Graduate Texts in Mathematics

59

Serge Lang

Cyclotomic Fields

Springer-Verlag
New York Heidelberg Berlin

Dr. Serge Lang
Department of Mathematics
Yale University
New Haven, Connecticut 06520
USA

AMS Subject Classification: 12C20, 12B30, 14G20

Library of Congress Cataloging in Publication Data
Lang, Serge, 1927–
Cyclotomic fields.
(Graduate texts in mathematics: 59)
Bibliography: p.
Includes index.
1. Fields, Algebraic. 2. Cyclotomy. I. Title.
II. Series.
QA247.L33 512'.3 77–25859

9 8 7 6 5 4 3 2 1

ISBN-13: 978-1-4612-9947-9 e-ISBN-13: 978-1-4612-9945-5
DOI: 10.1007/978-1-4612-9945-5

Foreword

Kummer's work on cyclotomic fields paved the way for the development of algebraic number theory in general by Dedekind, Weber, Hensel, Hilbert, Takagi, Artin and others. However, the success of this general theory has tended to obscure special facts proved by Kummer about cyclotomic fields which lie deeper than the general theory. For a long period in the 20th century this aspect of Kummer's work seems to have been largely forgotten, except for a few papers, among which are those by Pollaczek [Po], Artin–Hasse [A–H] and Vandiver [Va].

In the mid 1950's, the theory of cyclotomic fields was taken up again by Iwasawa and Leopoldt. Iwasawa viewed cyclotomic fields as being analogues for number fields of the constant field extensions of algebraic geometry, and wrote a great sequence of papers investigating towers of cyclotomic fields, and more generally, Galois extensions of number fields whose Galois group is isomorphic to the additive group of p-adic integers. Leopoldt concentrated on a fixed cyclotomic field, and established various p-adic analogues of the classical complex analytic class number formulas. In particular, this led him to introduce, with Kubota, p-adic analogues of the complex L-functions attached to cyclotomic extensions of the rationals. Finally, in the late 1960's, Iwasawa [Iw 11] made the fundamental discovery that there was a close connection between his work on towers of cyclotomic fields and these p-adic L-functions of Leopoldt–Kubota.

The classical results of Kummer, Stickelberger, and the Iwasawa–Leopoldt theories have been complemented by, and received new significance from the following directions:

1. The analogues for abelian extensions of imaginary quadratic fields in the context of complex multiplication by Novikov, Robert, and Coates–Wiles. Especially the latter, leading to a major result in the direction of the

Birch–Swinnerton-Dyer conjecture, new insight into the explicit reciprocity laws, and a refinement of the Kummer–Takagi theory of units to all levels.

2. The development by Coates, Coates–Sinnott and Lichtenbaum of an analogous theory in the context of K-theory.

3. The development by Kubert–Lang of an analogous theory for the units and cuspidal divisor class group of the modular function field.

4. The introduction of modular forms by Ribet in proving the converse of Herbrand's theorem.

5. The connection between values of zeta functions at negative integers and the constant terms of modular forms starting with Klingen and Siegel, and highly developed to congruence properties of these constant terms by Serre, for instance, leading to the existence of the p-adic L-function for arbitrary totally real fields.

6. The construction of p-adic zeta functions in various contexts of elliptic curves and modular forms by Katz, Manin, Mazur, Vishik.

7. The connection with rings of endomorphisms of abelian varieties or curves, involving complex multiplication (Shimura–Taniyama) and/or the Fermat curve (Davenport–Hasse–Weil and more recently Gross–Rohrlich).

There is at present no systematic introduction to the basic cyclotomic theory. The present book is intended to fill this gap. No connection will be made here with modular forms, the book is kept essentially purely cyclotomic, and as elementary as possible, although in a couple of places, we use class field theory.

Some basic conjectures remain open, notably: Vandiver's conjecture that h^+ is prime to p.

The Iwasawa–Leopoldt conjecture that the p-primary part of C^- is cyclic over the group ring, and therefore isomorphic to the group ring modulo the Stickelberger ideal. For prime level, Leopoldt and Iwasawa have shown that this is a consequence of the Vandiver conjecture. Cf. Chapter VI, §4.

Much of the cyclotomic theory extends to totally real number fields, as theorems or conjecturally. We do not touch on this aspect of the question. Cf. Coates' survey paper [Co 3], and especially Shintani [Sh].

There seems no doubt at the moment that essential further progress will be closely linked with the algebraic–geometric considerations, especially via the Fermat and modular curves.

I am very much indebted to John Coates, Ken Ribet and David Rohrlich for their careful reading of the manuscript, and for a large number of suggestions for improvement.

New Haven, Connecticut SERGE LANG
1978

Contents

Notation

$\mathbf{Z}(N)$ = integers mod $N = \mathbf{Z}/N\mathbf{Z}$.

If A is an abelian group, we usually denoted by A_N the elements $x \in A$ such that $Nx = 0$. Thus for a prime p, we denote by A_p the elements of order p. However, we also use p in this position for indexing purposes, so we rely to some extent on the context to make the intent clear. In his book, Shimura uses $A[p]$ for the kernel of p, and more generally, if A is a module over a ring, uses $A[\mathfrak{a}]$ for the kernel of an ideal $\mathfrak{a}$ in A. The brackets are used also in other contexts, like operators, as in Lubin–Tate theory. There is a dearth of symbols and positions, so some duplication is hard to avoid.

We let $A(N) = A/NA$. We let $A^{(p)}$ be the subgroup of A consisting of all elements annihilated by a power of p.

Character Sums 1

Character sums occur all over the place in many different roles. In this chapter they will be used at once to represent certain principal ideals, thus giving rise to annihilators in a group ring for ideal classes in cyclotomic fields.

They also occur as endomorphisms of abelian varieties, especially Jacobians, but we essentially do not consider this, except very briefly in §6. They occur in the computation of the cuspidal divisor class group on modular curves in [KL 6]. The interplay between the algebraic geometry and the theory of cyclotomic fields is one of the more fruitful activities at the moment in number theory.

§1. Character Sums Over Finite Fields

We shall use the following notation.

$F = F_q$ = finite field with q elements, $q = p^n$.
$\mathbf{Z}(N) = \mathbf{Z}/N\mathbf{Z}$.
ε = primitive pth root of unity in characteristic 0. Over the complex numbers, $\varepsilon = e^{2\pi i/p}$.
Tr = trace from F to F_p.
μ_N = group of Nth roots of unity.
$\lambda: F \to \mu_p$ the character of F given by

$$\lambda(x) = \varepsilon^{\mathrm{Tr}(x)}.$$

$\chi: F^* \to \mu_{q-1}$ denotes a character of the multiplicative group.
We extend χ to F by defining $\chi(0) = 0$.

The field $\mathbf{Q}(\mu_N)$ has an automorphism σ_{-1} such that

$$\sigma_{-1}: \zeta \mapsto \zeta^{-1}.$$

If $\alpha \in \mathbf{Q}(\mu_N)$ then the **conjugate** $\bar{\alpha}$ denotes $\sigma_{-1}\alpha$. Over the complex numbers, this is the **complex conjugate**.

The Galois group of $\mathbf{Q}(\mu_N)$ over $\mathbf{Q}$ is isomorphic to $\mathbf{Z}(N)^*$, under the map

$$c \mapsto \sigma_c$$

where

$$\sigma_c : \zeta \mapsto \zeta^c.$$

Let f, g be functions on F with values in a fixed algebraically closed field of characteristic 0. We define

$$S(f, g) = \sum_{x \in F} f(x)g(x).$$

We define the **Fourier transform** Tf by

$$Tf(y) = \sum_{x \in F} f(x)\lambda(-xy) = \sum f(x)\varepsilon^{-\mathrm{Tr}(xy)}.$$

Then Tf is again a function on F, identified with its character group by λ, and T is a linear map.

Theorem 1.1. *Let f^- be the function such that $f^-(x) = f(-x)$. Then $T^2 f = qf^-$, that is*

$$T^2 f(z) = qf(-z).$$

Proof. We have

$$\begin{aligned} T^2 f(z) &= \sum_y \sum_x f(x)\lambda(-yx)\lambda(-zy) \\ &= \sum_x f(x - z) \sum_y \lambda(-yx). \end{aligned}$$

If $x \neq 0$ then $y \mapsto \lambda(yx)$ is a non-trivial character, and the sum of the character over F is 0. Hence this last expression is

$$= qf(-z)$$

as desired.

We define the **convolution** $f * g$ between functions by the formula

$$(f * g)(y) = \sum_x f(x)g(y - x).$$

A change of variables shows that

$$f * g = g * f.$$

Theorem 1.2. *For functions f, g on F we have*

$$T(f * g) = (Tf)(Tg)$$

$$T(fg) = \frac{1}{q} Tf * Tg.$$

Proof. For the first formula we have

$$T(f * g)(z) = \sum_y (f * g)(y)\lambda(-zy) = \sum_y \sum_x f(x)g(y - x)\lambda(-zy).$$

We change the order of summation, let $t = y - x$, $y = x + t$, and find

$$= \sum_x f(x)\lambda(-zx) \sum_t g(t)\lambda(-zt)$$

$$= (Tf)(Tg)(z),$$

thereby proving the first formula.

The second formula follows from the first because T is an isomorphism on the space of functions on F, so that we can write $f = Tf_1$ and $g = Tg_1$ for some functions f_1, g_1. We then combine the first formula with Theorem 1.1 to get the second.

We shall be concerned with the **Gauss sums (Lagrange resolvant)**

$$S(\chi, \lambda) = S(\chi) = \sum_u \chi(u)\lambda(u)$$

where the sum is taken over $u \in F^*$. We could also take the sum over x in F since we defined $\chi(0) = 0$. Since λ is fixed, we usually omit the reference to λ in the notation. The Gauss sums have the following properties.

GS 0. *Let χ_1 be the trivial character 1 on F^*. Then*

$$S(\chi_1) = -1.$$

This is obvious from our conventions. It illustrates right at the beginning the pervasive fact, significant many times later, that the natural object to consider is $-S(\chi)$ rather than $S(\chi)$ itself. We shall also write

$$S(1) = S(1, \lambda),$$

but the convention remains in force that even for the trivial character, its value at 0 is 0.

GS 1. *For any character $\chi \neq 1$, we have $T\chi = \chi(-1)S(\chi)\chi^{-1}$.*

Proof. We have

$$T\chi(y) = \sum_x \chi(x)\lambda(-yx).$$

If $y = 0$ then $T\chi(y) = 0$ (summing the multiplicative character over the multiplicative group). If $y \neq 0$, we make a change of variables $x = -ty^{-1}$, and we find precisely the desired value

$$\chi(-1)S(\chi)\chi(y^{-1}).$$

GS 2. *We have* $S(\bar{\chi}) = \chi(-1)\overline{S(\chi)}$ *and for* $\chi \neq 1$, $S(\chi)S(\bar{\chi}) = \chi(-1)q$, *so*

$$S(\chi)\overline{S(\chi)} = q, \quad \textit{for } \chi \neq 1.$$

Proof. Note that $T^2\chi = T(\chi(-1)S(\chi)\chi^{-1}) = S(\chi)S(\chi^{-1})\chi$. But we also know that $T^2\chi = q\chi^-$. This proves **GS 2,** as the other statements are obvious.

Over the complex numbers, we obtain the absolute value

$$\boxed{|S(\chi)| = q^{1/2}.}$$

We define the **Jacobi sum**

$$J(\chi_1, \chi_2) = -\sum_x \chi_1(x)\chi_2(1 - x).$$

Observe the minus sign, a most useful convention. We have

$$J(1, 1) = -(q - 2).$$

GS 3. *If* $\chi_1\chi_2 \neq 1$ *then*

$$J(\chi_1, \chi_2) = -\frac{S(\chi_1)S(\chi_2)}{S(\chi_1\chi_2)}.$$

In particular, $J(1, \chi_2) = J(\chi_1, 1) = 1$. *If* $\chi_1\chi_2 = 1$ *but not both* χ_1, χ_2 *are trivial, then*

$$J(\chi_1, \chi_2) = \chi_1(-1).$$

Proof. We compute from the definitions:

$$\begin{aligned} S(\chi_1)S(\chi_2) &= \sum_x \sum_y \chi_1(x)\chi_2(y)\lambda(x + y) \\ &= \sum_x \sum_y \chi_1(x)\chi_2(y - x)\lambda(y) \\ &= \sum_x \sum_{u \neq 0} \chi_1(x)\chi_2(u - x)\lambda(u) + \sum_x \chi_1(x)\chi_2(-x). \end{aligned}$$

If $\chi_1\chi_2 \neq 1$, the last sum on the right is equal to 0. In the other sum, we interchange the order of summation, replace x by ux, and find

$$\sum_u \chi_1\chi_2(u)\lambda(u) \sum_x \chi_1(x)\chi_2(1-x),$$

thus proving the first assertion of **GS 3.** If $\chi_1\chi_2 = 1$, then the last sum on the right is equal to $\chi_1(-1)(q-1)$, and the second assertion follows from **GS 2.**

Next we give formulas showing how the Gauss sums transform under Galois automorphisms.

GS 4. $$S(\chi^p) = S(\chi).$$

Proof. Raising to the pth power is an automorphism of F, and therefore

$$\mathrm{Tr}(x^p) = \mathrm{Tr}(x).$$

Thus $S(\chi^p)$ is obtained from $S(\chi)$ by permuting the elements of F under $x \mapsto x^p$. The property is then obvious.

Let m be a positive integer dividing $q-1$, and suppose that χ has order m, meaning that

$$\chi^m = 1.$$

Then the values of χ are in $\mathbf{Q}(\mu_m)$ and

$$S(\chi) = S(\chi, \lambda) \in \mathbf{Q}(\mu_m, \mu_p).$$

For any integer c prime to m we have an automorphism $\sigma_{c,1}$ of $\mathbf{Q}(\mu_m, \mu_p)$ such that

$$\sigma_{c,1}\colon \zeta \mapsto \zeta^c \quad \text{and} \quad \sigma_{c,1} \text{ is identity on } \mu_p.$$

For any integer v prime to p, we have an automorphism $\sigma_{1,v}$ such that

$$\sigma_{1,v}\colon \varepsilon \mapsto \varepsilon^v \quad \text{and} \quad \sigma_{1,v} \text{ is identity on } \mu_m.$$

We can select v in a given residue class mod p *such that v is also prime to m. In the sequel we usually assume tacitly that v has been so chosen, in particular in the next property.*

GS 5. $$\sigma_{c,1}S(\chi) = S(\chi^c) \quad \textit{and} \quad \sigma_{1,v}S(\chi) = \bar{\chi}(v)S(\chi)$$

Proof. The first is obvious from the definitions, and the second comes by making a change of variable in the Gauss sum,

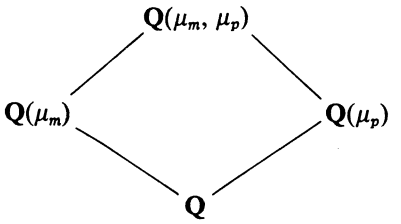
$$x \mapsto v^{-1}x.$$

Observe that

$$\sigma_{1,v}\lambda(x) = \varepsilon^{v\,\mathrm{Tr}(x)} = \varepsilon^{\mathrm{Tr}(vx)} = \lambda(vx).$$

The second property then drops out.

The diagram of fields is as follows.



From the action of the Galois group, we can see that the Gauss sum (Lagrange resolvant) satisfies a Kummer equation.

Theorem 1.3. *Assume that χ has order m.*

(i) *$S(\chi)^m$ lies in $\mathbf{Q}(\mu_m)$.*

(ii) *Let b be an integer prime to m, and let $\sigma_b = \sigma_{b,1}$. Then $S(\chi)^{b-\sigma_b}$ lies in $\mathbf{Q}(\mu_m)$.*

Proof. In each case we operate on the given expression by an automorphism $\sigma_{1,v}$ with an integer v prime to pm. Using **GS 5**, it is then obvious that the given expression is fixed under such an automorphism, and hence lies in $\mathbf{Q}(\mu_m)$.

§2. Stickelberger's Theorem

In the first section, we determined the absolute value of the Gauss sum. Here, we determine the prime factorization. We shall first express a character in terms of a canonical character determined by a prime.

Let $\mathfrak{p}$ be a prime ideal in $\mathbf{Q}(\mu_{q-1})$, lying above the prime number p. The residue class field of $\mathfrak{p}$ is identified with $F = F_q$. We keep the same notation as in §1. The equation $X^{q-1} - 1 = 0$ has distinct roots mod p, and hence reduction mod $\mathfrak{p}$ induces an isomorphism

$$\mu_{q-1} \xrightarrow{\approx} F^* = {F_q}^*.$$

Phrased another way, this means that there exists a unique character ω of F^* such that

$$\omega(u) \bmod \mathfrak{p} = u.$$

This character will be called the **Teichmuller character**. This last equation will also be written in the more usual form

$$\omega(u) \equiv u \pmod{\mathfrak{p}}.$$

The Teichmuller character generates the character group of F^*, so any character χ is an integral power of ω.

We let

$$\pi = \varepsilon - 1.$$

Let $\mathfrak{P}$ be a prime ideal lying above $\mathfrak{p}$ in $\mathbf{Q}(\mu_{q-1}, \mu_p)$. We use the symbol $A \sim B$ to mean that A/B is a unit, or the unit ideal, depending whether A, B are algebraic numbers or (fractional) ideals. We then have

$$\mathfrak{p} \sim \mathfrak{P}^{p-1}$$

because elementary algebraic number theory shows that p is totally ramified in $\mathbf{Q}(\varepsilon)$, and $\mathfrak{p}$ is totally ramified in $\mathbf{Q}(\mu_{q-1}, \mu_p)$.

Let k be an integer, and assume first that $0 \leq k < q - 1$. Write the p-adic expansion

$$k = k_0 + k_1 p + \cdots + k_{n-1} p^{n-1}$$

with $0 \leq k_i \leq p - 1$. We define

$$\boxed{s(k) = k_0 + k_1 + \cdots + k_{n-1}.}$$

For an arbitrary integer k, we define $s(k)$ to be periodic mod $q - 1$, and defined by the above sum in the range first assumed. For convenience, we also define

$$\boxed{\gamma(k) = k_0! \, k_1! \cdots k_{n-1}!}$$

to be the product of the $k_i!$ in the first range, and then also define $\gamma(k)$ by $(q - 1)$-periodicity for arbitrary integers k. If the dependence on q is desired, one could write

$$s_q(k) \quad \text{and} \quad \gamma_q(k).$$

Theorem 2.1. *For any integer k, we have the congruence*

$$\frac{S(\omega^{-k}, \varepsilon^{\mathrm{Tr}})}{(\varepsilon - 1)^{s(k)}} \equiv \frac{-1}{\gamma(k)} \pmod{\mathfrak{P}}.$$

In particular,

$$\mathrm{ord}_{\mathfrak{P}} S(\omega^{-k}) = s(k).$$

Remark. Once more, we see how much more natural the negative of the Gauss sum turns out to be, for we have

$$\frac{-S(\omega^{-k}, \lambda)}{\pi^{s(k)}} \equiv \frac{1}{\gamma(k)} \pmod{\mathfrak{P}}$$

with 1 instead of -1 on the right-hand side.

Proof of Theorem 2.1. If $k = 0$ then the relation of Theorem 2.1 is clear because both sides of the congruence to be proved are equal to -1. We assume $1 \leq k < q - 1$, and prove the theorem by induction. Suppose first that $k = 1$. Then

$$\begin{aligned} S(\omega^{-k}) &= \sum_u \omega(u)^{-1}\varepsilon^{\mathrm{Tr}(u)} \\ &= \sum \omega(u)^{-1}(1 + \pi)^{\mathrm{Tr}(u)} \\ &= \sum \omega(u)^{-1}(1 + (\mathrm{Tr}\, u)\pi + O(\pi^2)) \end{aligned}$$

(interpreting $\mathrm{Tr}\, u$ as an integer in the given residue class mod p). But

$$\begin{aligned} \omega(u)^{-1}\,\mathrm{Tr}(u) &\equiv u^{-1}(u + u^p + \cdots + u^{p^{n-1}}) \bmod \mathfrak{P} \\ &\equiv 1 + u^{p-1} + \cdots + u^{p^n-1-1}. \end{aligned}$$

Each $u \mapsto u^{p^j-1}$ is a non-trivial character of F^*. Hence

$$\sum \omega(u)^{-1}\,\mathrm{Tr}(u) \equiv q - 1 \equiv -1 \pmod{\mathfrak{P}}$$

and therefore

$$\frac{S(\omega^{-1})}{\pi} \equiv -1 \pmod{\mathfrak{P}}$$

thus proving the theorem for $k = 1$.

Assume now the result proved for $k - 1$, and write

$$\omega^{-k} = \omega^{-1}\omega^{-(k-1)}$$

for $1 < k < q - 1$. We distinguish two cases.

Case 1. $p|k$, so we can write $k = pk'$ with $1 \leq k' < q - 1$. Then trivially

$$s(k) = s(k') \quad \text{and} \quad \gamma(k) = \gamma(k')$$

because k has the same coefficients k_i as k', shifted only by one index. Let $\sigma_p = \sigma_{p,1}$, so σ_p leaves ε fixed. Since

$$\sigma_p S(\omega^{-k'}) = S(\omega^{-pk'}) = S(\omega^{-k}),$$

we find that applying σ_p to the inductive congruence

$$\frac{S(\omega^{-k'})}{\pi^{s(k')}} \equiv \frac{-1}{\gamma(k')} \pmod{\mathfrak{P}}$$

yields a proof for the present case, because σ_p is in the decomposition group of $\mathfrak{P}$, whence $\sigma_p\mathfrak{P} = \mathfrak{P}$.

Case 2. $p \nmid k$. Then $1 \leq k_0$. Furthermore,

$$s(k) = s(k-1) + 1 \quad \text{and} \quad \gamma(k-1) = (k_0 - 1)!\, k_1! \cdots k_{n-1}!.$$

Then

$$\frac{S(\omega^{-k})}{\pi^{s(k)}} = \frac{S(\omega^{-1}\omega^{-(k-1)})}{\pi^{s(k)}} \equiv \frac{S(\omega^{-1})}{\pi} \frac{S(\omega^{-(k-1)})}{\pi^{s(k-1)}} \frac{-1}{J(\omega^{-1}, \omega^{-(k-1)})}$$

$$\equiv -1 \cdot \frac{-1}{\gamma(k-1)} \frac{-1}{J(\omega^{-1}, \omega^{-(k-1)})} \pmod{\mathfrak{P}}.$$

To conclude the proof, it will suffices to get the right congruence for J. We use **GS 3** from §1, to get:

$$-J(\omega^{-1}, \omega^{-(k-1)}) \equiv \sum u^{-1}(1-u)^{-(k-1)+q-1} \pmod{\mathfrak{P}},$$

and the sum is at first taken for $u \neq 0, 1$, but with the additional positive exponent $q - 1$ which does not change anything, we may then suppose that the sum is taken for $u \neq 0$ in F. Hence we get further

$$\equiv \sum_{u \neq 0} \sum_{j=0}^{q-k} (-1)^j \binom{q-k}{j} u^{j-1}.$$

If $j \neq 1$ then $\sum u^{j-1} = 0$, so we get the further congruence

$$-J(\omega^{-1}, \omega^{-(k-1)}) \equiv (-1)(q-k)(q-\ ) \equiv -k_0 \pmod{\mathfrak{P}},$$

thereby proving the theorem.

Having obtained the order of the Gauss sum at one prime above p, we also want the full factorization. Suppose that m is an integer >1 and that $p \nmid m$. Let $\mathfrak{p}$ be a prime ideal above p in $\mathbf{Q}(\mu_m)$ and let

$$\mathbf{N}\mathfrak{p} = q = p^n.$$

Let k be an integer such that

$$\frac{k}{q-1} \text{ has order } m \text{ in } \mathbf{Q}/\mathbf{Z}.$$

Let $\langle t \rangle$ denote the smallest real number ≥ 0 in the residue class mod $\mathbf{Z}$ of a real number t. Let

$$G = \mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q}).$$

Define the **Stickelberger element** in the rational group ring

$$\boxed{\theta(k, \mathfrak{p}) = \sum_{c \in (\mathbf{Z}/m)^*} \left\langle \frac{kc}{q-1} \right\rangle \sigma_c^{-1} \in \mathbf{Q}[G].}$$

Let $\mathfrak{P}$ be the prime ideal in $\mathbf{Q}(\mu_m, \mu_p)$ lying above $\mathfrak{p}$. Let ω as before be the Teichmuller character on F_q^*. We let $\sigma_c = \sigma_{c,1}$.

Theorem 2.2. *We have the factorization*

$$S(\omega^{-k}) \sim \mathfrak{P}^{(p-1)\theta(k,\mathfrak{p})} \sim \mathfrak{p}^{\theta(k,\mathfrak{p})}.$$

Proof. We have

$$\begin{aligned} \operatorname{ord}\sigma_c^{-1} P\, S(\omega^{-k}) &= \operatorname{ord}_{\mathfrak{P}} \sigma_c S(\omega^{-k}) \\ &= \operatorname{ord}_{\mathfrak{P}} S(\omega^{-kc}) \\ &= s(kc) \end{aligned}$$

by Theorem 2.1. On the other hand, the isotropy group of $\mathfrak{p}$ in the Galois group G consists of the powers

$$\{\sigma_p{}^i\} \quad \text{for} \quad i = 0, \ldots, n-1.$$

Hence in the ideal $\mathfrak{p}^{\theta(k)}$ the prime $\sigma_c^{-1}\mathfrak{p}$ occurs with multiplicity

$$\sum_{i=0}^{n-1} \left\langle \frac{kcp^i}{q-1} \right\rangle.$$

Hence to prove Theorem 2.2 it will suffice to prove:

Lemma 1. *For any integer k we have*

$$s(k) = (p-1) \sum_{i=0}^{n-1} \left\langle \frac{kp^i}{q-1} \right\rangle.$$

Proof. We may assume that $1 \leq k < q-1$ since both sides are $(q-1)$-periodic in k, and the relation is obvious for $k = 0$. Since $p^n \equiv 1 \pmod{q-1}$ we find:

$$\begin{aligned} k &= k_0 + k_1 p + \cdots + k_{n-1} p^{n-1} \\ pk &\equiv k_{n-1} + k_0 p + \cdots + k_{n-2} p^{n-1} \pmod{q-1} \\ p^2 k &\equiv k_{n-2} + k_{n-1} p + \cdots + k_{n-3} p^{n-1} \pmod{q-1} \\ &\vdots \end{aligned}$$

Hence

$$\left\langle \frac{kp^i}{q-1} \right\rangle = \frac{\text{right-hand side of } i\text{th equation}}{q-1}.$$

Summing yields

$$\sum_{i=0}^{n-1} \left\langle \frac{kp^i}{q-1} \right\rangle = \frac{s(k)(1 + p + \cdots + p^{n-1})}{q-1} = s(k) \frac{1}{p-1},$$

thereby proving the lemma.

In Theorem 2.2 we note that the Gauss sum is not necessarily an element of $\mathbf{Q}(\mu_m)$, and the equivalence of ideals is true only in the appropriate extension field. Similarly, the Stickelberger element has rational coefficients. By the same procedure, we can both obtain an element in $\mathbf{Q}(\mu_m)$ and a corresponding element in the integral group ring, as follows.

For any integers $a, b \in \mathbf{Z}$ and any real number t, we have

$$b\langle t\rangle - \langle bt\rangle \in \mathbf{Z} \quad \textit{and} \quad \langle at\rangle + \langle bt\rangle - \langle (a+b)t\rangle \in \mathbf{Z}.$$

The proof is obvious. Let us define $R = \mathbf{Z}[G]$, and

$$I = \text{ideal of } R \text{ generated by all elements } \sigma_b - b \text{ with } b \text{ prime to } m.$$

Then the above remark shows that

$$I\theta \subset R = \mathbf{Z}[G].$$

Although we won't need it, we may prove the converse for general insight. The matter is analyzed further in Chapter 2, §3.

Lemma 2. *We have $I\theta = R\theta \cap R$.*

Proof. Note that $m \in I$ because

$$m = -(\sigma_{1+m} - (1+m)).$$

Suppose that an element of $R\theta$ lies in R, that is

$$\sum z(b)\sigma_b\theta \in R$$

with $z(b) \in \mathbf{Z}$. Then

$$\sum z(b)\left\langle \frac{bc}{m} \right\rangle \in \mathbf{Z} \quad \text{for all } c$$

whence

$$\sum z(b)b \equiv 0 \pmod{m},$$

and $\sum z(b)b$ is in I. But then

$$\sum z(b)\sigma_b = \sum z(b)(\sigma_b - b) + \sum z(b)b$$

is in I, thus proving the lemma.

It will be convenient to formulate the results in terms of the powers of one character, depending on the integer m. Thus we let

$$\chi_{\mathfrak{p}} = \omega_{\mathfrak{p}}^{-(\mathbf{N}\mathfrak{p}-1)/m}$$