Graduate Texts in Mathematics

Lawrence C. Washington

Introduction to Cyclotomic Fields

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.

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

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

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

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 $\zeta^{-1}\alpha$ is an algebraic integer, its trace from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$ is a rational integer: $\mathrm{Tr}(\zeta^{-1}\alpha) \in \mathbb{Z}$. 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 $\mathfrak{P}$ is a prime ideal with $\mathfrak{P} | (x + \zeta^i y)$ and $\mathfrak{P} | (x + \zeta^j y)$, where $i \neq j$. Then $\mathfrak{P} | (\zeta^i y - \zeta^j y) = (\text{unit})(1 - \zeta)y$. Therefore $\mathfrak{P} = (1 - \zeta)$ or $\mathfrak{P} | y$. Similarly, $\mathfrak{P}$ divides $\zeta^j(x + \zeta^i y) - \zeta^i(x + \zeta^j y) = (\text{unit})(1 - \zeta)x$, so $\mathfrak{P} = (1 - \zeta)$ or $\mathfrak{P} | x$. If $\mathfrak{P} \neq (1 - \zeta)$ then $\mathfrak{P} | x$ and $\mathfrak{P} | y$, which is impossible since $(x, y) = 1$. Therefore $\mathfrak{P} = (1 - \zeta)$. But then $x + y \equiv x + \zeta^i y \equiv 0 \bmod \mathfrak{P}$, the second congruence being by the choice of $\mathfrak{P}$. 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 $p | z$, 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 $\mathfrak{P}$ be a prime of $\mathbb{Q}(\zeta_{23})$ lying above $\mathfrak{p}$. We claim that $\mathfrak{P}$ is nonprincipal. The norm of $\mathfrak{P}$ 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, $f \neq 1$). 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 $\mathfrak{P}$ is principal, so is its norm. Therefore $\mathfrak{P}$ 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 $1 \le m \le n$.