Graduate Texts in Mathematics

69

Cyclotomic Fields II

Springer-Verlag

Serge Lang

Cyclotomic Fields II

Springer—Verlag
New York Heidelberg Berlin
World Publishing Corporation Beijing China

Serge Lang

Department of Mathematics
Yale University
New Haven, Connecticut 06520
USA

AMS Subject Classification (1980): 12A35

Library of Congress Cataloging in Publication Data

Lang, Serge, 1927–
Cyclotomic fields II.

(Graduate texts in mathematics; v. 69)
Bibliography: p.
Includes index.
1. Fields, Algebraic, 2. Cyclotomy. I. Title.
II. Series.
QA247.L34 512'.3 79-20459

Reprinted in China by World Publishing Corporation
For distribution and sale in the People's Republic of China only
只限在中华人民共和国发行

ISBN 0-387-90447-6 Springer-Verlag New York
ISBN 3-540-90447-6 Springer-Verlag Berlin Heidelberg
ISBN 7-5062-0099-6 World Publishing Corporation China

Graduate Texts in Mathematics

69

Serge Lang

Cyclotomic Fields II

Springer-Verlag
New York Heidelberg Berlin
World Publishing Corporation, Beijing, China

Serge Lang

Department of Mathematics
Yale University
New Haven, Connecticut 06520
USA

AMS Subject Classification (1980): 12A35

Library of Congress Cataloging in Publication Data

Lang, Serge, 1927–
Cyclotomic fields II.

(Graduate texts in mathematics; v. 69)
Bibliography: p.
Includes index.
1. Fields, Algebraic, 2. Cyclotomy. I. Title.
II. Series.
QA247.L34 512'.3 79-20459

Reprinted in China by World Publishing Corporation
For distribution and sale in the People's Republic of China only
只限在中华人民共和国发行

ISBN 0-387-90447-6 Springer-Verlag New York
ISBN 3-540-90447-6 Springer-Verlag Berlin Heidelberg
ISBN 7-5062-0099-6 World Publishing Corporation China

Preface

This second volume incorporates a number of results which were discovered and/or systematized since the first volume was being written. Again, I limit myself to the cyclotomic fields proper without introducing modular functions.

As in the first volume, the main concern is with class number formulas, Gauss sums, and the like. We begin with the Ferrero–Washington theorems, proving Iwasawa's conjecture that the p-primary part of the ideal class group in the cyclotomic $\mathbf{Z}_p$-extension of a cyclotomic field grows linearly rather than exponentially. This is first done for the minus part (the minus referring, as usual, to the eigenspace for complex conjugation), and then it follows for the plus part because of results bounding the plus part in terms of the minus part. Kummer had already proved such results (e.g. if $p \nmid h_p^-$ then $p \nmid h_p^+$). These are now formulated in ways applicable to the Iwasawa invariants, following Iwasawa himself.

After that we do what amounts to "Dwork theory," to derive the Gross–Koblitz formula expressing Gauss sums in terms of the p-adic gamma function. This lifts Stickelberger's theorem p-adically. Half of the proof relies on a course of Katz, who had first obtained Gauss sums as limits of certain factorials, and thought of using Washnitzer–Monsky cohomology to prove the Gross–Koblitz formula.

Finally, we apply these latter results to the Ferrero–Greenberg theorem, showing that $L_p'(0, \chi) \neq 0$ under the appropriate conditions. We take this opportunity to introduce a technique of Washington, who defined the p-adic analogues of the Hurwitz partial zeta functions, in a way making it possible to parallel the treatment from the complex case to the p-adic case, but in a much more efficient way.

All of these topics form a natural continuation of those of Volume I. Thus chapters are numbered consecutively, and the bibliography (suitably expanded) is similarly updated.

I am much indebted to Larry Washington and Neal Koblitz for a number of suggestions and corrections; and to Avner Asch for helping with the proofreading.

Larry Washington also read the first volume carefully, and made the following corrections with no other changes in the proofs:

Chapter 5, Theorem 1.2(ii), p. 127: read $e_n = dn + c_0$ for some constant c_0.

Chapter 7, Theorem 1.4, p. 174: the term $1/k^2$ should be $(-1)^k/k \cdot k!$ instead.

Chapter 8, Formulas **LS 6**, p. 207: one needs to assume that $[\pi](X)$ is a polynomial. This is satisfied if the formal group is the basic Lubin–Tate group, and the theorems proved are invariant under an isomorphism of such groups, so the proofs are valid without further change.

Washington also pointed out the reference to Vandiver [Va 2], where indeed Vandiver makes the conjecture:

> . . . However, about twenty-five years ago I conjectured that this number was never divisible by l [referring to h^+]. Later on, when I discovered how closely the question was related to Fermat's Last Theorem, I began to have my doubts, recalling how often conjectures concerning the theorem turned out to be incorrect. When I visited Furtwängler in Vienna in 1928, he mentioned that he had conjectured the same thing before I had brought up any such topic with him. As he had probably more experience with algebraic numbers than any mathematician of his generation, I felt a little more confident . . .

On the other hand, many years ago, Feit was unable to understand a step in Vandiver's "proof" that $p \nmid h^+$ implies the first case of Fermat's Last Theorem, and stimulated by this, Iwasawa found a precise gap which is such that the proof is still incomplete.

New Haven, Connecticut
1980

SERGE LANG

Contents Volume II

Contents Volume I

Notation

As in the first volume, if A is an abelian group and N a positive integer, we let A_N be the kernel of multiplication by N, and

$$A(N) = A/NA.$$

If p is a prime, we let $A^{(p)}$ be the subgroup of p-primary elements, that is, those elements annihilated by a power of p.

Measures and Iwasawa Power Series 10

This chapter gives a number of complements to Chapter 4. In §1 we extend the formalism of the associated power series to the change of variables

$$x \leftrightarrow \gamma^x$$

for $x \in \mathbf{Z}_p$ and γ equal to a topological generator of $1+p\mathbf{Z}_p$. A measure on $1+p\mathbf{Z}_p$ then corresponds to a measure on $\mathbf{Z}_p$, and we give relations between their associated power series. This is then applied to express Bernoulli numbers $B_{k,\chi}$ as values of power series. We write

$$\chi = \theta\omega^{-k}\psi = \theta_k\psi,$$

where first θ is an even character on $\mathbf{Z}(dp)^*$ (d prime to p), ω is the Teichmuller character, and ψ is a character on $1 + p\mathbf{Z}_p$. Let $\zeta = \psi(\gamma)$. Then

$$\frac{1}{k} B_{k,\chi} = f_{\theta,k}(\zeta - 1),$$

where $f_{\theta,k}$ depends only on θ and k. This allows a partial asymptotic determination of $\operatorname{ord}_p B_{k,\chi}$ when θ is fixed, and the conductor of ψ tends to infinity, due to Iwasawa [Iw 14], §7. This gives rise to the corresponding asymptotic estimate for the minus part of class numbers of cyclotomic extensions.

The Iwasawa expressions for the Bernoulli numbers gives an asymptotic value for their orders:

$$\operatorname{ord}_p B_{k,\theta_k\psi} = mp^n + \lambda n + c$$

for n sufficiently large, cond $\psi = p^{n+1}$. In order that $m \neq 0$, Iwasawa showed that a system of congruences had to be satisfied (essentially that the coefficients of the appropriate power series are $\equiv 0 \pmod p$). We derive these congruences here in each case successively. The next chapter is devoted to the proofs by Ferrero–Washington that these congruences cannot all be satisfied, whence the Iwasawa invariant m is equal to 0.

At the end of their paper, Ferrero–Washington conjecture that the invariant λ_p for the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}(\boldsymbol{\mu}_p)$ satisfies a bound

$$\lambda_p \ll \frac{\log p}{\log \log p}.$$

I am much indebted to Washington for communicating to me the exposition of the steps which lead to this conjecture, and which were omitted from their paper.

§1. Iwasawa Invariants for Measures

We let p be an odd prime for simplicity. The multiplicative group $1 + p\mathbf{Z}_p$ is then topologically cyclic, and we let γ denote a fixed topological generator. Then $\gamma \bmod p^n$ generates the finite cyclic group $1 + p\mathbf{Z}_p \bmod p^n$ for each positive integer n. For instance, we may take

$$\gamma = 1 + p.$$

[*Note*: If $p = 2$, then one has to consider $1 + 4\mathbf{Z}_2$ instead of $1 + 2\mathbf{Z}_2$.]

There is an isomorphism

$$\mathbf{Z}_p \to 1 + p\mathbf{Z}_p$$

given by

$$x \mapsto \gamma^x.$$

Its inverse is denoted by α, so that by definition

$$\alpha(\gamma^x) = x.$$

Let $d \geq 1$ be a positive integer prime to p. We shall consider measures on the projective system of groups

$$Z_n = \mathbf{Z}(dp^n) = \mathbf{Z}/dp^n\mathbf{Z} = \mathbf{Z}(d) \times \mathbf{Z}(p^n).$$

The projective limit is simply denoted by

$$Z = \mathbf{Z}(d) \times \mathbf{Z}_p.$$

A measure is then determined by a family of functions μ_n on Z_n, as in Chapter 2, §2. We let

$$Z^* = \mathbf{Z}(d) \times \mathbf{Z}_p^* \quad \text{and} \quad Z^{**} = \mathbf{Z}(d)^* \times \mathbf{Z}_p^*.$$

An element $z \in Z^*$ can be written uniquely in the form

$$z = (z_0, \eta\gamma^x) = (z_0, z_p) \qquad \text{with } z_0 \in \mathbf{Z}(d), \eta \in \boldsymbol{\mu}_{p-1}, x \in \mathbf{Z}_p.$$

We define the homomorphism

$$\alpha: Z^* \to \mathbf{Z}_p \quad \text{by} \quad \alpha(z_0, \eta\gamma^x) = x.$$

We define as usual

$$\langle z \rangle_p = \langle z \rangle = \langle z_p \rangle = \gamma^x,$$

so that $\alpha(z) = \alpha(\langle z \rangle)$. As above, we usually omit the index p on $\langle z \rangle_p$.

A continuous function on $\mathbf{Z}_p$ gives rise to a continuous function on $1+p\mathbf{Z}_p$ by composition with α, and conversely.

As in Chapter 2, §1 we let $\mathfrak{o}$ be the ring of p-integers in $\mathbf{C}_p$, and we let μ be an $\mathfrak{o}$-valued distribution, i.e. a measure.

By the basic correspondence between functionals and measures, we obtain the following theorem.

Theorem 1.1. *Let μ be a measure on Z with support in Z^*. Then there exists a unique measure $\alpha_*\mu$ on $\mathbf{Z}_p$ such that for any continuous function φ on $1+p\mathbf{Z}_p$ we have*

$$\int_{Z^*} \varphi(\langle a \rangle)\, d\mu(a) = \int_{\mathbf{Z}_p} \varphi(\gamma^x)\, d(\alpha_*\mu)(x).$$

We now describe the power series associated with $\alpha_*\mu$ modulo the polynomial

$$h_n(X) = (1 + X)^{p^n} - 1.$$

Thus we fix a value of $n \geq 0$, and for each $a \in Z^*$ we let $r(a)$ be the unique integer such that

$$0 \leq r(a) < p^n \quad \text{and} \quad r(a) \equiv \alpha(a) \bmod p^n.$$

Theorem 1.2. *Let f be the power series associated with $\alpha_* \mu$. Let*

$$Z_{n+1}^* = \mathbf{Z}(d) \times \mathbf{Z}(p^{n+1})^*$$

Then

$$f(X) \equiv \sum_{a \in Z_{n+1}^*} \mu_{n+1}(a)(1+X)^{r(a)} \bmod h_n(X).$$

Proof. By the definition of the associated power series, we have

$$f(X) \equiv \sum_{r=0}^{p^n-1} (\alpha_* \mu)(r)(1+X)^r.$$

But letting char denote the characteristic function, we have:

$$(\alpha_* \mu)(r \bmod p^n) = \int_{\mathbf{Z}_p} (\text{char of } r \bmod p^n)\, d(\alpha_* \mu)$$

$$= \int_{Z^*} (\text{char of } Z(d) \times \boldsymbol{\mu}_{p-1} \times \gamma^{r+p^n\mathbf{Z}_p})\, d\mu$$

(by Theorem 1.1)

$$= \sum_{\eta} \mu_{n+1}(\eta\gamma^r \bmod p^{n+1})$$

where this last sum is taken over $\eta \in \mathbf{Z}(d) \times \boldsymbol{\mu}_{p-1}$. This proves the theorem.

Corollary 1. *Let ψ be a nontrivial character of $1+p\mathbf{Z}_p$, with conductor p^{n+1}. Define $\psi(a) = \psi(\langle a \rangle)$. Let*

$$\psi(\gamma) = \zeta = \textit{primitive } p^n\text{-th } \textit{root of unity}.$$

Let f be the power series associated with $\alpha_* \mu$. Then

$$\int_{\mathbf{Z}_p^*} \psi\, d\mu = f(\zeta - 1).$$

Proof. We have

$$\begin{aligned}\int_{Z^*} \psi\, d\mu &= \int_{Z_p} \psi(\gamma^x)\, d(\alpha_* \mu)(x) && \text{(by Theorem 1.1)}\\ &= \int_{Z_p} \zeta^x\, d(\alpha_* \mu)(x)\\ &= f(\zeta - 1). && \text{(by Theorem 1.2 of Chapter 4).}\end{aligned}$$

This proves the corollary.

We continue with the same notation as in the theorem. We shall use the notation

$$B(\psi, \mu) = \int_{Z^*} \psi\, d\mu = f(\zeta_\psi - 1).$$

Suppose that there exists a rational number m such that the power series f can be written in the form

$$f(X) = p^m(c_0 + c_1 X + \cdots + c_{\lambda-1} X^{\lambda-1} + c_\lambda X^\lambda + \cdots)$$

where c_λ is a unit in $\mathfrak{o}$, and $c_0, \ldots, c_{\lambda-1} \in \mathfrak{m}$, the maximal ideal of $\mathfrak{o}$. We call m, λ the **Iwasawa invariants of** μ, or f. If the measure μ has values in the maximal ideal of the integers in a field where the valuation is discrete (which is the case in applications), then f has coefficients in that ring, and such m, λ exist if $f \neq 0$. If $m = 0$, then λ is the Weierstrass degree of f. In any case, λ is the Weierstrass degree of $p^{-m} f$.

As usual, we shall write

$$x \sim y$$

to mean that x, y have the same order at p.

Corollary 2. *There exists a positive integer n_0 (depending only on f) such that if $n \geq n_0$ and* cond $\psi = p^n$, *then*

$$B(\psi, \mu) \sim p^m(\zeta - 1)^\lambda$$

where ζ is a primitive p^n-th root of unity.

Proof. As $n \to \infty$, the values $|\zeta - 1|$ approach 1, and so the term $c_\lambda(\zeta - 1)^\lambda$ dominates in the power series $f(\zeta - 1)$ above.