\mathbb{Q}_p(\zeta_{p^{n+1}})$ to $\mathbb{Q}_p(\zeta_{p^n})$ maps $U_1^{(n+1)}$ into $U_1^{(n)}$, so we define

$$U = \varprojlim U_1^{(n)}.$$

Then U is Λ-module in the usual way and is also a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}_p)]$-module.

Theorem 13.38. *Let $u = (u_n) \in U$. Then there exists a unique $f_u \in \Lambda$ such that*

$$f_u(\zeta_{p^{n+1}}-1) = u_n \quad \textit{for all } n \ge 0.$$

The map

$$U \to \Lambda^\times$$
$$u \mapsto f_u$$

gives a bicontinuous isomorphism between U and the subgroup of $f \in \Lambda^\times$ satisfying

$$f(0) \equiv 1 \bmod p$$
$$f((1+T)^p - 1) = \prod_{\zeta^p=1} f(\zeta(1+T)-1). \tag{$*$}$$

Proof. Corollary 7.4 implies the uniqueness of f_u.

For simplicity, let $v_n = \zeta_{p^{n+1}} - 1$. Assume for the moment that f_u exists. Since

$$f_u(0) \equiv f_u(\zeta_p - 1) = u_0 \equiv 1 \bmod (\zeta_p - 1)$$

and since $f_u(0) \in \mathbb{Z}_p$, we have $f_u(0) \equiv 1 \bmod p$. Observe that the conjugates of $\zeta_{p^{n+1}}$ under $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}(\zeta_{p^n}))$ are $\{\zeta\zeta_{p^{n+1}} | \zeta^p = 1\}$. Therefore

$$\prod_{\zeta^p=1} f_u(\zeta(1 + v_n) - 1) = N_{n,n-1} f_u(v_n) = u_{n-1},$$

Also

$$f_u((1 + v_n)^p - 1) = f_u(v_{n-1}) = u_{n-1}.$$

Therefore, again by Corollary 7.4, we obtain (*). Observe that if f satisfies (*) then

$$N_{n,n-1} f(v_n) = f(v_{n-1}),$$

so

$$(f(v_n)) \in \varprojlim U_1^{(n)}.$$

We therefore have a homomorphism

$$\tilde{\Lambda} = \{f \in \Lambda^\times \text{ satisfying } (*)\} \xrightarrow{g} U.$$

Clearly $\tilde{\Lambda}$ is closed in $\Lambda^\times$, hence compact. The topology on U is induced from the product topology on $\prod_n U_1^{(n)}$, so U is compact. Any neighborhood of 1 in U contains a neighborhood of the form

$$V_{n,k} = \{(u_n) | u_n \equiv 1 (\bmod p^k), n \leq N\}.$$

If

$$f \equiv 1 \bmod (p, T)^{k\phi(p^{N+1})}$$

then

$$\begin{aligned} f(v_n) &\equiv 1 \bmod (p, v_n)^{k\phi(p^{N+1})} \\ &\equiv 1 \bmod p^k \quad \text{for } n \leq N. \end{aligned}$$

So the map g is continuous at 1, hence everywhere, since it is a homomorphism. Now assume the existence part of the theorem, so g is bijective. Any closed set of $\tilde{\Lambda}$ is compact, hence its image under g is compact, hence closed. So g sends closed sets to closed sets. Therefore g^{-1} is continuous, so g is bicontinuous (this argument shows that any continuous bijection between compact Hausdorff spaces is bicontinuous).

It remains to prove the existence. We need several lemmas.

Lemma 13.39. *There exists a unique map $N\colon \Lambda \to \Lambda$ such that*

$$(Nf)((1 + T)^p - 1) = \prod_{\zeta^p=1} f(\zeta(1 + T) - 1).$$

Proof. Let $g(T)$ be the power series on the right, defined by the product. Observe that for $\zeta^p = 1$,

$$g(\zeta(1+T)-1) = g(T).$$

Suppose we have $a_0, \ldots, a_{n-1} \in \mathbb{Z}_p$ and $g_n(T) \in \Lambda$ such that

$$g(T) = \sum_{i=0}^{n-1} a_i((1+T)^p - 1)^i + ((1+T)^p - 1)^n g_n(T).$$

For $n = 0$ this is trivial, which gets the induction started. Since

$$g_n(\zeta(1+T)-1) = g_n(T)$$

(everything else satisfies this, hence so does g_n),

$$g_n(\zeta - 1) = g_n(0), \quad \text{for } \zeta^p = 1.$$

Using the Weierstrass Preparation Theorem, we see that T and the minimal polynomial of $\zeta - 1$ both divide $g_n(T) - g_n(0)$, so

$$g_n(T) - g_n(0) = ((1+T)^p - 1)g_{n+1}(T)$$

for some $g_{n+1} \in \Lambda$. Letting $a_n = g_n(0)$, we obtain the above for $n+1$. Continuing, we get

$$g(T) - \sum_{i=0}^{\infty} a_i((1+T)^p - 1)^i \in \bigcap_{n \geq 0} (p, T)^n = 0.$$

Therefore we may let

$$(Nf)(T) = \sum_{i=0}^{\infty} a_i T^i.$$

Uniqueness follows from Corollary 7.4. This proves Lemma 13.39. □

Of course, the condition $(*)$ of the theorem says that $f(0) \equiv 1$ and $Nf = f$, for f corresponding to an element of U.

Lemma 13.40. *Let $f \in \Lambda$. Then*

$$(Nf)(v_{n-1}) = N_{n,n-1}(f(v_n)).$$

Proof. $(Nf)(v_{n-1}) = (Nf)((1+v_n)^p - 1)$

$$= \prod f(\zeta(1+v_n)-1) = N_{n,n-1}(f(v_n)),$$

as in a previous calculation. □

Lemma 13.41. *Let $f \in \Lambda$ and assume $f((1+T)^p - 1) \equiv 1 \bmod p^k\Lambda$. Then $f(T) \equiv 1 \bmod p^k\Lambda$.*

Proof. Let

$$f(T) = 1 + p^{\mu} \sum_{i=0}^{\infty} a_i T^i$$

for some $\mu \geq 0$, with μ maximal. Let a_n be the first coefficient such that $p \nmid a_n$. Then

$$\sum_{i=0}^{\infty} a_i((1+T)^p - 1)^i \equiv a_n T^{pn} + \sum_{i>n} a_i T^{pi} \not\equiv 0 \bmod p\Lambda.$$

Since

$$p^{\mu} \sum_{i=0}^{\infty} a_i((1+T)^p - 1)^i \equiv 0 \bmod p^k\Lambda,$$

we must have $\mu \geq k$. This completes the proof. □

Corollary 13.42. *$N\colon \Lambda^{\times} \to \Lambda^{\times}$ is continuous.*

Proof. Since N is a homomorphism it suffices to check continuity at 1. Lemma 13.41 and the definition of N yield the result. □

Lemma 13.43. *Suppose $f \in \Lambda^{\times}$. Then*

$$\frac{N^k f}{f} \equiv 1 \bmod p\Lambda$$

for all $k \geq 0$.

Proof. Since

$$\frac{N^k f}{f} = \frac{N(N^{k-1}f)}{N^{k-1}f} \cdots \frac{N(f)}{f},$$

it suffices to consider $k = 1$. We have

$$\frac{(Nf)((1+T)^p - 1)}{f((1+T)^p - 1)} = \frac{\prod f(\zeta(1+T) - 1)}{f((1+T)^p - 1)} \equiv \frac{f(T)^p}{f(T^p)} \equiv 1 \bmod(\zeta_p - 1),$$

therefore mod p. The result now follows from Lemma 13.41. □

Lemma 13.44. *Let $k \geq 1$. Then*

$$f \equiv 1 \bmod p^k\Lambda \Rightarrow Nf \equiv 1 \bmod p^{k+1}\Lambda.$$

Proof. Write $f(T) = 1 + p^k f_1(T)$. Then

$$f(\zeta(1+T) - 1) \equiv 1 + p^k f_1(T) \bmod(\zeta_p - 1)p^k.$$

Therefore

$$(Nf)((1+T)^p - 1) \equiv (1 + p^k f_1(T))^p \equiv 1 \bmod(\zeta_p - 1)p^k,$$

hence mod p^{k+1}. Lemma 13.41 completes the proof. □

Corollary 13.45. *Let $m \geq k \geq 0$ and let $f \in \Lambda^{\times}$. Then*

$$N^m f \equiv N^k f \bmod p^{k+1}.$$

Proof. Lemma 13.43 implies $N^{m-k}f/f \equiv 1 \bmod p\Lambda$. Lemma 13.44 yields the result. □

Corollary 13.46. *Let $f \in \Lambda^\times$. Then $N^\infty f = \lim N^k f$ exists.*

Proof. Corollary 13.45, plus the completeness of Λ. □

We can now prove Theorem 13.38. Let $u = (u_n) \in U$. For each n, choose $f_n(T) \in \Lambda$ such that

$$f_n(v_n) = u_n.$$

Let

$$g_m(T) = (N^m f_{2m})(T).$$

By Lemma 13.40

$$(N^k f_n)(v_{n-k}) = N_{n,n-k}\, f_n(v_n) = u_{n-k},$$

for $0 \le k \le n$. Therefore

$$(N^{m-n} g_m)(v_n) = (N^{2m-n} f_{2m})(v_n) = u_n,$$

for all $m \ge n$. By Corollary 13.45,

$$N^{m-n} g_m = N^{2m-n} f_{2m} \equiv N^m f_{2m} = g_m \bmod p^{m+1}\Lambda.$$

Letting $T = v_n$, we obtain

$$u_n \equiv g_m(v_n) \bmod p^{m+1},$$

for all $m \ge n$. Since $\Lambda^\times$ is compact, the sequence g_m has a cluster point $h \in \Lambda$, and

$$g_{m_i} \to h \quad \text{as } m_i \to \infty \text{ through a subsequence.}$$

Since $\bigcap_{N \ge 0} (p, v_n)^N = 0$ in $\mathbb{C}_p$, it follows that

$$g_{m_i}(v_n) \to h(v_n)$$

for each n. Therefore $u_n = h(v_n)$ for all n. This completes the proof of Theorem 13.38. □

The above proof of the existence is an adaptation of Coleman's proof for formal groups. I would like to thank John Coates for supplying the details.

We can now define the generalization of the Kummer homomorphism. Let $u \in U$ and let f_u be the associated power series. Recall that

$$D = (1 + T)\frac{d}{dT}.$$

For $k \ge 1$ define the Coates–Wiles homomorphism $\delta_k \colon U \to \mathbb{Z}_p$ by

$$\delta_k(u) = D^{k-1}(1 + T)\left.\frac{f_u'(T)}{f_u(T)}\right|_{T=0}.$$

Since $f_u \equiv 1 \bmod (p, T)$, $\log f_u(T) \in \mathbb{Q}_p[[T]]$ is defined, so $\delta_k(u)$ also equals $D^k \log f_u(T)|_{T=0}$. If $u = (u_0, u_1, \ldots) \in U$ then

$$\phi_k(u_0) = \delta_k(u) \bmod p, \qquad 2 \leq k \leq p-2.$$

Lemma 13.47. *$\delta_k(u)$ is a continuous function of u (it is "almost" continuous in k; see Proposition* 13.51).

PROOF. This follows immediately from the continuity of $u \mapsto f_u$. □

Identify $\mathbb{Z}_p^\times \simeq \operatorname{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, $a \mapsto \sigma_a$. An easy calculation yields the following.

Lemma 13.48. *Let $u \in U$ be associated to f_u, and let*

$$x = \sum b_a \sigma_a \in \mathbb{Z}_p[\operatorname{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})].$$

Then

$$f_{u^x}(T) = \prod f_u((1+T)^a - 1)^{b_a}. \qquad \square$$

It is trivial to check that everything above is defined; for example,

$$(1+T)^a = \sum \binom{a}{n} T^n \in \Lambda.$$

Lemma 13.49. *Let $a \in \mathbb{Z}_p^\times$ and $\sigma_a \in \operatorname{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$. Then, for $k \geq 1$,*

$$\delta_k(\sigma_a u) = a^k \delta_k(u).$$

PROOF. See the proof of Lemma 13.34. □

Lemma 13.50. *If $u \in U$ then*

$$\delta_k(\varepsilon_i u) = \begin{cases} 0, & \text{if } k \not\equiv i \bmod p-1 \\ \delta_k(u), & \text{if } k \equiv i \bmod p-1. \end{cases}$$

PROOF. See the proof of Lemma 13.35. Note that

$$\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^{-i}(a) \sigma_{\omega(a)}$$

is the idempotent since $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ corresponds to $\{\omega(a)\}$ in $\mathbb{Z}_p^\times$. □

Let $2 \leq i \leq p-2$ and let $\lambda = \lambda_i$ be as in Corollary 13.37. Let

$$\xi_i^{(n)} = \varepsilon_i \left(\frac{\lambda - \zeta_{p^{n+1}}}{\omega(\lambda - 1)} \right).$$

Then

$$N_{n,n-1}(\xi_i^{(n)}) = \varepsilon_i \prod_{\zeta^p=1} \left(\frac{\lambda - \zeta\zeta_{p^{n+1}}}{\omega(\lambda - 1)}\right)$$
$$= \varepsilon_i\left(\frac{\lambda^p - \zeta_{p^n}}{\omega(\lambda - 1)^p}\right) = \xi_i^{(n-1)},$$

so

$$\xi_i^\infty = (\xi_i^{(n)}) \in \varepsilon_i U.$$

Let γ_0 be a topological generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p))$, and define $\kappa_0 \in 1 + p\mathbb{Z}_p$ by $\zeta_{p^n}^{\gamma_0} = \zeta_{p^n}^{\kappa_0}$ for all $n \geq 1$. The following result will be crucial in the next section.

Proposition 13.51. *Let* $2 \leq i \leq p - 1$. *There exists* $h_i(T) \in \Lambda^\times$ *such that*

$$(1 - p^{k-1})\delta_k(\xi_i^\infty) = h_i(\kappa_0^k - 1) \quad \textit{for } k \equiv i \bmod p - 1.$$

Proof. By Lemma 13.50 we mav compute

$$\delta_k\left(\frac{\lambda - (1 + T)}{\omega(\lambda - 1)}\right)$$

Let

$$f(T) = (1 + T)\frac{d}{dT}\log\left(\frac{\lambda - (1 + T)}{\omega(\lambda - 1)}\right)$$
$$= 1 + \frac{\lambda}{(1 + T) - \lambda}.$$

Since $\lambda^p = \lambda$,

$$\frac{\lambda}{(1 + T)^p - \lambda} = \frac{1}{p}\sum_{\zeta^p=1} \frac{\lambda}{\zeta(1 + T) - \lambda}$$

(see the example at the end of Section 12.2). Let U be as in Proposition 12.8. Then

$$Uf(T) = f(T) - \frac{1}{p}\sum_{\zeta^p=1} f(\zeta(1 + T) - 1)$$
$$= \frac{\lambda}{1 + T - \lambda} - \frac{\lambda}{(1 + T)^p - \lambda}.$$

We obtain

$$(D^{k-1}Uf)(0) = (1 - p^{k-1})(D^{k-1}f)(0) = (1 - p^{k-1})\delta_k(\xi_i^\infty).$$

By Corollary 12.9,

$$(D^{k-1}Uf)(0) = \tilde{h}_i(\kappa_0^{k-1} - 1), \quad \text{for } k \equiv i \bmod p - 1,$$

for some $\tilde{h}_i \in \Lambda$. Letting

$$h_i(T) = \tilde{h}_i(\kappa_0^{-1}(1 + T) - 1) \in \Lambda,$$

we have

$$h_i(\kappa_0^k - 1) = \tilde{h}_i(\kappa_0^{k-1} - 1) = (1 - p^{k-1})\delta_k(\xi_i^\infty).$$

It remains to show that $h_i \in \Lambda^\times$. Let $k = i$, so $2 \le k \le p - 2$. Then

$$\delta_i(\xi_i^\infty) \equiv \phi_i(\xi_i^{(0)}) \not\equiv 0 \bmod p,$$

by the proof of Corollary 13.37. Since $1 - p^{i-1} \in \mathbb{Z}_p^\times$, $h_i(\kappa_0^i - 1)$ is a unit. Since $h_i(\kappa_0^i - 1) \equiv h_i(0) \bmod p$, $h_i(0) \in \mathbb{Z}_p^\times$. Therefore $h_i \in \Lambda^\times$. This proves Proposition 13.51. □

Lemma 13.52. *Let $h(T) \in \Lambda$ and $u \in U$. Then*

$$\delta_k(h(T)u) = h(\kappa_0^k - 1)\delta_k(u).$$

Proof. Since both sides are continuous in h, we may assume h is a polynomial; by linearity, we may assume $h(T) = (1 + T)^n$. Then $h(T)u = \gamma_0^n u$. By Lemma 13.49,

$$\delta_k(\gamma_0^n u) = \kappa_0^{nk}\delta_k(u) = h(\kappa_0^k - 1)\delta_k(u).$$

This completes the proof. □

§13.8 Local Units Modulo Cyclotomic Units

In this section we prove a beautiful theorem, due to Iwasawa, that relates the p-adic L-functions to the Galois structure of the local units modulo the closure of the cyclotomic units. We continue to assume $p \ge 3$.

Let $N_{m,n}$ be the norm from $\mathbb{Q}_p(\zeta_{p^{m+1}})$ to $\mathbb{Q}_p(\zeta_{p^{n+1}})$ and let N_n be the norm from $\mathbb{Q}_p(\zeta_{p^{n+1}})$ to $\mathbb{Q}_p$. Recall that $U_1^{(n)}$ denotes the local units of $\mathbb{Q}_p(\zeta_{p^{n+1}})$ which are congruent to 1 mod$(\zeta_{p^{n+1}} - 1)$. Let

$$U_n' = \{u \in U_1^{(n)} \mid N_n u = 1\}.$$

Lemma 13.53. *Let $u_n \in U_1^{(n)}$. Then*

$$u_n \in U_n' \Leftrightarrow \textit{for all } m \ge n, \textit{ there exists } u_m \in U_1^{(m)} \textit{ with } N_{m,n}(u_m) = u_n.$$

Proof. For simplicity, let $K_m = \mathbb{Q}_p(\zeta_{p^{m+1}})$. An element $a \in 1 + p\mathbb{Z}_p$ yields $\sigma_a \in \mathrm{Gal}(K_m/\mathbb{Q}_p)$, and

$$\sigma_a = 1 \Leftrightarrow a \equiv 1 \bmod p^{m+1}.$$

For $u_n \in U_1^{(n)}$, there is a corresponding element

$$\sigma^{(m)} = \sigma(u_n, K_m/K_n) \in \mathrm{Gal}(K_m/K_n) \subseteq \mathrm{Gal}(K_m/\mathbb{Q}_p),$$

and, by a property of the Artin symbol,

$$\sigma(u_n, K_m/K_n) = \sigma(N_n u_n, K_m/\mathbb{Q}_p) = \sigma_{N_n u_n}.$$

We also have

$$\sigma^{(m)} = 1 \Leftrightarrow u_n \in N_{m,n}(K_m^\times) \Leftrightarrow u_n \in N_{m,n}(U_1^{(m)})$$

(see the appendix on class field theory). The last equivalence follows since the norm of a nonunit is a nonunit, and the norm of a $(p-1)$st root of 1 is itself, hence not congruent to 1 $\operatorname{mod}(\zeta_{p^{n+1}} - 1)$. Therefore, putting everything together, we obtain

$$\begin{aligned} N_n u_n = 1 &\Leftrightarrow N_n u_n \equiv 1 \bmod p^{m+1} \quad \text{for all } m \geq n \\ &\Leftrightarrow \sigma^{(m)} = 1 \quad \text{for all } m \geq n \\ &\Leftrightarrow u \in N_{m,n}(U_1^{(m)}) \quad \text{for all } m \geq n. \end{aligned}$$

This completes the proof. □

Note that "$\Leftarrow$" also follows from setting $T = 0$, then dividing by $f(0)$, in $(*)$ of Theorem 13.38. Also, for $i \neq 0$,

$$\varepsilon_i U_n' = \varepsilon_i U_1^{(n)}$$

since $N_n = N_{n,0} N_0 = N_{n,0}((p-1)\varepsilon_0)$ and $\varepsilon_0 \varepsilon_i = 0$.

Theorem 13.54. *Let $2 \leq i \leq p-2$ and let ξ_i^∞ be as above. Then*

$$\begin{aligned} \Lambda &\simeq \varepsilon_i U \\ g &\mapsto g\xi_i^\infty, \end{aligned}$$

and

$$\begin{aligned} \Lambda/((1+T)^{p^n} - 1) &\simeq \varepsilon_i U_1^{(n)} \\ g &\mapsto g\xi_i^{(n)}. \end{aligned}$$

PROOF. We start with the second assertion. As above, let $K_n = \mathbb{Q}_p(\zeta_{p^{n+1}})$. By Corollary 13.37, $\xi_i = \xi_i^{(0)}$ generates $\varepsilon_i U_1' = \varepsilon_i U_1^{(0)}$ over $\mathbb{Z}_p = \Lambda/(T)$. Now let $n \geq 0$. Let $u_n \in \varepsilon_i U_1^{(n)}$. Then

$$N_{n,0}(u_n) \in U_1^{(0)} = \Lambda \xi_i^{(0)} = \Lambda(N_{n,0}(\xi_i^{(n)})) = N_{n,0}(\Lambda \xi_i^{(n)}).$$

Therefore

$$N_{n,0}\left(\frac{u_n}{g\xi_i^{(n)}}\right) = 1$$

for some $g \in \Lambda$. By Hilbert's Theorem 90,

$$\alpha \overset{\text{def}}{=} \frac{u_n}{g\xi_i^{(n)}} = \beta^{\gamma_0 - 1}$$

for some $\beta \in K_n^\times$. We want $\beta \in \varepsilon_i U_1^{(n)}$. As abelian groups

$$K_n^\times = \pi^{\mathbb{Z}} \times \{\lambda^{p-1} = 1\} \times U_1^{(n)},$$

where $\pi = \zeta_{p^{n+1}} - 1$. Therefore, for $N \geq 0$,

$$K_n^\times/(K_n^\times)^{p^N} = \pi^{\mathbb{Z}/p^N\mathbb{Z}} \times U_1^{(n)}/(U_1^{(n)})^{p^N}.$$

We may let ε_i act on this last space (it could not act on $K_n^\times$). Since $i \neq 0$, $\varepsilon_i(\pi) \bmod (K_n^\times)^{p^N}$ is represented by a unit; since $\varepsilon_i^2 = \varepsilon_i$, it is represented by an element of $\varepsilon_i U_1^{(n)}$. Therefore

$$\varepsilon_i(K_n^\times/(K_n^\times)^{p^N}) = \varepsilon_i(U_1^{(n)}/(U_1^{(n)})^{p^N}).$$

Consequently, for some $v_N \in U_1^{(n)}$,

$$\alpha = \varepsilon_i \alpha \equiv \varepsilon_i \beta^{\gamma_0 - 1} \equiv \varepsilon_i v_N^{\gamma_0 - 1} \bmod (K_n^\times)^{p^N}.$$

Since α and v_N are units, this yields a congruence $\bmod (U_1^{(n)})^{p^N}$. Since $U_1^{(n)}$ is compact, the sequence $\varepsilon_i v_N$ has a cluster point $v \in \varepsilon_i U_1^{(n)}$, and

$$\alpha = v^{\gamma_0 - 1} \in (\gamma_0 - 1)\varepsilon_i U_1^{(n)} = T\varepsilon_i U_1^{(n)}.$$

Therefore

$$u_n \equiv g\xi_i^{(n)} \bmod T\varepsilon_i U_1^{(n)}.$$

By Nakayama's Lemma (13.16), $\xi_i^{(n)}$ generates $\varepsilon_i U_1^{(n)}$ over Λ, since u_n was arbitrary. Since $(1 + T)^{p^n} = \gamma_0^{p^n}$ fixes $\xi_i^{(n)}$,

$$\Lambda/((1 + T)^{p^n} - 1) \to \varepsilon_i U_1^{(n)}$$

is surjective.

$U_1^{(n)}$ contains a subgroup of finite index which is mapped isomorphically via the logarithm to $\pi^N \mathbb{Z}_p[\zeta_{p^{n+1}}]$ for some N (see Proposition 5.7). By the normal basis theorem, there is an element of K_n, which we may assume to be in $\pi^N \mathbb{Z}_p[\zeta_{p^{n+1}}]$, whose $\mathrm{Gal}(K_n/\mathbb{Q}_p)$-conjugates are linearly independent over $\mathbb{Q}_p$. Therefore $\pi^N \mathbb{Z}_p[\zeta_{p^{n+1}}]$ contains a submodule of finite index isomorphic to the group ring. Consequently

$$\begin{aligned} \mathbb{Z}_p\text{-rank } \varepsilon_i U_1^{(n)} &= \mathbb{Z}_p\text{-rank } \varepsilon_i \pi^N \mathbb{Z}_p[\zeta_{p^{n+1}}] \\ &= \mathbb{Z}_p\text{-rank } \varepsilon_i \mathbb{Z}_p[\mathrm{Gal}(K_n/\mathbb{Q}_p)] = \mathbb{Z}_p\text{-rank } \mathbb{Z}_p[\mathrm{Gal}(K_n/K_0)] \\ &= p^n. \end{aligned}$$

By the division algorithm,

$$\Lambda/((1 + T)^{p^n} - 1) \simeq \mathbb{Z}_p^{p^n}$$

as $\mathbb{Z}_p$-modules. Therefore the above surjection must have trivial kernel, so

$$\Lambda/((1 + T)^{p^n} - 1) \simeq \varepsilon_i U_1^{(n)}.$$

Now let $u = (u_n) \in \varepsilon_i U = \varprojlim \varepsilon_i U_1^{(n)}$. Then

$$u_n = f_n(T)\xi_i^{(n)}$$

for some $f_n \in \Lambda$, uniquely determined $\bmod (1+T)^{p^n} - 1$. Since Λ is commutative,

$$f_{n-1}(T)\xi_i^{(n-1)} = u_{n-1} = N_{n,n-1}(u_n) = f_n(T)N_{n,n-1}(\xi_i^{(n)}) = f_n(T)\xi_i^{(n-1)}.$$

Consequently,

$$f_{n-1}(T) \equiv f_n(T) \bmod (1+T)^{p^{n-1}} - 1,$$

so $(f_n(T))$ determines an element $f(T) \in \Lambda = \varprojlim \Lambda/((1+T)^{p^n} - 1)$, and

$$u_n = f(T)\xi_i^{(n)}$$

for all n. If $u = 1$ then $f(T) \equiv 0 \bmod (1+T)^{p^n} - 1$ for all n, hence $f = 0$. Therefore

$$\Lambda \to \varepsilon_i U$$

is an isomorphism. This completes the proof of Theorem 13.54. □

Remark. Usually this theorem is proved by using local class field theory, plus the structure theorem for Λ-modules, to show that $\varepsilon_i U \simeq \Lambda$. It is then not hard to use Corollary 13.37 to show that ξ_i^∞ is a generator (see Lang [4]). In some ways, this give a "better" proof, since it applies to extensions of the theory where $\varepsilon_i U$ is not quite cyclic over Λ.

We now consider cyclotomic units. Let $C^{(n)}$ denote the cyclotomic units of $\mathbb{Q}(\zeta_{p^{n+1}})$, $C_1^{(n)} = C^{(n)} \cap U_1^{(n)}$, and $\overline{C_1^{(n)}}$ = closure in $U_1^{(n)}$. (See Exercise 13.8 for a description of $\overline{C_1^{(n)}}$). Then $\overline{C_1^{(n)}}$ is a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_p)]$ module. If $\varepsilon \in C^{(n)}$ then $\varepsilon^{p-1} \in C_1^{(n)}$ and

$$(\varepsilon^{p-1})^{1/(p-1)} \in \overline{C_1^{(n)}}$$

since $1/(p-1) \in \mathbb{Z}_p$. Note that $(\varepsilon^{p-1})^{1/(p-1)} = \varepsilon \Leftrightarrow \varepsilon \in C_1^{(n)}$. In general, we get the analogue of $\langle\varepsilon\rangle$, where $\varepsilon = \omega(\varepsilon)\langle\varepsilon\rangle$.

Fix a primitive root g mod p^2. Then g is a primitive root mod p^n for all $n \geq 1$. By Lemma 8.1 and Proposition 8.11.

$$\frac{\zeta_{p^{n+1}}^g - 1}{\zeta_{p^{n+1}} - 1} \quad \text{and} \quad -\zeta_{p^{n+1}}$$

generate $C^{(n)}$ as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_p)]$ module. But they are not in $C_1^{(n)}$. Let

$$\eta_n = \zeta_{p^{n+1}}^{(1-g)/2}\left(\frac{\zeta_{p^{n+1}}^g - 1}{\zeta_{p^{n+1}} - 1}\right)^{p-1}.$$

Then η_n and $\zeta_{p^{n+1}}$ generate $(C^{(n)})^{p-1}$. It follows that they generate $\overline{C_1^{(n)}}$ as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_p)]$ module.

Let $\overline{C_1} = \lim \overline{C_1^{(n)}}$, with respect to the norm map. Then $\overline{C_1}$ is a Λ-module and a $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$-module. Decompose $\overline{C_1}$ according to the idempotents:

$$\overline{C_1} = \bigoplus_{i=0}^{p-2} \varepsilon_i \overline{C_1}.$$

Then each $\overline{C_1}$ is a Λ-module. It is easy to see that

$$\varepsilon_i \overline{C_1} = 0, \quad i \text{ odd}, i \neq 1,$$
$$\varepsilon_1 \overline{C_1} = \varprojlim \langle \zeta_{p^{n+1}} \rangle;$$

this last module is isomorphic to $\mathbb{Z}_p$ but has a different Galois action (it is the T of Section 13.5). Henceforth we restrict to even i. Let

$$u = (u_n) \in \varepsilon_i \overline{C_1}.$$

Then

$$u_n = f_n(T)\varepsilon_i \eta_n$$

for some $f_n(T) \in \Lambda$. An easy calculation shows that

$$N_{n,n-1}(\varepsilon_i \eta_n) = \varepsilon_i \eta_{n-1}.$$

Therefore

$$\varepsilon_i \eta = (\varepsilon_i \eta_n) \in \varepsilon_1 \overline{C_1},$$

and

$$u_{n-1} = f_n(T)\varepsilon_i \eta_{n-1}.$$

Consider the set

$$S_n = \{f(T) \mid u_k = f(T)\varepsilon_i \eta_k \text{ for all } k \leq n\}.$$

Then S_n is closed in Λ and nonempty since $f_n \in S_n$. Clearly

$$S_0 \supseteq S_1 \supseteq \cdots.$$

Since Λ is compact, $\bigcap S_n \neq \varnothing$ (nested set property from topology). Let $f \in \bigcap S_n$. Then

$$u_n = f(T)\varepsilon_i \eta_n$$

for all n, so we obtain the following.

Lemma 13.55. *Let i be even. Then $\varepsilon_i \overline{C_1} = \Lambda \varepsilon_i \eta$. (This actually holds for all $i \neq 1$).* □

We are now ready to prove the main result of this section.

Theorem 13.56. *Let $i \not\equiv 0 \bmod p - 1$ be even. Then*

$$\varepsilon_i U / \varepsilon_i \overline{C_1} \simeq \Lambda/(f_i(T)),$$

where

$$f_i(\kappa_0^s - 1) = L_p(1 - s, \omega^i).$$

(κ_0 is defined by $\gamma_0 \zeta_{p^n} = \zeta_{p^n}^{\kappa_0}$ for all $n \geq 1$).

Proof. From Theorem 13.54,

$$\varepsilon_i \eta = g_i(T)\xi_i^\infty$$

for some $g_i \in \Lambda$, hence by Theorem 13.54 and Lemma 13.55

$$\varepsilon_i \overline{C_1} = g_i(T)\varepsilon_i U.$$

It remains to evaluate $g_i(T)$. To do this, we use the Coates–Wiles homomorphism δ_k with $k \equiv i \bmod p-1$. By Lemma 13.52,

$$\delta_k(\varepsilon_i \eta) = g_i(\kappa_0^k - 1)\delta_k(\xi_i^\infty).$$

By Proposition 13.51, we know that

$$(1 - p^{k-1})\delta_k(\xi_i^\infty) = h_i(\kappa_0^k - 1)$$

with $h_i \in \Lambda^\times$. By Lemma 13.50, $\delta_k(\varepsilon_i \eta) = \delta_k(\eta)$, so

$$g_i(\kappa_0^k - 1) = (1 - p^{k-1})h_i(\kappa_0^k - 1)^{-1}\delta_k(\eta).$$

To identify g_i, it suffices to evaluate $\delta_k(\eta)$. Let

$$f(T) = \left((1+T)^{(1-g)/2}\frac{(1+T)^g - 1}{(1+T) - 1}\right)^{p-1}.$$

Then $f(T) = f_\eta(T)$ in the notation of Theorem 13.38. We have

$$(1+T)\frac{f'}{f}(T) = (p-1)\left(\frac{1-g}{2} + \frac{g(1+T)^g}{(1+T)^g - 1} - \frac{1+T}{(1+T) - 1}\right).$$

Let $T = e^Z - 1$. Then $D = (1+T)(d/dT) = d/dZ$. We have

$$\begin{aligned}\frac{ge^{gZ}}{e^{gZ}-1} - \frac{e^Z}{e^Z-1} &= \frac{1}{Z}\left(\frac{gZ}{e^{gZ}-1} - \frac{Z}{e^Z-1}\right) + g - 1\\ &= g - 1 + \sum_{n=1}^{\infty}(g^n - 1)\frac{B_n}{n}\frac{Z^{n-1}}{(n-1)!}\end{aligned}$$

Therefore

$$\begin{aligned}\delta_k(\eta) &= D^{k-1}\left((1+T)\frac{f'}{f}\right)(0) = (g^k - 1)\frac{B_k}{k}\\ &= -(g^k - 1)(1 - p^{k-1})^{-1}L_p(1-k, \omega^i),\end{aligned}$$

since $k \equiv i \bmod p-1$. Returning to the above, we obtain

$$g_i(\kappa_0^k - 1) = -(g^k - 1)h_i(\kappa_0^k - 1)^{-1}L_p(1-k, \omega^i).$$

Let

$$a = \frac{(\log_p g)}{(\log_p \kappa_0)},$$

and let

$$V(T) = -\omega(g)^i(1+T)^a + 1.$$

Then

$$V(\kappa_0^k - 1) = -(g^k - 1) \quad \text{for } k \equiv i \bmod p-1,$$

and $V(0) = 1 - \omega(g)^i \not\equiv 0 \bmod p$, so $V \in \Lambda^\times$. Let

$$f_i(T) = g_i(T)h_i(T)V(T)^{-1}.$$

Then f_i and g_i generate the same ideal in Λ and

$$f_i(\kappa_0^k - 1) = L_p(1-k, \omega^i).$$

Since both sides are analytic in k, we may replace k by $s \in \mathbb{Z}_p$. This completes the proof. □

Notes

The basic references for this chapter are Iwasawa [25], Coates [7], and Serre [1]. The other papers by Iwasawa and those by R. Greenberg should also be consulted.

For arbitrary (non-cyclotomic) $\mathbb{Z}_p$-extensions, see Bloom [1], Bloom-Gerth [1], Cuoco [1], Cuoco-Monsky [1], Monsky [1], [2], R. Greenberg [1], and Babaĭcev [2].

For relations with K-theory, see Candiotti [1], Coates [1], R. Greenberg [6], and Kramer-Candiotti [1].

For determining how to start a $\mathbb{Z}_p$-extension, see Carroll [1], Carroll-Kisilevsky [1], and Bertrandias-Payan [1].

For capitulation (ideals becoming principal), see Ferrero [3] and Kuroda [1].

For a Hurwitz-type formula for the λ-invariant, see Kida [2], Iwasawa [29], and Kuz'min [3].

It has been conjectured that $\lambda = 0$ for all totally real fields. See Greenberg [5].

For the main conjecture, see Coates [7], [8], Greenberg [4], Mazur-Wiles [1], Ribet [5], and Oesterlé [2].

Theorem 13.56 is from Iwasawa [13]. The above proof comes from the proof used in the elliptic case by Coates-Wiles [4] in their work on the conjecture of Birch and Swinnerton-Dyer. For an extension to abelian fields, see Gillard [6], part II.

For more references, see the notes on Chapter 7.

Exercises

13.1. Suppose K_∞/K is a $\mathbb{Z}_p$-extension such that each K_n is a CM-field. Show that if Leopoldt's conjecture holds for K then K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension.

13.2. (a) Show that in a cyclotomic $\mathbb{Z}_p$-extension no prime splits completely.
(b) Suppose $\mathrm{Gal}(F/K) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Let $l \neq p$ be a prime. Show that the decomposition group of a prime $\tilde{l}$ above l is either trivial or isomorphic to $\mathbb{Z}_p$ (*Hint*: look at Frobenius). Conclude that there is a subextension $F_1 \subset F$ such that $\mathrm{Gal}(F_1/K) \simeq \mathbb{Z}_p$ and such that some prime above l splits completely in F_1/K.

13.3. (a) Show that if $\sqrt{2} \notin K$ then $K(\sqrt{2})/K$ is the first step of the cyclotomic $\mathbb{Z}_2$-extension of K.
(b) Show that $\mathbb{Q}(\sqrt{-6}, \sqrt{2})/\mathbb{Q}(\sqrt{-6})$ is unramified. Hence it is possible that K_1/K_0 is unramified in a $\mathbb{Z}_p$-extension (see also Exercise 13.4).
(c) Show that the ideal $(2, \sqrt{-6})$ is not principal in $\mathbb{Q}(\sqrt{-6})$ but is principal in $\mathbb{Q}(\sqrt{-6}, \sqrt{2})$. Show also that it represents a class in A^-. This shows that Proposition 13.26 does not hold for $p = 2$ (see also Ferrero [3]).

13.4. Let ψ_9 be a Dirichlet character of conductor 9 with $\psi_9^3 = 1$. Let χ_7 be of conductor 7 with $\chi_7^3 = 1$. Let K_0 be the field corresponding to $\chi_7\psi_9$ in the sense of Chapter 3. Show that K_0 is totally real. Show that the first step K_1 of the cyclotomic $\mathbb{Z}_3$-extension of K_0 corresponds to the group generated by χ_7 and ψ_9. Show that K_1/K_0 is unramified of degree 3. Hilbert's Theorem 94 (Hilbert [2]) states than in an unramified cyclic extension of odd prime degree p, at least one ideal class becomes principal. Conclude that the map $A_0 \to A_1$ is not injective. This shows that Proposition 13.26 does not hold for A_n^+.

13.5. Let M be a finitely generated Λ-module. Show that there is a unique (Hausdorff) topology which makes the action of Λ continuous, and show that M is compact with respect to this topology.

13.6. Let α be algebraic and irrational. Let $K \subset \bar{\mathbb{Q}}$ (= algebraic closure) be a maximal extension of $\mathbb{Q}$ not containing α. Show that $\mathrm{Gal}(\bar{\mathbb{Q}}/K) \simeq \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}_p$ for some p (cf. Lang [6], Ch. 8, Exercise 3).

13.7. Show that for each $n \geq 1$ there are infinitely many cyclic extensions of $\mathbb{Q}$ of degree p^n which are not contained in the $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Show this is also true with $\mathbb{Q}$ replaced by any number field K. This shows that not every such extension starts a $\mathbb{Z}_p$-extension.

13.8. Show that $C_1^{(n)}$ (Section 13.8) is the set of products of the form

$$\prod_i (\zeta_{p^{n+1}}^{a_i} - 1)^{n_i}$$

with $p \nmid a_i$, $\sum n_i = 0$, and $\prod a_i^{n_i} \equiv 1 \bmod p$.

13.9. (a) Observe that the Kummer homomorphism can be defined for any unit u (i.e., we do not need $u \equiv 1 \bmod (\zeta_p - 1)$). Suppose $\varepsilon \in \mathbb{Z}[\zeta_p]$ is a global unit which is congruent to a rational integer mod p. Show that $\phi_k(\varepsilon) = 0$, $2 \leq k \leq p - 3$.
(b) Let p be a regular prime. Show that for $i, k = 2, 4, \ldots, p - 3$,

$$\phi_k(E_k) \neq 0$$

$$\phi_k(E_i) = 0, \qquad i \neq k,$$

where E_k is as in Chapter 8.

(c) Let ε be as in (a) and assume p is regular. Show that ε is the pth power of a unit of $\mathbb{Z}[\zeta_p]$.

13.10. Show that if p is regular then Theorem 13.56 is trivially true.

13.11. Let K_∞/K_0 be a $\mathbb{Z}_p$-extension. Suppose $K_\infty \subseteq L$, L/K_0 is Galois, and L/K_∞ is unramified. Let $G = \mathrm{Gal}(L/K_0)$, $X = \mathrm{Gal}(L/K_\infty)$, and $\Gamma = G/X = \mathrm{Gal}(K_\infty/K_0)$.
(a) Let $\not{p}$ be a prime of L which is totally ramified in K_∞/K_0 and let $I \subseteq G$ be its inertia group. Show that for $n \geq 0$, I^{p^n} is the inertia group in $\mathrm{Gal}(L/K_n)$ for $\not{p}$, and that $I^{p^n} \simeq \Gamma^{p^n}$ under the map $G \to \Gamma$.
(b) Suppose F/K_0 is a finite extension with $F \subseteq L$. Show that I^{p^n} acts trivially on F for n sufficiently large. Conclude that, for n large, the (possibly trivial) extension FK_n/K_n is unramified at $\not{p}$.
(c) Suppose X is abelian. Show that each finite subextension of L/K_∞ is obtained by lifting an abelian extension F/K_n, for some n, to K_∞. Use (b) to show that we may assume the extension F/K_n is unramified.
(d) Conclude that the field $L = \bigcup L_n$ in the proof of Theorem 13.13 is the maximal unramified abelian p-extension of K_∞.

13.12. Let M be a Λ-module. Define $M^\Gamma = \{m \in M \mid \gamma_m = m$ for all $\gamma \in \Gamma\}$ and $M_\Gamma = M/TM$. Then M^Γ and M_Γ are the largest submodule and quotient, respectively, on which Γ acts trivially. Observe that M^Γ is the kernel of multiplication by T. Suppose M^Γ and M_Γ are finite. Define

$$Q(M) = \frac{|M^\Gamma|}{|M_\Gamma|}$$

(this is a Herbrand quotient. See Lang [1], p. 179).
(a) Show that if M is finite then $Q(M) = 1$ (*Hint*: $M/M^\Gamma \simeq TM$).
(b) Suppose $0 \to A \to B \to C \to 0$ is an exact sequence of Λ-modules. Show that $Q(A)Q(C) = Q(B)$ in the sense that if two factors are defined, so is the third and equality holds (*Hint*: Apply the Snake Lemma to two copies of the sequence, with vertical maps multiplication by T).
(c) Suppose $M = \Lambda/(f)$ with $f(0) \neq 0$. Show that $Q(M) = |f(0)|_p$.
(d) Extend (c) to $M = \bigoplus \Lambda/(f_i)$.
(e) Suppose M is a Λ-module with $M \sim \bigoplus \Lambda/(f_i)$. Let $F = \prod f_i$, and suppose $F(0) \neq 0$. Show that $Q(M) = |F(0)|_p$.
(f) Show that the Main Conjecture for $\mathbb{Q}(\zeta_p)$ implies that $|\varepsilon_i A_0| = |B_{1,\omega^{-i}}|_p^{-1}$ (compare p. 299. *Hint*: Prop. 13.22. The analytic class number formula changes the inequalities to equalities, so you do not need to know M^Γ).

Chapter 14

The Kronecker–Weber Theorem

The Kronecker–Weber theorem asserts that every abelian extension of the rationals is contained in a cyclotomic field. It was first stated by Kronecker in 1853, but his proof was incomplete. In particular, there were difficulties with extensions of degree a power of 2. Even in the proof we give below this case requires special consideration. The first proof was given by Weber in 1886 (there was still a gap; see Neumann [1]). Both Kronecker and Weber used the theory of Lagrange resolvents. In 1896, Hilbert gave another proof which relied more on an analysis of ramification groups. Now, the theorem is usually given as an easy consequence of class field theory. We do this in the Appendix. The main point is that in an abelian extension the splitting of primes is determined by congruence conditions, and we already know that p splits in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \bmod n$.

The purpose of the present chapter is to give a proof of the Kronecker–Weber theorem independent of class field theory. Our argument is a modification of one of Shafarevich (see Narkiewicz [1]), where the global result is deduced from the corresponding result for local fields $\mathbb{Q}_p$. Except for a few minor references, this chapter is independent of the rest of the book.

One significance of the Kronecker–Weber theorem is that it shows how to generate abelian extensions of $\mathbb{Q}$ via an analytic function, namely $e^{2\pi i x}$ evaluated at rational x. For abelian extensions of imaginary quadratic fields, this is accomplished with elliptic modular functions in the theory of complex multiplication. In general, the situation is called Hilbert's Twelfth Problem.

Theorem 14.1 (Kronecker–Weber). *If $K/\mathbb{Q}$ is a finite abelian extension, then*

$$K \subseteq \mathbb{Q}(\zeta_n)$$

for some n.

Theorem 14.2. *If $K/\mathbb{Q}_p$ is a finite abelian extension, then*

$$K \subseteq \mathbb{Q}_p(\zeta_n)$$

for some n.

PROOF. We first show it suffices to prove 14.2.

14.2 (for all p) $\Rightarrow$ 14.1.

Assume $K/\mathbb{Q}$ is abelian. Let p be a prime which ramifies in this extension. Let K_p be the completion at a prime above p. Then $K_p/\mathbb{Q}_p$ is abelian, so

$$K_p \subseteq \mathbb{Q}_p(\zeta_{n_p})$$

for some n_p. Let p^{e_p} be the exact power of p dividing n_p and let

$$n = \prod_{p \text{ ramifies}} p^{e_p}.$$

We claim $K \subseteq \mathbb{Q}(\zeta_n)$. Let $L = K(\zeta_n)$, so $L/\mathbb{Q}$ is abelian and if p ramifies in $L/\mathbb{Q}$ then p ramifies in $K/\mathbb{Q}$. Also, if L_p denotes the completion at a suitable prime of L above p,

$$L_p = K_p(\zeta_n) \subseteq \mathbb{Q}_p(\zeta_{p^{e_p}\cdot n'}) \quad \text{with } (n', p) = 1.$$

Let I_p be the inertia group for p in $L/\mathbb{Q}$. Then I_p may be computed locally, so

$$I_p \simeq \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p),$$

which has order $\phi(p^{e_p})$. Let $I \subseteq \mathrm{Gal}(L/\mathbb{Q})$ be the group generated by all I_p with p ramified (p finite). Since $\mathrm{Gal}(L/\mathbb{Q})$ is abelian,

$$|I| \le \prod |I_p| = \prod \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

Lemma 14.3. *If $F/\mathbb{Q}$ is an extension in which no finite prime ramifies, then $F = \mathbb{Q}$.*

PROOF. A theorem of Minkowski (see Exercise 2.5) states that every ideal class of F contains an integral ideal of norm less than or equal to

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{d_F}$$

where $n = [F : \mathbb{Q}]$, d_F is the absolute value of the discriminant, and $r_2 \le n/2$ is the number of complex places. In particular, this quantity must be at least 1, so

$$\sqrt{d_F} \ge \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2} \ge \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2} \stackrel{\text{def}}{=} b_n.$$

Since $b_2 > 1$ and

$$\frac{b_{n+1}}{b_n} = \left(1 + \frac{1}{n}\right)^n \frac{\pi}{4} \geq 2\frac{\pi}{4} > 1,$$

we must have, if $n \geq 2$,

$$d_F > 1.$$

Consequently there exists a prime p dividing d_F, which means p ramifies. This proves Lemma 14.3. □

Returning to the above, we consider the fixed field F of I. Then $F/\mathbb{Q}$ is unramified at all finite primes, so $F = \mathbb{Q}$. Therefore

$$I = \mathrm{Gal}(L/\mathbb{Q}),$$

hence

$$[L:\mathbb{Q}] = |I| \leq [\mathbb{Q}(\zeta_n):\mathbb{Q}].$$

Since

$$\mathbb{Q}(\zeta_n) \subseteq K(\zeta_n) = L,$$

we have equality, so

$$K \subseteq \mathbb{Q}(\zeta_n).$$

This proves "14.2 ⇒ 14.1." □

We are now reduced to the local situation, where the structure of extensions is much simpler. We shall often use the following well-known result.

Lemma 14.4. *Let K and L be finite extensions of $\mathbb{Q}_p$ such that K/L is unramified. Then*

(a) *$K = L(\zeta_n)$ for some n with $p \nmid n$, and*
(b) *$\mathrm{Gal}(K/L)$ is cyclic.*

Also, for fixed L and for every integer $m \geq 1$, there exists a unique unramified extension K of L which is cyclic of degree m.

We sketch the proof. First consider (a) and (b), and assume K/L is Galois. Let $\mathcal{O}_K$ and $\not{p}_K$ be the integers and maximal ideal for K and define $\mathcal{O}_L$ and $\not{p}_L$ similarly. Since K/L is unramified, there is a canonical isomorphism

$$\mathrm{Gal}(K/L) \simeq \mathrm{Gal}(\mathcal{O}_K \bmod \not{p}_K/\mathcal{O}_L \bmod \not{p}_L)$$

(if there were ramification, we would have to mod out by the inertia group on the left). The right-hand side is an extension of finite fields, hence cyclic. If K/L is not necessarily Galois, then the Galois closure yields a cyclic Galois group; so K/L is already Galois and cyclic. This proves (b). Since every nonzero element of a finite field is a root of unity of order prime to p, we may choose $\zeta_n \in \mathcal{O}_K \bmod \mathfrak{p}_K$ with $(n, p) = 1$ which generates the extension of finite fields. Since $X^n - 1 = 0$ has a solution mod $\mathfrak{p}_K$, Hensel's lemma (note $p \nmid n$) yields a solution in $\mathcal{O}_K$, which generates the extension K/L because of the isomorphism of Galois groups. This proves (a). To prove the last statement, let ζ_n with $p \nmid n$ generate an extension of $\mathcal{O}_L/\mathfrak{p}_L$ of degree m. Then $L(\zeta_n)/L$ is unramified and, by the isomorphism of Galois groups, is cyclic of degree m. If there are two such extensions, then the composition is unramified, hence cyclic by (b). Therefore the two extensions must coincide. This proves the lemma. □

In the proof of Theorem 14.2, it will be convenient to know what the answer will be. Unramified extensions of $\mathbb{Q}_p$ will be given by Lemma 14.4. In particular, we already have a good supply of unramified extensions. The ramified extensions of $\mathbb{Q}_p$ will be subfields of $\mathbb{Q}_p(\zeta_{p^n})$. Since our list of abelian extensions already includes such subfields, we can produce totally ramified extensions $K/\mathbb{Q}_p$ with any group

$$\mathrm{Gal}(K/\mathbb{Q}_p) \subseteq \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}, & p \neq 2, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}, & p = 2, \end{cases}$$

for all $n \geq 0$. The fact that we can get $(\mathbb{Z}/2\mathbb{Z})^2$ for $p = 2$ will cause slight problems.

We now start the proof of Theorem 14.2. Observe that it suffices to assume

$$\mathrm{Gal}(K/\mathbb{Q}_p) \simeq \mathbb{Z}/q^m\mathbb{Z}, \qquad q = \text{prime}, m \geq 1.$$

We consider three cases: $p \neq q$, $p = q \neq 2$, and $p = q = 2$.

Case I. $q \neq p$

Lemma 14.5. *Let K and L be finite extensions of $\mathbb{Q}_p$ and let $\mathfrak{p}_L$ be the maximal ideal of the integers of L. Suppose K/L is totally ramified of degree e with $p \nmid e$ (i.e., K/L is tamely ramified). Then there exists $\pi \in L$ of order 1 at $\mathfrak{p}_L$ and a root α of*

$$X^e - \pi = 0$$

such that $K = L(\alpha)$.

PROOF. Let $|x|$ be the absolute value on $\mathbb{C}_p$ (= completion of the algebraic closure of $\mathbb{Q}_p$). Let $\pi_0 \in \mathfrak{p}_L$ be of order 1. Choose $\beta \in K$ to be a uniformizing parameter, so that

$$|\beta|^e = |\pi_0|.$$

Then

$$\beta^e = \pi_0 u \quad \text{with } u \in U_K = \text{units of } K.$$

Since K/L is totally ramified, the extension of residue class fields is trivial. Consequently

$$u \equiv u_0 \bmod \mathfrak{p}_K \quad \text{with } u_0 \in U_L.$$

Therefore

$$u = u_0 + x \quad \text{with } x \in \mathfrak{p}_K.$$

Let $\pi = \pi_0 u_0$, so

$$\beta^e = \pi_0 u_0 + \pi_0 x = \pi + \pi_0 x$$

and

$$|\beta^e - \pi| < |\pi_0| = |\pi|.$$

Let $\alpha_1, \ldots, \alpha_e$ be the roots of

$$f(X) = X^e - \pi.$$

Since the α's differ by roots of unity,

$$|\alpha_i| = |\alpha_j| \quad \text{for all } i, j,$$

so

$$|\alpha_i - \alpha_1| \leq \operatorname{Max}(|\alpha_i|, |\alpha_1|) = |\alpha_1|.$$

But

$$\prod_{i \neq 1} |\alpha_i - \alpha_1| = |f'(\alpha_1)| = |e\alpha_1^{e-1}| = |\alpha_1|^{e-1}.$$

Consequently

$$|\alpha_i - \alpha_1| = |\alpha_1|, \qquad i \neq 1.$$

Since

$$\prod_i |\beta - \alpha_i| = |f(\beta)| < |\pi| = \prod_i |\alpha_i|,$$

we must have for some α_i, say α_1, that

$$|\beta - \alpha_1| < |\alpha_1|.$$

Therefore

$$|\beta - \alpha_1| < |\alpha_i - \alpha_1|, \qquad i \neq 1.$$

By Krasner's lemma (Lemma 5.3),

$$L(\alpha_1) \subseteq L(\beta) \subseteq K.$$

But $f(X)$ is irreducible by the Eisenstein criterion, so

$$[L(\alpha_1) : L] = e = [K : L].$$

This completes the proof of Lemma 14.5. □

Lemma 14.6. $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$.

Proof. Let

$$\begin{aligned} g(X) &= \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + pX^{p-2} + \cdots + p. \end{aligned}$$

Then

$$0 = g(\zeta_p - 1) \equiv (\zeta_p - 1)^{p-1} + p \bmod (\zeta_p - 1)^p,$$

so

$$u = \frac{(\zeta_p - 1)^{p-1}}{-p} \equiv 1 \bmod (\zeta_p - 1).$$

It follows that

$$u_1 = \lim_{n \to \infty} u^{-(1+p+\cdots+p^n)}$$

exists in $\mathbb{Q}_p(\zeta_p)$ and satisfies

$$u_1^{p-1} = u.$$

Therefore $(-p)^{1/(p-1)} \in \mathbb{Q}_p(\zeta_p)$. Since $X^{p-1} + p$ is irreducible over $\mathbb{Q}_p$ by the Eisenstein criterion, the lemma follows easily. □

Now assume $K/\mathbb{Q}_p$ is abelian of degree q^m. Let $L/\mathbb{Q}_p$ be the maximal unramified subextension (= fixed field of the inertia group). Then

$$L \subseteq \mathbb{Q}_p(\zeta_p)$$

for some n, by Lemma 14.4. Let $e = [K : L]$. Since e is a power of q, $p \nmid e$, so K/L is totally and tamely ramified. By Lemma 14.5,

$$K = L(\pi^{1/e}).$$

for some π of order 1 in L. Since $L/\mathbb{Q}_p$ is unramified, p has order 1 in L, so

$$\pi = -up$$

for some unit $u \in L$. Since u is a unit and $p \nmid e$, the extension $L(u^{1/e})/L$ is unramified; hence by Lemma 14.4

$$L(u^{1/e}) \subseteq L(\zeta_M) \subseteq \mathbb{Q}_p(\zeta_{Mn})$$

for some M. In particular, $\mathbb{Q}_p(u^{1/e}) \subseteq \mathbb{Q}_p(\zeta_{Mn})$, so

$$\mathbb{Q}_p(u^{1/e})/\mathbb{Q}_p$$

is abelian. Since $K/\mathbb{Q}_p$ is abelian, $\mathbb{Q}_p(\pi^{1/e})/\mathbb{Q}_p$ is abelian. It follows that

$$\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$$

is also abelian. But $X^e + p$ is irreducible over $\mathbb{Q}_p$. It yields an abelian, hence Galois, extension of $\mathbb{Q}_p$, so

$$\mathbb{Q}_p((-p)^{1/e}) = \mathbb{Q}_p(\zeta_e(-p)^{1/e})$$

for a primitive eth root of unity ζ_e. Therefore

$$\zeta_e \in \mathbb{Q}_p((-p)^{1/e}).$$

Since $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is totally ramified, so is the subextension $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$. But $p \nmid e$, so the latter extension is trivial and $\zeta_e \in \mathbb{Q}_p$. Therefore $e | p - 1$ (if $p = 2$ we obtain $e = 1$ or 2, but since $q \neq p$, $e = 2$ is excluded).

We may now put things back together. By Lemma 14.6,

$$\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p(\zeta_p).$$

Therefore

$$K = L(\pi^{1/e}) \subseteq L(u^{1/e}, (-p)^{1/e}) \subseteq \mathbb{Q}_p(\zeta_{Mnp}).$$

This finishes Case I.

Case II. $p = q \neq 2$

Lemma 14.7. *Let F be a field of characteristic $\neq p$, let $M = F(\zeta_p)$, and let $L = M(a^{1/p})$ for some $a \in M$. Define the character ω: $\mathrm{Gal}(M/F) \to \mathbb{Z}_p$ by $\sigma\zeta_p = \zeta_p^{\omega(\sigma)}$. Then*

$$L/F \text{ is abelian} \Rightarrow \sigma(a) \equiv a^{\omega(\sigma)} \bmod (M^\times)^p$$

for all $\sigma \in \mathrm{Gal}(M/F)$.

Remarks. $\mathbb{Z}_p$ acts on $M^\times/(M^\times)^p$ in the obvious way, so $a^{\omega(\sigma)} \bmod (M^\times)^p$ is defined. The converse of the lemma is also true but will not be needed. One first shows that L/F is Galois, then reverses the proof below to obtain abelian. The lemma is sometimes stated as

$$L/F \text{ is abelian} \Leftrightarrow \text{there exists } c \in M \text{ such that } \sigma_g\, a = a^g c^p,$$

where σ_g: $\zeta_p \mapsto \zeta_p^g$ generates $\mathrm{Gal}(M/F)$.

Proof of Lemma 14.7. Let $G = \mathrm{Gal}(M/F)$ and $H = \mathrm{Gal}(L/M)$. Then G acts on H as follows. If $\sigma \in G$, extend it to an element of $\mathrm{Gal}(L/F)$. Then define $h^\sigma = \sigma h \sigma^{-1}$. This is well-defined since H is abelian. In fact, since L/F is abelian, this action is trivial.

Let A be the subgroup of $M^\times/(M^\times)^p$ generated by a. We have the Kummer pairing

$$H \times A \to W_p = p\text{th roots of unity},$$

$$\langle h, a\rangle = \frac{h(a^{1/p})}{a^{1/p}}.$$

It is bilinear and nondegenerate. As in Chapter 10, we have

$$\langle h^\sigma, a^\sigma\rangle = \langle h, a\rangle^\sigma, \qquad \sigma \in G.$$

Since G acts trivially on H and acts on W_p via ω,

$$\langle h, a^{\omega(\sigma)}\rangle = \langle h, a\rangle^\sigma = \langle h^\sigma, a^\sigma\rangle = \langle h, a^\sigma\rangle$$

for all h. Since the pairing is nondegenerate,

$$a^{\omega(\sigma)} \equiv a^\sigma \bmod (M^\times)^p.$$

This completes the proof of Lemma 14.7. □

Let $K/\mathbb{Q}_p$ be cyclic of degree p^m. We already have a totally ramified cyclic extension $K_r/\mathbb{Q}_p$ of degree p^m contained in $\mathbb{Q}(\zeta_{p^{m+1}})$, namely the fixed field of the subgroup of order $p - 1$ in the Galois group. There is also an unramified cyclic extension $K_u/\mathbb{Q}_p$ of degree p^m (Lemma 14.4) which equals $\mathbb{Q}_p(\zeta_n)$ for some n. Since $K_r \cap K_u = \mathbb{Q}_p$,

$$\operatorname{Gal}(K_r K_u/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^m\mathbb{Z})^2.$$

Suppose $K \not\subseteq \mathbb{Q}(\zeta_{p^{m+1}}, \zeta_n)$. Then

$$\operatorname{Gal}(K(\zeta_{p^{m+1}}, \zeta_n)/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^m\mathbb{Z})^2 \times \mathbb{Z}/p^{m'}\mathbb{Z}$$

for some $m' > 0$. This group has $(\mathbb{Z}/p\mathbb{Z})^3$ as a quotient, so there is a field N such that

$$\operatorname{Gal}(N/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3.$$

The following lemma finishes the proof of Case II.

Lemma 14.8. *Assume $p \neq 2$. There are no extensions $N/\mathbb{Q}_p$ with* $\operatorname{Gal}(N/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$.

Proof. If we have such an N, then $N(\zeta_p)/\mathbb{Q}_p$ is abelian and

$$\operatorname{Gal}(N(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \simeq (\mathbb{Z}/p\mathbb{Z})^3$$

This is a Kummer extension so there is a corresponding subgroup

$$B \subseteq \mathbb{Q}_p(\zeta_p)^\times/(\mathbb{Q}_p(\zeta_p)^\times)^p$$

with $B \simeq (\mathbb{Z}/p\mathbb{Z})^3$ and $\mathbb{Q}_p(\zeta_p)(B^{1/p}) = N(\zeta_p)$. Let $a \in B$ and let $L = \mathbb{Q}_p(\zeta_p, a^{1/p})$. Then $L/\mathbb{Q}_p$ is abelian, so

$$\sigma a \equiv a^{\omega(\sigma)} \bmod (\mathbb{Q}_p(\zeta_p)^\times)^p, \qquad \sigma \in \operatorname{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p).$$

Let v be the valuation on $\mathbb{Q}_p(\zeta_p)$ with $v(\zeta_p - 1) = 1$. Then

$$v(a) = v(\sigma a) \equiv \omega(\sigma) v(a) \bmod p, \qquad \text{for all } \sigma.$$

Since $\sigma\zeta_p \neq \zeta_p$ if $\sigma \neq 1$, we have $\omega(\sigma) \not\equiv 1 \bmod p$ for such σ. Therefore

$$v(a) \equiv 0 \bmod p.$$

Since

$$\mathbb{Q}_p(\zeta_p)^\times = (\zeta_p - 1)^{\mathbb{Z}} \times W_{p-1} \times U_1$$

where $U_1 = \{u \equiv 1 \bmod \zeta_p - 1\}$, we may change a by a pth power to obtain $a \in U_1$. So we may assume

$$B \subseteq U_1/U_1^p,$$

and $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ acts via the character ω.

Let $\pi = \zeta_p - 1$ and let $u = 1 + b\pi + \cdots \in U_1$ (with $b \in \mathbb{Z}$). Since

$$\zeta_p^b \equiv 1 + b\pi \bmod \pi^2,$$

we have $u_1 = \zeta_p^{-b}u \equiv 1 \bmod \pi^2$. An easy calculation shows that $u_1^p \equiv 1 \bmod \pi^{p+1}$, hence $u^p \equiv 1 \bmod \pi^{p+1}$. Conversely, if $u_2 \equiv 1 \bmod \pi^{p+1}$, then

$$\frac{1}{p}\log_p u_2 \equiv 0 \bmod \pi^2,$$

hence

$$u = \exp\left(\frac{1}{p}\log_p u_2\right)$$

converges to an element of U_1 and $u^p = u_2$ (see Section 5.1; alternatively, the binomial series for $(1 + u_2 - 1)^{1/p}$ converges). Therefore

$$U_1^p = \{u \equiv 1 \bmod \pi^{p+1}\}.$$

Again, let $u \in U_1$. Write $u = \zeta_p^b u_1$ with $u_1 \equiv 1 \bmod \pi^2$. If $u \in B$ then

$$\sigma u \equiv u^{\omega(\sigma)} \bmod U_1^p, \qquad \sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$$

Since ζ_p^b already satisfies this relation, so does u_1. Write

$$u_1 = 1 + c\pi^d + \cdots$$

with $c \in \mathbb{Z}$, $(c, p) = 1$, and $d \geq 2$. Since $(\sigma\pi)/\pi \equiv \omega(\sigma) \bmod \pi$,

$$\sigma u_1 = 1 + c\omega(\sigma)^d\pi^d + \cdots.$$

But

$$u_1^{\omega(\sigma)} = 1 + c\omega(\sigma)\pi^d + \cdots.$$

Since $\sigma u_1 \equiv u_1^{\omega(\sigma)} \bmod U_1^p$ for all σ, we must have either $d \geq p + 1$ or $d \equiv 1 \bmod p - 1$. The first means that u_1 is in U_1^p, the second that $d = p$. Clearly $1 + \pi^p$ generates modulo U_1^p the subgroup of $u_1 \equiv 1 \bmod \pi^p$. Putting everything back together, we obtain

$$B \subseteq \langle \zeta_p, 1 + \pi^p \rangle \subseteq U_1/U_1^p.$$

where $\langle x, y \rangle$ denotes the subgroup generated by x and y. Since $B \simeq (\mathbb{Z}/p\mathbb{Z})^3$, we have a contradiction. This proves Lemma 14.8. □

Case III. $p = q = 2$

We already have a totally ramified abelian extension $K_r = \mathbb{Q}_2(\zeta_{2^{m+2}})$ with

$$\mathrm{Gal}(K_r/\mathbb{Q}_2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}.$$

We also have an unramified extension K_u with

$$\mathrm{Gal}(K_u/\mathbb{Q}_2) \simeq \mathbb{Z}/2^m\mathbb{Z}.$$

Since $K_r \cap K_u = \mathbb{Q}_2$,

$$\mathrm{Gal}(K_rK_u/\mathbb{Q}_2) \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^m\mathbb{Z})^2.$$

Let $K/\mathbb{Q}_2$ be cyclic of degree 2^m and suppose $K \not\subseteq K_rK_u$. Then $\mathrm{Gal}(KK_rK_u/\mathbb{Q}_2)$ has exponent 2^m, requires at most 4 generators, one of which has order 2, and has $\mathrm{Gal}(K_rK_u/\mathbb{Q}_2)$ as a quotient by a nontrivial subgroup. Therefore

$$\mathrm{Gal}(KK_rK_u/\mathbb{Q}_2) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^m\mathbb{Z})^2 \times \mathbb{Z}/2^{m'}\mathbb{Z}, & \text{with } m' \geq 1, \\ \text{or} & \\ (\mathbb{Z}/2^m\mathbb{Z})^2 \oplus (\mathbb{Z}/2^{m'}\mathbb{Z}), & \text{with } m \geq m' \geq 2. \end{cases}$$

Therefore there is a field N with

$$\mathrm{Gal}(N/\mathbb{Q}_2) \simeq \begin{cases} (\mathbb{Z}/2\mathbb{Z})^4 \\ \text{or} \\ (\mathbb{Z}/4\mathbb{Z})^3. \end{cases}$$

We shall show this is impossible. The first corresponds to four independent quadratic extensions of $\mathbb{Q}_2$. We have

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \{\pm 1\} \times U_1/U_1^2$$

where $U_1 = \{u \equiv 1 \bmod 4\}$. As in Case II, it is easy to see that $U_1^2 = \{u \equiv 1 \bmod 8\}$, hence

$$U_1/U_1^2 \simeq \mathbb{Z}/2\mathbb{Z}.$$

Therefore

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^3.$$

By Kummer theory, the first possibility is now eliminated.

Suppose now that $\mathrm{Gal}(N/\mathbb{Q}_2) \simeq (\mathbb{Z}/4\mathbb{Z})^3$. Then $i = \sqrt{-1} \in N$, otherwise we could add it to N and obtain a subfield whose Galois group would be $(\mathbb{Z}/2\mathbb{Z})^4$, which we just excluded. It follows easily that there is a field L with

$$\mathbb{Q}_2(i) \subset L \subset N$$

and

$$\mathrm{Gal}(L/\mathbb{Q}_2) \simeq \mathbb{Z}/4\mathbb{Z}$$

(proof: every subgroup of $(\mathbb{Z}/4\mathbb{Z})^3$ of order 32 contains a subgroup of the form $(\mathbb{Z}/4\mathbb{Z})^2$. Let L be the fixed field).

Let σ be a generator of $\mathrm{Gal}(L/\mathbb{Q}_2)$. Then σ^2 generates $\mathrm{Gal}(L/\mathbb{Q}_2(i))$ and $\sigma(i) = -i$. We may write

$$L = \mathbb{Q}_2(i, \alpha)$$

with $\alpha^2 \in \mathbb{Q}_2(i)$. We also have $L = \mathbb{Q}_2(i, \sigma\alpha)$ and $(\sigma\alpha)^2 = \sigma(\alpha^2) \in \mathbb{Q}_2(i)$, since $\mathbb{Q}_2(i)/\mathbb{Q}_2$ is Galois. Therefore

$$\sigma^2(\alpha) = -\alpha \quad \text{and} \quad \sigma^2(\sigma\alpha) = -\sigma\alpha.$$

It follows that $\sigma\alpha/\alpha$ is fixed by σ^2, so

$$\frac{\sigma\alpha}{\alpha} = A + Bi \in \mathbb{Q}_2(i)$$

and

$$\frac{\sigma^2\alpha}{\sigma\alpha} = \sigma(A + Bi) = A - Bi.$$

We obtain

$$-1 = \frac{\sigma^2\alpha}{\alpha} = \frac{\sigma^2\alpha}{\sigma\alpha}\frac{\sigma\alpha}{\alpha} = A^2 + B^2.$$

Lemma 14.9. $A^2 + B^2 = -1$ *has no solutions in* $\mathbb{Q}_2$.

Proof. We may transform this to

$$A_1^2 + A_2^2 + A_3^2 = 0$$

with $A_i \in \mathbb{Z}_2$, $1 \le i \le 3$, and $2 \nmid A_i$ for some i. But there are no nontrivial solutions mod 8. This completes the proof of the lemma. □

The lemma shows that we have a contradiction. Therefore $K \subseteq K_r K_u \subseteq \mathbb{Q}_2(\zeta_M)$ for some M. This finishes Case III, so Theorem 14.2 is completely proved. □

Notes

The Kronecker–Weber theorem was first stated by Kronecker [1] and was proved by Weber [1]. Later proofs were given by Hilbert [1] and Speiser [1]. See also M. Greenberg [1] and Ribenboim [2]. Our use of Lemma 14.5 in Case I, which allows us to avoid using higher ramification groups, is similar to the proof of Abhyankar's lemma in Cornell [1]. A global proof of Theorem 14.1 which has the same flavor as the present proof may be found in Long [1]. A proof, similar to the above, of a more general local Kronecker-Weber theorem has recently been given by Rosen [2]. For two more proofs of the global theorem, plus some interesting historical remarks, see Neumann [1].

Appendix

In this appendix, we summarize, usually without proofs, some of the basic machinery that is needed in the book. The first section, on inverse limits, is used in Chapters 12 and 13. Infinite Galois theory and ramification theory are used primarily in Chapter 13. The main points of the section are that the usual Galois correspondence holds if we work with closed subgroups and that we may talk about ramification for infinite extensions, even though the rings involved are not necessarily Dedekind domains (much of this section comes from a course of Iwasawa in 1971). The last section summarizes those topics from class field theory that we use in the book. The reader willing to believe that the Galois group of the maximal unramified abelian extension is isomorphic to the ideal class group (and variants of this statement) will have enough background to read all but certain parts of Chapter 13.

§1 Inverse Limits

Let I be a directed set. This means that there is a partial ordering on I, and for every $i, j \in I$ there exists $k \in I$ with $i \leq k, j \leq k$. For each $i \in I$, let A_i be a set (or group, ring, etc.). We assume that whenever $i \leq j$ there is a map $\phi_{ji}\colon A_j \to A_i$ such that $\phi_{ii} = id$ and $\phi_{ji}\phi_{kj} = \phi_{ki}$ whenever $i \leq j \leq k$. This situation is called an inverse system.

Let $A = \prod A_i$ and define the *inverse limit* by

$$\varprojlim A_i = \{(\ldots, a_i, \ldots) \in A \mid \phi_{kj}(a_k) = a_j \text{ whenever } j \leq k\}.$$

For each i, there is a map $\phi_i\colon \varprojlim A_i \to A_i$ induced by the projection $A \to A_i$. Clearly $\phi_{ji}\phi_j = \phi_i$.

Assume now that each A_i is a Hausdorff topological space. Then A is given the product topology and $\varprojlim A_i$ receives the topology it inherits from A.

We assume the maps ϕ_{ji} are continuous. The maps ϕ_i are always continuous: If U_i is open in A_i then $\phi_i^{-1}(U_i)$ is the intersection in A of an open set of A (definition of product topology) and $\varprojlim A_i$, hence open. The topology of $\varprojlim A_i$ is generated by unions and finite intersections of such sets $\phi_i^{-1}(U_i)$. In fact, every open set contains $\phi_k^{-1}(U_k)$ for some k and some U_k (proof: it suffices to show that $\phi_i^{-1}(U_i) \cap \phi_j^{-1}(U_j) = \phi_k^{-1}(U_k)$ for some k. Choose $k \geq i, j$ and let $U_k = \phi_{kj}^{-1}(U_j) \cap \phi_{ki}^{-1}(U_i)$).

We claim that $\varprojlim A_i$ is closed in A. Suppose $a = (\ldots, a_i, \ldots) \notin \varprojlim A_i$. Then $\phi_{ji}(a_j) \neq a_i$ for some i, j. Let U_1 and U_2 be neighborhoods of $\phi_{ji}(a_j)$ and a_i, respectively, such that $U_1 \cap U_2 = \varnothing$. Let $U_3 = \phi_{ji}^{-1}(U_1)$ and let

$$U = U_2 \times U_3 \times \prod_{k \neq i, j} A_k \subseteq A.$$

Then $a \in U$ but $U \cap \varprojlim A_i = \varnothing$. Since U is open, it follows that $\varprojlim A_i$ is closed.

Suppose now that each A_i is finite, with the discrete topology. Then A is compact, hence $\varprojlim A_i$ is compact. Also, $\varprojlim A_i$ can be shown to be nonempty and totally disconnected (the only connected sets are points). An inverse limit of finite sets is called *profinite*. If each A_i is a finite group and the maps ϕ_{ji} are homomorphisms, then $\varprojlim A_i$ is a compact group in the natural manner. It can be shown that all compact totally disconnected groups are profinite. Also, if G is profinite then $G = \varprojlim G/U$, where U runs through the open normal subgroups (necessarily of finite index, by compactness) of G, ordered by inclusion.

Examples. (1) Let I be the positive integers, $A_i = \mathbb{Z}/p^i\mathbb{Z}$, ϕ_{ji}: $a \bmod p^j \mapsto a \bmod p^i$. Then $\varprojlim \mathbb{Z}/p^i\mathbb{Z} = \mathbb{Z}_p$, the p-adic integers. The maps ϕ_i are the natural maps $\mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$. In essence, the ith component represents the ith partial sum of the p-adic expansion.

(2) Let I be the positive integers ordered by $m \leq n$ if $m \mid n$. If $m \mid n$, there is a natural map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Let $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. It can be shown, via the Chinese Remainder Theorem, that $\hat{\mathbb{Z}} \simeq \prod_{\text{all } p} \mathbb{Z}_p$.

For more on inverse limits, see Shatz [1] or any book on homological algebra.

§2 Infinite Galois Theory and Ramification Theory

Let K/k be an algebraic extension of fields and assume it is also Galois (normal, and generated by roots of separable polynomials). As usual, $G = \mathrm{Gal}(K/k)$ is the group of automorphisms of K which fix k pointwise. Suppose $k \subseteq F \subseteq K$ with F/k finite. Then $G_F = \mathrm{Gal}(K/F)$ is of finite index in G. The topology on G is defined by letting such G_F form a basis for the neighborhoods of the identity in G. Then G is profinite, and

$$G \simeq \varprojlim G/G_F \simeq \varprojlim \operatorname{Gal}(F/k),$$

where F runs through the normal finite subextensions F/k, or through any subsequence of such F such that $\bigcup F = K$. The ordering on the indices F is via inclusion ($F_1 \subseteq F_2$) and the maps used to obtain the inverse limit are the natural maps $\operatorname{Gal}(F_2/k) \to \operatorname{Gal}(F_1/k)$. The fundamental theorem of Galois theory now reads as follows:

There is a one-one correspondence between closed subgroups H of G and fields L with $k \subseteq L \subseteq K$:

$$H \leftrightarrow \textit{fixed field of } H,$$

$$\operatorname{Gal}(K/L) \leftrightarrow L.$$

Open subgroups correspond to finite extensions, normal subgroups correspond to normal extensions, etc.

Examples. (1) Consider $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$. An element $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ is determined by its action on ζ_{p^n} for all $n \geq 1$. For each n we have $\sigma\zeta_{p^n} = \zeta_{p^n}^{a_n}$ for some $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, and clearly $a_n \equiv a_{n-1} \bmod p^{n-1}$. So we obtain an element of

$$\mathbb{Z}_p^\times = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times = \varprojlim \operatorname{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}).$$

Conversely, if $a \in \mathbb{Z}_p^\times$ then $\sigma\zeta_{p^n} = \zeta_{p^n}^a$ defines an automorphism. The closed (and open) subgroup $1 + p^n\mathbb{Z}_p$ corresponds to its fixed field $\mathbb{Q}(\zeta_{p^n})$.

(2) Let $\mathbb{F}$ be a finite field and let $\bar{\mathbb{F}}$ be its algebraic closure. For each n, there is a unique extension of $\mathbb{F}$ of degree n, and the Galois group is cyclic, generated by the Frobenius. Therefore

$$\operatorname{Gal}(\bar{\mathbb{F}}/\mathbb{F}) \simeq \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Now suppose that k is an algebraic extension of $\mathbb{Q}$, not necessarily of finite degree. Let $\mathcal{O}_k$ be the ring of all algebraic integers in k and let $\not{p}$ be a nonzero prime ideal of $\mathcal{O}_k$. Then $\not{p} \cap \mathbb{Z}$ is nonzero (if $\alpha \in \not{p}$, $\operatorname{Norm}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \in \not{p} \cap \mathbb{Z}$) and prime, hence $\not{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p. Therefore

$$\mathbb{Z}/p\mathbb{Z} \simeq (\mathbb{Z} + \not{p})/\not{p} \subseteq \mathcal{O}_k/\not{p}.$$

It is easy to see that $\mathcal{O}_k/\not{p}$ is a field and is an algebraic extension of $\mathbb{Z}/p\mathbb{Z}$ (since $\mathcal{O}_k$ is integral over $\mathbb{Z}$). In fact, $\operatorname{Gal}((\mathcal{O}_k/\not{p})/(\mathbb{Z}/p\mathbb{Z}))$ is abelian since any finite extension of a finite field is cyclic, and an inverse limit of abelian groups is clearly abelian.

Let K/k be an algebraic extension, again not necessarily finite. Let $\mathcal{P}$ be a nonzero prime ideal of $\mathcal{O}_K$ and let $\not{p} = \mathcal{P} \cap \mathcal{O}_k$, which is a prime ideal of $\mathcal{O}_k$.

Then $\mathcal{O}_K/\mathcal{P}$ is an extension of $\mathcal{O}_k/\mathfrak{p}$; in fact, it is an abelian extension since $\mathcal{O}_K/\mathcal{P}$ is abelian over $\mathbb{Z}/p\mathbb{Z}$. Conversely, suppose we are given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$. Then there exists $\mathcal{P}$ in $\mathcal{O}_K$ lying above $\mathfrak{p}$; that is, $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_k$ (see Lang [6], Chapter 9, Proposition 9; or Lang [1], Chapter 1, Proposition 9).

Lemma. *Suppose K/k is a Galois extension. Let $\mathcal{P}$ and $\mathcal{P}'$ be primes of K lying above $\mathfrak{p}$. Then there exists $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma\mathcal{P} = \mathcal{P}'$.*

PROOF. We know the lemma is true for finite extensions (see Lang [6], Chapter 9, Proposition 11, or Lang [1], Chapter 1, Proposition 11). Choose a sequence of fields

$$k = F_0 \subseteq \cdots \subseteq F_n \subseteq \cdots \subseteq K$$

such that $K = \bigcup F_n$ and such that each F_n/k is a finite Galois extension. Such a sequence exists since the algebraic closure of $\mathbb{Q}$ is countable. Let

$$\mathfrak{p}_n = \mathcal{P} \cap \mathcal{O}_{F_n}, \qquad \mathfrak{p}'_n = \mathcal{P}' \cap \mathcal{O}_{F_n}.$$

Since F_n/k is finite, there exists $\tau_n \in \mathrm{Gal}(F_n/k)$ such that $\tau_n(\mathfrak{p}_n) = \mathfrak{p}'_n$. Let $\sigma_n \in \mathrm{Gal}(K/k)$ restrict to τ_n. Since $\mathrm{Gal}(K/k)$ is compact, the sequence $\{\sigma_n\}$ has a cluster point σ. There is a subsequence $\{\sigma_{n_i}\}$ which converges to σ (*a priori*, we would have to use a subnet. But subsequences suffice since $\mathrm{Gal}(K/k)$ satisfies the first countability axiom. This follows from the fact that the set of finite subextensions of K/k is countable). For simplicity, assume $\lim \sigma_n = \sigma$. Let m be arbitrary. Since $\mathrm{Gal}(K/F_m)$ is an open neighborhood of 1, $\sigma^{-1}\sigma_n \in \mathrm{Gal}(K/F_m)$ for $n \geq m$ sufficiently large. Hence, $\sigma^{-1}\sigma_n\mathfrak{p}_m = \mathfrak{p}_m$, so $\sigma\mathfrak{p}_m = \sigma_n\mathfrak{p}_m = \sigma_n(\mathfrak{p}_n \cap \mathcal{O}_{F_m}) = \mathfrak{p}'_n \cap \mathcal{O}_{F_m} = \mathfrak{p}'_m$. Since $\mathcal{P} = \bigcup \mathfrak{p}_m$ and $\mathcal{P}' = \bigcup \mathfrak{p}'_m$, we have $\sigma\mathcal{P} = \mathcal{P}'$. This completes the proof. □

We now want to discuss ramification. However, $\mathcal{O}_k$ and $\mathcal{O}_K$ are not necessarily Dedekind domains. For example, if $k = \mathbb{Q}(\zeta_{p^\infty})$ and $\mathfrak{p} = (\zeta_p - 1, \zeta_{p^2} - 1, \ldots)$ then $\mathfrak{p}^p = \mathfrak{p}$, since $(\zeta_{p^{n+1}} - 1)^p = (\zeta_{p^n} - 1)$. This means that we cannot define ramification via factorization of primes. Instead we use inertia groups. Let K/k be a Galois extension, as above, and let $\mathcal{P}$ lie above $\mathfrak{p}$. Define the *decomposition group* by

$$Z = Z(\mathcal{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K/k) \,|\, \sigma\mathcal{P} = \mathcal{P}\}.$$

We claim Z is closed, hence there is a corresponding fixed field. Let the notations be as in the proof of the lemma and let $Z_n = \{\sigma \,|\, \sigma(\mathfrak{p}_n) = \mathfrak{p}_n\}$. Then $Z \subseteq Z_n$ for all n, and since $\mathcal{P} = \bigcup \mathfrak{p}_n$ we have $Z = \cap Z_n$. Since $\mathrm{Gal}(K/F_n) \subseteq Z_n$, we have Z_n open, hence closed (it is the complement of its open cosets). Therefore Z is closed, as claimed.

Now define the *inertia group* by

$$T = T(\mathcal{P}/\mathfrak{p}) = \{\sigma \,|\, \sigma \in Z, \sigma(\alpha) \equiv \alpha \bmod \mathcal{P} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

It is easy to show that T is a closed subgroup. As with the case of finite extensions, we have an exact sequence

$$1 \to T \to Z \to \mathrm{Gal}((\mathcal{O}_K/\mathcal{P})/(\mathcal{O}_k/\not{p})) \to 1.$$

The surjectivity may be proved by using the fact that we have surjectivity for finite extensions (Lang [1] or [6], Proposition 14).

Suppose now that K/k is an algebraic extension but not necessarily Galois. Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Then $\bar{\mathbb{Q}}/K$ and $\bar{\mathbb{Q}}/k$ are Galois extensions. Let $\mathcal{P}$ be a prime of K lying over the prime $\not{p}$ of k. Choose a prime ideal $\mathcal{D}$ of $\mathcal{O}_{\bar{\mathbb{Q}}}$ lying above $\mathcal{P}$. We have

$$\begin{aligned} T(\mathcal{D}/\not{p}) &\subseteq \mathrm{Gal}(\bar{\mathbb{Q}}/k), \\ T(\mathcal{D}/\mathcal{P}) &\subseteq \mathrm{Gal}(\bar{\mathbb{Q}}/K) \subseteq \mathrm{Gal}(\bar{\mathbb{Q}}/k), \\ T(\mathcal{D}/\mathcal{P}) &= T(\mathcal{D}/\not{p}) \cap \mathrm{Gal}(\bar{\mathbb{Q}}/k). \end{aligned}$$

Define the *ramification index* by

$$e(\mathcal{P}/\not{p}) = [T(\mathcal{D}/\not{p}) : T(\mathcal{D}/\mathcal{P})],$$

which is possibly infinite. If $\mathcal{D}'$ is another prime lying above $\mathcal{P}$ then $\mathcal{D}' = \sigma\mathcal{D}$ for some $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$, and

$$\begin{aligned} T(\mathcal{D}'/\not{p}) &= \sigma T(\mathcal{D}/\not{p})\sigma^{-1}, \\ T(\mathcal{D}'/\mathcal{P}) &= \sigma T(\mathcal{D}/\mathcal{P})\sigma^{-1}. \end{aligned}$$

Therefore the index $e(\mathcal{P}/\not{p})$ does not depend on the choice of $\mathcal{D}$. If K/k is Galois then there is the natural restriction map

$$\mathrm{Gal}(\bar{\mathbb{Q}}/k) \to \mathrm{Gal}(K/k)$$

with kernel $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$. It is easy to see that the induced map $T(\mathcal{D}/\not{p}) \to T(\mathcal{P}/\not{p})$ is surjective, with kernel equal to $T(\mathcal{D}/\mathcal{P})$. Therefore

$$T(\mathcal{D}/\not{p})/T(\mathcal{D}/\mathcal{P}) \simeq T(\mathcal{P}/\not{p})$$

and

$$e(\mathcal{P}/\not{p}) = |T(\mathcal{P}/\not{p})|.$$

So the ramification index equals the order of the inertia group, for Galois extensions. It follows that the definition agrees with the usual one for finite extensions.

To consider archimedean primes, we proceed slightly differently. An archimedean place of k is either an embedding $\phi: k \to \mathbb{R}$ or a pair of complex-conjugate embeddings $(\psi, \bar{\psi})$, with $\bar{\psi} \neq \psi$ and $\psi: k \to \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, any embedding ϕ or ψ may be extended to an embedding $\bar{\mathbb{Q}} \to \mathbb{C}$ (use Zorn's lemma). In particular, we can extend to K. If K/k is Galois and ϕ_1 and ϕ_2 are two extensions of ϕ, then $\phi_2^{-1}\phi_1 \in \mathrm{Gal}(K/k)$. Hence $\phi_1 = \phi_2\sigma$ for some σ. If $(\psi_1, \bar{\psi}_1)$ and $(\psi_2, \bar{\psi}_2)$ extend ϕ, we have $\psi_1 = \psi_2\sigma$, hence $(\psi_1, \bar{\psi}_1) = (\psi_2, \bar{\psi}_2)\sigma$, for some σ. A similar result holds for extensions of complex places, so the Galois group acts transitively on the extensions of a given place.

If K/k is Galois, w is an archimedean place of K, and v is the place of k below w, then we define

$$T(w/v) = Z(w/v) = \{\sigma \in \mathrm{Gal}(K/k) \,|\, w\sigma = w\}.$$

It is easy to see that T is nontrivial only when v is real, $w = (\psi, \bar{\psi})$ is complex, and $\sigma \neq 1$ is the "complex conjugation" $\psi^{-1}\bar{\psi}\ (= \bar{\psi}^{-1}\psi)$, which permutes ψ and $\bar{\psi}$ and has order 2. Therefore

$$|T(w/v)| = 1 \text{ or } 2.$$

We may now define the ramification indices for archimedean primes just as we did for finite primes.

For more on the above, see Iwasawa [6], §6.

§3 Class Field Theory

This section consists of three subsections. The first treats global class field theory from the classical viewpoint of ideal groups. The second discusses local class field theory. In the third, we return to the global case, this time using the language of idèles.

We only consider some of the highlights of the theory and give no indications of the proofs. The interested reader can consult, for example, Lang [1], Neukirch [1], Hasse [2], or the articles by Serre and Tate in Cassels and Fröhlich [1].

Global Class Field Theory (first form)

Let k be a number field of finite degree over $\mathbb{Q}$. Let $\mathfrak{M}_0 = \prod \not{p}_i^{e_i}$ denote an integral ideal of k and let $\mathfrak{M}_\infty$ denote a formal squarefree product (possibly empty) of real archimedean places of k. Then $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$ is called a *divisor* of k. For example, $\mathfrak{M} = 1$, $\mathfrak{M} = \infty$, $\mathfrak{M} = 5^3 \cdot 17^2 \cdot \infty$, and $\mathfrak{M} = 3 \cdot 37 \cdot 103$ are divisors of $\mathbb{Q}$. If $\alpha \in k^\times$, then we write $\alpha \equiv 1 \bmod^* \mathfrak{M}$ if (i) $v_{\not{p}_i}(\alpha - 1) \geq e_i$ for all primes $\not{p}_i$ (with $e_i > 0$) in the factorization of $\mathfrak{M}_0$, and (ii) $\alpha > 0$ at the real embeddings corresponding to the archimedean places in $\mathfrak{M}_\infty$. Let $P_{\mathfrak{M}}$ denote the group of principal fractional ideals of k which have a generator $\alpha \equiv 1 \bmod^* \mathfrak{M}$. Let $I_{\mathfrak{M}}$ be the group of fractional ideals relatively prime to $\mathfrak{M}$ (note that $I_{\mathfrak{M}} = I_{\mathfrak{M}_0}$). The quotient $I_{\mathfrak{M}}/P_{\mathfrak{M}}$ is a finite group, called the generalized ideal class group mod $\mathfrak{M}$.

For example, let $k = \mathbb{Q}$, let n be a positive integer, and let $\mathfrak{M} = n$. The group I_n consists of ideals generated by rational numbers relatively prime to

n. Let (r) be such an ideal. Then (r) is generated by $+r$ and by $-r$. If $(r) \in P_n$ then we must have $\pm r \equiv 1 \bmod n$, hence $r \equiv \pm 1 \bmod n$. It follows that

$$I_n/P_n \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}/\{\pm 1\}.$$

Now suppose $\mathfrak{M} = n\infty$. The group $I_{n\infty}$ is the same as I_n, but if $(r) \in P_{n\infty}$ then we must be able to take a *positive* generator congruent to 1 mod n, so we need $|r| \equiv 1 \bmod n$. If $|r| \equiv -1 \bmod n$ then $(r) \notin P_{n\infty}$ (unless $n = 2$), so the archimedean factor makes $P_{\mathfrak{M}}$ smaller. It follows easily that

$$I_{n\infty}/P_{n\infty} \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

The effect of the archimedean primes is apparent in the case of a real quadratic field k. Let $\mathfrak{M}_0 = 1$ and let $\mathfrak{M}_{\infty} = \infty_1\infty_2$ be the product of the two (real) archimedean places. Suppose the fundamental unit ε has norm -1, so ε is positive at one place and negative at the other. Let $(\alpha) = (-\alpha) = (\varepsilon\alpha) = (-\varepsilon\alpha)$ be a principal ideal of k. One of the generators for (α) is positive at both ∞_1 and ∞_2, so every principal ideal has a totally positive generator, and $P = P_1 = P_{\infty_1\infty_2}$. Of course,

$$I_1/P_1 = \text{ideal class group}.$$

By definition,

$$I_{\infty_1\infty_2}/P_{\infty_1\infty_2} = \text{narrow ideal class group}.$$

So we find that the narrow and ordinary class groups are the same. It will follow from subsequent theorems that the narrow ideal class group corresponds to the maximal abelian extension of k which is unramified at all finite places.

Now suppose ε has norm $+1$. Choose $\alpha \in k$ such that $\alpha > 0$ at ∞_1 and $\alpha < 0$ at ∞_2 (for example, $\alpha = 1 + \sqrt{d}$). Then (α) has no totally positive generator, hence $P_{\infty_1\infty_2} \neq P_1$ (the index is easily seen to be 2). Therefore the narrow ideal class group is twice as large as the ordinary class group in this case.

We return to the general situation, so k is a number field of finite degree over $\mathbb{Q}$. Let $\mathcal{O}_k$ denote the ring of integers of k. Consider a finite Galois extension K/k. Let $\not p$ be a prime of $\mathcal{O}_k$ and $\mathcal{P}$ a prime of $\mathcal{O}_K$ above $\not p$. Let $N\not p = |\mathcal{O}_k/\not p| =$ norm to $\mathbb{Q}$ of $\not p$. The finite field $\mathcal{O}_K/\mathcal{P}$ is a finite extension of $\mathcal{O}_k/\not p$ with Galois group generated by the Frobenius $(x \mapsto x^{N\not p})$. Let $Z(\mathcal{P}/\not p)$ be the decomposition group and $T(\mathcal{P}/\not p)$ the inertia group. There is an exact sequence

$$1 \to T(\mathcal{P}/\not p) \to Z(\mathcal{P}/\not p) \to \mathrm{Gal}((\mathcal{O}_K/\mathcal{P})/(\mathcal{O}_k/\not p)) \to 1.$$

Suppose $\mathcal{P}$ is unramified over $\not p$. Then $T = 1$, so Z is cyclic, generated by the (global) Frobenius $\sigma_{\mathcal{P}}$, which is uniquely determined by the relation

$$\sigma_{\mathcal{P}} x \equiv x^{N\not p} \bmod \mathcal{P} \quad \text{for all } x \in \mathcal{O}_K.$$

Suppose τ is an automorphism of K such that $\tau(k) = k$. Then $\tau\mathscr{P}$ is unramified over $\tau\not{p}$. Since $\sigma_{\mathscr{P}}\tau^{-1}x \equiv (\tau^{-1}x)^{N\not{p}} \bmod \mathscr{P}$, we have $\tau\sigma_{\mathscr{P}}\tau^{-1}x \equiv x^{N\not{p}} \bmod \tau\mathscr{P}$. Since $N\not{p} = N\tau\not{p}$, we obtain

$$\sigma_{\tau\mathscr{P}} = \tau\sigma_{\mathscr{P}}\tau^{-1}.$$

If K/k is abelian then $\sigma_{\tau\mathscr{P}} = \sigma_{\mathscr{P}}$ for all $\tau \in \mathrm{Gal}(K/k)$. Hence $\sigma_{\mathscr{P}}$ depends only on the prime $\not{p}$ of k, so we let

$$\sigma_{\not{p}} = \sigma_{\mathscr{P}}.$$

We may extend by multiplicativity to obtain a map, called the *Artin map*,

$$I_{\mathfrak{d}} \to \mathrm{Gal}(K/k),$$

where $\mathfrak{d}$ is the relative discriminant of K/k. What are the kernel and image?

Theorem 1. *Let K/k be a finite abelian extension. Then there exists a divisor $\mathfrak{f}$ of k (the minimal such divisor is called the conductor of K/k) such that the following hold:*

(i) *a prime $\not{p}$ (finite or infinite) ramifies in $K/k \Leftrightarrow \not{p} \mid \mathfrak{f}$.*

(ii) *If $\mathfrak{M}$ is a divisor with $\mathfrak{f} \mid \mathfrak{M}$ then there is a subgroup H with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$ such that*

$$I_{\mathfrak{M}}/H \simeq \mathrm{Gal}(K/k),$$

the isomorphism being induced by the Artin map. In fact, $H = P_{\mathfrak{M}}N_{K/k}(I_{\mathfrak{M}}(K))$, where $I_{\mathfrak{M}}(K)$ is the group of ideals of K relatively prime to $\mathfrak{M}$.

Theorem 2. *Let $\mathfrak{M}$ be a divisor for k and let H be a subgroup of $I_{\mathfrak{M}}$ with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$. Then there exists a unique abelian extension K/k, ramified only at primes dividing $\mathfrak{M}$ (however, some primes dividing $\mathfrak{M}$ could be unramified), such that $H = P_{\mathfrak{M}}N_{K/k}(I_{\mathfrak{M}}(K))$ and*

$$I_{\mathfrak{M}}/H \simeq \mathrm{Gal}(K/k)$$

under the Artin map.

Theorem 3. *Let K_1/k and K_2/k be abelian extensions of conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$, let $\mathfrak{M}$ be a multiple of $\mathfrak{f}_1$ and $\mathfrak{f}_2$, and let $H_1, H_2 \subseteq I_{\mathfrak{M}}$ be the corresponding subgroups. Then*

$$H_1 \subseteq H_2 \Leftrightarrow K_1 \supseteq K_2.$$

The above theorems summarize the most basic facts. We now derive some consequences.

In Theorem 2, let $\mathfrak{M} = 1$ and let $H = P_{\mathfrak{M}} = P$. We obtain an abelian extension K/k with

$$\mathrm{Gal}(K/k) \simeq I/P \simeq \text{ideal class group of } k.$$

By Theorem 1(i), K/k is unramified, and any unramified abelian extension has $\mathfrak{f} = 1$ and corresponds to a subgroup containing $P_1 = P$. By Theorem 3, K is maximal, so we have proved the following important result.

Theorem 4. *Let k be a number field and let K be the maximal unramified (including ∞) abelian extension of k. Then*

$$\mathrm{Gal}(K/k) \simeq \textit{ideal class group of } k,$$

the isomorphism being induced by the Artin map. (The field K is called the Hilbert class field of k).

We note an interesting consequence. Let $\mathfrak{p}$ be a prime ideal of k. Then $\mathfrak{p}$ splits completely in the Hilbert class field $\Leftrightarrow$ the decomposition group for $\mathfrak{p}$ is trivial $\Leftrightarrow \sigma_{\mathfrak{p}} = 1 \Leftrightarrow \mathfrak{p} \in P \Leftrightarrow \mathfrak{p}$ is principal.

Similarly, for a prime number p, we may choose $H \supseteq P$ such that $H/P =$ non-p-part of I/P. Then $I/H \simeq p$-Sylow subgroup of I/P. The field (= Hilbert p-class field) corresponding to H is the maximal unramified abelian p-extension of k.

We now justify a statement made in Section 10.2. Let K be the Hilbert class field (or p-class field) of k, let $F \subseteq k$, and suppose k/F is Galois. Then K/F is also Galois, by the maximality of K. As in Chapter 10, $G = \mathrm{Gal}(k/F)$ acts on $\mathrm{Gal}(K/k)$ (let $\tau \in G$; extend to $\tilde{\tau} \in \mathrm{Gal}(K/F)$; then $\sigma^\tau = \tilde{\tau}\sigma\tilde{\tau}^{-1}$). Also, G acts on the ideal class group of k. Let $\mathfrak{p}$ be a prime ideal of k. Then $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$ under the Artin map, and $\tau\mathfrak{p} \mapsto \sigma_{\tau\mathfrak{p}} = \tilde{\tau}\sigma_{\mathfrak{p}}\tilde{\tau}^{-1} = (\sigma_{\mathfrak{p}})^\tau$, by a formula preceding Theorem 1. Therefore

$$\mathrm{Gal}(K/k) \simeq \text{ideal class group of } k$$

as $\mathrm{Gal}(k/F)$-modules, as was claimed in Chapter 10.

We now need another property of the Artin map. Suppose we have fields F, k, M, and K, as in the diagram, with K/k and M/F abelian.

$$\begin{tikzcd}
 & & & K & \mathfrak{P} \\
\mathfrak{p} & k \arrow[r, dash] & Mk \arrow[ur, dash] & & \\
\tilde{\mathfrak{p}} & F \arrow[u, dash] \arrow[r, dash] & M \arrow[u, dash] & \tilde{\mathfrak{P}} &
\end{tikzcd}$$

(we do not assume $M \cap k = F$). Let $\mathfrak{p}$ be a prime ideal of k, unramified in K/k, and let $\mathfrak{P}$ lie above $\mathfrak{p}$. Similarly, let $\tilde{\mathfrak{p}}$ and $\tilde{\mathfrak{P}}$ be the primes of F and M lying below $\mathfrak{p}$ and $\mathfrak{P}$, respectively. We also assume that $\tilde{\mathfrak{p}}$ is unramified in M/F. Let $f = [\mathcal{O}_k/\mathfrak{p} : \mathcal{O}_F/\tilde{\mathfrak{p}}]$ be the residue class degree. Then $\mathrm{Norm}_{k/F}\, \mathfrak{p} = \tilde{\mathfrak{p}}^f$ and $N\mathfrak{p} = (N\tilde{\mathfrak{p}})^f$. Since $\mathcal{O}_M \subseteq \mathcal{O}_K$, we have

$$\sigma_{\mathfrak{p}}^{K/k}|_M x \equiv x^{N\mathfrak{p}} \bmod \tilde{\mathfrak{P}}, \quad \text{for } x \in \mathcal{O}_M.$$

We have used the notation $\sigma^{K/k}_{\mathfrak{p}}|_M$ to mean "$\sigma_{\mathfrak{p}}$ for the extension K/k, restricted to M." But

$$\sigma^{M/F}_{\mathrm{Norm}\,\mathfrak{p}} x = (\sigma^{M/F}_{\tilde{\mathfrak{p}}})^f x \equiv x^{N\tilde{\mathfrak{p}}^f} = x^{N\mathfrak{p}} \bmod \tilde{\mathscr{P}}.$$

Therefore

$$\sigma^{K/k}_{\mathfrak{p}}|_M = \sigma^{M/F}_{\mathrm{Norm}\,\mathfrak{p}}.$$

We give an application. Suppose M is the Hilbert class field of F and K is the Hilbert class field of k. Furthermore, assume $M \cap k = F$. Then $\mathrm{Gal}(Mk/k) \simeq \mathrm{Gal}(M/F)$, via restriction; hence $\mathrm{Gal}(K/k) \to \mathrm{Gal}(M/F)$ surjectively via restriction. We have the following diagram ($I_k/P_k =$ ideal class group of k, etc.):

$$\begin{tikzcd}
I_k/P_k \arrow[r, "\sim"] \arrow[d, "\text{Norm}"] & \mathrm{Gal}(K/k) \arrow[d, "\text{restr.}"] \\
I_F/P_F \arrow[r, "\sim"] & \mathrm{Gal}(M/F).
\end{tikzcd}$$

The horizontal maps are the Artin maps. The diagram commutes by what we just proved. Since our assumptions imply that the arrow on the right is surjective, Norm is also surjective. So we have proved the following.

Theorem 5 ($=$ Theorem 10.1). *Suppose the extension of number fields k/F contains no unramified abelian subextensions L/K with $L \neq K$. Then the norm map from the ideal class group of k to the ideal class group of F is surjective and the class number h_F divides h_k.*

We now relate the above theorems to abelian extensions of $\mathbb{Q}$. Let n be a positive integer and consider $\mathbb{Q}(\zeta_n)$. Let $p \nmid n$. As we showed in Chapter 2, the Frobenius σ_p is given by $\sigma_p(\zeta_n) = \zeta_n^p$. Thus we have a map

$$I_n \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}.).$$

If $(a, n) = 1$ and $a > 0$, then $(a) \mapsto \sigma_a$, so the map is surjective (in fact, by Dirichlet's theorem, it is surjective when restricted to prime ideals). We now determine the kernel. Let $r \in \mathbb{Q}$ with $(r) \in I_n$. Write $|r| = \prod p_i^{b_i}$. Then, as ideals, $(r) = \prod (p_i)^{b_i}$, so

$$\sigma_{(r)} = \prod \sigma_{p_i}^{b_i} = \sigma_{|r|},$$

where $\sigma_{|r|}(\zeta_n) = \zeta_n^{|r|}$ ($|r| \bmod n$ is a well-defined element of $(\mathbb{Z}/n\mathbb{Z})^\times$). Therefore

$$\begin{aligned} \sigma_{(r)} = 1 &\Leftrightarrow |r| \equiv 1 \bmod n \\ &\Leftrightarrow (r) \in P_{n\infty}. \end{aligned}$$

Since $I_n = I_{n\infty}$, we obtain

$$I_{n\infty}/P_{n\infty} \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

under the Artin map. This of course agrees with the fact that $I_{n\infty}/P_{n\infty} \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

What happens if we leave off ∞ and consider I_n/P_n? By Theorem 1(i), we cannot have ramification at ∞ and it is not hard to show that the corresponding field is $\mathbb{Q}(\zeta_n)^+$. This agrees with our previous calculation that $I_n/P_n \simeq (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$.

Suppose now that K is a number field and $K/\mathbb{Q}$ is abelian. By Theorem 1, there exists a divisor $\mathfrak{M}$ and a subgroup H with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$. We may assume $\mathfrak{M} = n\infty$, with $n \in \mathbb{Z}$. By Theorem 3, K is contained in the field corresponding to $P_{n\infty}$, namely $\mathbb{Q}(\zeta_n)$. We obtain the following.

Theorem 6 (Kronecker–Weber). *Let K be an abelian extension of $\mathbb{Q}$. Then K is contained in a cyclotomic field.*

Let $K/\mathbb{Q}$ be abelian and let $H \supseteq P_{n\infty}$ be the corresponding subgroup. Since

$$I_{n\infty}/P_{n\infty} \simeq (\mathbb{Z}/n\mathbb{Z})^\times,$$

the group $H/P_{n\infty}$ corresponds to a subgroup of congruence classes mod n. Since

$$(p) \text{ splits completely} \Leftrightarrow \sigma_p = 1 \Leftrightarrow (p) \in H,$$

we find that the primes that split completely are determined by congruence conditions mod n. In fact, this property characterizes abelian extensions.

Let $p \equiv 1 \pmod 4$ and let $q \neq p$ be an odd prime. Then q splits in $\mathbb{Q}(\sqrt{p}) \Leftrightarrow (p/q) = 1 \Leftrightarrow$ (by Quadratic Reciprocity) $(q/p) = 1 \Leftrightarrow q$ is a square mod p, which is equivalent to q lying in certain congruence classes mod p. Let $\{1, \tau\} = \mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$. Since q splits $\Leftrightarrow \sigma_q = 1$, we have shown that $\sigma_q = 1$ if q is a square mod p, $\sigma_q = \tau$ if not. Now let $r \in \mathbb{Q}$ with $(r) \in I_p$ (i.e., $(r, p) = 1$). Write $|r| = \prod q^b$ and $\sigma_{(r)} = \prod \sigma_q^b$. It is easy to see that

$$\begin{aligned} \sigma_{(r)} = 1 &\Leftrightarrow |r| \text{ is a square mod } p \\ &\Leftrightarrow r \text{ is a square mod } p \end{aligned}$$

(since $p \equiv 1 \bmod 4$). Let H denote the group of ideals in I_p generated by squares mod p. We have shown (the main step was Quadratic Reciprocity) that H is the kernel of the Artin map. In particular,

$$P_p \subseteq H.$$

Conversely, the fact that $P_p \subseteq H$ implies Quadratic Reciprocity for p: Since $H \subset I_p$ has index 2, it must consist of the squares mod p, because

$$I_p/P_p \simeq (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$$

is cyclic. Therefore

$$\left(\frac{p}{q}\right) = 1 \Leftrightarrow q \text{ splits} \Leftrightarrow \sigma_q = 1 \Leftrightarrow q \text{ is a square mod } p$$

$$\Leftrightarrow \left(\frac{q}{p}\right) = 1.$$

In general, the fact that the kernel of the Artin map contains $P_{\mathfrak{M}}$ (Theorem 1(ii)) is one of the most important parts of the theory. For example, it was the major step in the above proof of the Kronecker–Weber theorem.

Local Class Field Theory

Let k be a finite extension of $\mathbb{Q}_p$. We may write

$$k^\times = \pi^{\mathbb{Z}} \times U = \pi^{\mathbb{Z}} \times W' \times U_1,$$

where π = a uniformizing parameter for k,
$\pi^{\mathbb{Z}} = \{\pi^n \mid n \in \mathbb{Z}\}$,
U = local units,
W' = the roots of unity in k of order prime to p,
$U_1 = \{x \in U \mid x \equiv 1 \bmod \pi\}$.

Theorem 7. *Let K/k be a finite abelian extension. There is a map (called the Artin map)*

$$k^\times \to \mathrm{Gal}(K/k)$$

$$a \mapsto (a, K/k)$$

which induces an isomorphism

$$k^\times/N_{K/k}K^\times \simeq \mathrm{Gal}(K/k),$$

where $N_{K/k}$ denotes the norm mapping. Let T denote the inertia subgroup of Gal(K/k). *Then*

$$U_k/N_{K/k}U_K \simeq T.$$

If K/k is unramified then Gal(K/k) *is cyclic, generated by the Frobenius F, and*

$$(a, K/k) = F^{v_\pi(a)},$$

Theorem 8. *Let $H \subseteq k^\times$ be an open subgroup of finite index. Then there exists a unique abelian extension K/k such that $H = N_{K/k}K^\times$.*

Theorem 9. *Let K_1 and K_2 be finite abelian extensions of k. Then $K_1 \subseteq K_2 \Leftrightarrow N_{K_1/k}K_1^\times \supseteq N_{K_2/k}K_2^\times$.*

The Artin map satisfies the expected properties. For example, if σ is an automorphism of the algebraic closure of k then

$$(\sigma a, \sigma K/\sigma k) = \sigma(a, K/k)\sigma^{-1}.$$

Also, if K/k and M/F are abelian, with $F \subseteq k$ and $M \subseteq K$ (see the diagram in the previous subsection), then, for $a \in k^\times$,

$$(a, K/k)|_M = (N_{k/F}a, M/F).$$

The above theorems may be modified to include infinite abelian extensions K/k. Let $\hat{k}^\times$ be the profinite completion of $k^\times$. This means

$$\hat{k}^\times \overset{\text{def}}{=} \varprojlim k^\times/H$$

where H runs through (a cofinal subsequence of) open subgroups of finite index. Write $k^\times \simeq \pi^{\mathbb{Z}} \times W' \times U_1$, as above, and let H be of finite index. By taking a smaller H if necessary, we may assume

$$k^\times/H \simeq (\mathbb{Z}/m\mathbb{Z}) \times W' \times U_1/U_1^{p^n}$$

for some m and n. It is easy to see that

$$U_1 = \varprojlim \mathrm{U}_1/U_1^{p^n}, \qquad W' = \varprojlim W'.$$

But

$$\varprojlim \mathbb{Z}/m\mathbb{Z} = \hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$$

(see the section on inverse limits). Therefore, we may formally write

$$\hat{k}^\times \simeq \pi^{\hat{\mathbb{Z}}} \times W' \times U_1 \simeq \pi^{\hat{\mathbb{Z}}} \times U.$$

Theorem 10. *Let k be a finite extension of $\mathbb{Q}_p$ and let k^{ab} denote the maximal abelian extension of k. There is a continuous isomorphism*

$$\hat{k}^\times \simeq \mathrm{Gal}(k^{ab}/k).$$

This induces a one–one correspondence between abelian extensions K/k and closed subgroups $H \subseteq \hat{k}^\times$. If H corresponds to K,

$$\hat{k}^\times/H \simeq \mathrm{Gal}(K/k).$$

Let $\tilde{N}_{K/k}(U_K) = \bigcap_L N_{L/k}(U_L)$, where L runs through all finite subextensions of K/k. Then

$$U_k/\tilde{N}_{K/k}(U_K) \simeq T(K/k),$$

the inertia subgroup of Gal(K/k).

We give an example. Let $k = \mathbb{Q}_p$. Then

$$\mathbb{Q}_p^\times \simeq p^{\mathbb{Z}} \times W_{p-1} \times (1 + p\mathbb{Z}_p) \simeq p^{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

Let $(n, p) = 1$ and let $c \geq 0$. We have the following diagram:

$$\begin{tikzcd}
 & \mathbb{Q}_p(\zeta_{np^c}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}_p(\zeta_n) \arrow[dr, dash] & & \mathbb{Q}_p(\zeta_{p^c}) \arrow[dl, dash] \\
 & \mathbb{Q}_p &
\end{tikzcd}$$

Let $a = p^b u \in \mathbb{Q}_p^\times$. Then

$$\begin{aligned}(a, \mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) &= (p^b, \mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \\ &= F^b \colon \zeta_n \mapsto \zeta_n^{p^b}\end{aligned}$$

(F = Frobenius). The group U maps to the inertia subgroup, which is isomorphic to $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^c})/\mathbb{Q}_p)$. It can be shown that $(u, \mathbb{Q}(\zeta_{np^c})/\mathbb{Q}_p)$ yields the map $\zeta_{p^c} \mapsto \zeta_{p^c}^{u^{-1}}$, where $\zeta_{p^c}^{u^{-1}}$ is defined in the usual manner. It is now easy to see that W_{p-1} corresponds to the (tamely ramified) extension $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ and that $1 + p\mathbb{Z}_p$ corresponds to the (wildly ramified) extension $\mathbb{Q}_p(\zeta_{p^c})/\mathbb{Q}_p(\zeta_p)$.

Now consider the infinite extension $\mathbb{Q}_p^{ab}/\mathbb{Q}_p$. We have

$$\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \simeq \hat{\mathbb{Q}}_p^\times \simeq p^{\hat{\mathbb{Z}}} \times \mathbb{Z}_p^\times$$

We know (Chapter 14) that

$$\begin{aligned}\mathbb{Q}_p^{ab} &= \mathbb{Q}_p(\zeta_3, \zeta_4, \ldots) \\ &= \mathbb{Q}_p(\zeta_{p^\infty})\mathbb{Q}_p(\{\zeta_n \mid (p, n) = 1\}).\end{aligned}$$

We have

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \simeq \mathbb{Z}_p^\times.$$

Since Galois groups of unramified extensions are isomorphic to Galois groups of extensions of finite fields, it follows that

$$\mathrm{Gal}(\mathbb{Q}_p(\{\zeta_n \mid (p, n) = 1\})/\mathbb{Q}_p) \simeq \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}} \simeq p^{\hat{\mathbb{Z}}}.$$

Global Class Field Theory (second form)

Let k be a number field and let $\wp$ be a prime (finite or infinite) of k. Let $k_\wp$ and $U_\wp$ denote the completion of k at $\wp$ and the local units of $k_\wp$, respectively. If $\wp$ is archimedean, let $U_\wp = k_\wp^\times$. Define the *idèle group* of k by

$$J_k = \{(\ldots, x_\wp, \ldots) \in \prod_p k_\wp^\times \mid x_\wp \in U_\wp \text{ for almost all } \wp\}$$

("almost all" means "for all but finitely many"). Topologize J_k by giving

$$U = \prod U_\wp$$

the product topology and letting U be an open set of $J_k^\cdot$. Then J_k becomes a locally compact group.

It is easy to see that there is an embedding

$$k^\times \hookrightarrow J_k$$

(diagonally) and it can be shown that the image is discrete. The image is called the subgroup of principal idèles. Let

$$C_k = J_k/k^\times$$

be the group of idèle classes.

Let K/k be a finite extension. If $\mathscr{P}$ is a prime of K above the prime $\not{p}$ of k, then we have a norm map on the completions $N_{\mathscr{P}/\not{p}}\colon K_{\mathscr{P}} \to k_{\not{p}}$. Let $x = (\ldots, x_{\mathscr{P}}, \ldots) \in J_K$. Define

$$N_{K/k}(x) = (\ldots, y_{\not{p}}, \ldots) \in J_k,$$

where

$$y_{\not{p}} = \prod_{\mathscr{P}|\not{p}} N_{\mathscr{P}/\not{p}} x_{\mathscr{P}}.$$

It is not hard to show that if $x = (\ldots, x, \ldots)$ is principal, then $N_{K/k}x = (\ldots, N_{K/k}x, \ldots)$, which is also principal. Therefore we have a map

$$N_{K/k}\colon C_K \to C_k.$$

Theorem 11. *Let K/k be a finite abelian extension. There is an isomorphism*

$$J_k/k^\times N_{K/k}J_K = C_k/N_{K/k}C_K \simeq \mathrm{Gal}(K/k).$$

The prime $\not{p}$ (finite or infinite) is unramified in $K/k \Leftrightarrow U_{\not{p}} \subseteq k^\times N_{K/k}J_K$. ($U_{\not{p}}$ embeds in J_k via $u_{\not{p}} \mapsto (1, \ldots, u_{\not{p}}, \ldots, 1)$).

Theorem 12. *If H is an open subgroup of C_k of finite index then there is a unique abelian extension K/k such that $N_{K/k}C_K = H$. Equivalently, if H is open of finite index in J_k, and $k^\times \subseteq H$, then there exists a unique abelian extension K/k such that $k^\times N_{K/k}J_K = H$.*

Theorem 13. *Let K_1 and K_2 be finite abelian extensions of k. Then*

$$K_1 \subseteq K_2 \Leftrightarrow k^\times N_{K_1/k}J_{K_1} \supseteq k^\times N_{K_2/k}J_{K_2}.$$

The above theorems may also be stated for infinite extensions. Let D_k denote the connected component of the identity in C_k.

Theorem 14. (a) *If K/k is abelian, then there is a closed subgroup H with $D_k \subseteq H \subseteq C_k$, such that*

$$C_k/H \Leftrightarrow \mathrm{Gal}(K/k).$$

The prime $\not{p}$ is unramified $\Leftrightarrow k^\times U_{\not{p}}/k^\times \subseteq H$.

(b) *Given a closed subgroup H with $D_k \subseteq H \subseteq C_k$ (equivalently, C_k/H is totally disconnected), there is a unique abelian extension corresponding to H, as in* (a).

As a simple example, let K be the Hilbert class field of k. Since K/k is unramified everywhere, $U = \prod U_{\mathfrak{p}} \subseteq k^\times N_{K/k} J_K$. Since K is maximal, $k^\times U$ is the subgroup corresponding to K, hence

$$J_k/k^\times U \simeq \mathrm{Gal}(K/k).$$

There is a natural map

$$J_k \to \text{ideals of } k$$
$$(\ldots, x_{\mathfrak{p}}, \ldots) \mapsto \prod_{\text{finite } \mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}.$$

The kernel is U. If we consider the induced map to the ideal class group, we obtain

$$J_k/k^\times U \simeq \text{ideal class group of } k.$$

Therefore $\mathrm{Gal}(K/k)$ is isomorphic to the ideal class group, as we showed previously.

Tables

§1 Bernoulli Numbers

This table from H. Davis [1], pp. 230–231, gives the value of $(-1)^{n+1}B_{2n}$ for $1 \leq n \leq 62$. In this book we have numbered the Bernoulli numbers so that $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, and $B_{2n+1} = 0$ for $n \geq 1$. Some authors use different numbering systems and a different choice of signs. For more Bernoulli numbers, see H. Davis [1] and Knuth–Buckholtz [1]. For prime factorizations, see Wagstaff [1].

n	Numerator	Denominator	n
1	1	6	1
2	1	30	2
3	1	42	3
4	1	30	4
5	5	66	5
6	691	2730	6
7	7	6	7
8	3617	510	8
9	43867	798	9
10	1 74611	330	10
11	8 54513	138	11
12	2363 64091	2730	12
13	85 53103	6	13
14	2 37494 61029	870	14
15	861 58412 76005	14322	15
16	770 93210 41217	510	16
17	257 76878 58367	6	17
18	26315 27155 30534 77373	1919190	18
19	2 92999 39138 41559	6	19
20	2 61082 71849 64491 22051	13530	20

n	Numerator	Denominator	*n*
21	15 20097 64391 80708 02691	1806	21
22	278 33269 57930 10242 35023	690	22
23	5964 51111 59391 21632 77961	282	23
24	560 94033 68997 81768 62491 27547	46410	24
25	49 50572 05241 07964 82124 77525	66	25
26	80116 57181 35489 95734 79249 91853	1590	26
27	29 14996 36348 84862 42141 81238 12691	798	27
28	2479 39292 93132 26753 68541 57396 63229	870	28
29	84483 61334 88800 41862 04677 59940 36021	354	29
30	121 52331 40483 75557 20403 04994 07982 02460 41491	56786730	30
31	123 00585 43408 68585 41953 03985 74033 86151	6	31
32	10 67838 30147 86652 98863 85444 97914 26479 42017	510	32
33	1 47260 00221 26335 65405 16194 28551 93234 22418	64722	33
	99101 … … … … … … … …		
34	7877 31308 58718 72814 19091 49208 47460 62443 47001	30	34
35	1505 38134 73333 67003 80307 65673 77857 20851 14381	4686	35
	60235 … … … … … … … …		
36	58279 54961 66994 41104 38277 24464 10673 65282 48830	140100870	36
	18442 60429 … … … … … … …		
37	34152 41728 92211 68014 33007 37314 72635 18668 83077	6	37
	83087 … … … … … … … …		
38	246 55088 82593 53727 07687 19604 05851 99904 36526	30	38
	78288 65801 … … … … …		
39	41 48463 65575 40082 82951 79035 54954 20734 92199	3318	39
	37537 24004 83487 … … … … … …		
40	4 60378 42994 79457 64693 55749 69019 04684 97942	230010	40
	57872 75128 89196 56867 … … … … …		
41	1 67701 41491 85145 83682 31545 09786 26990 02077	498	41
	36027 57025 34148 81613 … … … … …		
42	20 24576 19593 52903 60231 13116 01117 31009 98991	3404310	42
	73911 98090 87728 10839 32477 … … … …		
43	660 71461 94176 78653 57384 78474 26261 49627 78306	6	43
	86653 38893 17619 96983 … … … … …		
44	13114 26488 67401 75079 95511 42401 93118 43345 75027	61410	44
	55720 28644 29691 98905 74047 … … … …		
45	117 90572 79021 08279 98841 23351 24921 50837 75254	272118	45
	94966 96471 16231 54521 57279 22535 … … …		
46	129 55859 48207 53752 79894 27828 53857 67496 59341	1410	46
	48371 94351 43023 31632 68299 46247 … … …		
47	122 08138 06579 74446 96073 01679 41320 12039 58508	6	47
	41520 26966 21436 21510 52846 49447 … … …		
48	2 11600 44959 72665 13097 59772 81098 24233 67304	4501770	48
	39543 89060 23415 06387 33420 05066 83499 87259 …		
49	67 90826 06729 05495 62405 11175 46403 60560 73421	6	49
	95728 50448 75090 73961 24999 29470 58239 … …		
50	945 98037 81912 21252 95227 43306 94937 21872 70284	33330	50
	15330 66936 13338 56962 04311 39541 51972 47711 …		
51	32040 19410 86090 70782 43020 78211 62417 75491 81719	4326	51
	71527 17450 67900 25010 86861 53083 66781 58791 …		

n	Numerator	Denominator	n
52	31 95336 31363 83001 12871 03352 79617 42746 71189	1590	52
	60607 82727 38327 10347 01628 49568 36554 97212 24053		
53	3637 39031 72617 41440 81518 20151 59342 71692 31298	642	53
	64058 16900 38930 81637 82818 79873 38620 23465 72901		
54	34 69342 24784 78287 89552 08865 93238 52541 39976	209191710	54
	67857 60491 14687 00058 91371 50126 63197 24897 59230		
	65973 38057		
55	7645 99294 04847 42892 24813 42467 24347 50052 87524	1518	55
	13412 30790 66835 93870 75979 76062 69585 77997 79302		
	17515		
56	26508 79602 15509 97133 52597 21468 51620 14443 15149	1671270	56
	91925 09896 45178 84276 80966 75651 48755 15366 78120		
	35526 00109		
57	217 37832 31936 91633 33310 76108 66529 91475 72115	42	57
	66790 90831 36080 61101 14933 60548 42345 93650 90418		
	86185 62649		
58	30 95539 16571 84297 69125 13458 03384 14168 69004	1770	58
	12806 43298 44245 50404 57210 08957 52457 19682 71388		
	19959 57547 52259		
59	36 69631 19969 71311 15349 47151 58558 50066 84606	6	59
	36108 06992 04301 05944 06764 14485 04580 64618 89371		
	77635 45170 95799		
60	515 07486 53507 91090 61843 99685 78499 83274 09517	2328255930	60
	03532 62675 21309 28691 67199 29747 49229 85358 81132		
	93670 77682 67780 32820 70131		
61	49 63366 60792 62581 91253 26374 75990 75743 87227	6	61
	90311 06013 97703 09311 79315 06832 14100 43132 90331		
	13678 09803 79685 64431		
62	95876 77533 42471 28750 77490 31075 42444 62057 88300	30	62
	13297 33681 95535 12729 35859 33544 35944 41363 19436		
	10268 47268 90946 09001		

§2 Irregular Primes

This table lists the irregular primes $p \leq 4001$ along with the even indices $2a$, $0 \leq 2a \leq p - 3$, such that $p | B_{2a}$. It is essentially the table of Lehmer–Lehmer–Vandiver–Selfridge–Nicol which is printed in Borevich–Shafarevich [1], but there are four additional entries (for $p = 1381, 1597, 1663, 1877$), which were originally missed because of machine error and which were later found by W. Johnson (see Johnson [1]; this paper gives a list of irregular primes for $p < 8000$).

In order to obtain information about generalized Bernoulli numbers and about class groups, see Corollary 5.15 and Theorems 6.17 and 6.18. For a report on the irregular primes $p < 125000$, see Wagstaff [1].

p	$2a$	p	$2a$	p	$2a$
37	32	577	52	1061	474
59	44	587	90, 92	1091	888
67	58	593	22	1117	794
101	68	607	592	1129	348
103	24	613	522	1151	534, 784, 968
131	22	617	20, 174, 338	1153	802
149	130	619	428	1193	262
157	62, 110	631	80, 226	1201	676
233	84	647	236, 242, 554	1217	784, 866, 1118
257	164	653	48	1229	784
263	100	659	224	1237	874
271	84	673	408, 502	1279	518
283	20	677	628	1283	510
293	156	683	32	1291	206, 824
307	88	691	12, 200	1297	202, 220
311	292	727	378	1301	176
347	280	751	290	1307	382, 852
353	186, 300	757	514	1319	304
379	100, 174	761	260	1327	466
389	200	773	732	1367	234
401	382	797	220	1381	266
409	126	809	330, 628	1409	358
421	240	811	544	1429	996
433	366	821	744	1439	574
461	196	827	102	1483	224
463	130	839	66	1499	94
467	94, 194	877	868	1523	1310
491	292, 336, 338	881	162	1559	862
523	400	887	418	1597	842
541	86	929	520, 820	1609	1356
547	270, 486	953	156	1613	172
557	222	971	166	1619	560

p	$2a$	p	$2a$	p	$2a$
1621	980	2357	2204	3181	3142
1637	718	2371	242, 2274	3203	2368
1663	270, 1508	2377	1226	3221	98
1669	388, 1086	2381	2060	3229	1634
1721	30	2383	842, 2278	3257	922
1733	810, 942	2389	776	3313	2222
1753	712	2411	2126	3323	3292
1759	1520	2423	290, 884	3329	1378
1777	1192	2441	366, 1750	3391	2232, 2534
1787	1606	2503	1044	3407	2076, 2558
1789	848, 1442	2543	2374	3433	1300
1811	550, 698, 1520	2557	1464	3469	1174
1831	1274	2579	1730	3491	2544
1847	954, 1016, 1558	2591	854, 2574	3511	1416, 1724
1871	1794	2621	1772	3517	1836, 2586
1877	1026	2633	1416	3529	3490
1879	1260	2647	1172	3533	2314, 3136
1889	242	2657	710	3539	2082, 2130
1901	1722	2663	1244	3559	344, 1592
1933	1058, 1320	2671	404, 2394	3581	1466
1951	1656	2689	926	3583	1922
1979	148	2753	482	3593	360, 642
1987	510	2767	2528	3607	1976
1993	912	2777	1600	3613	2082
1997	772, 1888	2789	1984, 2154	3617	16, 2856
2003	60, 600	2791	2554	3631	1104
2017	1204	2833	1832	3637	2526, 3202
2039	1300	2857	98	3671	1580
2053	1932	2861	352	3677	2238
2087	376, 1298	2909	400, 950	3697	1884
2099	1230	2927	242	3779	2362
2111	1038	2939	332, 1102, 2748	3797	1256
2137	1624	2957	138, 788	3821	3296
2143	1916	2999	776	3833	1840, 1998, 3286
2153	1832	3011	1496	3851	216, 404
2213	154	3023	2020	3853	748
2239	1826	3049	700	3881	1686, 2138
2267	2234	3061	2522	3917	1490
2273	876, 2166	3083	1450	3967	106
2293	2040	3089	1706	3989	1936
2309	1660, 1772	3119	1704	4001	534

§3 Class Numbers

The following table gives the value and prime factorization of the relative class number h_n^- of $\mathbb{Q}(\zeta_n)$ for $1 \le \phi(n) \le 256$, $n \not\equiv 2 \pmod 4$. It is extracted from Schrutka von Rechtenstamm [1], which also lists the contributions from the various odd characters in the analytic class number formula. Some of the large factors were only checked for primality by a pseudo-primality test, so there is a small chance that some of the "prime" factorizations include composites. For values of h_p^- for $257 < p < 521$, see Lehmer–Masley [1]. A few of the factorizations below have been obtained from this paper.

Since the size of h_n^- depends more on the size of $\phi(n)$ than of n, we have arranged the table according to degree.

For h^+ there are the following results (see van der Linden [1]):

(a) If n is a prime power with $\phi(n) \le 66$ then $h_n^+ = 1$.
(b) If n is not a prime power and $n \le 200$, $\phi(n) \le 72$, then $h_n^+ = 1$, except for $h_{136}^+ = 2$ and the possible exceptions $n = 148$ and $n = 152$. Also, we have $h_{165}^+ = 1$.

If we assume the generalized Riemann hypothesis, then the following hold:

(c) If n is a prime power with $\phi(n) < 162$ then $h_n^+ = 1$. We have $h_{163}^+ = 4$.
(d) If n is not a prime power and $n \le 200$, then $h_n^+ = 1$, with the following exceptions: $h_{136}^+ = 2$, $h_{145}^+ = 2$, $h_{183}^+ = 4$.

It is possible to obtain examples of $h_p^+ > 1$ using quadratic subfields (Ankeny–Chowla–Hasse [1], S.-D. Lang [1]), or using cubic subfields (see the tables in M.-N. Gras [3] and Shanks [1]), or using both (Cornell–Washington [1]). See also Takeuchi [1].

Kummer determined the structure of the minus part of the class group of $\mathbb{Q}(\zeta_p)$ for $p < 100$. By (a) above, this is the whole class group for $p \le 67$; by (c), it is the whole class group for $p < 100$ if we assume the generalized Riemann hypothesis. All the groups have square-free order, hence are cyclic, with the following possible exceptions: 29, 31, 41, and 71. In these cases, 29 yields $(2) \times (2) \times (2)$, 31 yields (9), 41 yields $(11) \times (11)$, and 71 yields $(7^2 \cdot 79241)$, Here (m) denotes the cyclic group $\mathbb{Z}/m\mathbb{Z}$. See Kummer [5, pp. 544, 907–918], Iwasawa [16], and Section 10.1. For more techniques, see Cornell–Rosen [1] and Gerth [5].

n	$\phi(n)$	h^-	n	$\phi(n)$	h^-	n	$\phi(n)$	h^-	n	$\phi(n)$	h^-
1	1	1	36	12	1	56	24	2	41	40	$121 = 11^2$
3	2	1	17	16	1	72	24	3	55	40	$10 = 2 \cdot 5$
4	2	1	32	16	1	84	24	1	75	40	11
5	4	1	40	16	1	29	28	$8 = 2^3$	88	40	$55 = 5 \cdot 11$
8	4	1	48	16	1	31	30	$9 = 3^2$	100	40	$55 = 5 \cdot 11$
12	4	1	60	16	1	51	32	5	132	40	11
7	6	1	19	18	1	64	32	17	43	42	211
9	6	1	27	18	1	68	32	$8 = 2^3$	49	42	43
15	8	1	25	20	1	80	32	5	69	44	$69 = 3 \cdot 23$
16	8	1	33	20	1	96	32	$9 = 3^2$	92	44	$201 = 3 \cdot 67$
20	8	1	44	20	1	120	32	$4 = 2^2$	47	46	$695 = 5 \cdot 139$
24	8	1	23	22	3	37	36	37	65	48	$64 = 2^6$
11	10	1	35	24	1	57	36	$9 = 3^2$	104	48	$351 = 3^3 \cdot 13$
13	12	1	39	24	2	63	36	7	105	48	13
21	12	1	45	24	1	76	36	19	112	48	$468 = 2^2 \cdot 3^2 \cdot 13$
28	12	1	52	24	3	108	36	19			

n	$\phi(n)$	h^-	n	$\phi(n)$	h^-
140	48	$39 = 3 \cdot 13$	135	72	$75961 = 37 \cdot 2053$
144	48	$507 = 3 \cdot 13^2$	148	72	$4\,827501 = 3^2 \cdot 7 \cdot 19 \cdot 37 \cdot 109$
156	48	$156 = 2^2 \cdot 3 \cdot 13$	152	72	$1\,666737 = 3^5 \cdot 19^3$
168	48	$84 = 2^2 \cdot 3 \cdot 7$	216	72	$1\,714617 = 3^2 \cdot 19 \cdot 37 \cdot 271$
180	48	$75 = 3 \cdot 5^2$	228	72	$238203 = 3^2 \cdot 7 \cdot 19 \cdot 199$
53	52	4889	252	72	$71344 = 2^4 \cdot 7^3 \cdot 13$
81	54	2593	79	78	$100\,146415 = 5 \cdot 53 \cdot 377911$
87	56	$1536 = 2^9 \cdot 3$	123	80	$8\,425472 = 2^{12} \cdot 11^2 \cdot 17$
116	56	$10752 = 2^9 \cdot 3 \cdot 7$	164	80	$82\,817240 = 2^3 \cdot 5 \cdot 11^2 \cdot 71 \cdot 241$
59	58	$41421 = 3 \cdot 59 \cdot 233$	165	80	$92620 = 2^2 \cdot 5 \cdot 11 \cdot 421$
61	60	$76301 = 41 \cdot 1861$	176	80	$29\,371375 = 5^3 \cdot 11 \cdot 41 \cdot 521$
77	60	$1280 = 2^8 \cdot 5$	200	80	$14\,907805 = 5 \cdot 11^2 \cdot 41 \cdot 601$
93	60	$6795 = 3^2 \cdot 5 \cdot 151$	220	80	$856220 = 2^2 \cdot 5 \cdot 31 \cdot 1381$
99	60	$2883 = 3 \cdot 31^2$	264	80	$1\,875500 = 2^2 \cdot 5^3 \cdot 11^2 \cdot 31$
124	60	$45756 = 2^2 \cdot 3^2 \cdot 31 \cdot 41$	300	80	$1\,307405 = 5 \cdot 11^2 \cdot 2161$
85	64	$6205 = 5 \cdot 17 \cdot 73$	83	82	$838\,216959 = 3 \cdot 279405653$
128	64	$359057 = 17 \cdot 21121$	129	84	$37\,821539 = 7 \cdot 29 \cdot 211 \cdot 883$
136	64	$111744 = 2^7 \cdot 3^2 \cdot 97$	147	84	$5\,874617 = 7 \cdot 29 \cdot 43 \cdot 673$
160	64	$31365 = 3^2 \cdot 5 \cdot 17 \cdot 41$	172	84	$792\,653572 = 2^2 \cdot 43 \cdot 211 \cdot 21841$
192	64	$61353 = 3^2 \cdot 17 \cdot 401$	196	84	$82\,708823 = 43 \cdot 71 \cdot 27091$
204	64	$15440 = 2^4 \cdot 5 \cdot 193$	89	88	$13379\,363737 = 113 \cdot 118401449$
240	64	$6400 = 2^8 \cdot 5^2$	115	88	$44\,697909 = 3 \cdot 331 \cdot 45013$
67	66	$853513 = 67 \cdot 12739$	184	88	$1486\,137318 = 2 \cdot 3 \cdot 23 \cdot 67^2 \cdot 2399$
71	70	$3\,882809 = 7^2 \cdot 79241$	276	88	$131\,209986 = 2 \cdot 3 \cdot 23^2 \cdot 67 \cdot 617$
73	72	$11\,957417 = 89 \cdot 134353$	141	92	$1257\,700495 = 5 \cdot 47 \cdot 139^2 \cdot 277$
91	72	$53872 = 2^4 \cdot 7 \cdot 13 \cdot 37$	188	92	$24260\,850805 = 5 \cdot 47 \cdot 139 \cdot 742717$
95	72	$107692 = 2^2 \cdot 13 \cdot 19 \cdot 109$	97	96	$411322\,842001 = 577 \cdot 3457 \cdot 206209$
111	72	$480852 = 2^2 \cdot 3^2 \cdot 19^2 \cdot 37$	119	96	$1238\,459625 = 3^4 \cdot 5^3 \cdot 13 \cdot 97^2$
117	72	$132678 = 2 \cdot 3^6 \cdot 7 \cdot 13$	153	96	$2416\,282880 = 2^8 \cdot 5 \cdot 11^2 \cdot 15601$

n	$\phi(n)$	h^-
195	96	$22\,151168 = 2^{17} \cdot 13^2$
208	96	$29904\,190875 = 3^3 \cdot 5^3 \cdot 13^3 \cdot 37 \cdot 109$
224	96	$14989\,501800 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17 \cdot 769$
260	96	$531\,628032 = 2^{20} \cdot 3 \cdot 13^2$
280	96	$265\,454280 = 2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37 \cdot 73$
288	96	$32899\,636107 = 3^5 \cdot 13^2 \cdot 457 \cdot 1753$
312	96	$1621\,069632 = 2^6 \cdot 3^3 \cdot 7 \cdot 13^3 \cdot 61$
336	96	$930\,436416 = 2^6 \cdot 3^3 \cdot 7 \cdot 13 \cdot 61 \cdot 97$
360	96	$523\,952100 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 109^2$
420	96	$10\,229232 = 2^4 \cdot 3 \cdot 13^3 \cdot 97$
101	100	$3\,547404\,378125 = 5^5 \cdot 101 \cdot 601 \cdot 18701$
125	100	$57708\,445601 = 2801 \cdot 20\,602801$
103	102	$9\,069094\,643165 = 5 \cdot 103 \cdot 1021 \cdot 17\,247691$
159	104	$223233\,182255 = 5 \cdot 53^2 \cdot 3251 \cdot 4889$
212	104	$6\,789574\,466337 = 3 \cdot 13 \cdot 1093 \cdot 4889 \cdot 32579$
107	106	$63\,434933\,542623 = 3 \cdot 743 \cdot 9859 \cdot 2\,886593$
109	108	$161\,784800\,122409 = 17 \cdot 1009 \cdot 9431\,866153$
133	108	$157577\,452812 = 2^2 \cdot 3^{10} \cdot 13 \cdot 19 \cdot 37 \cdot 73$
171	108	$503009\,425548 = 2^2 \cdot 3^6 \cdot 7 \cdot 19 \cdot 73 \cdot 109 \cdot 163$
189	108	$105778\,197511 = 7 \cdot 37 \cdot 109 \cdot 127 \cdot 163 \cdot 181$
324	108	$5\,770749\,978919 = 19 \cdot 2593 \cdot 117\,132157$
121	110	$12\,188792\,628211 = 67 \cdot 353 \cdot 20021 \cdot 25741$
113	112	$1612\,072001\,362952 = 2^3 \cdot 17 \cdot 11\,853470\,598257$
145	112	$1\,467250\,393088 = 2^{14} \cdot 281 \cdot 421 \cdot 757$
232	112	$248\,372639\,563776 = 2^{18} \cdot 3 \cdot 7 \cdot 13 \cdot 43^2 \cdot 1877$
348	112	$5\,889026\,949120 = 2^{18} \cdot 3^2 \cdot 5 \cdot 7 \cdot 71317$
177	116	$81\,730647\,171051 = 3 \cdot 59 \cdot 233 \cdot 523 \cdot 3\,789257$
236	116	$4509\,195165\,737013 = 3 \cdot 59 \cdot 233 \cdot 109337\,677693$
143	120	$36\,027143\,124175 = 5^2 \cdot 7 \cdot 61^2 \cdot 661 \cdot 83701$
155	120	$84\,473643\,916800 = 2^9 \cdot 3^4 \cdot 5^2 \cdot 631 \cdot 129121$
175	120	$4\,733255\,370496 = 2^8 \cdot 61 \cdot 271 \cdot 601 \cdot 1861$
183	120	$767\,392851\,521600 = 2^6 \cdot 5^2 \cdot 31^3 \cdot 41 \cdot 211 \cdot 1861$
225	120	$15\,175377\,535571 = 11 \cdot 61 \cdot 331 \cdot 2791 \cdot 24481$
231	120	$298807\,787520 = 2^{16} \cdot 3^2 \cdot 5 \cdot 11 \cdot 61 \cdot 151$
244	120	$30953\,273659\,007535 = 3^3 \cdot 5 \cdot 11 \cdot 41 \cdot 61 \cdot 691 \cdot 1861 \cdot 6481$
248	120	$12239\,782830\,975744 = 2^8 \cdot 3^2 \cdot 11^2 \cdot 31^2 \cdot 41 \cdot 211 \cdot 5281$
308	120	$12\,767325\,061120 = 2^{21} \cdot 5 \cdot 7 \cdot 31^2 \cdot 181$
372	120	$307\,999672\,562880 = 2^6 \cdot 3^2 \cdot 5 \cdot 31 \cdot 41^2 \cdot 151 \cdot 13591$
396	120	$44\,485944\,574929 = 3 \cdot 11 \cdot 13 \cdot 31^3 \cdot 181 \cdot 19231$
127	126	$2\,604529\,186263\,992195 = 5 \cdot 13 \cdot 43 \cdot 547 \cdot 883 \cdot 3079 \cdot 626599$
255	128	$16\,881405\,898800 = 2^4 \cdot 3 \cdot 5^2 \cdot 17^2 \cdot 73 \cdot 353 \cdot 1889$
256	128	$10\,449592\,865393\,414737 = 17 \cdot 21121 \cdot 29\,102880\,226241$
272	128	$239445\,927053\,918208 = 2^{15} \cdot 3^2 \cdot 13 \cdot 17 \cdot 41 \cdot 97 \cdot 577 \cdot 1601$
320	128	$39497\,094130\,144005 = 3^2 \cdot 5 \cdot 17^4 \cdot 41 \cdot 97 \cdot 337 \cdot 7841$
340	128	$1212\,125245\,952000 = 2^{12} \cdot 5^3 \cdot 17 \cdot 73 \cdot 593 \cdot 3217$
384	128	$107878\,055185\,500777 = 3^2 \cdot 17 \cdot 401 \cdot 1697 \cdot 21121 \cdot 49057$
408	128	$4710\,612981\,841920 = 2^{16} \cdot 3^2 \cdot 5 \cdot 41 \cdot 97 \cdot 193 \cdot 2081$
480	128	$617\,689081\,497600 = 2^{11} \cdot 3^4 \cdot 5^2 \cdot 7^4 \cdot 17 \cdot 41 \cdot 89$
131	130	$28\,496379\,729272\,136525 = 3^3 \cdot 5^2 \cdot 53 \cdot 131 \cdot 1301 \cdot 4673\,706701$
161	132	$17033\,926767\,658911 = 3^2 \cdot 11 \cdot 67^3 \cdot 22111 \cdot 25873$
201	132	$252655\,290579\,982532 = 2^2 \cdot 11 \cdot 23^2 \cdot 67^2 \cdot 12739 \cdot 189817$

n	$\phi(n)$	h^-
207	132	57569 648362 893621 $= 3^2 \cdot 23 \cdot 67 \cdot 727 \cdot 17491 \cdot 326437$
268	132	28 431682 983759 502069 $= 7 \cdot 23 \cdot 67^2 \cdot 1607 \cdot 12739 \cdot 1\ 921657$
137	136	646 901570 175200 968153 $= 17^2 \cdot 47737 \cdot 46\ 890540\ 621121$
139	138	1753 848916 484925 681747 $= 3^2 \cdot 47^2 \cdot 277^2 \cdot 967 \cdot 1188\ 961909$
213	140	20 748314 966568 340907 $= 7^2 \cdot 41 \cdot 43 \cdot 281 \cdot 421 \cdot 25621 \cdot 79241$
284	140	1858 128446 456993 562103 $= 7^2 \cdot 29 \cdot 71 \cdot 113 \cdot 281 \cdot 79241 \cdot 7\ 319621$
185	144	13 767756 481797 006325 $= 5^2 \cdot 7^2 \cdot 13 \cdot 37^2 \cdot 53^2 \cdot 9433 \cdot 23833$
219	144	219 406633 996698 095616 $= 2^{12} \cdot 3^2 \cdot 17^2 \cdot 37 \cdot 89 \cdot 46549 \cdot 134353$
273	144	21198 594942 959616 $= 2^{20} \cdot 3^2 \cdot 7 \cdot 13^2 \cdot 19 \cdot 37^2 \cdot 73$
285	144	34397 734347 893592 $= 2^3 \cdot 3^4 \cdot 13 \cdot 19 \cdot 37^2 \cdot 73 \cdot 109^2 \cdot 181$
292	144	26883 466789 548427 261560 $= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 89 \cdot 109 \cdot 181^2 \cdot 433 \cdot 577 \cdot 134353$
296	144	8269 489911 111632 618625 $= 3^2 \cdot 5^3 \cdot 7^3 \cdot 17^2 \cdot 19 \cdot 37^2 \cdot 109 \cdot 397 \cdot 65881$
304	144	1764 209801 444986 506285 $= 3^5 \cdot 5 \cdot 19^3 \cdot 37^3 \cdot 73 \cdot 109 \cdot 525241$
315	144	3990 441973 190400 $= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^3 \cdot 13^2 \cdot 37^2 \cdot 97$
364	144	2 153601 104578 560000 $= 2^{14} \cdot 3^7 \cdot 5^4 \cdot 7 \cdot 13^5 \cdot 37$
380	144	3 118301 079203 997232 $= 2^4 \cdot 7 \cdot 13 \cdot 19^2 \cdot 53^2 \cdot 73 \cdot 109 \cdot 433 \cdot 613$
432	144	859 095743 251563 370449 $= 3^2 \cdot 13^2 \cdot 19 \cdot 37^2 \cdot 109 \cdot 271 \cdot 541 \cdot 1\ 358821$
444	144	55 382724 129516 879312 $= 2^4 \cdot 3^4 \cdot 7 \cdot 19^3 \cdot 37^2 \cdot 109^2 \cdot 54721$
456	144	17 643537 152468 843364 $= 2^2 \cdot 3^7 \cdot 7^2 \cdot 19^4 \cdot 199 \cdot 487 \cdot 3259$
468	144	6 618931 810639 948800 $= 2^{10} \cdot 3^{10} \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13^4 \cdot 181$
504	144	2 077452 902069 895168 $= 2^{16} \cdot 3^{13} \cdot 7^6 \cdot 13^2$
540	144	1 892923 169092 229025 $= 3^2 \cdot 5^2 \cdot 19^2 \cdot 37 \cdot 73 \cdot 109 \cdot 2053 \cdot 38557$
149	148	687887 859687 174720 123201 $= 3^2 \cdot 149 \cdot 512\ 966338\ 320040\ 805461$
151	150	2 333546 653547 742584 439257 $= 7 \cdot 11^2 \cdot 281 \cdot 25951 \cdot 1\ 207501 \cdot 312\ 885301$
157	156	56 234327 700401 832767 069245 $= 5 \cdot 13^2 \cdot 157^2 \cdot 1093 \cdot 1873 \cdot 418861 \cdot 3\ 148601$
169	156	546489 564291 684778 075637 $= 313 \cdot 1873 \cdot 4733 \cdot 196\ 953296\ 289361$
237	156	130445 289884 021402 281355 $= 5 \cdot 7 \cdot 13 \cdot 53 \cdot 157 \cdot 3433 \cdot 4421 \cdot 6007 \cdot 377911$
316	156	22 036970 003952 429517 953845 $= 5 \cdot 13^2 \cdot 53 \cdot 79 \cdot 2393 \cdot 377911 \cdot 6887\ 474101$
187	160	38816 037673 830728 480329 $= 17^2 \cdot 41 \cdot 241 \cdot 4801 \cdot 299681 \cdot 9\ 447601$
205	160	78821 910689 378365 476000 $= 2^5 \cdot 3^2 \cdot 5^3 \cdot 11^2 \cdot 41 \cdot 101^2 \cdot 661 \cdot 4261 \cdot 15361$
328	160	82 221729 062003 473169 480000 $=$ $2^6 \cdot 5^4 \cdot 11^2 \cdot 17 \cdot 31 \cdot 71 \cdot 101 \cdot 241 \cdot 521 \cdot 35\ 801081$
352	160	5 578700 230786 671358 855375 $= 5^3 \cdot 11 \cdot 41^2 \cdot 113 \cdot 281 \cdot 521 \cdot 1801 \cdot 2801 \cdot 28921$
400	160	1 692044 042657 239185 550625 $= 5^4 \cdot 11^4 \cdot 41 \cdot 61 \cdot 101 \cdot 601 \cdot 26261 \cdot 46381$
440	160	3690 827552 653792 584000 $= 2^6 \cdot 3 \cdot 5^3 \cdot 11 \cdot 31^2 \cdot 61^2 \cdot 181 \cdot 1381 \cdot 15641$
492	160	331431 584848 686177 320960 $= 2^{20} \cdot 5 \cdot 11^2 \cdot 17 \cdot 41 \cdot 71 \cdot 241 \cdot 1321 \cdot 33161$
528	160	20215 309155 022994 375000 $= 2^3 \cdot 5^7 \cdot 11^2 \cdot 31 \cdot 41 \cdot 61 \cdot 101 \cdot 521 \cdot 65521$
600	160	7166 325608 289022 528100 $= 2^2 \cdot 5^2 \cdot 11^3 \cdot 41 \cdot 101 \cdot 131 \cdot 601 \cdot 2161 \cdot 76421$
660	160	20 090237 237998 576000 $= 2^7 \cdot 5^3 \cdot 11^2 \cdot 31 \cdot 181 \cdot 421 \cdot 1381 \cdot 3181$
163	162	2708 534744 692077 051875 131636 $= 2^2 \cdot 181 \cdot 23167 \cdot 365473 \cdot 441\ 845817\ 162679$
243	162	14 948557 667133 129512 662807 $= 2593 \cdot 5764\ 966319\ 758245\ 087799$ (composite)
249	164	13 898958 132089 743179 099753 $= 3 \cdot 279\ 405653 \cdot 16581\ 575906\ 876567$
332	164	2233 138758 192814 382133 816279 $= 3 \cdot 80279 \cdot 612377 \cdot 54\ 192407 \cdot 279\ 405653$
167	166	28121 189830 322933 178315 382891 $= 11 \cdot 499 \cdot 5\ 123189\ 985484\ 229035\ 947419$
203	168	4 413278 155436 385292 173312 $= 2^{14} \cdot 3^2 \cdot 7^2 \cdot 29 \cdot 3907 \cdot 26041 \cdot 207\ 015901$
215	168	8 562946 718506 556895 170449 $= 7^2 \cdot 19 \cdot 29 \cdot 37 \cdot 211 \cdot 757 \cdot 2017 \cdot 22709 \cdot 1\ 171633$
245	168	122845 138181 874350 560487 $= 13^2 \cdot 43 \cdot 127 \cdot 631 \cdot 43793 \cdot 4816\ 871221$
261	168	18 379288 588511 605529 995776 $= 2^9 \cdot 3^2 \cdot 61 \cdot 421 \cdot 883 \cdot 10753 \cdot 38011 \cdot 430333$
344	168	10789 946893 536931 852748 197440 $=$ $2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 29 \cdot 43 \cdot 197 \cdot 211 \cdot 21841 \cdot 929419 \cdot 1\ 525987$
392	168	112 070797 379361 142494 415714 $= 2 \cdot 43^2 \cdot 71 \cdot 617 \cdot 953 \cdot 27091 \cdot 28393 \cdot 943741$

n	$\phi(n)$	h^-
516	168	38 888604 320171 861798 243568 = $2^4 \cdot 3^2 \cdot 7 \cdot 29 \cdot 43^2 \cdot 71 \cdot 211 \cdot 883 \cdot 21841 \cdot 2\ 490307$
588	168	482059 253351 850013 395157 = $7 \cdot 29 \cdot 43 \cdot 71 \cdot 673 \cdot 2017 \cdot 3571 \cdot 5923 \cdot 27091$
173	172	1 702546 266654 155847 516780 034265 = $5 \cdot 20297 \cdot 231169 \cdot 72\ 571729\ 362851\ 870621$
267	176	12963 312320 905811 283854 380235 = $5 \cdot 23 \cdot 113 \cdot 1123 \cdot 5237 \cdot 26687 \cdot 53681 \cdot 118\ 401449$
345	176	506186 308788 058155 105915 = $3 \cdot 5 \cdot 11 \cdot 23 \cdot 331 \cdot 4159 \cdot 45013 \cdot 2152\ 502881$
356	176	4 707593 989354 615385 004311 705592 = $2^3 \cdot 3 \cdot 11 \cdot 23 \cdot 113 \cdot 463 \cdot 15269 \cdot 19207 \cdot 426757 \cdot 118\ 401449$
368	176	243320 115114 433657 103908 135020 = $2^2 \cdot 3 \cdot 5 \cdot 11^2 \cdot 23^3 \cdot 67^2 \cdot 89 \cdot 2069 \cdot 2399 \cdot 8537 \cdot 162713$
460	176	197 739166 909616 827795 207545 = $3 \cdot 5 \cdot 11 \cdot 67 \cdot 331 \cdot 617 \cdot 17029 \cdot 45013 \cdot 114\ 259861$
552	176	767 354245 926929 350377 606384 = $2^4 \cdot 3 \cdot 23^5 \cdot 67^2 \cdot 617 \cdot 2399 \cdot 10781 \cdot 34673$
179	178	77 281577 212030 298592 756974 721745 = $5 \cdot 1069 \cdot 14458\ 667392\ 334948\ 286764\ 635121$
181	180	211 421757 749987 541697 225501 539625 = $5^3 \cdot 37 \cdot 41 \cdot 61 \cdot 1321 \cdot 2521 \cdot 5\ 488435\ 782589\ 277701$
209	180	4551 326160 887085 824176 768000 = $2^{10} \cdot 5^3 \cdot 11 \cdot 61 \cdot 271 \cdot 264\ 250891 \cdot 739\ 979551$
217	180	3724 911233 451940 358045 813517 = $3^5 \cdot 7 \cdot 11 \cdot 37 \cdot 241 \cdot 541 \cdot 571 \cdot 691 \cdot 2161 \cdot 2791 \cdot 17341$
279	180	18164 714706 446857 534815 843195 = $3^6 \cdot 5 \cdot 7 \cdot 13 \cdot 151 \cdot 211 \cdot 1321 \cdot 2551 \cdot 4591 \cdot 5011 \cdot 22171$
297	180	1078 851803 253231 276755 717661 = $3^2 \cdot 31^2 \cdot 199 \cdot 8191 \cdot 1\ 674991 \cdot 45687\ 081331$
235	184	81765 924684 755483 300654 973515 = $5 \cdot 139 \cdot 1657 \cdot 453377 \cdot 156604\ 975201\ 463093$
376	184	237 637802 564280 802840 123241 975060 = $2^2 \cdot 5 \cdot 47 \cdot 139 \cdot 18493 \cdot 742717 \cdot 3\ 536987 \cdot 37437\ 658303$
564	184	431950 475833 835326 053345 383630 = $2 \cdot 5 \cdot 47^3 \cdot 139^3 \cdot 277 \cdot 599 \cdot 742717 \cdot 1\ 257089$
191	190	165008 365487 223656 458987 611326 929859 = $11 \cdot 13 \cdot 51263 \cdot 612\ 771\ 091 \cdot 36\ 733950\ 669733\ 713761$
193	192	546617 105913 568165 545650 752630 767041 = $6529 \cdot 15361 \cdot 29761 \cdot 91969 \cdot 10\ 369729 \cdot 192026\ 280449$
221	192	5 562629 629465 863945 291002 496000 = $2^{10} \cdot 3^6 \cdot 5^3 \cdot 17 \cdot 31^2 \cdot 61 \cdot 73 \cdot 113 \cdot 193 \cdot 1297 \cdot 3529 \cdot 8209$
291	192	161 230789 161196 289366 922423 524464 = $2^4 \cdot 7 \cdot 13^2 \cdot 17^2 \cdot 577 \cdot 1489 \cdot 3457 \cdot 5641 \cdot 206209 \cdot 8\ 531233$
357	192	1504 490803 465665 772083 088125 = $3^4 \cdot 5^4 \cdot 7^4 \cdot 13^2 \cdot 37 \cdot 97^3 \cdot 1873 \cdot 1\ 157953$
388	192	145666 644086 003914 044409 030660 616112 = $2^4 \cdot 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot 37 \cdot 577 \cdot 3457 \cdot 5857 \cdot 13441 \cdot 206209 \cdot 69\ 761089$
416	192	1370 350108 087898 680332 276597 421875 = $3^9 \cdot 5^7 \cdot 7^2 \cdot 13^5 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 241 \cdot 409 \cdot 17401$
448	192	327 965590 186830 575092 883770 837200 = $2^4 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17^2 \cdot 577^2 \cdot 769 \cdot 13697 \cdot 299569 \cdot 471073$
476	192	1 099745 163233 204819 353212 762000 = $2^4 \cdot 3^6 \cdot 5^3 \cdot 11^2 \cdot 13 \cdot 47^2 \cdot 97^4 \cdot 241 \cdot 1489 \cdot 6833$
520	192	285052 110419 192727 742709 760000 = $2^{42} \cdot 3^4 \cdot 5^4 \cdot 7^3 \cdot 13^3 \cdot 17 \cdot 37^2 \cdot 73$

n	$\phi(n)$	h^-
560	192	54738 664378 286829 420235 392000 = $2^{10} \cdot 3^5 \cdot 5^3 \cdot 7 \cdot 13^2 \cdot 17 \cdot 37 \cdot 73 \cdot 97^2 \cdot 181 \cdot 193 \cdot 241 \cdot 409$
576	192	1157 874338 412588 470629 857952 431771 = $3^5 \cdot 13^2 \cdot 17 \cdot 401 \cdot 457 \cdot 1753 \cdot 1873 \cdot 1\,751377 \cdot 1573\,836529$
612	192	4 600831 021854 761317 711337 226240 = $2^{20} \cdot 3 \cdot 5 \cdot 11^2 \cdot 61 \cdot 73 \cdot 97 \cdot 193 \cdot 241 \cdot 15601 \cdot 7\,712737$
624	192	2 180486 664807 803314 987752 000000 = $2^9 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 13^5 \cdot 17^3 \cdot 37 \cdot 61 \cdot 97 \cdot 109 \cdot 409$
672	192	438246 323791 968232 985203 468800 = $2^9 \cdot 3^7 \cdot 5^2 \cdot 7^3 \cdot 13 \cdot 17 \cdot 61 \cdot 73 \cdot 97 \cdot 769 \cdot 8761 \cdot 70969$
720	192	222312 165238 308958 816217 760000 = $2^8 \cdot 3^4 \cdot 5^4 \cdot 7^2 \cdot 13^3 \cdot 19^2 \cdot 37^2 \cdot 109^2 \cdot 277 \cdot 313^2$
780	192	409 113496 073931 085358 039040 = $2^{46} \cdot 3 \cdot 5 \cdot 13^5 \cdot 61 \cdot 109 \cdot 157$
840	192	84 878288 737639 882168 320000 = $2^{14} \cdot 3^4 \cdot 5^4 \cdot 7^2 \cdot 13^4 \cdot 19 \cdot 37^2 \cdot 73 \cdot 97 \cdot 397$
197	196	5 532802 218713 600706 095993 713290 631720 = $2^3 \cdot 5 \cdot 1877 \cdot 7841 \cdot 9398\,302684\,870866\,656225\,611549$
199	198	18 844055 286602 530802 019847 012721 555487 = $3^4 \cdot 19 \cdot 727 \cdot 25\,645093 \cdot 207293\,548177 \cdot 3\,168190\,412839$
275	200	18 124664 091430 165276 567871 093750 = $2 \cdot 5^{12} \cdot 11^3 \cdot 41^2 \cdot 61 \cdot 71 \cdot 101 \cdot 241 \cdot 461 \cdot 541 \cdot 631$
303	200	32442 006711 177310 012824 426376 953125 = $5^{10} \cdot 61 \cdot 101 \cdot 601 \cdot 5701 \cdot 6701 \cdot 18701 \cdot 1255\,817401$
375	200	22 533972 115769 639175 905217 196211 = $11 \cdot 2801 \cdot 12101 \cdot 244301 \cdot 20\,602801 \cdot 12007\,682201$
404	200	28 160409 852152 369458 876449 426375 546875 = $5^7 \cdot 7 \cdot 41 \cdot 61 \cdot 101^2 \cdot 601 \cdot 2351 \cdot 18701 \cdot 40351 \cdot 1892\,989601$
500	200	20244 072859 233305 618155 148176 257775 = $5^2 \cdot 11 \cdot 401 \cdot 2801 \cdot 20\,602801 \cdot 94\,315301 \cdot 33728\,676001$
309	204	360807 306655 167078 388646 788532 317360 = $2^4 \cdot 5 \cdot 17 \cdot 103^2 \cdot 239 \cdot 1021 \cdot 3299 \cdot 233683 \cdot 7\,707223 \cdot 17\,247691$
412	204	311 393365 861041 316591 357682 493761 574005 = $5 \cdot 7 \cdot 103 \cdot 1021 \cdot 2347 \cdot 306511 \cdot 17\,247691 \cdot 54\,115489 \cdot 125\,998867$
265	208	169406 792495 647432 946133 820476 066925 = $5^2 \cdot 53 \cdot 1093 \cdot 4889 \cdot 12377 \cdot 19813 \cdot 11\,452741 \cdot 8519\,216837$
424	208	1435 850573 295225 659918 796765 068953 277637 = $3^4 \cdot 13 \cdot 79 \cdot 677 \cdot 1093 \cdot 4889 \cdot 13469 \cdot 32579 \cdot 2\,805713 \cdot 3875\,328913$
636	208	1 127233 629616 849856 487768 072597 188295 = $3 \cdot 5 \cdot 13^3 \cdot 53^2 \cdot 1093^2 \cdot 3251 \cdot 4889 \cdot 32579 \cdot 19684\,564069$
211	210	49238 446584 179914 120276 706365 116286 443831 = $3^2 \cdot 7^2 \cdot 41 \cdot 71 \cdot 181 \cdot 281^2 \cdot 421 \cdot 1051 \cdot 12251 \cdot 113\,981701 \cdot 4343\,510221$
321	212	41 597545 536058 643707 857919 997509 485501 = $3 \cdot 743 \cdot 9859 \cdot 2\,886593 \cdot 10\,109009 \cdot 64868\,018727\,424243$
428	212	70300 542035 941044 246482 693928 842589 712617 = $3 \cdot 743 \cdot 3181 \cdot 9859 \cdot 2\,886593 \cdot 348390\,669416\,638151\,886259$
247	216	13 453389 127871 713260 541632 243338 018775 = $3^9 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19^2 \cdot 73^2 \cdot 109^2 \cdot 127 \cdot 157 \cdot 163 \cdot 181 \cdot 397 \cdot 613 \cdot 1009$
259	216	15 168897 693915 178656 178325 215530 382842 = $2 \cdot 3^{20} \cdot 7^6 \cdot 13^2 \cdot 17^2 \cdot 19^3 \cdot 37 \cdot 73^3 \cdot 271 \cdot 14149$
327	216	503 374795 561927 637884 794232 382274 404226 = $2 \cdot 3^7 \cdot 13 \cdot 17 \cdot 37 \cdot 379 \cdot 1009 \cdot 2377 \cdot 47629 \cdot 34\,465933 \cdot 9431\,866153$

n	$\phi(n)$	h^-
333	216	84 239369 799126 310123 807613 556409 560000 = $2^{6} \cdot 3^{6} \cdot 5^{4} \cdot 7^{2} \cdot 13^{2} \cdot 19^{5} \cdot 37^{2} \cdot 43 \cdot 73 \cdot 523 \cdot 111637 \cdot 561529$
351	216	2 881839 794389 013705 029278 932481 257394 = $2 \cdot 3^{12} \cdot 7 \cdot 13 \cdot 19^{6} \cdot 37^{2} \cdot 73 \cdot 631 \cdot 2341 \cdot 31393 \cdot 136657$
399	216	1178 892414 491021 808120 869355 574272 = $2^{10} \cdot 3^{20} \cdot 7 \cdot 13 \cdot 19^{2} \cdot 37 \cdot 61 \cdot 73^{2} \cdot 577 \cdot 829 \cdot 1747$
405	216	289942 114683 805443 433002 828021 894577 = $37 \cdot 487 \cdot 541 \cdot 2053 \cdot 2593 \cdot 1\,583767 \cdot 3527\,772707\,308141$
436	216	893749 713826 042123 652446 227238 954966 290576 = $2^{4} \cdot 3^{7} \cdot 17 \cdot 19^{2} \cdot 163 \cdot 757 \cdot 1009 \cdot 3\,016927 \cdot 1174\,772971 \cdot 9431\,866153$
532	216	1 995278 293629 608216 703343 220411 633664 = $2^{12} \cdot 3^{10} \cdot 7^{3} \cdot 13 \cdot 19^{3} \cdot 31 \cdot 37^{2} \cdot 73^{2} \cdot 109 \cdot 1693 \cdot 2377 \cdot 2719$
648	216	4207 762445 242777 294033 981083 075596 417079 = $3^{3} \cdot 19 \cdot 37 \cdot 271^{2} \cdot 2593 \cdot 117\,132157 \cdot 157\,470427 \cdot 63112\,572037$
684	216	9 549392 972039 711651 917872 649044 836352 = $2^{14} \cdot 3^{6} \cdot 7^{2} \cdot 13 \cdot 19^{2} \cdot 37^{2} \cdot 73 \cdot 109 \cdot 127 \cdot 163 \cdot 199 \cdot 1693 \cdot 3637 \cdot 12583$
756	216	434848 520210 868494 245767 938408 147152 = $2^{4} \cdot 7^{3} \cdot 13 \cdot 19^{3} \cdot 37^{3} \cdot 109 \cdot 127^{2} \cdot 163 \cdot 181^{2} \cdot 271 \cdot 757 \cdot 9109$
253	220	256 271685 260834 247944 985594 908530 991952 = $2^{4} \cdot 3 \cdot 11^{4} \cdot 1409 \cdot 3301 \cdot 26951 \cdot 79861 \cdot 13\,962631 \cdot 2608\,886831$
363	220	23 207253 826992 628179 863710 751562 290176 = $2^{10} \cdot 67 \cdot 89 \cdot 353 \cdot 20021 \cdot 25741 \cdot 20\,891667\,283264\,099631$
484	220	29678 406487 322012 695719 894464 039435 383271 = $67 \cdot 353 \cdot 14411 \cdot 20021 \cdot 25741 \cdot 167971 \cdot 1\,005892\,255694\,569981$
223	222	217 076412 323050 485246 172261 728619 107578 141363 = $7 \cdot 43 \cdot 17\,909933\,575379 \cdot 11\,757537\,731851 \cdot 3424\,804483\,726447$
339	224	87309 027165 405351 637092 447907 404827 688960 = $2^{15} \cdot 3 \cdot 5 \cdot 17 \cdot 71 \cdot 113 \cdot 127 \cdot 281 \cdot 2137 \cdot 14449 \cdot 99709 \cdot 11\,853470\,598257$
435	224	299190 086533 933244 039620 216234 180608 = $2^{39} \cdot 3 \cdot 13 \cdot 29^{2} \cdot 113^{2} \cdot 281 \cdot 421 \cdot 757 \cdot 1289 \cdot 11257$
452	224	229 865767 233324 575111 010848 122335 548084 846592 = $2^{23} \cdot 3^{2} \cdot 7 \cdot 13^{2} \cdot 17 \cdot 29 \cdot 281 \cdot 24809 \cdot 168617 \cdot 374669 \cdot 11\,853470\,598257$
464	224	12 164820 242320 422627 042467 644729 294439 055360 = $2^{30} \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17^{2} \cdot 29^{5} \cdot 43^{2} \cdot 1877 \cdot 4621 \cdot 226129 \cdot 386093$
580	224	776 785847 831995 632448 594543 440172 154880 = $2^{39} \cdot 3 \cdot 5 \cdot 7^{2} \cdot 29 \cdot 281 \cdot 421 \cdot 463 \cdot 757 \cdot 1\,131397 \cdot 1\,413077$
696	224	6438 349938 668172 599554 162206 096280 780800 = $2^{38} \cdot 3^{3} \cdot 5^{2} \cdot 7^{2} \cdot 13 \cdot 29 \cdot 43^{3} \cdot 113 \cdot 1093 \cdot 1429 \cdot 1877 \cdot 71317$
227	226	2888 747573 690533 630075 559971 022165 906726 932055 = $5 \cdot 2939^{3} \cdot 1692\,824021\,974901 \cdot 13\,444015\,915122\,722869$
229	228	10934 752550 628778 589695 733157 034481 831976 032377 = $13 \cdot 17 \cdot 457 \cdot 7753 \cdot 705053 \cdot 47\,824141 \cdot 414153\,903321\,692666\,991589$
233	232	348185 729880 711782 527290 176798 948867 695747 163449 = $233 \cdot 1433 \cdot 1\,042818\,810684\,723912\,819200\,922459\,107271\,266041$ (composite)
295	232	670508 644900 926208 004253 553219 885108 451604 = $2^{2} \cdot 3 \cdot 59 \cdot 233 \cdot 349 \cdot 41413 \cdot 9\,342293 \cdot 3483\,942493 \cdot 8\,640296\,021597$
472	232	19371 983746 349662 149124 469187 254723 339443 284387 = $3^{2} \cdot 29 \cdot 59^{5} \cdot 233 \cdot 42283 \cdot 135257 \cdot 168143 \cdot 4\,237829 \cdot 109337\,677693$
708	232	7 622833 744450 532364 757064 890176 317824 613409 = $3 \cdot 59 \cdot 233 \cdot 523 \cdot 2\,069383 \cdot 3\,789257 \cdot 109337\,677693 \cdot 412212\,149161$

n	$\phi(n)$	h^-
239	238	19 252683 042543 984486 813299 844961 436592 191498 141760 = $2^{6} \cdot 3 \cdot 5 \cdot 511123 \cdot 14\,136487 \cdot 123373\,184789 \cdot 22497\,399987\,891136\,953079$
241	240	74 361351 053524 744837 764467 869162 082791 741351 378657 = $47^{2} \cdot 13921 \cdot 15601 \cdot 2\,359873 \cdot 126\,767281 \cdot 518123\,008737\,871423\,891201$
287	240	75 414262 624860 852745 819151 571359 184834 222400 = $2^{6} \cdot 5^{2} \cdot 7 \cdot 11^{7} \cdot 13 \cdot 31^{2} \cdot 61 \cdot 521 \cdot 1201 \cdot 1609 \cdot 2521 \cdot 8641 \cdot 20673\,617161$
305	240	135 088091 280028 160307 240417 262034 056281 285000 = $2^{3} \cdot 3^{2} \cdot 5^{4} \cdot 13^{2} \cdot 37 \cdot 41^{4} \cdot 61^{3} \cdot 1861 \cdot 2281 \cdot 3061 \cdot 24061 \cdot 37501 \cdot 63841$
325	240	958286 131671 211592 542476 979144 265746 218304 = $2^{6} \cdot 61^{3} \cdot 101 \cdot 1201 \cdot 2141 \cdot 7681 \cdot 11701 \cdot 194521 \cdot 849721 \cdot 17\,098621$
369	240	528 852535 797845 727358 844974 839889 196910 080000 = $2^{12} \cdot 5^{4} \cdot 11^{6} \cdot 17 \cdot 19 \cdot 31 \cdot 271 \cdot 421 \cdot 4801 \cdot 16921 \cdot 1256\,507775\,765241$
385	240	18 696191 070960 590983 421400 100896 768000 = $2^{31} \cdot 3^{2} \cdot 5^{3} \cdot 11 \cdot 19^{2} \cdot 31 \cdot 157 \cdot 1021 \cdot 9661 \cdot 16141 \cdot 2\,514961$
429	240	1880 049931 342806 129486 552279 849583 657000 = $2^{3} \cdot 5^{3} \cdot 7 \cdot 11^{3} \cdot 31 \cdot 61^{3} \cdot 181 \cdot 571 \cdot 661 \cdot 39521 \cdot 83701 \cdot 126\,901681$
465	240	6056 875285 186558 003929 869566 624727 040000 = $2^{19} \cdot 3^{6} \cdot 5^{4} \cdot 7 \cdot 31 \cdot 61 \cdot 151 \cdot 181 \cdot 631 \cdot 1481 \cdot 1801 \cdot 129121 \cdot 322501$
488	240	3 971856 968532 956975 396384 265567 521800 430781 628875 = $3^{3} \cdot 5^{3} \cdot 11^{2} \cdot 31^{2} \cdot 41^{2} \cdot 43 \cdot 61 \cdot 101 \cdot 151 \cdot 421 \cdot 691 \cdot 1861 \cdot 4721 \cdot 6481 \cdot 34171 \cdot 265\,892761$
495	240	151 284295 307196 895954 238278 778191 913580 = $2^{2} \cdot 3 \cdot 5 \cdot 7 \cdot 11^{3} \cdot 29^{2} \cdot 31^{3} \cdot 181^{2} \cdot 229 \cdot 241^{2} \cdot 421 \cdot 2131 \cdot 3361 \cdot 8221$
496	240	686038 372620 782033 886901 075737 481803 287781 408768 = $2^{15} \cdot 3^{2} \cdot 11^{4} \cdot 31^{4} \cdot 37 \cdot 41 \cdot 61^{2} \cdot 97 \cdot 211 \cdot 241 \cdot 601 \cdot 4621 \cdot 5281 \cdot 14281 \cdot 29501$
525	240	29 585677 490787 726928 862791 955910 586368 = $2^{12} \cdot 3^{4} \cdot 11 \cdot 13 \cdot 31^{2} \cdot 61^{4} \cdot 271 \cdot 331 \cdot 601 \cdot 1861 \cdot 467 \cdot 132041$
572	240	5 290237 648692 385160 711880 570308 851548 534375 = $3 \cdot 5^{5} \cdot 7 \cdot 19^{2} \cdot 31 \cdot 41 \cdot 61^{2} \cdot 421 \cdot 661 \cdot 27631 \cdot 72271 \cdot 83701 \cdot 1015\,122781$
616	240	894031 197420 910862 005847 489304 819295 846400 = $2^{40} \cdot 5^{2} \cdot 7 \cdot 11^{5} \cdot 13 \cdot 31^{4} \cdot 181 \cdot 211 \cdot 2161 \cdot 4621 \cdot 6301$
620	240	19 441064 004704 709948 640099 632484 806819 840000 = $2^{26} \cdot 3^{4} \cdot 5^{4} \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 421 \cdot 631 \cdot 5821 \cdot 66931 \cdot 129121 \cdot 502081$
700	240	126016 649965 778239 405605 204267 365457 285120 = $2^{12} \cdot 3^{5} \cdot 5 \cdot 11 \cdot 13 \cdot 31 \cdot 59^{2} \cdot 61^{2} \cdot 271 \cdot 601 \cdot 1861 \cdot 9181 \cdot 44641 \cdot 3\,549901$
732	240	1339 692320 604469 611903 838974 531410 116492 800000 = $2^{12} \cdot 3^{3} \cdot 5^{5} \cdot 11 \cdot 13 \cdot 19^{2} \cdot 31^{3} \cdot 41 \cdot 61^{2} \cdot 211 \cdot 691 \cdot 1861 \cdot 6481 \cdot 25301 \cdot 371341$
744	240	181 082733 783181 938577 850646 686177 657202 278400 = $2^{17} \cdot 3^{5} \cdot 5^{2} \cdot 11^{5} \cdot 31^{2} \cdot 41^{2} \cdot 101 \cdot 131 \cdot 151 \cdot 211 \cdot 541 \cdot 5281 \cdot 13591 \cdot 53401$
792	240	5 042681 390633 567588 773182 959215 349464 474500 = $2^{2} \cdot 3^{2} \cdot 5^{3} \cdot 11^{2} \cdot 13^{2} \cdot 19 \cdot 31^{5} \cdot 61^{2} \cdot 181 \cdot 1381 \cdot 5521 \cdot 5791 \cdot 19231 \cdot 176161$
900	240	744248 582096 150452 589487 856013 489542 134375 = $3 \cdot 5^{5} \cdot 11^{2} \cdot 61 \cdot 211 \cdot 331 \cdot 811 \cdot 2161 \cdot 2791 \cdot 24481 \cdot 334261 \cdot 3847\,430341$
924	240	228 281655 906261 469381 852055 785911 091200 = $2^{39} \cdot 3^{5} \cdot 5^{2} \cdot 7 \cdot 11^{2} \cdot 31^{4} \cdot 61 \cdot 101 \cdot 151 \cdot 181 \cdot 691 \cdot 751$
251	250	95469 181654 584518 651828 574432 658888 070113 445087 403827 = $7 \cdot 11 \cdot 348270001 \cdot 9\,631365\,977251 \cdot 369631\,114567\,755437\,243663\,626501$
301	252	205430 142293 947345 943779 193986 871148 546394 604544 = $2^{10} \cdot 3^{3} \cdot 7^{7} \cdot 19 \cdot 43^{2} \cdot 211 \cdot 631 \cdot 6301 \cdot 14827 \cdot 16843 \cdot 19531 \cdot 122599 \cdot 511939$
381	252	11 479286 278091 328075 258484 555696 616781 110509 888215 = $3^{2} \cdot 5 \cdot 7^{2} \cdot 13 \cdot 37 \cdot 43^{2} \cdot 547 \cdot 631 \cdot 673 \cdot 883 \cdot 3079 \cdot 6007 \cdot 626599 \cdot 2\,185471 \cdot 1126\,755757$

n	$\phi(n)$	h^-
387	252	1 348400 009635 509434 335776 865706 103793 086610 214753 = $7^3 \cdot 13^2 \cdot 19^2 \cdot 29 \cdot 43 \cdot 211^2 \cdot 463 \cdot 883 \cdot 967 \cdot 1933 \cdot 3067 \cdot 3319 \cdot 4621 \cdot 125287 \cdot 257713$
441	252	2427 799098 355426 760759 007408 851329 652222 396831 = $7^4 \cdot 29 \cdot 43^5 \cdot 127 \cdot 337 \cdot 673 \cdot 2731 \cdot 11173 \cdot 43051 \cdot 1\ 271383 \cdot 4\ 930381$
508	252	103042 170932 346966 742775 797541 839182 084871 642467 503360 = $2^8 \cdot 5 \cdot 7^2 \cdot 13^3 \cdot 19 \cdot 43^3 \cdot 547 \cdot 757 \cdot 883^2 \cdot 2143 \cdot 3079 \cdot 626599 \cdot 2\ 664901 \cdot 139\ 159441$
257	256	5 452485 023419 230873 223822 625555 964461 476422 854662 168321 = $257 \cdot 20738\ 946049 \cdot 1\ 022997\ 744563\ 911961\ 561298\ 698183\ 419037\ 149697$
512	256	6 262503 984490 932358 745721 482528 922841 978219 389975 605329 = $17 \cdot 21121 \cdot 76\ 532353 \cdot 29\ 102880\ 226241 \cdot 7830\ 753969\ 553468\ 937988\ 617089$
544	256	4584 742688 639592 322280 890443 396756 015190 545059 020800 = $2^{30} \cdot 3^8 \cdot 5^2 \cdot 7^4 \cdot 13 \cdot 17^6 \cdot 31^2 \cdot 41^4 \cdot 97 \cdot 353 \cdot 433 \cdot 577 \cdot 929 \cdot 1601$
640	256	112 066740 284710 541318 559132 951039 771578 615246 011365 = $3^2 \cdot 5 \cdot 17^4 \cdot 41 \cdot 97^2 \cdot 337 \cdot 7841 \cdot 9473 \cdot 21121 \cdot 376801 \cdot 69\ 470881 \cdot 5584\ 997633$
680	256	77483 560514 02244 288033 941979 251535 291351 040000 = $2^{41} \cdot 3^7 \cdot 5^4 \cdot 13 \cdot 17^3 \cdot 41 \cdot 73 \cdot 97 \cdot 593 \cdot 977 \cdot 3217 \cdot 19489 \cdot 38273$
768	256	1067 969144 915565 716868 049522 568978 331378 093561 484521 = $3^2 \cdot 17 \cdot 401 \cdot 1697 \cdot 13313 \cdot 21121 \cdot 49057 \cdot 175361 \cdot 198593 \cdot 733697 \cdot 29\ 102880\ 226241$
816	256	793553 314770 547109 801192 086472 747224 274042 880000 = $2^{38} \cdot 3^8 \cdot 5^4 \cdot 13 \cdot 17^4 \cdot 41^2 \cdot 97 \cdot 113 \cdot 193 \cdot 577 \cdot 1601 \cdot 2081 \cdot 94849$
960	256	20130 907061 992729 156753 037152 064135 304760 934400 = $2^{14} \cdot 3^4 \cdot 5^2 \cdot 7^6 \cdot 17^7 \cdot 41 \cdot 89 \cdot 97 \cdot 337 \cdot 401 \cdot 433 \cdot 593 \cdot 7841 \cdot 130513$
1020	256	11 412817 953927 959213 205123 673154 912256 000000 = $2^{42} \cdot 3^3 \cdot 5^6 \cdot 17^3 \cdot 73 \cdot 193 \cdot 353 \cdot 593 \cdot 1889 \cdot 3217 \cdot 69857$

Bibliography

The following concentrates mainly on the period 1970–1981, since the period 1940–1970 is covered in *Reviews in Number Theory* (ed. by W. LeVeque; American Mathematical Society, 1974), especially Volume 5. For very early works, see the references in Hilbert [2]. The reader should also consult Kummer's *Collected Papers* for numerous papers, many of which are still valuable reading. The books of Narkiewicz and Ribenboim [1] also contain useful bibliographies.

A note "MR **12**: 345" refers to a review in *Mathematical Reviews* (similarly for "LeVeque" or "Zentralblatt"). These are given mostly for articles in less accessible journals, for untranslated articles in Japanese or Russian, when the review lists errors or additional information, or when the review gives a good summary of a difficult article.

Adachi, N.

1. Generalization of Kummer's criterion for divisibility of class numbers. *J. Number Theory*, **5** (1973), 253–265. MR **48**: 11041.

Adleman, L., Pomerance, C., and Rumely, R.

1. On distinguishing prime numbers from composite numbers (to appear).

Amice, Y.

1. Interpolation *p*-adique. *Bull. Soc. Math. France*, **92** (1964), 117–180.
2. *Les Nombres p-Adiques*. Presse Universitaire de France, 1975.

Amice, Y. and Fresnel, J.

1. Fonctions zêta *p*-adiques des corps de nombres abéliens réels. *Acta Arith.*, **20** (1972), 353–384.

Amice, Y. and Vélu, J.

1. Distributions *p*-adiques associées aux séries de Hecke. *Astérisque*, **24-25** (1975), 119–131.

Ankeny, N., Artin, E., and Chowla, S.

1. The class number of real quadratic number fields. *Ann. of Math.* (2), **56** (1952), 479–493.

Ankeny, N. and Chowla, S.

1. The class number of the cyclotomic field. *Canad. J. Math.*, **3** (1951), 486–494.

Ankeny, N., Chowla, S., and Hasse, H.

1. On the class number of the maximal real subfield of a cyclotomic field. *J. reine angew. Math.*, **217** (1965), 217–220.

Ax, J.

1. On the units of an algebraic number field. *Illinois J. Math.*, **9** (1965), 584–589.

Ayoub, R.

1. On a theorem of Iwasawa. *J. Number Theory*, **7** (1975), 108–120.

Babaĭcev, V.

1. Some questions in the theory of Γ-extensions of algebraic number fields, *Izv. Akad. Nauk. SSSR Ser. Mat.*, **40** (1976), 477–487, 709; 715–726, 949; Translation: *Math. USSR Izvestia*, **10** (1976), 451–460; 675–685.
2. On the boundedness of Iwasawa's μ-invariant (Russian). *Izv. Akad. Nauk. SSSR, Ser. Mat.*, **44** (1980), 3–23; Translation:*Math. USSR Izvestia*, **16** (1980), 1–19.

Barsky, D.

1. Analyse p-adique et congruences. Sém. de Théorie des Nombres, Bordeaux, 1975–1976, Exp. no. 21, 9 pp. MR **56**:2969.
2. Analyse p-adique et nombres de Bernoulli. *C. R. Acad. Sci. Paris, Sér. A-B*, **283** (1976), A1069–A1072.
3. Fonction génératrice et congruences (application aux nombres de Bernoulli). Sém. Delange–Pisot–Poitou, Théorie des Nombres, 17e année, 1975/1976, fasc. 1, Exp. no. 21, 16 pp.
4. Fonctions zêta p-adiques d'une classe de rayon des corps de nombres totalement réels. Groupe d'Etude d'Analyse Ultramétrique, 5e année, 1977/1978, Exp. no. 16, 23 pp. MR **80g**: 12009.
5. Transformation de Cauchy p-adique et algèbre d'Iwasawa. *Math. Ann.*, **232** (1978), 255–266.
6. Majoration du nombre de zéros des fonctions L p-adiques dans un disque (to appear).
7. On Morita's p-adic gamma function. *Math. Proc. Cambridge Philos. Soc.*, **89** (1981), 23–27.

Bašmakov, M. and Al'-Nader, N.

1. Behavior of the curve $x^3 + y^3 = 1$ in a cyclotomic Γ-extension, *Mat. Sbornik*, **90** 132 (1973), 117–130; English trans.: *Math. USSR-Sb.*, **19** (1973), 117–130.

Bašmakov, M. and Kurochkin, A.

1. Rational points on a modular curve over a two-cyclotomic field. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, **57** (1976), 5–7; English trans.: *J. Soviet Math.*, **11**, no. 4 (1979), 511–513.

Bass, H.

1. Generators and relations for cyclotomic units. *Nagoya Math. J.*, **27** (1966), 401–407 (see Ennola [2]).

Báyer, P.

1. Values of the Iwasawa L-functions at the point $s = 1$. *Arch. Math. (Basel)*, **32** (1979), 38–54.
2. The irregularity index of prime numbers (Spanish). *Collect. Math.*, **30** (1979), no. 1, 11–20.

Báyer, P. and Neukirch, J.

1. On values of zeta functions and l-adic Euler characteristics. *Invent. math.*, **50** (1978/1979), 35–64.

Beach, B., Williams, H., and Zarnke, C.

1. Some computer results on units in quadratic and cubic fields. Proc. of the Twenty-Fifth Summer Meeting of the Canadian Math. Congress, Lakehead Univ., 1971, 609–648. MR **49**:2656.

Berger, A.

1. Recherches sur les nombres et les fonctions de Bernoulli. *Acta Math.*, **14** (1890/1891), 249–304.

Bertrandias, F. and Payan, J.-J.

1. Γ-extensions et invariants cyclotomiques. *Ann. Sci. Ecole Norm. Sup.* (4), **5** (1972), 517–543.

Bloom, J.

1. On the invariants of some $\mathbb{Z}_l$-extensions. *J. Number Theory*, **11** (1979), 239–256.

Bloom, J. and Gerth, F.

1. The Iwasawa invariant μ in the composite of two $\mathbb{Z}_l$-extensions. *J. Number Theory*, **13** (1981), 262–267.

Borel, A.

1. Cohomologie de SL_n et valeurs de fonctions zêta aux points entiers. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4), **4** (1977), no. 4, 613–636; errata, **7** (1980), no. 2, 373.

Borevich, Z. and Shafarevich, I.

1. *Number Theory*. Academic Press: London and New York, 1966.

Brückner, H.

1. Explizites Reziprozitätsgesetze und Anwendungen. Vorlesungen aus dem Fachbereich Math. der Univ. Essen, Heft 2 (1979), 83 pp. Zentralblatt **437**:12001.

Brumer, A.

1. On the units of algebraic number fields. *Mathematika*, **14** (1967), 121–124.
2. Travaux récents d'Iwasawa et de Leopoldt. Sém. Bourbaki, 1966/1967, Exp. no. 325, 14 pp.
3. The class group of all cyclotomic integers. *J. Pure Appl. Algebra*, **20** (1981), 107–111.

Candiotti, A.

1. Computations of Iwasawa invariants and K_2. *Compositio math.*, **29** (1974), 89–111.

Carlitz, L.

1. Arithmetic properties of generalized Bernoulli numbers. *J. reine angew. Math.*, **202** (1959), 174–182.
2. A generalization of Maillet's determinant and a bound for the first factor of the class number. *Proc. Amer. Math. Soc.*, **12** (1961), 256–261.

Carroll, J.

1. On determining the quadratic subfields of $\mathbb{Z}_2$-extensions of complex quadratic fields, *Compositio Math.*, **30** (1975), 259–271.

Carroll, J. and Kisilevsky, H.

1. Initial layers of $\mathbb{Z}_l$-extensions of complex quadratic fields. *Compositio Math.*, **32** (1976), 157–168.
2. On Iwasawa's λ-invariant for certain $\mathbb{Z}_l$-extensions (to appear).

Cartier, P. and Roy, Y.

1. Certains calculs numériques relatifs à l'interpolation p-adique des séries de Dirichlet. *Modular functions of one variable, III* (Antwerp 1972), 269–349. Springer Lecture Notes in Mathematics, vol. 350 (1973).

Cassels, J. and Fröhlich, A.

1. *Algebraic Number Theory* (ed. by J. Cassels and A. Fröhlich). Academic Press: London and New York, 1967.

Cassou-Noguès, P.

1. Formes linéaires p-adiques et prolongement analytique. Sém. de Théorie des Nombres, Bordeaux, 1970–1971, Exp. no. 14, 7 pp. MR **53**:2904.
2. Formes linéaires p-adiques et prolongement analytique. *Bull. Soc. Math. France, Mém.*, no. 39–40 (1974), 23–26.
3. Fonctions L p-adiques des corps de nombres totalement réels. Sém. Delange-Pisot-Poitou, Théorie des Nombres, 19e année, 1977/1978, Exp. no. 33, 15 pp.
4. Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. *Invent. math.*, **51** (1979), 29–59.
5. Analogues p-adiques des fonctions Γ-multiples, *Astérisque*, **61** (1979), 43–55.
6. p-adic L-functions for elliptic curves with complex multiplication. I. *Compositio Math.*, **42** (1980/1981), 31–56.
7. Analogues p-adiques de certaines fonctions arithmétiques. Sém. de Théorie des Nombres, Bordeaux, 1970–1971, Exp. no. 24, 12 pp., MR **53**: 363.
8. Fonctions p-adiques attachées à des formes quadratiques. Groups d'Etude d'Analyse Ultrametrique, 3e année, 1975/76, Exp. no. 16, 24 pp. MR **58**: 27906.

Childs, L.

1. Stickelberger relations on tame Kummer extensions of prime degree. Proc. of the Queen's Number Theory Conf., 1979 (Kingston, Ontario; ed. by P. Ribenboim). *Queen's Papers in Pure and Applied Math.*, no. 54 (1980), 249–256.
2. Stickelberger relations and tame extensions of prime degree, *Ill. J. Math.*, **25** (1981), 258–266.

Clayburgh, J.

1. *It's My Turn.* Directed by Claudia Weill; starring Jill Clayburgh, Michael Douglas, and Charles Grodin. Distributed by Warner-Columbia Films; 1980.

Coates, J.

1. On K_2 and some classical conjectures in algebraic number theory. *Ann. of Math.*, **95** (1972), 99–116.
2. K-theory and Iwasawa's analogue of the Jacobian. *Algebraic K-Theory, II* (Seattle 1972), 502–520. Springer Lecture Notes in Mathematics, vol. 342 (1973).
3. Research problems: Arithmetic questions in K-theory. *Algebraic K-theory, II* (Seattle 1972), 521–523. Springer Lecture Notes in Mathematics, vol. 342 (1973).
4. On Iwasawa's analogue of the Jacobian for totally real number fields. *Analytic Number Theory* (Proc. Sympos. Pure Math., vol. 25; St. Louis), 51–61. Amer. Math. Soc.: Providence, 1973.
5. Fonctions zêta partielles d'un corps de nombres totalement réel. Sém. Delange-Pisot-Poitou, Théorie des Nombres, 16e année, 1974/1975, fasc. 1, Exp. no. 1, 9pp.
6. The arithmetic of elliptic curves with complex multiplication. Proc. Int. Congress of Math.: Helsinki, 1978, 351–355.
7. p-adic L-functions and Iwasawa's theory. *Algebraic Number Fields* (Durham Symposium, 1975; ed. by A. Fröhlich), 269–353. Academic Press: London, 1977.
8. Travaux de Mazur–Wiles sur les corps cyclotomiques. Sém. Bourbaki, Juin 1981.

Coates, J. and Lichtenbaum, S.

1. On l-adic zeta functions. *Ann. of Math.* (2), **98** (1973), 498–550.

Coates, J. and Sinnott, W.

1. An analogue of Stickelberger's theorem for the higher K-groups. *Invent. math.*, **24** (1974), 149–161.
2. On p-adic L-functions over real quadratic fields. *Invent. math.*, **25** (1974), 253–279.
3. Integrality properties of the values of partial zeta functions. *Proc. London Math. Soc.* (3), **34** (1977), 365–384.

Coates, J. and Wiles, A.

1. Explicit reciprocity laws. *Astérisque*, **41-42** (1977), 7–17.

2. Kummer's criterion for Hurwitz numbers. *Algebraic Number Theory* (Kyoto conference, 1976; ed. by Iyanaga). Jap. Soc. Promotion Sci.: Tokyo, 1977, 9–23.
3. On the conjecture of Birch and Swinnerton-Dyer. *Invent. math.*, **39** (1977), 223–251.
4. On p-adic L-functions and elliptic units. *J. Austral. Math. Soc., Ser. A*, **26** (1978), 1–25.

Cohn, H.
1. A device for generating fields of even class number. *Proc. Amer. Math. Soc.*, **7** (1956), 595–598.
2. A numerical study of Weber's real class number calculation. I. *Numer. Math.*, **2** (1960), 347–362. (Equ. 3.14 is incorrect, hence the results are incomplete).

Coleman, R.
1. Division values in local fields. *Invent. math.*, **53** (1979), 91–116.

Cornell, G.
1. Abhyankar's lemma and the class group. *Number Theory Carbondale 1979* (ed. by M. Nathanson). Springer Lecture Notes in Mathematics, vol. 751, (1971), 82–88.

Cornell, G. and Rosen, M.
1. Group-theoretic constraints on the structure of the class group. *J. Number Theory*, **13** (1981), 1–11.
2. Cohomological analysis of the class group extension problem. Proc. Queen's Number Theory Conf., 1979 (Kingston, Ontario; ed. by P. Ribenboim). *Queen's Papers in Pure and Applied Math.*, no. 54 (1980), 287–308.

Cornell, G. and Washington, L.
1. Class numbers of cyclotomic fields (to appear).

Cuoco, A.
1. The growth of Iwasawa invariants in a family. *Compositio Math.*, **41** (1980), 415–437.

Cuoco, A. and Monsky, P.
1. Class numbers in $\mathbb{Z}_p^d$-extensions. *Math. Ann.*, **255** (1981), 235–258.

Davenport, H. and Hasse, H.
1. Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen. *J. reine angew. Math.*, **172** (1935), 151–182.

Davis, D.
1. Computing the number of totally positive circular units which are squares. *J. Number Theory*, **10** (1978), 1–9.

Davis, H.
1. *Tables of the Mathematical Functions*, vol. II. Principia Press of Trinity University: San Antonio, Texas, 1963.

Deligne, P. and Ribet, K.
1. Values of abelian L-functions at negative integers over totally real fields. *Invent. math.*, **59** (1980), 227–286.

Dénes, P.
1. Über irreguläre Kreiskörper. *Publ. Math. Debrecen*, **3** (1953), 17–23.
2. Über Grundeinheitssysteme der irregulären Kreiskörper von besonderen Kongruenzeigenschaften. *Publ. Math. Debrecen*, **3** (1954), 195–204.
3. Über den zweiten Faktor der Klassenzahl und den Irregularitatsgrad der irregulären Kreiskörper. *Publ. Math. Debrecen*, **4** (1956), 163–170.

Diamond, J.
1. The p-adic log gamma function and p-adic Euler constants. *Trans. Amer. Math. Soc.*, **233** (1977), 321–337.
2. The p-adic gamma measures. *Proc. Amer. Math. Soc.*, **75** (1979), 211–217.

3. On the values of p-adic L-functions at positive integers. *Acta Arith.*, **35** (1979), 223–237.

Diaz y Diaz, F.

1. Tables minorant la racine n-ième du discriminant d'un corps de degré n. Publ. Math: Orsay, 1980.

Dummit, D.

1. The structure of Galois modules in $\mathbb{Z}_p$-extensions. Ph.D. Thesis, Princeton Univ., 1980.

Edwards, H.

1. *Fermat's Last Theorem, a Genetic Introduction to Algebraic Number Theory.* Graduate Texts in Mathematics, Springer-Verlag: New York–Berlin–Heidelberg, 1977.

Eichler, M.

1. Eine Bemerkung zur Fermatschen Vermutung. *Acta Arith.*, **11** (1965), 129–131, 261.
2. Zum 1. Fall der Fermatschen Vermutung. Eine Bemerkung zu zwei Arbeiten von. L. Skula und H. Brückner. *J. reine angew. Math.*, **260** (1975), 214.
3. *Introduction to the Theory of Algebraic Numbers and Functions.* Academic Press: New York and London, 1966.

Eisenstein, G.

1. Über ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze. *J. reine angew. Math.*, **39** (1850), 351–364; *Mathematische Werke*, II, 623–636. Chelsea: New York, 1975.

Ellison, W.

1. *Les Nombres Premiers* (en collaboration avec M. Mendès France). Hermann: Paris, 1975.

Ennola, V.

1. Some particular relations between cyclotomic units. *Ann. Univ. Turku., Ser. AI*, no. 147 (1971).
2. On relations between cyclotomic units. *J. Number Theory*, **4** (1972), 236–247; errata: MR **45**: 8633.
3. Proof of a conjecture of Morris Newman. *J. reine angew. Math.*, **264** (1973), 203–206.

Ernvall, R.

1. Generalized Bernoulli numbers, generalized irregular primes, and class number. *Ann. Univ. Turku., Ser. AI*, no. 178 (1979), 72 pp.

Ernvall, R. and Metsänkylä, T.

1. Cyclotomic invariants and E-irregular primes. *Math. Comp.*, **32** (1978), 617–629; corrigenda, **33** (1979), 433.

Federer, L.

1. Regulators, Iwasawa modules, and the main conjecture for $p = 2$, *Modern Trends in Number Theory Related to Fermat's Last Theorem*, Birkhäuser: Boston–Basel–Stuttgart, to appear.

Federer, L. and Gross, B.

1. Regulators and Iwasawa modules. *Invent. math.*, **62** (1981), 443–457.

Ferrero, B.

1. An explicit bound for Iwasawa's λ-invariant. *Acta Arith.*, **33** (1977), 405–408.
2. Iwasawa invariants of abelian number fields. *Math. Ann.*, **234** (1978), 9–24.
3. The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields, *Amer. J. Math.*, **102** (1980), 447–459.
4. Iwasawa invariants of abelian number fields, Ph.D. Thesis, Princeton Univ., 1975.

Ferrero, B. and Greenberg, R.

1. On the behaviour of p-adic L-functions at $s = 0$. *Invent. math.*, **50** (1978), 91–102.

Ferrero, B. and Washington, L.

1. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math.*, **109** (1979), 377–395.

Fitting, H.

1. Die Determinantenideale eines Moduls. *Jahresbericht Deutsch. Math.-Verein.*, **46** (1936), 195–228.

Fresnel, J.

1. Nombres de Bernoulli et fonctions L p-adiques. *Ann. Inst. Fourier, Grenoble*, **17** (1967), fasc. 2, 281–333.
2. Fonctions zêta p-adiques des corps de nombres abéliens réels. *Bull. Soc. Math. France*, Mém. no. 25 (1971), 83–89.
3. Valeurs des fonctions zêta aux entiers négatifs. Sém. de Théorie des Nombres, Bordeaux, 1970–1971, Exp. no. 27, 30 pp. MR **52**: 13676.

Friedman, E.

1. Ideal class groups in basic $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extensions of abelian number fields (to appear in *Invent. math.*).

Fröhlich, A.

1. On non-ramified extensions with prescribed Galois group. *Mathematika*, **9** (1962), 133–134.
2. On the absolute class-group of Abelian number fields. *J. London Math. Soc.*, **29** (1954), 211–217; **30** (1955), 72–80.
3. On a method for the determination of class number factors in number fields. *Mathematika*, **4** (1957), 113–121.
4. Stickelberger without Gauss sums. *Algebraic Number Fields* (Durham Symposium, 1975; ed. by A. Fröhlich), 589–607. Academic Press: London, 1977.

Furtwängler, P.

1. Über die Klassenzahlen der Kreisteilungskörper. *J. reine angew. Math.*, **140** (1911), 29–32.

Furuta, Y.

1. On class field towers and the rank of ideal class groups. *Nagoya Math. J.*, **48** (1972), 147–157.

Galkin, V.

1. The first factor of the class number of ideals of a cyclotomic field (Russian). *Uspehi Mat. Nauk*, **27** (1972), no. 6 (168), 233–234. MR **52**: 13727.

Galovich, S. and Rosen, M.

1. The class number of cyclotomic function fields. *J. Number Theory*, **13** (1981), 363–375.

Garbanati, D.

1. Unit signatures, and even class numbers, and relative class numbers. *J. reine angew. Math.*, **274/275** (1975), 376–384.
2. Units with norm -1 and signatures of units. *J. reine angew. Math.*, **283/284** (1976), 164–175.

Gerth, F.

1. Structure of l-class groups of certain number fields and $\mathbb{Z}_l$-extensions. *Mathematika*, **24** (1977), 16–33.
2. The Hasse norm principle in cyclotomic number fields. *J. reine angew. Math.*, **303/304** (1978), 249–252.
3. Upper bounds for an Iwasawa invariant. *Compositio Math.*, **39** (1979), 3–10.
4. The Iwasawa invariant μ for quadratic fields. *Pacific J. Math.*, **80** (1979), 131–136.
5. The ideal class groups of two cyclotomic fields. *Proc. Amer. Math. Soc.*, **78** (1980), 321–322.

Giffen, C.

1. Diffeotopically trivial periodic diffeomorphisms. *Invent. math.*, **11** (1970), 340–348.

Gillard, R.

1. Remarques sur certaines extensions prodiédrales de corps de nombres. *C. R. Acad. Sci. Paris, Sér. A-B*, **282** (1976), A13–A15.
2. $\mathbb{Z}_l$-extensions, fonctions L l-adiques et unités cyclotomiques. Sém. de Théorie des Nombres, Bordeaux, 1976–1977, Exp. no. 24, 19 pp. MR **80k**: 12016.
3. Formulations de la conjecture de Leopoldt et étude d'une condition suffisante. *Abh. Math. Sem. Univ. Hamburg*, **48** (1979), 125–138.
4. Sue le groupe des classes des extensions abéliennes réelles. Sém. Delange–Pisot–Poitou, Théorie des Nombres, 18e année, 1976/1977, Exp. no. 10, 6 pp.
5. Extensions abéliennes et répartition modulo 1. *Astérisque*, **61** (1979), 83–93.
6. Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_l$-extensions. *Ann. Inst. Fourier, Grenoble*, **29** (1979), fasc. 1, 49–79; fasc. 4, 1–15.
7. Unités elliptiques et unités cyclotomiques. *Math. Ann.*, **243** (1979), 181–189.
8. Remarques sur les unités cyclotomiques et les unités elliptiques. *J. Number Theory*, **11** (1979), 21–48.
9. Unités elliptiques et fonctions L p-adiques. Sém. de Théorie des Nombres, Paris 1979–1980 (Sém. Delange–Pisot–Poitou), 99–122. Birkhäuser: Boston–Basel–Stuttgart, 1981.
10. Unités elliptiques et fonctions L p-adiques. *Compositio Math.*, **42** (1981), 57–88.
11. Unités elliptiques et unités de Minkowski. *J. Math. Soc. Japan*, **32** (1980), 697–701.

Gillard, R. and Robert, G.

1. Groupes d'unités elliptiques. *Bull. Soc. Math. France*, **107** (1979), 305–317.

Gold, R.

1. Γ-extensions of imaginary quadratic fields. *Pacific J. Math.*, **40** (1972), 83–88.
2. The non-triviality of certain $\mathbb{Z}_l$-extensions. *J. Number Theory*, **6** (1974), 369–373.
3. Examples of Iwasawa invariants. *Acta Arith.*, **26** (1974–75), 21–32, 233–240.
4. Γ-extensions of imaginary quadratic fields. II. *J. Number Theory*, **8** (1976), 415–419.
5. $\mathbb{Z}_3$-invariants of real and imaginary quadratic fields. *J. Number Theory*, **8** (1976), 420–423.

Goldstein, L.

1. On the class numbers of cyclotomic fields. *J. Number Theory*, 5 (1973), 58–63.

Goss, D.

1. v-adic zeta functions, L-series and measures for function fields. *Invent. math.*, **55** (1979), 107–116, 117–119.

Gras, G.

1. Remarques sur la conjecture de Leopoldt. *C. R. Acad. Sci. Paris, Sér. A-B*, **274** (1972), A377–A380.
2. Parité du nombre de classes et unités cyclotomiques. *Astérisque*, **24-25** (1975), 37–45.
3. Critère de parité du nombre de classes des extensions abéliennes réelles de $\mathbb{Q}$ de degré impair. *Bull. Soc. Math. France*, **103** (1975), 177–190.
4. Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés. *Ann. Inst. Fourier, Grenoble*, **27** (1977), fasc. 1, 1–66.
5. Etude d'invariants relatifs aux groupes des classes des corps abéliens. *Astérisque*, **41-42** (1977), 35–53.
6. Approche numérique de la structure du groupe des classes des extensions abéliennes de $\mathbb{Q}$. *Bull. Soc. Math. France*, Mém. no. 49–50 (1977), 101–107.
7. Nombre de ϕ-classes invariantes. Application aux classes des corps abéliens. *Bull. Soc. Math. France*, **106** (1978), no. 4, 337–364.
8. Sur l'annulation en 2 des classes relatives des corps abéliens. *C. R. Math. Rep. Acad. Sci. Canada* **1** (1978/1979), no. 2, 107–110. MR **80k**: 12017.
9. Sur la construction des fonctions L p-adiques abéliennes. Sém. Delange–Pisot–Poitou, Théorie des Nombres, 20e année, 1978/1979, Exp. no. 22, 20 pp.

10. Annulation du groupe des l-classes généralisées d'une extension abélienne réelle de degré premier à l. *Ann. Inst. Fourier, Grenoble*, **29** (1979), fasc. 1, 15–32.
11. Canonical divisibilities of values of p-adic L-functions (to appear).

Gras, G. and Gras, M.-N.

1. Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de $\mathbb{Q}$ de degré premier impair. *Ann. Inst. Fourier, Grenoble*, **25** (1975), fasc. 1, 1–22.
2. Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\mathbb{Q}$. *Bull. Sci. Math.* (2), **101** (1977), no. 2, 97–129.

Gras, M.-N.

1. (= M-N. Montouchet) Sur le nombre de classes de sous-corps cubique cyclique de $\mathbb{Q}^{(p)}$, $p \equiv 1 \bmod 3$, *Proc. Japan Acad.*, **47** (1971), 585–586.
2. Sur le nombre de classes du sous-corps cubique de $\mathbb{Q}^{(p)}$, $p \equiv 1$ (3). Sém. de Théorie des Nombres, Bordeaux, 1971–1972, Exp. no. 2 bis, 9 pp. MR **53**: 346.
3. Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$. *J. reine angew. Math.*, **277** (1975), 89–116.
4. Calcul de nombres de classes par dévissage des unités cyclotomiques. *Bull. Soc. Math. France*, Mém. no. 49–50 (1977), 109–112.
5. Classes et unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$. *Ann. Inst. Fourier, Grenoble*, **29** (1979), fasc. 1, 107–124.

Greenberg, M.

1. An elementary proof of the Kronecker–Weber theorem. *Amer. Math. Monthly*, **81** (1974), 601–607; correction, **82** (1975), 803.

Greenberg, R.

1. The Iwasawa invariants of Γ-extensions of a fixed number field. *Amer. J. Math.*, **95** (1973), 204–214 (see Monsky [2]).
2. On a certain l-adic representation. *Invent. math.*, **21** (1973), 117–124.
3. A generalization of Kummer's criterion. *Invent. math.*, **21** (1973), 247–254 (see Kudo [3]).
4. On p-adic L-functions and cyclotomic fields. *Nagoya Math. J.*, **56** (1975), 61–77; part II, **67** (1977), 139–158; part III, to appear.
5. On the Iwasawa invariants of totally real number fields. *Amer. J. Math.*, **98** (1976), 263–284.
6. A note on K_2 and the theory of $\mathbb{Z}_p$-extensions. *Amer. J. Math.*, **100** (1978), 1235–1245.
7. On 2-adic L-functions and cyclotomic invariants. *Math. Z.*, **159** (1978), 37–45.
8. On the structure of certain Galois groups. *Invent. math.*, **47** (1978), 85–99.
9. On the Jacobian variety of some algebraic curves. *Compositio Math.*, **42** (1981), 345–359.

Gross, B.

1. On the factorization of p-adic L-series. *Invent. math.*, **57** (1980), 83–95.
2. On the behavior of p-adic L-functions at $s = 0$. *J. Math. Soc. Japan* (to appear).

Gross, B. and Koblitz, N.

1. Gauss sums and the p-adic gamma function. *Ann. of Math.*, **109** (1979), 569–581.

Grossman, E.

1. Sums of roots of unity in cyclotomic fields. *J. Number Theory*, **9** (1977), 321–329.

Halin, V. and Jakovlev, A.

1. Universal norms in Γ-extensions (Russian). *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, **71** (1977), 251–255, 287. MR **57**: 12452.

Harris, M.

1. Systematic growth of Mordell–Weil groups of Abelian varieties in towers of number fields. *Invent. math.* **51** (1979), 123–141.

Hasse, H.

1. *Über die Klassenzahl abelscher Zahlkörper.* Akademie-Verlag: Berlin, 1952.
2. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper.* Physica-Verlag: Würzburg-Wien, 1965.
3. Eine Folgerung aus H.-W. Leopoldts Theorie der Geschlechter abelscher Zahlkörper. *Math. Nachr.*, **42** (1969), 261–262.
4. *Number Theory.* Grundlehren der math. Wiss., no. 229. Springer-Verlag: New York–Berlin–Heidelberg, 1980.

Hatada, K.

1. On the values at rational integers of the p-adic Dirichlet L-functions. *J. Math. Soc. Japan*, **31** (1979), 7–27.

Hayashi, H.

1. On Takagi's basis in prime cyclotomic fields. *Mem. Fac. Sci. Kyushu Univ. Ser. A.* **25** (1971), 265–270.

Henniart, G.

1. Lois de réciprocité explicites. Sém. de Théorie des Nombres, Paris 1979–1980 (Sém. Delange–Pisot–Poitou), 135–149. Birkhäuser: Boston–Basel–Stuttgart, 1981.

Herbrand, J.

1. Sur les classes des corps circulaires. *J. Math. Pures Appl.* (9), **11** (1932), 417–441.

Hilbert, D.

1. Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper. *Nachr. Ges. Wiss. Göttingen*, 1896, 29–39; *Gesammelte Abhandlungen*, vol. I, 53–62. Chelsea: New York, 1965.
2. Die Theorie der algebraischen Zahlkörper. *Jahresbericht Deutsch. Math.-Verein*, **4** (1897), 175–546; *Gesammelte Abhandlungen*, vol. I, 63–363. Chelsea: New York, 1965.

Hoffstein, J.

1. Some analytic bounds for zeta functions and class numbers. *Invent. math.*, **55** (1979), 37–47.

Horn, J.

1. Cyclotomic units and p-adic L-functions. Ph.D. Thesis, Stanford Univ., 1976 (see *Dissertation Abstracts International*, vol. 37B, no 10 (1977), 5129-B).

Iimura, K.

1. A note on the Stickelberger ideal of conductor level. *Arch. Math.* (*Basel*), **36** (1981), 45–52.

Inkeri, K.

1. On the second case of Fermat's Last Theorem. *Ann. Acad. Sci. Fenn., Ser. A*, **60** (1949), 32 pp.

Ireland, K. and Rosen, M.

1. *Elements of Number Theory. Including an Introduction to Equations Over Finite Fields.* Bogden and Quigley: Tarrytown-on-Hudson, N.Y., 1972; 2nd edition, revised and expanded, to appear with Springer-Verlag.

Ishida, M.

1. *The Genus Fields of Algebraic Number Fields.* Springer Lecture Notes in Mathematics, vol. 555 (1976).

Iwasawa, K.

1. On solvable extensions of algebraic number fields. *Ann. of Math.* (2), **58** (1953), 548–572.
2. On Galois groups of local fields. *Trans. Amer. Math. Soc.*, **80** (1955), 448–469.
3. A note on class numbers of algebraic number fields. *Abh. Math. Sem. Univ. Hamburg*, **20** (1956), 257–258.

4. A note on the group of units of an algebraic number field. *J. Math. Pures et Appl.*, **35** (1956), 189–192.
5. On some invariants of cyclotomic fields. *Amer. J. Math.*, **80** (1958), 773–783; erratum, **81** (1959), 280.
6. On Γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, **65** (1959), 183–226.
7. Sheaves for algebraic number fields. *Ann. of Math.* (2), **69** (1959), 408–413.
8. On some properties of Γ-finite modules. *Ann. of Math.* (2) **70** (1959), 291–312.
9. On the theory of cyclotomic fields. *Ann. of Math.* (2), **70** (1959), 530–561.
10. On local cyclotomic fields. *J. Math. Soc. Japan*, **12** (1960), 16–21.
11. A class number formula for cyclotomic fields. *Ann. of Math.* (2), **76** (1962), 171–179. (Equation (9) is inaccurate for the 2-component).
12. On a certain analogy between algebraic number fields and function fields (Japanese). Sûgaku **15** (1963), 65–67. MR **28**:5054; LeVeque R30-21.
13. On some modules in the theory of cyclotomic fields. *J. Math. Soc. Japan*, **16** (1964), 42–82.
14. Some results in the theory of cyclotomic fields. *Number Theory* (Proc. Sympos. Pure Math., vol. 8), 66–69. Amer. Math. Soc.: Providence, 1965.
15. Some modules in local cyclotomic fields. *Les Tendances Géom. en Algèbre et Théorie des Nombres*, 87–96. Editions du Centre Nat. de la Recherche Sci., Paris, 1966. MR **34**:4251; LeVeque S30-34.
16. A note on ideal class groups. *Nagoya Math. J.*, **27** (1966), 239–247.
17. On explicit formulas for the norm residue symbol. *J. Math. Soc. Japan*, **20** (1968), 151–165 (see Kudo [4]).
18. On p-adic L-functions. *Ann. of Math.* (2), **89** (1969), 198–205.
19. Analogies between number fields and function fields. *Some Recent Advances in the Basic Sciences*, vol. 2, 203–208. Belfer Grad. School of Science, Yeshiva Univ.: New York, 1969. MR **41**:172; LeVeque R02-58.
20. Skew-symmetric forms for number fields. *Number Theory* (Proc. Sympos. Pure Math., vol. 20; Stony Brook), 86. Amer. Math. Soc.: Providence, 1971.
21. On some infinite Abelian extensions of algebraic numbers fields. *Actes du Cong. Int. Math.* (Nice, 1970), Tome 1, 391–394. Gauthier-Villars: Paris, 1971.
22. On the μ-invariants of cyclotomic fields. *Acta Arith.*, **21** (1972), 99–101.
23. *Lectures on p-Adic L-functions.* Annals of Math. Studies no. 74. Princeton Univ. Press: Princeton, N.J., 1972.
24. On the μ-invariants of $\mathbb{Z}_l$-extensions. *Number theory, Algebraic Geometry and Commutative Algebra* (in honor of Y. Akizuki). Kinokuniya: Tokyo, 1973, 1–11.
25. On $\mathbb{Z}_l$-extensions of algebraic number fields. *Ann. of Math.* (2), **98** (1973), 246–326. MR **50**:2120.
26. A note on Jacobi sums. *Symposia Math.*, **15** (1975), 447–459.
27. A note on cyclotomic fields. *Invent. math.*, **36** (1976), 115–123.
28. Some remarks on Hecke characters. *Algebraic Number Theory* (Kyoto Int. Sympos., 1976), 99–108. Japanese Soc. Promotion Sci.: Tokyo, 1977.
29. Riemann–Hurwitz formula and p-adic Galois representations for number fields, *Tôhoku Math. J.*, **33** (1981), 263–288.

Iwasawa, K. and Sims, C.

1. Computation of invariants in the theory of cyclotomic fields. *J. Math. Soc. Japan*, **18** (1966), 86–96.

Jehne, W.

1. Bemerkung über die p-Klassengruppe des p^γ-ten Kreiskörpers. *Arch. Math.* (*Basel*), **10** (1959), 442–427.

Johnson, W.

1. On the vanishing of the Iwasawa invariant μ_p for $p < 8000$. *Math. Comp.*, **27** (1973), 387–396.

2. Irregular prime divisors of the Bernoulli numbers. *Math. Comp.*, **28** (1974), 653–657.
3. Irregular primes and cyclotomic invariants. *Math. Comp.*, **29** (1975), 113–120.
4. p-adic proofs of congruences for the Bernoulli numbers. *J. Number Theory*, **7** (1975), 251–265.

Katz, N.

1. p-adic L-functions via moduli of elliptic curves. *Algebraic Geometry* (Proc. Sympos. Pure Math., vol. 29; Arcata), 479–506. Amer. Math. Soc.: Providence, 1975.
2. The congruences of Clausen–von Staudt and Kummer for Bernoulli–Hurwitz numbers. *Math. Ann.*, **216** (1975), 1–4.
3. p-adic interpolation of real analytic Eisenstein series. *Ann. of Math.* (2), **104** (1976), 459–571. MR **58**:22071.
4. Formal groups and p-adic interpolation. *Astérisque*, **41-42** (1977), 55–65.
5. The Eisenstein measure and p-adic interpolation. *Amer. J. Math.*, **99** (1977), 238–311. MR **58**:5602.
6. p-adic L-functions for *CM* fields. *Invent. math.*, **49** (1978), 199–297.
7. Another look at p-adic L-functions for totally real fields. *Math. Ann.*, **255** (1981), 33–43.
8. p-adic L-functions, Serre–Tate local moduli, and ratios of solutions of differential equations. *Proc. Int. Cong. Math.: Helsinki*, 1978, 365–371.

Kawasaki, T.

1. On the class number of real quadratic fields, *Mem. Fac. Sci. Kyushu Univ. Ser. A*, **35** (1981), 159–171.

Kersey, D.

1. Modular units inside cyclotomic units. *Ann. of Math.* (2), **112** (1980), 361–380.

Kervaire, M. and Murthy, M.

1. On the projective class group of cyclic groups of prime power order. *Comment. Math. Helvet.*, **52** (1977), 415–452.

Kida, Y.

1. On cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields. *Tôhoku Math. J.* (2), **31** (1979), 91–96.
2. l-extensions of *CM*-fields and cyclotomic invariants. *J. Number Theory*, **12** (1980), 519–528.
3. Cyclotomic $\mathbb{Z}_2$-extensions of J-fields (to appear).

Kimura, N.

1. Kummersche Kongruenzen für die Verallgemeinerten Bernoullischen Zahlen. *J. Number Theory*, **11** (1979), 171–187.

Kiselev, A.

1. An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers (Russian). *Dokl. Akad. Nauk SSSR (N.S.)*, **61** (1948), 777–779. MR **10**:236; LeVeque R14–10.

Knuth, D. and Buckholtz, T.

1. Computation of Tangent, Euler, and Bernoulli Numbers. *Math. Comp.*, **21** (1967), 663–688.

Kobayashi, S.

1. Divisibilité du nombre de classes des corps abéliens réels. *J. reine angew. Math.*, **320** (1980), 142–149.

Koblitz, N.

1. *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics, no. 58. Springer-Verlag: New York–Berlin–Heidelberg, 1977.
2. Interpretation of the p-adic log gamma function and Euler constants using the Bernoulli measure. *Trans. Amer. Math. Soc.*, **242** (1978), 261–269.

3. A new proof of certain formulas for p-adic L-functions. *Duke Math. J.*, **46** (1979), 455–468.
4. *p-Adic Analysis: a Short Course on Recent Work*. London Math. Soc. Lecture Note Series, no. 46. Cambridge Univ. Press: Cambridge, 1980.

Kramer, K. and Candiotti, A.
1. On K_2 and $\mathbb{Z}_l$-extensions of number fields. *Amer. J. Math.*, **100** (1978), 177–196.

Kronecker, L.
1. Über die algebraisch auflösbaren Gleichungen. *Monatsber. K. Preuss. Akad. Wiss. Berlin*, 1853, 365–374. *Mathematische Werke*, vol. 4, 3–11. Chelsea: New York, 1968.

Kubert, D.
1. The universal ordinary distribution. *Bull. Soc. Math. France*, **107** (1979), 179–202.
2. The $\mathbb{Z}/2\mathbb{Z}$ cohomology of the universal ordinary distribution. *Bull. Soc. Math. France*, **107** (1979), 203–224.

Kubert, D. and Lang, S.
1. Distributions on toroidal groups. *Math. Zeit.*, **148** (1976), 33–51.
2. Iwasawa theory in the modular tower. *Math. Ann.*, **237** (1978), 97–104.
3. Stickelberger ideals. *Math. Ann.*, **237** (1978), 203–212.
4. The index of Stickelberger ideals of order 2 and cuspidal class numbers. *Math. Ann.*, **237** (1978), 213–232.
5. Modular units inside cyclotomic units. *Bull. Soc. Math. France*, **107** (1979), 161–178 (see Gillard [7] and Kersey [1]).
6. *Modular Units*. Springer-Verlag, New York–Heidelberg–Berlin, 1981.

Kubota, T. and Leopoldt, H. W.
1. Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-funktionen. *J. reine angew. Math.*, **214/215** (1964), 328–339.

Kudo, A.
1. On Iwasawa's explicit formula for the norm residue symbol. *Mem. Fac. Sci. Kyushu Univ. Ser. A*, **26** (1972), 139–148.
2. On a class number relation of imaginary abelian fields. *J. Math. Soc. Japan*, **27** (1975), 150–159.
3. On a generalization of a theorem of Kummer. *Mem. Fac. Sci. Kyushu Univ. Ser. A*, **29** (1975), 255–261.
4. Generalized Bernoulli numbers and the basic $\mathbb{Z}_p$-extensions of imaginary quadratic number fields. *Mem. Fac. Sci. Kyushu Univ. Ser. A*, **32** (1978), 191–198.

Kühnová, J.
1. Maillet's Determinant D_{p^n+1}. *Arch. Math. (Brno)*, **15** (1979), 209–212.

Kuipers, L. and Niederreiter, H.
1. *Uniform Distribution of Sequences*. Wiley-Interscience: New York, 1974.

Kummer, E.
1. Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren. *J. reine angew. Math.*, **35** (1847), 327–367. *Collected Papers*, I, 211–251.
2. Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ. *Monatsber. Akad. Wiss. Berlin*, 1847, 132–139. *Collected Papers*, I, 274–281.
3. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *J. reine angew. Math.*, **44** (1852), 93–146. *Collected Papers*, I, 485–538.
4. Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers. *J. Math. Pures et Appl.*, **16** (1851), 377–498. *Collected Papers*, vol. I, 363–484.
5. *Collected Papers* (ed. by A. Weil). Springer-Verlag: New York–Berlin–Heidelberg, 1975.

Kurčanov, P.

1. Elliptic curves of infinite rank over Γ-extensions. *Mat. Sbornik* **90** (132) (1973), 320–324; English trans.: *Math. USSR Sb.*, **19** (1973), 320–324.
2. The rank of elliptic curves over Γ-extensions. *Mat. Sbornik*, **93** (135) (1974), 460–466; English trans.: *Math. USSR Sb.*, **22** (1974), 465–472.

Kuroda, S.-N.

1. Über den allgemeinen Spiegelungsatz für Galoissche Zahlkörper. *J. Number Theory*, **2** (1970), 282–297.
2. Kapitulation von Idealklassen in einer Γ-Erweiterung. Sem. on Modern Methods in Number Theory. Inst. of Statistical Math.: Tokyo, 1971, 4 pp. MR **51**: 12782 (see Kuroda [1]).

Kuz'min, L.

1. The Tate module of algebraic number fields. *Izv. Akad. Nauk SSSR, Ser. Mat.*, **36** (1972), 267–327; English trans.: *Math. USSR-Izv.* **6** (1972), 263–321.
2. Cohomological dimension of some Galois groups. *Izv. Akad. Nauk SSSR, Ser. Mat.*, **39** (1975), 487–495; English trans.: *Math. USSR-Izv.*, **9** (1975), 455–463.
3. Some duality theorems for cyclotomic Γ-extensions over algebraic number fields of *CM*-type. *Izv. Akad. Nauk SSSR, Ser. Mat.*, **43** (1979), 483–546; English trans.: *Math. USSR-Izv.*, **14** (1980), 441–498.

Lang, S.

1. *Algebraic Number Theory.* Addison-Wesley: Reading, MA, 1970.
2. Classes d'idéaux et classes de diviseurs. Sém. Delange–Pisot–Poitou, Théorie des Nombres, 18e année, 1976/1977, fasc. 2, Exp. no. 28, 9 pp.
3. Sur la conjecture de Birch–Swinnerton-Dyer (d'après J. Coates et A. Wiles). Sém. Bourbaki, 1976/1977, Exp. no. 503. Springer Lecture Notes in Mathematics, vol. 677 (1978), 189–200.
4. *Cyclotomic Fields.* Graduate Texts in Mathematics, Springer-Verlag: New York, 1978.
5. *Cyclotomic Fields, II.* Graduate Texts in Mathematics, Springer-Verlag: New York, 1980.
6. *Algebra.* Addison-Wesley: Reading, MA, 1965.
7. *Complex Analysis.* Addison-Wesley: Reading, MA, 1977.
8. Units and class numbers in number theory and algebraic geometry, *Bull. Amer. Math. Soc.* (to appear).

Lang, S.-D.

1. Note on the class number of the maximal real subfield of a cyclotomic field. *J. reine angew. Math.*, **290** (1977), 70–72.

Lehmer, D. H.

1. Applications of digital computers. *Automation and Pure Mathematics*, 219–231. Ginn: Boston, 1963.
2. Harry Schultz Vandiver, 1882–1973. *Bull. Amer. Math. Soc.*, **80** (1974), 817–818.
3. Prime factors of cyclotomic class numbers. *Math. Comp.*, **31** (1977), 599–607.
4. On Fermat's quotient, base two. *Math. Comp.*, **36** (1981), 289–290.

Lehmer, D. H., Lehmer, E., and Vandiver, H.

1. An application of high-speed computing to Fermat's Last Theorem. *Proc. Nat. Acad. Sci., USA*, **40** (1954), 25–33.

Lehmer, D. H. and Masley, J.

1. Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$. *Math. Comp.*, **32** (1978), 577–582, microfiche suppl.

Lenstra, H. W.

1. Euclid's algorithm in cyclotomic fields. *J. London Math. Soc.*, **10** (1975), 457–465.
2. Euclidean number fields of large degree. *Invent. math.*, **38** (1977), 237–254.

3. Quelques exemples d'anneaux euclidiens. *C. R. Acad. Sci., Sér. A*, **286** (1978), A683–A685.
4. Euclidean number fields. *Math. Intelligencer 2*, no. 1 (1979), 6–15; no. 2 (1980), 73–77, 99–103.
5. Vanishing sums of roots of unity. Proc. Bicentennial Cong. Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978), Part II, 249–268, Math. Centre Tracts, 101, Math. Centrum, Amsterdam, 1979. MR **81c**: 10044.
6. Rational functions invariant under a cyclic group. Proc. of the Queen's Number Theory Conf., 1979 (Kingston, Ontario; ed. by P. Ribenboim). *Queen's Papers in Pure and Applied Math.*, no. 54 (1980), 91–99.
7. Test rapide de primalité d'Adleman. Sém. Bourbaki, Juin 1981.

Leopodt, H. W.

1. Zur Geschlechtertheorie in abelschen Zahlkörpern. *Math. Nachr.*, **9** (1953), 351–362.
2. Über Einheitengruppe und Klassenzahl reeller Zahlkörper. *Abh. Deutsch. Akad. Wiss. Berlin, Kl. Math. Nat. 1953*, no. 2, 48 pp. (1954).
3. Eine Verallgemeinerung der Bernoullischen Zahlen. *Abh. Math. Sem. Univ. Hamburg*, **22** (1958), 131–140.
4. Zur Struktur der l-Klassengruppe galoisscher Zahlkörper. *J. reine angew. Math.*, **199** (1958), 165–174. MR **20**: 3116 ; LeVeque R26–12.
5. Über Klassenzahlprimteiler reeller abelscher Zahlkörper als Primteiler verallgemeinerter Bernoullischer Zahlen. *Abh. Math. Sem. Univ. Hamburg*, **23** (1959), 36–47.
6. Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers. *J. reine angew. Math.*, **201** (1959), 119–149.
7. Über Fermatquotienten von Kreiseinheiten und Klassenzahlformeln modulo p. *Rend. Circ. Mat. Palermo* (2), **9** (1960), 39–50.
8. Zur Approximation des p-adischen Logarithmus. *Abh. Math. Sem. Univ. Hamburg*, **25** (1961), 77–81.
9. Zur Arithmetik in abelschen Zahlkörpern, *J. reine angew. Math.*, **209** (1962), 54–71.
10. Eine p-adische Theorie der Zetawerte. II. Die p-adische Γ-Transformation. *J. reine angew. Math.*, **274/275** (1975), 224–239.

Lepistö, T.

1. On the growth of the first factor of the class number of the prime cyclotomic field. *Ann. Acad. Sci. Fenn., Ser. AI*, No. 577 (1974), 21 pp.

Liang, J.

1. On the integral basis of the maximal real subfield of a cyclotomic field. *J. reine angew. Math.*, **286/287** (1976), 223–226.

Liang, J. and Toro, E.

1. On the periods of the cyclotomic field. *Abh. Math. Sem. Univ. Hamburg*, **50** (1980), 127–134.

Lichtenbaum, S.

1. On the values of zeta and L-functions, I. *Ann. of Math.* (2), **96** (1972), 338–360.
2. Values of zeta-functions, étale cohomology, and algebraic K-theory. *Algebraic K-theory II*, 489–501. Springer Lecture Notes in Mathematics, vol. 342 (1973) (see Borel [1]).
3. Values of zeta and L-functions at zero. *Astérisque*, **24-25** (1975), 133–138.
4. On p-adic L-functions associated to elliptic curves. *Invent. math.*, **56** (1980), 19–55.

Linden, F. van der

1. Class number computations of real abelian number fields. Preprint. Univ. of Amsterdam, 1980.

Long, R.

1. *Algebraic Number Theory.* Marcel Dekker: New York, 1977.

Loxton, J.

1. On a cyclotomic diophantine equation. *J. reine angew. Math.*, **270** (1974), 164–168.

Lubin, J. and Rosen, M.

1. The norm map for ordinary abelian varieties, *J. Algebra*, **52** (1978), 236–240.

Mahler, K.

1. *Introduction to p-Adic Numbers and Their Functions.* Cambridge Tracts in Maths. 64. Cambridge Univ. Press: Cambridge: 1973.

Mäki, S.

1. *The Determination of Units in Real Cyclic Sextic Fields.* Springer Lecture Notes in Mathematics, vol. 797 (1980).

Manin, J.

1. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, **26** (1971), 7–71; English trans.: *Russian Math. Surveys*, **26** (1971), 7–78.
2. Periods of cusp forms, and p-adic Hecke series. *Mat. Sbornik* (*N.S.*) **92** (134) (1973), 378–401; English trans.: *Math. USSR-Sb.*, **21** (1973), 371–393.
3. Values of p-adic Hecke series at lattice points of the critical strip. *Mat. Sbornik* (*N.S.*), **93** (135) (1974), 621–626; English trans.: *Math. USSR-Sb.*, **22** (1974), 631–637.
4. Non-archimedean integration and Jacquet–Langlands p-adic L-functions. *Uspehi Mat. Nauk*, **31** (1976), 5–54: English trans.: *Russian Math. Surveys*, **31** (1976), 5–57.
5. Modular forms and number theory. Proc. Int. Cong. Math.: Helsinki, 1978, 177–186.

Manin, J. and Višik, M.

1. p-adic Hecke series of imaginary quadratic fields. *Mat. Sbornik* (*N.S.*), **95** (137) (1974), 357–383; English trans.: *Math. USSR-Sb.*, **24** (1974), 345–371.

Marcus, D.

1. *Number Fields.* Springer-Verlag: New York, 1977.

Martinet, J.

1. Tours de corps de classes et estimations de discriminants. *Invent. math.*, **44** (1978), 65–73.
2. Petits discriminants. *Ann. Inst. Fourier, Grenoble*, **29** (1979), fasc. 1, 159–170.

Masley, J.

1. On the class number of cyclotomic fields. Ph.D. Thesis, Princeton Univ., 1972.
2. Solution of the class number two problem for cyclotomic fields. *Invent. math.*, **28** (1975), 243–244.
3. On Euclidean rings of integers in cyclotomic fields. *J. reine angew. Math.*, **272** (1975), 45–48.
4. Odyzko bounds and class number problems. *Algebraic Number Fields* (Durham Symposium, 1975; ed. by A. Fröhlich), 465–474. Academic Press: London, 1977.
5. Solution of small class number problems for cyclotomic fields. *Compositio Math.*, **33** (1976), 179–186.
6. On the first factor of the class number of prime cyclotomic fields. *J. Number Theory*, **10** (1978), 273–290.
7. Class numbers of real cyclic number fields with small conductor. *Compositio Math.*, **37** (1978), 297–319.
8. Where are number fields with small class number? *Number Theory Carbondale 1979* (ed. by M. Nathanson). Springer Lecture Notes in Mathematics, vol. 751 (1979), 221–242.
9. Class groups of abelian number fields. Proc. Queen's Number Theory Conf., 1979 (Kingston, Ontario; ed. by P. Ribenboim). *Queen's Papers in Pure and Applied Math.*, no. 54 (1980), 475–497.

Masley, J. and Montgomery, H.

1. Cyclotomic fields with unique factorization. *J. reine angew. Math.*, **286/287** (1976), 248–256.

Mazur, B.

1. Rational points of abelian varieties with values in towers of number fields. *Invent. math.*, **18** (1972), 183–266.
2. Review of E. E. Kummer's *Collected Papers. Bull. Amer. Math. Soc.*, **83** (1977), 976–988.
3. On the arithmetic of special values of L-functions. *Invent. math.*, **55** (1979), 207–240.

Mazur, B. and Swinnerton-Dyer, H.

1. Arithmetic of Weil curves. *Invent. math.*, **18** (1972), 183–266.

Mazur, B. and Wiles, A.

1. Class fields of abelian extensions of $\mathbb{Q}$. Preprint.

McCarthy, P.

1. *Algebraic Extensions of Fields.* Blaisdell; Ginn: Boston, 1966.

McCulloh, L.

1. A Stickelberger condition on Galois module structure for Kummer extensions of prime degree. *Algebraic Number Fields* (Durham Symposium, 1975; ed. by A. Fröhlich), 561–588. Academic Press: London, 1977.
2. A class number formula for elementary-abelian-group rings. *J. Algebra*, **68** (1981), 443–452.

Metsänkylä, T.

1. Über den ersten Faktor der Klassenzahl des Kreiskörpers. *Ann. Acad. Sci. Fenn., Ser. AI*, No. 416 (1967), 48 pp.
2. Über die Teilbarkeit des ersten Faktors der Klassenzahl des Kreiskörpers. *Ann. Univ. Turku., Ser. AI*, No. 124 (1968), 6 pp.
3. On prime factors of the relative class numbers of cyclotomic fields. *Ann. Univ. Turku., Ser. AI*, No. 149 (1971), 8 pp.
4. On the growth of the first factor of the cyclotomic class number. *Ann. Univ. Turku., Ser. AI*, No. 155 (1972), 12 pp.
5. A class number congruence for cyclotomic fields and their subfields. *Acta Arith.*, **23** (1973), 107–116.
6. Class numbers and μ-invariants of cyclotomic fields. *Proc. Amer. Math. Soc.*, **43** (1974), 299–300.
7. On the Iwasawa invariants of imaginary abelian fields. *Ann. Acad. Sci. Fenn., Ser. AI, Math.*, **1** (1975), no. 2, 343–353.
8. On the cyclotomic invariants of Iwasawa. *Math. Scand.*, **37** (1975), 61–75.
9. Distribution of irregular prime numbers. *J. reine angew. Math.*, **282** (1976), 126–130.
10. Iwasawa invariants and Kummer congruences. *J. Number Theory*, **10** (1978), 510–522.
11. Note on certain congruences for generalized Bernoulli numbers. *Arch. Math. (Basel)*, **30** (1978), 595–598.
12. An upper bound for the λ-invariant of imaginary abelian fields (to appear).

Miki, H.

1. On $\mathbb{Z}_p$-extensions of complete p-adic power series fields and function fields. *J. Fac. Sci. Univ. Tokyo, Sec. IA*, **21** (1974), 377–393.
2. On unramified abelian extensions of a complete field under a discrete valuation with arbitrary residue field of characteristic $p \neq 0$ and its application to wildly ramified $\mathbb{Z}_p$-extensions. *J. Math. Soc. Japan*, **29** (1977), 363–371.
3. A relation between Bernoulli numbers. *J. Number Theory*, **10** (1978), 297–302.

4. On the maximal abelian l-extension of a finite algebraic number field with given ramification. *Nagoya Math. J.*, **70** (1978), 183–202.

Milgram, R. J.

1. Odd index subgroups of units in cyclotomic fields and applications. *Algebraic K-theory, Evanston 1980*, Springer Lecture Notes in Mathematics, vol. 854 (1981), 269–298.

Milnor, J.

1. *Introduction to Algebraic K-Theory*. Ann. of Math. Studies, no. 72. Princeton Univ. Press: Princeton, 1971.

Monsky, P.

1. On p-adic power series. *Math. Ann.*, **255** (1981), 217–227.
2. Some invariants of $\mathbb{Z}_p^d$-extensions. *Math. Ann.*, **255** (1981), 229–233.

Morita, Y.

1. A p-adic analogue of the Γ-function. *J. Fac. Sci. Univ. Tokyo, Sec. IA*, **22** (1975), 255–266.
2. On the Hurwitz–Lerch L-functions. *J. Fac. Sci. Univ. Tokyo, Sec. IA*, **24** (1977), 29–43.
3. A p-adic integral representation of the p-adic L-function. *J. reine angew. Math.*, **302** (1978), 71–95.
4. On the radius of convergence of the p-adic L-function. *Nagoya Math. J.*, **75** (1979), 177–193.
5. The integral forms of p-adic L-functions (Japanese). Research on microlocal analysis. Proc. Symp. RIMS, Kyoto 1977, 30–37. Zentralblatt **436**: 12015.
6. Examples of p-adic arithmetic functions, *Algebraic Number Theory* (Kyoto conference, 1976; ed. by Iyanaga), Jap. Soc. Promotion Sci.: Tokyo, 1977, 143–148.

Moser, C.

1. Représentation de -1 comme somme de carrées dans un corps cyclotomique quelconque. *J. Number Theory*, **5** (1973), 139–141.
2. Nombre de classes d'une extension cyclique réelle de $\mathbb{Q}$, de degré 4 ou 6 et de conducteur premier (to appear).

Moser, C. and Payan, J.

1. Majoration du nombre de classes d'un corps cubique cyclique de conducteur premier (to appear).

Nakazato, H.

1. A remark on Ribet's theorem. *Proc. Japan Acad., Ser. A, Math. Sci.*, **56** (1980), no. 4, 192–195.

Narkiewicz, W.

1. *Elementary and Analytic Theory of Algebraic Numbers*. Monografie Matematyczne, No. 57. Polish Scientific Publishers (PWN): Warsaw, 1974.

Neukirch, J.

1. *Klassenkörpertheorie*. Bibliographisches Institut: Mannheim–Wien–Zurich, 1969.

Neumann, O.

1. Two proofs of the Kronecker–Weber theorem "according to Kronecker, and Weber," *J. reine angew. Math.*, **323** (1981), 105–126.

Newman, M.

1. A table of the first factor for prime cyclotomic fields. *Math. Comp.*, **24** (1970), 215–219.
2. Units in cyclotomic number fields. *J. reine angew. Math.*, **250** (1972), 3–11 (see Loxton [1], Ennola [3]).
3. Diophantine equations in cyclotomic fields. *J. reine angew. Math.*, **265** (1974), 84–89.

Nielsen, N.

1. *Traite Elémentaire des Nombres de Bernoulli.* Gauthier-Villars: Paris, 1923.

Northcott, D.

1. *Finite Free Resolutions.* Cambridge Tracts in Maths., no. 71, Cambridge Univ. Press: Cambridge, 1976.

Odlyzko, A.

1. Some analytic estimates of class numbers and discriminants. *Invent. math.*, **29** (1975), 275–286.
2. Lower bounds for discriminants of number fields. *Acta Arith.*, **29** (1976), 275–297.
3. Lower bounds for discriminants of number fields, II. *Tôhoku Math. J.*, **29** (1977), 209–216.
4. On conductors and discriminants. *Algebraic Number Fields* (Durham Symposium, 1975; ed. by A. Fröhlich), 377–407. Academic Press: London, 1977.

Oesterlé, J.

1. Travaux de Ferrero et Washington sur le nombre de classes d'idéaux des corps cyclotomiques. Sém. Bourbaki, 1978/1979, Exp. no. 535. Springer Lecture Notes in Mathematics, vol. 770 (1980), 170–182.
2. Une nouvelle formulation de la conjecture d'Iwasawa. Sém. Delange–Pisot–Poitou, Théorie des Nombres, 1980/1981 (to appear with Birkhäuser).

Ojala, T.

1. Euclid's algorithm in the cyclotomic field $\mathbb{Q}(\zeta_{16})$. *Math. Comp.*, **31** (1977), 268–273.

Oriat, B.

1. Relations entre les 2-groupes des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$. *Ann. Inst. Fourier, Grenoble*, **27** (1977), fasc. 2, 37–59.
2. Généralisation du "Spiegelungsatz." *Astérisque*, 61 (1979), 169–175.
3. Annulation de groupes de classes réelles. *Nagoya Math. J.*, **81** (1981), 45–56.

Oriat, B. and Satgé, Ph.

1. Un essai de généralisation du "Spiegelungsatz." *J. reine angew. Math.*, **307/308** (1979), 134–159.

Osipov, Ju.

1. p-adic zeta functions (Russian). *Uspehi Mat. Nauk*, **34** (1979), 209–210; English trans.: *Russian Math. Surveys*, **34** (1979), 213–214.
2. p-adic zeta functions and Bernoulli numbers (Russian). *Studies in Number Theory 6, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.* (*LOMI*), **93** (1980), 192–203.

Pajunen, S.

1. Computations on the growth of the first factor for prime cyclotomic fields. *Nordisk. Tidskr. Informationsbehandling* (*BIT*), **16** (1976), no. 1, 85–87; **17** (1977), no. 1, 113–114. MR **53**:5533, MR **55**:10425.

Pei, Ding Yi and Feng, Ke Qin

1. A note on the independence of units of cyclotomic fields (Chinese). *Acta Math. Sinica*, **23** (1980), no. 5, 773–778.

Plymen, R.

1. Cyclotomic integers and the inner invariant of Connes. *J. London Math. Soc.*, (2), **22** (1980), 14–20.

Poitou, G.

1. Sur les petits discriminants. Sém. Delange–Pisot–Poitou, Théorie des Nombres, 18e année, 1976/1977. Exp. no. 6, 17 pp.
2. Minorations de discriminants (d'après A. M. Odlyzko). Sém. Bourbaki, 1975/1976. Exp. no. 479. Springer Lecture Notes in Mathematics, vol. 567 (1977), 136–153.

Pollaczek, F.

1. Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswürzeln. *Math. Zeit.*, **21** (1924), 1–38.

Queen, C.

1. The existence of p-adic abelian L-functions. *Number Theory and Algebra*, 263–288. Academic Press: New York, 1977.

Ramachandra, K.

1. On the units of cyclotomic fields. *Acta Arith.*, **12** (1966), 165–173.

Ribenboim, P.

1. *13 Lectures on Fermat's Last Theorem*, Springer-Verlag: New York, 1979.
2. *Algebraic Numbers*. Wiley-Interscience: New York, 1972.

Ribet, K.

1. p-adic interpolation via Hilbert modular forms. *Algebraic Geometry* (Proc. Sympos. Pure Math., vol. 29; Arcata), 581–592. Amer. Math. Soc.: Providence, 1975.
2. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Invent. math.*, **34** (1976), 151–162.
3. Sur la recherche des p-extensions non-ramifiées de $\mathbb{Q}(\mu_p)$. Groupe d'Etude d'Algèbre (Marie-Paule Malliavin), 1re année, 1975/1976, Exp. no. 2, 3 pp. MR **80f**: 12005.
4. p-adic L-functions attached to characters of p-power order. Sém. Delange–Pisot–Poitou, Théorie des Nombres, 19e année, 1977/1978, Exp. no. 9, 8 pp.
5. *Fonctions L p-adiques et théorie d'Iwasawa*. Cours rédigé par Ph. Satgé. Publ. Math.: Orsay, 1979.
6. Report on p-adic L-functions over totally real fields. *Astérisque*, **61** (1979), 177–192.

Rideout, D.

1. On a generalization of a theorem of Stickelberger, Ph.D. Thesis, McGill Univ., 1970 (see *Dissertation Abstracts International*, vol. 32B, No. 1 (1971) 438-B).

Robert, G.

1. Unités elliptiques. *Bull. Soc. Math. France*, Mém. **36** (1973), 77 pp.
2. Nombres de Hurwitz et regularité des idéaux premiers. Sém. Delange–Pisot–Poitou, Théorie des Nombres, 16e année, 1974/1975, Exp. no. 21, 7 pp.
3. Nombres de Hurwitz et unités elliptiques. *Ann. Scient. Ec. Norm. Sup.*, **11** (1978), 297–389.

Rosen, M.

1. The asymptotic behavior of the class group of a function field over a finite field, *Arch. Math. (Basel)*, **24** (1973), 287–296.
2. An elementary proof of the local Kronecker–Weber theorem, *Trans. Amer. Math. Soc.*, **265** (1981), 599–605.

Rubin, K.

1. On the arithmetic of CM elliptic curves in $\mathbb{Z}_p$-extensions, Ph.D. thesis, Harvard Univ., 1981.

Sarkisjan, Ju.

1. Profinitely generated Γ-modules (Russian). *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, **86** (1979), 157–161. Translation: *J. Soviet Math.*, **17** (1981), No. 4, 2058–2061.

Sarkisjan, Ju. and Jakovlev, A.

1. Homological determination of Γ-modules (Russian). *Zop. Naučn, Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, **64** (1976), 104–126. Translation: *J. Soviet Math.*, **17** (1981), No. 2, 1783–1801.

Schaffstein, K.

1. Tafel der Klassenzahlen der reellen quadratischen Zahlkörper mit Primzahldiskriminante unter 12000 und zwischen 100000–101000 und 1000000–1001000. *Math. Ann.*, **98** (1928), 745–748.

Schertz, R.

1. Über die analytische Klassenzahlformel für reelle abelsche Zahlkörper. *J. reine angew. Math.*, **307/308** (1979), 424–430.

Schmidt, C.-G.

1. Die Relationen von Gausschen Summen und Kreiseinheiten. *Arch. Math.* (*Basel*), **31** (1978/1979), 457–463.
2. Grössencharaktere und Relativklassenzahl abelscher Zahlkörper. *J. Number Theory*, **11** (1979), 128–159.
3. Über die Führer von Gausschen Summen als Grössencharaktere. *J. Number Theory*, **12** (1980), 283–310.
4. Die Relationenfaktorgruppen von Stickelberger–Elementen und Kreiszahlen. *J. reine angew. Math.*, **315** (1980), 60–72.
5. Gauss sums and the classical Γ-function. *Bull. London Math. Soc.*, **12** (1980), 344–346.

Schmidt, H.

1. Zur Theorie und Anwendung Bernoulli–Nörlundscher Polynome und gewissen Verallgemeinerungen der Bernoullischen und der Stirlingschen Zahlen. *Arch. Math.* (*Basel*), **33** (1979/1980), 364–374.

Schneider, P.

1. Über die Werte der Riemannschen Zetafunktion an den ganzzahligen Stellen. *J. reine angew. Math.*, **313** (1980), 189–194.

Scholz, A.

1. Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. *J. reine angew. Math.*, **166** (1932), 201–203.

Schrutka von Rechtenstamm, G.

1. Tabelle der (Relativ)-Klassenzahlen der Kreiskörper, deren ϕ-Funktion des Wurzelexponenten (Grad) nicht grösser als 256 ist. *Abh. Deutschen Akad. Wiss. Berlin, Kl. Math. Phys.*, no. 2 (1964), 1–64.

Sen, S.

1. On explicit reciprocity laws. *J. reine angew. Math.*, **313** (1980), 1–26; **323** (1981), 68–87.

Serre, J.-P.

1. Classes des corps cyclotomiques (d'après K. Iwasawa). Sém. Bourbaki, 1958, Exp. no. 174, 11 pp.
2. Formes modulaires et fonctions zêta p-adiques. *Modular functions of one variable, III* (Antwerp 1972), 191–268. Springer Lecture Notes in Mathematics, Vol. 350 (1973); correction: *Modular functions, IV*. 149–150, Springer Lecture Notes in Mathematics, Vol. 476 (1975).
3. Sur le résidu de la fonction zêta p-adique d'un corps de nombres. *C. R. Acad. Sci. Paris, Sér. A*, **287** (1978), A183–A188.

Shafarevich, I.

1. A new proof of the Kronecker-Weber theorem (Russian). *Trudy Mat. Inst. Steklov*, **38** (1951), 382–387 (see Narkiewicz [1]).

Shanks, D.

1. The simplest cubic fields. *Math. Comp.*, **28** (1974), 1137–1152.

Shatz, S.

1. *Profinite Groups, Arithmetic, and Geometry*. Ann. of Math. Studies, no. 67. Princeton Univ. Press: Princeton, 1972.

Shimura, G.

1. *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten and Princeton Univ. Press: Princeton, 1971.

Shintani, T.

1. 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.

Shirai, S.

1. On the central ideal class group of cyclotomic fields. *Nagoya Math. J.*, **75** (1979), 133–143.

Shiratani, K.

1. A generalization of Vandiver's congruence. *Mem. Fac. Sci. Kyushu Univ., Ser. A*, **25** (1971), 144–151.
2. Kummer's congruence for generalized Bernoulli numbers and its application. *Mem. Fac. Sci. Kyushu Univ., Ser. A*, **26** (1972), 119–138.
3. On certain values of p-adic L-functions. *Mem. Fac. Sci. Kyushu Univ., Ser. A*, **28** (1974), 59–82.
4. On a kind of p-adic zeta functions. *Algebraic Number Theory* (Kyoto conference, 1976; ed. by Iyanaga), Jap. Soc. Promotion Sci.: Tokyo, 1977, 213–217.
5. On a formula for p-adic L-functions. *J. Fac. Sci. Univ. Tokyo, Sec. IA*, **24** (1977), 45–53.

Siegel, C.

1. Zu zwei Bermerkungen Kummers. *Nachr. Akad. Wiss. Göttingen, Math.-phys. Kl.* (1964), no. 6, 51–57; *Gesammelte Abhandlungen*. Springer-Verlag: Berlin, 1966, vol. III, 436–442.

Sinnott, W.

1. On the Stickelberger ideal and the circular units of a cyclotomic field. *Ann. of Math.* (2), **108** (1978), 107–134.
2. On the Stickelberger ideal and the circular units of an abelian field. *Invent. math.*, **62** (1980), 181–234.
3. On the Stickelberger ideal and the circular units of an abelian field. *Sém. de Théorie des Nombres, Paris 1979–1980*(Sém. Delange–Pisot–Poitou), 277–286. Birkhäuser: Boston–Basel–Stuttgart, 1981.

Skula, L.

1. Non-possibility to prove infinity of regular primes from some theorems. *J. reine angew. Math.*, **291** (1977), 162–181.
2. On certain ideals of the group ring $\mathbb{Z}[G]$. *Arch. Math. (Brno)*, **15** (1979), no. 1, 53–66.
3. Index of irregularity of a prime. *J. reine angew. Math.*, 315 (1980), 92–106.
4. Another proof of Iwasawa's class number formula (to appear).

Slavutskiĭ, I.

1. Local properties of Bernoulli numbers and a generalization of the Kummer–Vandiver theorem (Russian). *Izv. Vysš. Učebn. Zaved. Matematika*, 1972, no. 3 (118), 61–69. MR **46**:151.
2. Generalized Bernoulli numbers that belong to unequal characters, and an extension of Vandiver's theorem (Russian). *Leningrad Gos. Ped. Inst. Učen. Zap.*, **496** (1972), čast' 1, 61–68. MR **46**:7194.

Snyder, C.

1. A concept of Bernoulli numbers in algebraic function fields. *J. reine angew. Math.*, **307/308** (1979), 295–308.
2. A concept of Bernoulli numbers in algebraic function fields (II), *Manuscripta Math.*, **35** (1981), 69–89.

Soulé, C.

1. On higher p-adic regulators, *Alg. K-theory, Evanston 1980*, Springer Lecture Notes in Mathematics, vol. 854 (1981), 372–401.

Speiser, A.

1. Zerlegungsgruppe. *J. reine angew. Math.*, **149** (1919), 174–188.

Stepanov, S.

1. Proof of the Davenport–Hasse relations. *Mat. Zametki*, **27** (1980), 3–6; English trans.: *Math. Notes Acad. Sci. USSR*, **27** (1980), 3–4.

Stichtenoth, H.

1. Zur Divisorklassengruppe eines Kongruenzfunktionenkörpers. *Arch. Math.* (*Basel*), **32** (1979), 336–340.

Stickelberger, L.

1. Über eine Verallgemeinerung der Kreistheilung. *Math. Ann.*, **37** (1890), 321–367.

Sunseri, R.

1. Zeros of p-adic L-functions and densities relating to Bernoulli numbers. Ph.D. Thesis, Univ. of Illinois, 1979.

Sze, A.

1. On the values of L-functions at negative integers, Ph.D. thesis, Cornell Univ., 1976 (see *Dissertation Abstracts International*, vol. 37B, No. 10 (1977), 5141-B).

Takeuchi, H.

1. On the class number of the maximal real subfield of a cyclotomic field, *Canad. J. Math.*, **33** (1981), 55–58.

Tate, J.

1. Letter from Tate to Iwasawa on a relation between K_2 and Galois cohomology. *Algebraic K-theory II* (Seattle 1972), 524–527. Springer Lecture Notes in Mathematics, Vol. 342 (1973).
2. Relations between K_2 and Galois cohomology. *Invent. math.*, **36** (1976), 257–274.
3. Problem 9: The general reciprocity law. *Mathematical Developments Arising from Hilbert Problems* (Proc. Sympos. Pure Math., vol. 28), 311–322. Amer. Math. Soc.: Providence, 1976.
4. *Sur la conjecture de Stark.* Cours redigé par D. Bernardi et N. Schappacher (to appear with Birkhäuser: Boston–Basel–Stuttgart).

Topunov, V.

1. A connection of cyclotomic fields with the ring of cyclic matrices of prime and of primary order (Russian). *Moskov. Gos. Ped. Inst. Učen. Zap.*, No. 375 (1971), 215–223. MR **48**:2110.

Uchida, K.

1. Class numbers of imaginary abelian number fields. *Tôhoku Math. J.* (2), **23** (1971), 97–104, 335–348, 573–580.
2. Imaginary abelian number fields with class number one. *Tôhoku Math. J.* (2), **24** (1972), 487–499.
3. On a cubic cyclic field with discriminant 163^2. *J. Number Theory*, **8** (1976), 346–349 (see Shanks [1]).
4. Class numbers of cubic cyclic fields. *J. Math. Soc. Japan*, **26** (1974), 447–453.

Uehara, T.

1. Vandiver's congruence for the relative class number of an imaginary abelian field. *Mem. Fac. Kyushu Univ., Ser. A*, **29** (1975), 249–254.
2. Fermat's Conjecture and Bernoulli numbers. *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, No. 6 (1978), 9–14. MR **80a**:12008.

Ullom, S.

1. Class groups of cyclotomic fields and group rings. *J. London Math. Soc.* (2), **17** (1978), 231–239.
2. Upper bounds for p-divisibility of sets of Bernoulli numbers. *J. Number Theory*, **12** (1980), 197–200.

Vandiver, H.

1. Fermat's Last Theorem: Its history and the nature of the known results concerning it. *Amer. Math. Monthly*, **53** (1946), 555–578; **60** (1953), 164–167.

Višik, M.

1. Non-archimedean measures connected with Dirichlet series. *Mat. Sbornik* (*N.S.*), **99** (141) (1976), 248-260. English trans.: *Math. USSR-Sb.*, **28** (1976), 216-228.
2. The p-adic zeta function of an imaginary quadratic field and the Leopoldt regulator. *Mat. Sbornik* (*N.S.*), **102** (144) (1977), 173-181; English trans.: *Math. USSR-Sb.*, **31** (1977), 151-158 (1978).

Volkenborn, A.

1. On generalized p-adic integration. *Bull. Soc. Math. France*, Mém. no. 39-40 (1974), 375-384.

Wagstaff, S.

1. The irregular primes to 125,000. *Math. Comp.*, **32** (1978), 583-591.
2. Zeros of p-adic L-functions. *Math. Comp.*, **29** (1975), 1138-1143.
3. p-Divisibility of certain sets of Bernoulli numbers. *Math. Comp.*, **34** (1980), 467-649.

Waldschmidt, M.

1. Transcendance et exponentielles en plusieurs variables. *Invent. math.*, **63** (1981), 97-127.

Washington, L.

1. Class numbers and $\mathbb{Z}_p$-extensions. *Math. Ann.*, **214** (1975), 177-193.
2. A note on p-adic L-functions. *J. Number Theory*, **8** (1976), 245-250.
3. The class number of the field of 5^nth roots of unity. *Proc. Amer. Math. Soc.*, **61** (1976), 205-208.
4. The calculation of $L_p(1, \chi)$. *J. Number Theory*, **9** (1977), 175-178.
5. Euler factors for p-adic L-functions. *Mathematika*, **25** (1978), 68-75.
6. Kummer's calculation of $L_p(1, \chi)$. *J. reine angew. Math.*, **305** (1979), 1-8.
7. The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension. *Invent. math.*, **49** (1979), 87-97.
8. Units of irregular cyclotomic fields. *Ill. J. Math.*, **23** (1979), 635-647.
9. The derivative of p-adic L-functions. *Acta Arith.*, **40** (1980), 109-115.
10. Class numbers and cyclotomic $\mathbb{Z}_p$-extensions. Proc. Queen's Number Theory Conf., 1979 (Kingston, Ontario; ed. by P. Ribenboim). *Queen's Papers in Pure and Applied Math.*, no. 54 (1980), 119-127.
11. p-adic L-functions at $s = 0$ and $s = 1$. Springer Lecture Notes in Mathematics (Grosswald Symposium, Philadelphia, 1980) (to appear).
12. Zeroes of p-adic L-functions. Sém. Delange-Pisot Poitou, Théorie des Nombres, 1980/1981 (to appear with Birkhäuser: Boston-Basel-Stuttgart).

Watabe, M.

1. On class numbers of some cyclotomic fields. *J. reine angew. Math.*, **301** (1978), 212-215; correction: **329** (1981), 176.

Weber, H.

1. Theorie der Abel'schen Zahlkörper. *Acta Math.*, **8** (1886), 193-263.

Weil, A.

1. Number of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, **55** (1949), 497-508. *Collected Papers*, vol. I, 399-410.
2. Jacobi sums as "Grössencharaktere." *Trans. Amer. Math. Soc.*, **73** (1952), 487-495. *Collected Papers*, vol. II, 63-71. Springer-Verlag: New York, 1979.
3. La cyclotomie jadis et naguère. *Sém. Bourbaki, 1973/1974*, Exp. no. 452, Springer Lecture Notes in Mathematics, Vol. 431 (1975), 318-338; *l'Enseignement Math.*, **20** (1974), 247-263. *Collected Papers*, vol. III, 311-327.
4. Sommes de Jacobi et caractères de Hecke, Gött. Nachr. 1974, Nr. 1, 14 pp. *Collected Papers*, vol. III, 329-342.
5. *Courbes Algébriques et Variétés Abéliennes.* Hermann: Paris, 1971.

6. *Basic Number Theory*, 3rd ed. Springer-Verlag: New York, 1974.

Whittaker, E. and Watson, G.

1. *A Course of Modern Analysis*, 4th ed. Cambridge Univ. Press: Cambridge, 1958.

Wiles, A.

1. Higher explicit reciprocity laws. *Ann. of Math.* (2), **107** (1978), 235–254.
2. Modular curves and the class group of $Q(\zeta_p)$. *Invent. math.*, **58** (1980), 1–35.

Woodcock, C.

1. A note on some congruences for the Bernoulli numbers B_m. *J. London Math. Soc.* (2), **11** (1975), 256.

Yahagi, O.

1. Construction of number fields with prescribed l-class groups. *Tokyo J. Math.*, **1** (1978), no. 2, 275–283.

Yamaguchi, I.

1. On a Bernoulli numbers conjecture. *J. reine angew. Math.*, **288** (1976), 168–175. MR **54**: 12628.

Yamamoto, K.

1. On a conjecture of Hasse concerning multiplicative relations of Gaussian sums. *J. Combin. Theory*, **1** (1966), 476–489.
2. The gap group of multiplicative relationships of Gaussian sums. *Symp. Math.*, **15** (1975), 427–440.

Yamamoto, S.

1. On the rank of the p-divisor class group of Galois extensions of algebraic number fields. *Kumamoto J. Sci.* (*Math.*), **9** (1972), 33–40. MR **46**: 1757 (note: Theorem 3 listed in the review applies only to $\mathbb{Q}(\zeta_p)$, not $\mathbb{Q}(\zeta_{p^{n+1}})$).

List of Symbols

ζ_n	nth root of unity, 9
f_χ	conductor, 19
$\hat{G}$	character group, 21
$H^\perp$	annihilator, 22
$L(s, \chi)$	L-series, 29
$L_p(s, \chi)$	p-adic L-function, 57
$\tau(\chi)$	Gauss sum, 29
B_n	Bernoulli number, 30
$B_{n,\chi}$	generalized Bernoulli number, 30
$B_n(X)$	Bernoulli polynomial, 31
$\zeta(s, b)$	Hurwitz zeta function, 30
K^+	maximal real subfield, 38
h^+	class number of K^+, 38
h^-	relative class number, 38
Q	unit index, 39
R_K	regulator, 41
$R_{K,p}$	p-adic regulator, 70
$\mathbb{C}_p$	completion of algebraic closure of $\mathbb{Q}_p$, 48
exp	p-adic exponential, 49
$\log_p$	p-adic logarithm, 50
q	4 or p, 51
$\omega(a)$	Teichmüller character, 51
$\langle a \rangle$	51
$\binom{X}{n}$	52
$g(\chi)$	Gauss sum, 88

$J(\chi_1, \chi_2)$	Jacobi sum, 88
θ	Stickelberger element, 93
$\{x\}$	fractional part, 93
$\varepsilon_\chi, \varepsilon_i$	idempotents, 100
A_i	ith component of class group, 101
A^-	minus component, 101, 192
λ, μ, ν	Iwasawa invariants, 127
K_∞	$\mathbb{Z}_p$-extension, 264
Λ	$\mathbb{Z}_p[[T]]$, 268
$A \sim B$	pseudo-isomorphism, 271
Γ	276
ν_n	278
$\nu_{n,e}$	280
ω_n	291

Index

Adams, J. C., 86
Ankeny–Artin–Chowla, 81, 85
Artin map, 338, 342

Baker–Brumer theorem, 74
Bass' theorem, 151, 260
Bernoulli
  distribution, 233, 238
  numbers, 6, 30, 347
  polynomials, 31
Brauer–Siegel theorem, 42

Capitulation of ideal classes, 40, 185, 286, 317
Carlitz, L., 86
Class field
  theory, 336ff.
  towers, 222
Class number formulas, 37ff., 71, 77ff., 151ff.
CM-field, 38ff., 185, 192, 193
Coates–Wiles homomorphism, 307
Conductor, 19, 338
Conductor–discriminant formula, 27, 34
Cyclotomic
  polynomial, 12, 18
  units, 2, 143ff., 313
  $\mathbb{Z}_p$-extension, 128, 286

Davenport–Hasse relation, 112
Dirichlet characters, 19ff.
Dirichlet's theorem, 13, 34
Discriminant, 9
Distinguished polynomial, 115
Distributions, 231ff., 251ff.

Eichler, M., 107
Ennola, V., 262
Even character, 19
Exponential function, 49

Fermat curve, 90
Fermat's Last Theorem, 1, 107, 167ff.
First factor, 38
Fitting ideal, 297
Frobenius automorphism, 14, 337
Function fields, 128, 129, 296
Functional equation, 29, 34, 86

Gamma transform, 241
Γ-extension, 127
Gauss sum, 29, 35, 36, 87ff.
Generalized Bernoulli numbers, 30

Herbrand's theorem, 102
Hurwitz zeta function, 30, 55

Idèles, 344
Imprimitive characters, 205
Index of Stickelberger ideal, 103
Infinite Galois theory, 332ff.
Integration, 237ff.

Inverse limits, 331
Irregular primes, 7, 62, 63, 165, 193, 350
Iwasawa
  algebra (= Λ), 268
  function, 69, 246, 261
  invariants, 127, 276
  theorem, 103, 276

Jacobi sums, 88

Krasner's lemma, 48
Kronecker-Weber theorem, 319ff., 341
Kubert's theorem (= 12.18), 260
Kummer
  congruences, 61, 141, 241
  homomorphism, 300
  lemma (= 5.36), 79, 162
  pairing, 188ff., 292

λ, 127, 141, 201, 276
Λ-modules, 268ff.
L-functions, 29ff., 57ff.
Lenstra, H. W., 18
Leopoldt's conjecture, 71ff., 265, 291
Local units, 163, 310ff.
Logarithm, 50
Logarithmic derivative, 299

Mahler's theorem, 52
Main conjecture, 146, 198, 199, 295ff.
Masley, J., 204
Maximal real subfield, 38
Measures, 236ff.
Mellin transform, 242
Minkowski
  bound, 17, 320
  unit, 72
Montgomery, H., 204
μ, 127, 130, 276, 284, 286

Nakayama's lemma, 279
Normal numbers, 136, 142

Odd character, 19
Odlyzko, A., 221
Ordinary distribution, 234

p-adic class number formula, 71, 77ff.
p-adic L-functions, 57ff., 117ff., 199, 239, 251, 295, 314
p-adic regulator, 70ff., 77, 78, 85, 86
Parity of class numbers, 184, 193
Partial zeta function, 30, 95
Periods, 16
Polya-Vinogradov inequality, 214
Primitive character, 19, 28
Probability, 62, 86, 108, 112, 159
Pseudo-isomorphic, 271
Punctured distribution, 233

Quadratic
  fields, 17, 45, 46, 81ff., 111, 190, 337
  reciprocity, 18, 341

Ramachandra units, 147
Rank, 186-193
Reflection theorems, 187ff.
Regular prime, 7, 62, 63
Regulator, 40, 70, 77, 78, 85, 86
Relative class number, 38
Residue formula, 37, 71, 165
Ribet's theorem, 102

Scholz's theorem, 83, 190
Second factor, 38
Sinnott, W., 103, 147
Spiegelungsatz (= reflection theorem), 187ff.
Splitting laws, 14
Stickelberger
  element, 93, 119
  ideal, 94, 195, 298
  theorem, 94
Stirling's series, 58

Teichmüller character (= ω), 51, 57
Twist, 294

Uchida, K., 204
Uniform distribution, 134ff.
Universal distribution, 251ff.

Vandiver's conjecture, 78, 157ff., 186, 195ff.
Von Staudt-Clausen, 55, 141

Wagstaff, S., 181
Weierstrass preparation theorem, 115
Weyl criterion, 135

Zeta function for curves, 92, 128, 296
$\mathbb{Z}_p$-extension, 127, 263ff.

听雨尘心@含藏识

免费电子书下载

http://realking1980.bokee.com