Stickelberger Ideal

A dissertation submitted to
Indian Institute of Science Education and Research Berhampur
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Sanyam Gupta

Indian Institute of Science Education and Research Berhampur
Transit campus (Govt. ITI Building)
Engineering School Road
Berhampur 760010 Odisha, India

May, 2022

Supervisor: Dr. Prem Prakash Pandey

© Sanyam Gupta 2022
All rights reserved

Certificate of Examination

This is to certify that the dissertation titled "Stickelberger Ideal" submitted by Mr. Sanyam Gupta (Roll No. 17089) towards the partial fulfillment of the BS-MS dual degree program of the Institute has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Prem Prakash Pandey
(Supervisor)
Dated: December 29, 2023

Committee:

Dr. Prem Prakash Pandey

Dr. Kasi Viswanadham G

Dr. Senthil Raani

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Prem Prakash Pandey at the Indian Institute of Science Education and Research Berhampur.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgment of collaborative research and discussions. This thesis is a bonafide record of original work done by me, and all sources listed within have been detailed in the bibliography.

Sanyam Gupta
(Candidate)

In my capacity as the supervisor of the candidate's project work, I confirm that the above statements of the candidate are true to the best of my knowledge.

Dr. Prem Prakash Pandey
(Supervisor)
Dated: December 29, 2023

Acknowledgements

I express my sincere gratitude to my thesis supervisor Dr. Prem Prakash Pandey for his constant motivation and help throughout the project. He helped clarify my innumerable doubts and guided me in the right direction to complete this project. His passion for mathematics and overall exuberance is contagious. It has kept me determined throughout the year and has made me look forward to a career in academia with great gusto.

I also thank Mr. Mahesh Kumar Ram and Mr. Nimish Mahapatra for several fruitful discussions and their help throughout this project. Finally, I thank my family and friends for all the support.

Abstract

This thesis is a comprehensive study of the Stickelberger theorem on annihilators of class groups of cyclotomic fields. The exposition closely follows the book of Washington [32]. The thesis is self-contained. Moreover, our perspective is to study the Stickelberger ideal in reference to many related topics and not limit ourselves to just studying these two theorems (Stickelberger and Iwasawa). Many natural questions are raised (not sure if for the first time), and some positive results on them are also reported.

Contents

Chapter 1

Introduction

The *ideal class group* $\mathrm{Cl}(K)$ of a number field K is the quotient group J_K/P_K, where J_K is the group of non-zero fractional ideals of the ring of integers of K, and P_K is its subgroup of principal ideals. The order $h(K)$ of $\mathrm{Cl}(K)$ is finite and is called *class number* of K. Let $\mathfrak{a}$ be an ideal of K, then the ideal $\mathfrak{a}^{h(k)}$ is a principal ideal. For this very reason, the class groups were introduced, though in a different language, by Kummer in his work on Fermat's last theorem. Explicit knowledge of the structure of class groups is hardly understood. Very little knowledge is known even about the class number $h(K)$, and in fact, this was the main obstacle in the way of Kummer's attack on Fermat's last Theorem.

The most attractive results about the structure of the class group of number fields in the literature are for quadratic and cyclotomic fields. Even then, the information on the class number of cyclotomic fields is far from reasonable.

For any positive integer n we denote by ζ_n, a primitive n-th root of unity. Let $K = \mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field, where m is a positive integer. We know that the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ acts on the class group $\mathrm{Cl}(K)$, the latter then naturally becomes a module over the group ring $\mathbb{Z}[G]$ (formal $\mathbb{Z}$-sums on G). Since the group structure in the class group is usually seen as multiplication (not addition), it is natural to write "scalar" $\gamma \in \mathbb{Z}[G]$ as exponents when they act on an ideal class x, not as multipliers from the left. That is, x^γ instead of γx. This extra structure of the class group (as a $\mathbb{Z}[G]$-module) offers some remedy. The Stickelberger ideal of K – as we shall see – provides one tool to convert any ideal into a principal ideal just as the class number did in Kummer's approach.

For $a \in (\mathbb{Z}/m\mathbb{Z})^*$, define $\sigma_a \in G$ as $\sigma_a : \zeta_m \mapsto \zeta_m^a$. It is well known that the map

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^* &\to G \\ a &\mapsto \sigma_a\end{aligned}$$

is a group isomorphism. Let $\mathfrak{p}$ be a prime in $\mathbb{Z}[\zeta_m]$ that is relatively prime to m. Then $\mathfrak{p}^{m\Theta}$ is a principal ideal in $\mathbb{Q}(\zeta_m)$, where

$$\Theta := \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^*} \left\{ \frac{a}{m} \right\} \sigma_a^{-1} \in \mathbb{Q}[G]$$

is the Stickelberger element of K. In other words, the ideal class of $\mathfrak{p}$ in the ideal class group is annihilated by $m\Theta$. Let $I_S := \mathbb{Z}[G] \cap \Theta\mathbb{Z}[G]$ be the Stickelberger ideal of K. Then, more generally, we have the following celebrated result of Stickelberger.

Theorem 1.1 (Stickelberger)**.** *Let I_S be the Stickelberger ideal of $\mathbb{Q}(\zeta_m)$. Then I_S annihilates the ideal class group Cl_m of $\mathbb{Q}(\zeta_m)$; in other words, for any $\gamma \in I_S$ and any fractional ideal $\mathfrak{a}$ of $\mathbb{Q}(\zeta_m)$ the ideal $\mathfrak{a}^\gamma$ is a principal ideal.*

Let $a = -1$, then σ_a sends every root of unity to its inverse; but this is the same as its complex conjugate. That is, σ_a coincides with the complex conjugation, which induces an automorphism of any normal field extension of $\mathbb{Q}$ inside $\mathbb{C}$, and which is commonly denoted by j. The fixed field of j inside K is denoted by K^+ and coincides with the intersection $K \cap \mathbb{R}$. In fact, we have $K^+ = \mathbb{Q}(\cos(2\pi/m))$. The class number $h(K^+)$ is always a divisor of $h(K)$ (see Lemma 4.4). The quotient $h(K)/h(K^+)$ is written $h(K)^-$ and is known as *minus part of the class number* or simply the minus class number.

It turns out that in the minus part, the Stickelberger ideal not only *annihilate* but also gives a very good idea of the *size* of the class group. We now explain what the minus part of a $\mathbb{Z}[G]$-module is.

For every $\mathbb{Z}[G]$-module M, we define $M^+ = \{x \in M : j \cdot x = x\}$ and $M^- = \{x \in M : j \cdot x = -x\}$. So M^+ is the kernel of multiplication by $(1-j)$ and M^- is the kernel of multiplication by $(1+j)$. We call M^+ the *plus part* of M and M^- the *minus part* of M. We can then look at the minus part $I_S^- \subset \mathbb{Z}[G]^-$ of the Stickelberger ideal I_S. The following beautiful result is due to Iwasawa [12].

Theorem 1.2 (Iwasawa)**.** *Let $K = \mathbb{Q}(\zeta_m)$ and $G = \mathrm{Gal}(K/\mathbb{Q})$; assume that $m = p^n$ is a prime power. Then $[\mathbb{Z}[G]^- : I_S^-] = h(K)^-$.*

The techniques used by Iwasawa in his proof of the above theorem are based on representations of a semi-simple algebra. There is another proof, by Skula [27], where he constructs a special basis of I_S^- and obtains Iwasawa's class number formula by calculating the determinant of the transition matrix from a certain basis of $\mathbb{Z}[G]^-$ to this basis of I_S^-. The proof presented in this thesis closely follows the beautiful exposition of Chapman [4].

A generalization of Iwasawa's theorem to arbitrary cyclotomic fields is due to Sinnott (see [25]). We will discuss this in Chapter 5. In Chapter 2 we develop the necessary background from algebra which is needed for our purposes. In Chapter 3 we study the prime ideal factorization of certain Gauss sums and prove Theorem 1.1. Chapter 4 focuses on the index of various ideals in the group ring $\mathbb{Z}[G]$ and the proof of Theorem 1.2.

Along the way, we present several natural questions related to the Stickelberger ideal. We also report some positive results on these questions.

Chapter 2

Preliminaries

In this chapter, we briefly recall some of the properties of the characters of finite abelian groups. Subsequently, we define two types of sum using these characters, called Gauss and Jacobi sums.

2.1 Characters of Finite Abelian Groups

Let G be a multiplicative **finite abelian group**, and let K be a field with the property that **the characteristic of K does not divide** $\#G$. Denote by $\overline{K}$ the algebraic closure of K.

Definition 2.1 (K-character)**.** Any group homomorphism $\chi : G \to \overline{K}^*$ is a K-character of G.

Let χ_1 and χ_2 be two K-characters of G, define their product $\chi_1\chi_2(g) := \chi_1(g)\chi_2(g)$ for all $g \in G$, then, under this multiplication, the set of all K-characters of G forms a group called the *character group* of G and is denoted by $\widehat{G}$. The identity element of $\widehat{G}$ is *trivial character* defined by $\mathbb{1}(g) = 1$ for all $g \in G$, the inverse of a character $\chi \in \widehat{G}$ is χ^{-1} defined as $\chi^{-1}(g) := \chi(g)^{-1}$.

Proposition 2.2. *The group of characters $\widehat{G}$ is isomorphic to G. In particular, there are exactly $\#G$ distinct characters.*

Proof. We use induction on $\#G$. First, assume that G is a cyclic group of finite order m. The map $\chi \mapsto \chi(g)$ is then an isomorphism of $\widehat{G}$ and the group of m-th roots of unity in $\overline{K}$. Since the characteristic of K does not divide m, the latter group is again cyclic of order m. This shows that $\widehat{G} \cong G$.

Now, let G not be cyclic. Then it is a direct sum of two non-trivial subgroups: $G = G_1 \oplus G_2$. Consider the homomorphism $\phi : \widehat{G} \to \widehat{G}_1 \times \widehat{G}_2$ defined by $\chi \mapsto (\chi|_{G_1}, \chi|_{G_2})$, and the homomorphism $\varphi : \widehat{G}_1 \times \widehat{G}_2 \to \widehat{G}$, which to each pair (χ_1, χ_2) associates the character $\chi \in \widehat{G}$ defined by $\chi(g_1 g_2) = \chi_1(g_1)\chi_2(g_2)$. It is easy to see that the two homomorphisms are inverses of each other. Hence $\widehat{G} \cong \widehat{G}_1 \oplus \widehat{G}_2$. Since, by induction, $\widehat{G}_1 \cong G_1$ and $\widehat{G}_2 \cong G_2$, we obtain $\widehat{G} \cong G$. ■

Proposition 2.3. *Let χ be a character of G. If $\chi \neq \mathbb{1}$, then $\sum_g \chi(g) = 0$, where the sum is over all $g \in G$. If $\chi = \mathbb{1}$, the value of the sum is $\#G$.*

Proof. Since $\chi \neq \mathbb{1}$, there exists $g \in G$ such that $\chi(g) \neq 1$. We obtain

$$\chi(g) \sum_{h \in G} \chi(h) = \sum_{h \in G} \chi(gh) = \sum_{h \in G} \chi(h).$$

Since $\chi(g) \neq 1$, we must have $\sum_{h \in G} \chi(h) = 0$. ■

Denote by $\overline{K}^G$ the $\overline{K}$-vector space of $\overline{K}$-valued functions on G. Let $e_g \in \overline{K}^G$ be defined as

$$e_g(h) = \begin{cases} 1 & h = g \\ 0 & h \neq g \end{cases},$$

then it is easy to see that $\{e_g\}_{g \in G}$ is a linearly independent subset of $\overline{K}^G$. Furthermore, any $f \in \overline{K}^G$ can be written as

$$f = \sum_{g \in G} f(g) e_g,$$

thus $\{e_g\}_{g \in G}$ is a basis of $\overline{K}^G$ and the dimension of $\overline{K}^G$ is $\#G$. It is a well-known fact that the K-characters of G form a linearly independent subset of $\overline{K}^G$. This statement is usually attributed to E. Artin (see [2, p. 34]).

Proposition 2.4 (E. Artin)**.** *Let $\chi_1, \chi_2, \ldots, \chi_n$ be distinct K-characters of G. They are linearly independent over $\overline{K}$.*

Proof. We use induction on n. The case $n = 1$ is trivial. Suppose $n > 1$. We make the inductive hypothesis that no set of less than n distinct characters is dependent. Suppose now that

$$a_1 \chi_1(g) + a_2 \chi_2(g) + \cdots + a_n \chi_n(g) = 0 \tag{2.1}$$

for some coefficients $a_i \in \overline{K}$ and every $g \in G$. We want to show that all a_i are 0.

Since $\chi_1 \neq \chi_n$, for some $g_0 \in G$ we have $\chi_1(g_0) \neq \chi_n(g_0)$. Substitute $g_0 g$ in place of g in Equation (2.1):

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \cdots + a_n\chi_n(g_0)\chi_n(g) = 0 \tag{2.2}$$

for all $g \in G$. Now multiply Equation (2.1) by $\chi_n(g_0)$:

$$a_1\chi_n(g_0)\chi_1(g) + a_2\chi_n(g_0)\chi_2(g) + \cdots + a_n\chi_n(g_0)\chi_n(g) = 0 \tag{2.3}$$

for all $g \in G$. Subtracting Equation (2.3) from Equation (2.2), the last terms cancel:

$$a_1(\chi_1(g_0) - \chi_n(g_0))\chi_1(g) + \cdots + a_n(\chi_{n-1}(g_0) - \chi_n(g_0))\chi_{n-1}(g) = 0 \tag{2.4}$$

for all $g \in G$. This is a linear dependence relation among the characters $\chi_1, \chi_2, \ldots, \chi_{n-1}$, so by induction, all coefficients $a_i(\chi_i(g_0) - \chi_n(g_0))$ are 0. In particular, $a_1(\chi_1(g_0) - \chi_n(g_0)) = 0$. Since $\chi_1(g_0) \neq \chi_n(g_0)$ we must have $a_1 = 0$. By arguing in a similar way using $\chi_2, \ldots, \chi_{n-1}$ in place of χ_1, we obtain $a_i = 0$ for $i = 1, \ldots, n-1$. Therefore, Equation (2.1) becomes $a_n\chi_n(g) = 0$ for all $g \in G$, so $a_n = 0$ since χ_n has non-zero values. ■

Proposition 2.4 along with Proposition 2.2 implies that the characters of G form a basis of the space $\overline{K}^G$ of $\overline{K}$-valued functions on G.

Proposition 2.5. *Let G be a finite abelian group and K be a field of characteristic not dividing $\#G$. Then the K-characters of the group G form a $\overline{K}$-basis of the vector space $\overline{K}^G$. In particular, the $\#G \times \#G$ matrix $[\chi(g)]_{\substack{\chi \in \widehat{G} \\ g \in G}}$ is non-degenerate.*

Proof. We have already given a proof of the first statement. For the second statement, we note that if $\chi \in \widehat{G}$, then

$$\chi = \sum_{g \in G} \chi(g) e_g,$$

thus the matrix $[\chi(g)]_{\substack{\chi \in \widehat{G} \\ g \in G}}$ is a matrix of base change from $\{e_g\}_{g \in G}$ to $\{\chi\}_{\chi \in \widehat{G}}$, therefore it is non-degenerate. ■

For a character $\chi \in \widehat{G}$, we denote by K_χ the extension of K generated by the values of χ. More specifically, K_χ is the d-th cyclotomic extension of K, where d is the order of χ. In particular, K_χ is a Galois extension of K.

Suppose $\sigma \in \mathrm{Gal}(K_\chi/K)$, then $\sigma \circ \chi$ is also a K-character of G. We say that two characters

$\chi, \chi' \in \widehat{G}$ are conjugates (over K) if $K_\chi = K_{\chi'}$ and there exists $\sigma \in \mathrm{Gal}(K_\chi/K)$ such that $\chi' = \sigma \circ \chi$. It is clear that the conjugacy relation is an equivalence relation on $\widehat{G}$, and that the equivalence class of $\chi \in \widehat{G}$ contains exactly $[K_\chi : K]$ elements. Let us denote the set of representatives of the equivalence classes by M, then we have the following equality

$$\sum_{\chi \in M} [K_\chi : K] = \#G.$$

Note 1. This conjugacy relation between the characters of G is not the same as the usual definition of conjugate elements in a group. Throughout this thesis, we mean the above definition of the conjugacy relation between characters of G.

2.2 Dirichlet Characters

Let n be a positive integer. A *Dirichlet character modulo n* is a $\mathbb{C}$-character of the abelian group $(\mathbb{Z}/n\mathbb{Z})^*$, i.e., a multiplicative homomorphism

$$\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*.$$

We call n the *modulus* of χ.

Example 2.1.
- Let p be an odd prime, and let $\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*$ be the Legendre symbol modulo p, that is, $\chi(a) = \left(\frac{a}{p}\right)$.
- Let $i = \sqrt{-1}$, and define $\chi : (\mathbb{Z}/5\mathbb{Z})^* \to \mathbb{C}^*$ by $\chi(1) = 1$, $\chi(2) = i$, $\chi(3) = -i$, $\chi(4) = -1$.

If χ is a Dirichlet character of modulus n and $n|m$, then using the natural homomorphism $\varphi : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$, we can define $\chi' = \chi \circ \varphi$. Now χ' is also a Diriclet character, but of modulus m. In this situation, we say that χ' is induced by χ.

Let f_χ be the minimal modulus for the Dirichlet character χ, that is, χ is not induced by any Dirichlet character of modulus smaller than f_χ. Call f_χ the *conductor* of χ. A Dirichlet character defined modulo its conductor is called *primitive*.

Example 2.2.
- Let $\chi : (\mathbb{Z}/12\mathbb{Z})^* \to \mathbb{C}^*$ be given by $\chi(1) = 1, \chi(5) = -1, \chi(7) = 1, \chi(11) = -1$. Since $\chi(a + 3k) = \chi(a)$ we see that χ is induced by the character $\psi : (\mathbb{Z}/3\mathbb{Z})^* \to \mathbb{C}^*$, where $\psi(1) = 1$, $\psi(2) = -1$. Furthermore, ψ is primitive. We conclude that $f_\chi = 3$.

- Let $\chi : (\mathbb{Z}/12\mathbb{Z})^* \to \mathbb{C}^*$ be given by $\chi(1) = 1$, $\chi(5) = -1, \chi(7) = -1, \chi(11) = 1$. It is easy to check that χ is primitive, whence $f_\chi = 12$.

A Dirichlet character χ also may be regarded as a function $\chi : \mathbb{Z} \to \mathbb{C}$ by letting

$$\chi(a) = \begin{cases} \chi(a \mod f_\chi) & \text{if } (a, f_\chi) = 1 \\ 0 & \text{if } (a, f_\chi) \neq 1. \end{cases}$$

We also refer to this periodic funtion on $\mathbb{Z}$ as a Dirichlet character, and we do not distinguish notationally between a Dirichlet character as a function on $(\mathbb{Z}/f_\chi\mathbb{Z})^*$ and the periodic function on $\mathbb{Z}$ associated to it.

2.3 Group Rings

Definition 2.6. Let G be a finite group and R be a commutative ring with unity. The *group ring* of G over R, which we denote by $R[G]$, is the set of all formal R-linear combinations of the elements of G:

$$R[G] := \left\{ \sum_{g \in G} a_g g : a_g \in R \right\}.$$

We define the addition and multiplication on $R[G]$ in the obvious way:

$$\sum_g a_g g + \sum_g b_g g = \sum_g (a_g + b_g) g,$$

$$\sum_g a_g g \cdot \sum_{g'} b_{g'} g' = \sum_{h \in G} \left(\sum_{gg'=h} a_g b_{g'} \right) h.$$

It is easy to see that $R[G]$ is a commutative ring with these operations. The unity of the group ring $R[G]$ is the identity element e of G. This suggests the following convention: *in the group ring, we identify e and* 1, where 1 is the unity of R.

In this thesis, the group G is usually abelian, and R is either the ring of integers $\mathbb{Z}$ or a field.

2.3.1 The Group Ring $\mathbb{Z}[G]$

Let G be a finite abelian group, then $\mathbb{Z}[G]$ is the group ring of G over $\mathbb{Z}$. If A is an abelian group (written multiplicatively, say) on which the group G acts, then the abelian group A

is called a G-module. Since G acts on A, the latter naturally becomes a module over the group ring $\mathbb{Z}[G]$ through the following formula

$$\left(\sum_{g\in G} a_g g\right)\cdot v = \prod_{g\in G}(g\cdot v)^{a_g}, \quad v\in A.$$

If $\theta = \sum_{g\in G} a_g g$, then it is customary to write v^θ instead of $\theta\cdot v$, so that the formula $\theta_1\cdot(\theta_2\cdot v) = (\theta_1\theta_2)\cdot v$ translates into the identity $v^{\theta_1\theta_2} = (v^{\theta_1})^{\theta_2}$, where it is essential that G be an abelian group.

Let E be an abelian extension of $\mathbb{Q}$ with the Galois group G. Then we have various G-modules (called in this case *Galois modules*): the *additive group* E, the *multiplicative group* $E^\times$, the *group of units* U_E, the *class group* $\mathrm{Cl}(E)$, etc. In this thesis, we focus on $\mathrm{Cl}(E)$ as a Galois module.

2.3.2 The Group Algebra $K[G]$

Let G be a finite abelian group and K be a field of characteristic not dividing $\#G$. The group ring $K[G]$ is called the *group algebra* of G over K. It is easy to see that $K[G]$ is the free vector space over the field K of dimension $\#G$. We can extend the K-characters of G linearly to $K[G]$: given $\chi\in\widehat{G}$, we define the map $K[G]\to K_\chi$ by

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g\chi(g).$$

Clearly, this map is a ring homomorphism. We denote this ring homomorphism by χ, and call it a character of $K[G]$. The set of all characters of $K[G]$ will again be denoted by $\widehat{G}$.

Fix an ordering of G, say $G=\{g_1,g_2,\ldots,g_n\}$, then $x=\sum_{i=1}^n a_i g_i\in K[G]$ can be written as a column vector:

$$x = [a_1,a_2,\ldots,a_n]^t.$$

Proposition 2.7. *If $x\in K[G]$ satisfies $\chi(x)=0$ for all $\chi\in\widehat{G}$, then $x=0$.*

Proof. Let $A=[\chi(g)]_{\substack{\chi\in\widehat{G}\\ g\in G}}$, then $Ax=[\chi(x)]^t_{\chi\in\widehat{G}}$. Recall from Proposition 2.5 that A is not degenerate. Thus, $Ax=0$ cannot have a non-trivial solution. ∎

2.3.3 The Weight Function and the Norm Element

In this section we recall the most basic notions about the group rings. Let G be a finite abelian group and R be a commutative ring with unity. We define *weight function* $w : R[G] \to R$ by

$$w\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g.$$

It is easy to verify that the weight function is additive and multiplicative.

Proposition 2.8. *For any $x, y \in R[G]$*

$$w(x+y) = w(x) + w(y), \quad w(xy) = w(x)w(y).$$

Thus, the weight function is a ring homomorphism. Its kernel, consisting of elements of weight 0 is called the *augmentation ideal* of the group ring $R[G]$.

The *norm element* of $R[G]$ is

$$N = \sum_{g\in G} g.$$

It is obvious that $xN = Nx = x$ for any $x \in G$. Extending this by linearity, we obtain the following property.

Proposition 2.9. *For any $x \in R[G]$ we have $xN = Nx = w(x)N$. In particular, $R[G]N = NR[G] = RN$.*

The ideal RN is called the *norm ideal* of the group ring $R[G]$. If the cardinality $\#G$ is an invertible element of R (which is, in particular, the case if R is a field of characteristic not dividing $\#G$) the, writing each $x \in R[G]$ as $x - w(x)\#G^{-1}N + w(x)\#G^{-1}N$, we obtain the following.

Proposition 2.10. *Assume that $\#G$ is an invertible element of R. Then $R[G]$ is the direct sum of its augmentation ideal and its norm ideal.*

2.3.4 Semi-smiplicity of the Group Ring

Definition 2.11. A commutative ring is semi-simple if it is isomorphic to a direct product of finitely many fields.

It is remarkably easy to describe the ideals of a semisimple ring. Let R be a semi-simple ring and write it as a direct product of finitely many fields: $R = K_1 \times K_2 \times \cdots \times K_s$. Let

$\Lambda = \{1, 2, \ldots, s\}$. For $\lambda \in \Lambda$, denote by $1_\lambda = (x_1, \ldots, x_s) \in R$, such that $x_\lambda = 1$ and $x_\mu = 0$ for $\mu \neq \lambda$. The following result completely describes the ideals of a semi-simple ring R.

Proposition 2.12. *Let $R = K_1 \times K_2 \times \cdots \times K_s$ be a semi-simple ring.*

1. *For $\Lambda' \subseteq \Lambda$, let $I_{\Lambda'}$ consist of $x = (x_1, \ldots, x_s) \in R$ such that $x_\lambda = 0$ for all $\lambda \notin \Lambda'$. Then $I_{\Lambda'}$ is an ideal of R. Conversely, any ideal of R is equal to $I_{\Lambda'}$ for some $\Lambda' \subseteq \Lambda$.*
2. *The ideal $I_{\Lambda'}$ is principal; it is generated by the element*

$$1_{\Lambda'} = \sum_{\lambda \in \Lambda'} 1_\lambda .$$

The proof of the above proposition is elementary, and we omit it.

In this thesis, our goal is to study the ideals of $\mathbb{Q}[G]$ and $\mathbb{C}[G]$. It turns out that the group algebra $K[G]$ is semi-simple.

Theorem 2.13 (The Abelian Maschke Theorem)**.** *Let G be a finite abelian group and K be a field of characteristic not dividing $\#G$. Choose a system $M = \{\chi_1, \chi_2, \ldots, \chi_s\}$ of representatives of conjugacy classes of characters of G. Then the ring homomorphism*

$$\begin{aligned} \phi : K[G] &\to \prod_{i=1}^{s} K_{\chi_i} \\ x &\mapsto (\chi_i(x)), \end{aligned}$$

is an isomorphism. In particular, the ring $K[G]$ is semi-simple.

Proof. First, note that ϕ is also a linear map from $K[G]$ to $\prod_{\chi \in M} K_\chi$ and that the ring homomorphism ϕ is an isomorphism if and only if the linear map ϕ is a linear isomorphism. Let x be in the kernel of ϕ, that is, $\chi(x) = 0$ for any character $\chi \in M$. Since conjugate characters vanish simultaneously at x, we obtain $\chi(x) = 0$ for all $\chi \in \widehat{G}$. Proposition 2.7 implies that $x = 0$. Hence, ϕ is a monomorphism. Since

$$\sum_{i=1}^{s} [K_{\chi_i} : K] = \#G,$$

the K-dimensions of $K[G]$ and $\prod_{i=1}^{s} K_{\chi_i}$ are equal. Therefore, we have an isomorphism. ■

Let I be an ideal of $K[G]$, and $\Lambda = \{1, 2, \ldots, s\}$. The image $\phi(I)$ of the ideal I under ϕ is

an ideal of $\prod_{i=1}^{s} K_{\chi_i}$. From Proposition 2.12, we have

$$\phi(I) = \{(x_i) \in \prod_{i=1}^{s} K_{\chi_i} : x_i = 0 \; \forall \; i \notin \Lambda'\}$$

for some $\Lambda' \subseteq \Lambda$. Thus,

$$I = \{x \in K[G] : \chi_i(x) = 0 \; \forall \; i \notin \Lambda'\},$$

that is, I is the common kernel of characters $\{\chi_i\}_{\Lambda'}$. The ideals of $K[G]$ can be characterized as common kernels of characters from the set M: for a subset N of M let I_N be the common kernel of characters from the complement $M \setminus N$. Then I_N is an ideal of $K[G]$, and any ideal of $K[G]$ is equal to I_N for some $N \subseteq M$. The ideal I_N is isomorphic, as a K-vector space, $\prod_{\chi \in N} K_\chi$. Thus,

$$\dim_K I_N = \sum_{\chi \in N} [K_\chi : K]. \tag{2.5}$$

Furthermore, if $\alpha \in K[G]$ then the principal ideal (α) is equal to I_N, where N consists of characters $\chi \in M$ non-vanishing at α. Therefore,

$$\dim_K(\alpha) = \sum_{\chi(\alpha) \neq 0} [K_\chi : K]. \tag{2.6}$$

Since conjugate characters vanish at α simultaneously and since for every χ there are exactly $[K_\chi : K]$ characters conjugate to χ, the above equality becomes

$$\dim_K(\alpha) = \sum_{\substack{\chi(\alpha) \neq 0 \\ \chi \in \widehat{G}}} 1. \tag{2.7}$$

That is, the K-dimension of the principal ideal (α) is equal to the number of characters $\chi \in \widehat{G}$ non-vanishing at α.

2.4 Idempotents

Retaining the notation of previous sections, we now give an explicit K-basis of I_N as a K-vector space and an explicit generator of I_N as a principal ideal. We achieve this under

an additional assumption,

$$K \text{ contains } \#G\text{-roots of unity.} \tag{2.8}$$

Assumption (2.8) implies that $K_\chi = K$ for all characters χ, or equivalently, every character is conjugate only to itself. Thus, the isomorphism in Theorem 2.13 gives

$$\phi : K[G] \to K^{\#G}.$$

Definition 2.14. Let χ be a character of G, set

$$\varepsilon_\chi := \frac{1}{\#G} \sum_{g \in G} \chi(g) g^{-1} \in K[G],$$

called the *idempotent* of χ.

The idempotents of characters have many remarkable properties; here we list a few of them.

Proposition 2.15. *1. For any characters χ and χ' we have*

$$\chi'(\varepsilon_\chi) = \begin{cases} 1 & \text{if } \chi = \chi', \\ 0 & \text{if } \chi \neq \chi'. \end{cases}$$

2. For any $x \in K[G]$ we have $x\varepsilon_\chi = \chi(x)\varepsilon_\chi$.

3. For any character χ we have $\varepsilon_\chi^2 = \varepsilon_\chi$.

4. We have

$$\sum_\chi \varepsilon_\chi = 1.$$

Proof. We have

$$\chi'(\varepsilon_\chi) = \frac{1}{\#G} \sum_{g \in G} \chi(g)\chi'(g)^{-1} = \begin{cases} 1 & \text{if } \chi = \chi', \\ 0 & \text{if } \chi \neq \chi'. \end{cases}$$

We get the last equality by applying Theorem 2.3 to $\chi(\chi')^{-1}$.

Let $x \in G$, then

$$\begin{aligned} x\varepsilon_\chi &= \frac{1}{\#G}\sum_{g\in G}\chi(g)xg^{-1} \\ &= \chi(x)\frac{1}{\#G}\sum_{g\in G}\chi(gx^{-1})(gx^{-1})^{-1} \\ &= \chi(x)\varepsilon_\chi \end{aligned}$$

by linearity, it extends to $x \in K[G]$, which proves Part 2. Parts 1 and 2 immediately imply Part 3. For Part 4, we have

$$\sum_\chi \varepsilon_\chi = \frac{1}{\#G}\sum_{g\in G} g^{-1}\sum_\chi \chi(g),$$

by Theorem 2.3 the inner sum vanishes except if $g = 1$, in which case it equals $\#G$, which proves Part 4. ■

Example 2.3. The idempotent of the trivial character is $\frac{1}{\#G}N$, where $N = \sum_{g\in G} g$ is the norm element of G.

Proposition 2.16. *$B = \{\varepsilon_\chi\}_\chi$ is a K-basis of $K[G]$. Furthermore, $B_N = \{\varepsilon_\chi\}_{\chi\in N}$ is a K-basis of I_N.*

Proof. Let $\alpha \in K[G]$, then

$$\sum_\chi \chi(\alpha)\varepsilon_\chi = \sum_\chi \alpha\varepsilon_\chi = \alpha\sum_\chi \varepsilon_\chi = \alpha.$$

Moreover if $\sum_\chi a_\chi\varepsilon_\chi = 0$, then using Part 1 of Proposition 2.15 we have $\chi'(\sum_\chi a_\chi\varepsilon_\chi) = a_{\chi'} = 0$, which implies that $\{\varepsilon_\chi\}_\chi$ is linearly independent. Thus, B is a basis for $K[G]$.

Recall, $I_N = \{x \in K[G] : \chi(x) = 0\ \forall\ \chi \in \widehat{G}\setminus N\}$. Let $\alpha = \sum_{\chi\in\widehat{G}} a_\chi\varepsilon_\chi \in I_N$, since $\chi(\alpha) = 0$ for all $\chi \in \widehat{G}\setminus N$, we have $a_\chi = 0$ for all $\chi \in \widehat{G}\setminus N$. Again, using Part 1 of Proposition 2.15 we conclude that $\{\varepsilon_\chi\}_{\chi\in N}$ is linearly independent. ■

2.5 Gauss Sums

In this section, by a character of a finite abelian group G we mean a $\mathbb{C}$-character, that is, a homomorphism $G \to \mathbb{C}^*$.

Let p be a prime and $q = p^n$ for some positive integer n. Let $\mathbb{F}_q$ be the finite field with q elements, so that $\mathbb{F}_q$ is a finite extension of $\mathbb{F}_p$ (finite field with p elements) of degree n.

Lemma 2.17. *The trace map* $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ *is a surjective homomorphism.*

Proof. We know that $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is a finite cyclic group of order n generated by the Frobenius element $\sigma : \alpha \mapsto \alpha^p$. Thus, the trace of $x \in \mathbb{F}_q$ is

$$\mathrm{Tr}(x) = x + \sigma(x) + \cdots + \sigma^{n-1}(x) = x + x^p + \cdots + x^{p^{n-1}},$$

this polynomial is of degree $p^{n-1} < p^n = |\mathbb{F}_q|$, hence there is $\alpha \in \mathbb{F}_q$ such that $\mathrm{Tr}(\alpha) \neq 0$, which implies that Tr is surjective. ■

Let ζ_p be a primitive p-th root of unity. We use the trace map to define an *additive* character $\psi : \mathbb{F}_q \to \mathbb{C}^*$ as $\psi(a) = \zeta_p^{\mathrm{Tr}(a)}$. Since Tr is surjective, there exists $a \in \mathbb{F}_q$ such that $\psi(a) \neq 1$, thus ψ is a non-trivial character. Let $\widehat{\mathbb{F}_q^*}$ be the group of characters on $\mathbb{F}_q^*$. We extend $\chi \in \widehat{\mathbb{F}_q^*}$ to $\mathbb{F}_q$ by defining $\chi(0) = 0$ and the function $\chi : \mathbb{F}_q \to \mathbb{C}$ thus obtained will be referred as *multiplicative* character on $\mathbb{F}_q$.

Definition 2.18. Let χ be a character on $\mathbb{F}_q$. Set

$$g(\chi) := -\sum_{a \in \mathbb{F}_q} \chi(a)\psi(a),$$

where the sum is over all a in $\mathbb{F}_q$. The sum $g(\chi)$ is called a *Gauss sum* on $\mathbb{F}_q$ belonging to the character χ.

Gauss sums are essential arithmetical objects; they are indispensable in analytic number theory, algebraic number theory, arithmetic geometry, cryptography, etc. However, we use Gauss sums merely as a tool for proving Stickelberger's theorem. In this section, we list all the properties of Gauss sums required for this purpose.

Proposition 2.19. *Let* χ *be a character of G, and* $\overline{\chi} = \chi^{-1}$. *Then*

1. $g(\mathbb{1}) = 1$;
2. $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$;
3. *if* $\chi \neq \mathbb{1}$, $g(\chi)g(\overline{\chi}) = \chi(-1)q$;
4. *if* $\chi \neq \mathbb{1}$, $g(\chi)\overline{g(\chi)} = q$.

Proof. Since ψ is non-trivial, $-g(\mathbb{1}) = \sum_{a\in\mathbb{F}_q} \psi(a) = 0$ (by Proposition 2.3). To prove (2), we observe that $\overline{\psi(a)} = \psi(-a)$, so that

$$\begin{aligned}\chi(-1)\overline{g(\chi)} &= -\sum \chi(-1)\overline{\chi}(a)\psi(-a)\\ &= -\sum \overline{\chi}(-1)\overline{\chi}(a)\psi(-a)\\ &= -\sum \overline{\chi}(-a)\psi(-a)\\ &= g(\overline{\chi}).\end{aligned}$$

Notice that (3) follows from (2) and (4). To prove (4) consider the following:

$$\begin{aligned}g(\chi)\overline{g(\chi)} &= \sum_{a,b\neq 0} \chi(a)\overline{\chi(b)}\psi(a)\psi(-b)\\ &= \sum_{a,b\neq 0} \chi(ab^{-1})\psi(a-b)\\ &= \sum_{b,c\neq 0} \chi(c)\psi(b(c-1)).\end{aligned}$$

Substituting $a = bc$ gives

$$\begin{aligned}g(\chi)\overline{g(\chi)} &= \sum_{b\neq 0} \chi(1)\psi(0) + \sum_{c\neq 0,1} \chi(c)\sum_{b\neq 0} \psi(b(c-1))\\ &= q-1+\sum_{c\neq 0,1} \chi(c)\sum_{b\neq 0} \psi(b(c-1)).\end{aligned}$$

For $c \neq 1$, we have $\sum_{b\neq 0} \psi(b(c-1)) = -1$, therefore,

$$g(\chi)\overline{g(\chi)} = q-1+(-1)(-1) = q.$$

■

2.6 Multiplicative Combinations of Gauss Sums

Let χ be a character of order dividing m, then $g(\chi)$ is an algebraic integer in $\mathbb{Q}(\zeta_p, \zeta_m)$. However, remarkably, certain simple multiplicative combinations of several Gauss sums lies in a much smaller field.

Definition 2.20. Let χ and λ be two multiplicative characters of $\mathbb{F}_q$ and set

$$J(\chi,\lambda) = -\sum_{\substack{a+b=1\\ a,b\in\mathbb{F}_q}} \chi(a)\lambda(b) = -\sum_{a\in\mathbb{F}_q} \chi(a)\lambda(1-a).$$

The sum $J(\chi,\lambda)$ is called a *Jacobi sum*.

Note that if χ and λ have orders dividing m then $J(\chi,\lambda)$ is an algebraic integer in $\mathbb{Q}(\zeta_m)$. See Weil [34] and [35] for amazing properties of Gauss sums and Jacobi sums. Here are some such properties:

Proposition 2.21. *Let χ and λ be non-trivial characetrs. Then*

1. $J(\mathbb{1},\mathbb{1}) = 2-q$;
2. $J(\mathbb{1},\chi) = J(\chi,\mathbb{1}) = 1$ *if* $\chi \neq \mathbb{1}$;
3. $J(\chi,\overline{\chi}) = \chi(-1)$ *if* $\chi \neq \mathbb{1}$;
4. *If* $\chi\lambda \neq \mathbb{1}$, *then*
$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Proof. Part (1) is immediate and part (2) is an immediate consequence of Proposition 2.3. To prove Part (3) and (4) we compute

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_{a,b} \chi(a)\lambda(b)\psi(a+b) \\ &= \sum_{a,b} \chi(a)\lambda(b-a)\psi(b) \\ &= \sum_{\substack{a,b\\ b\neq 0}} \chi(a)\lambda(b-a)\psi(b) + \sum_{a} \chi(a)\lambda(-a). \end{aligned}$$

If $\chi\lambda \neq \mathbb{1}$, then the second sum vanishes (by Orthogonality relations). If $\chi\lambda = \mathbb{1}$, then it equals $\chi(-1)(q-1)$. The first sum equals (let $a = bc$)

$$\sum_{\substack{b,c\\ b\neq 0}} \chi(b)\lambda(b)\chi(c)\lambda(1-c)\psi(b) = g(\chi\lambda)J(\chi,\lambda).$$

If $\chi\lambda \neq \mathbb{1}$, we obtain Part (4). If $\chi\lambda = \mathbb{1}$, use Part(2) of Proposition 2.19, along with $g(\mathbb{1}) = 1$, to obatin Part (3). This completes the proof. ■

Corollary 2.22. *If χ, λ are characters of orders dividing m, then*

$$\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$

is an algebraic integer in $\mathbb{Q}(\zeta_m)$.

Proof. If $\chi\lambda \neq \mathbb{1}$ then use proposition 2.21(4). The other cases are also easy to check. ■

For any b coprime to m define $\sigma_b \in \mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_m)/\mathbb{Q})$ by

$$\sigma_b : \zeta_p \mapsto \zeta_p, \quad \zeta_m \mapsto \zeta_m^b.$$

Proposition 2.23. *Assume $\chi^m = \mathbb{1}$. Then for any b coprime to m the number*

$$g(\chi)^{b-\sigma_b} := \frac{g(\chi)^b}{g(\chi)^{\sigma_b}}$$

is an algebriac integer in $\mathbb{Q}(\zeta_m)$. In particular, $g(\chi)^m \in \mathbb{Q}(\zeta_m)$.

Proof. We observe that

$$\begin{aligned} g(\chi)^{\sigma_b} &= -\sum_{a\in\mathbb{F}} \sigma_b(\chi(a))\sigma_b(\psi(a)) \\ &= -\sum_{a\in\mathbb{F}} \chi(a)^b\psi(a) = g(\chi^b). \end{aligned}$$

Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_m)/\mathbb{Q}(\zeta_m))$ such that $\tau : \zeta_p \mapsto \zeta_p^c$ for some $p \nmid c$. Then

$$\begin{aligned} g(\chi)^\tau &= -\sum_{a\in\mathbb{F}} \chi(a)\psi(ac) \\ &= -\chi(c)^{-1}\sum_{a\in\mathbb{F}} \chi(a)\psi(a) = \chi(c)^{-1}g(\chi). \end{aligned}$$

Similarly, $g(\chi^b)^\tau = \chi(c)^{-b}g(\chi^b)$, hence

$$\tau\left(\frac{g(\chi)^b}{g(\chi^b)}\right) = \frac{(g(\chi)^\tau)^b}{g(\chi^b)^\tau} = \frac{\chi(c)^{-b}g(\chi)^b}{\chi(c)^{-b}g(\chi^b)} = \frac{g(\chi)^b}{g(\chi^b)}.$$

Since $\frac{g(\chi)^b}{g(\chi^b)}$ is an algebraic integer (from Corollary 2.22), the first claim follows. To prove

the second claim take $b = 1 + m$. ■

Proposition 2.24. $g(\chi^p) = g(\chi)$.

Proof. Let $a \in \mathbb{F}$, and σ be the Frobenius, then

$$\mathrm{Tr}(a) = a + \sigma(a) + \cdots + \sigma^{n-1}(a).$$

Since, $\mathrm{Tr}(a) \in \mathbb{F}_p$, by *Fermat's little theorem* we have $\mathrm{Tr}(a)^p = \mathrm{Tr}(a)$, but

$$\mathrm{Tr}(a)^p \equiv a^p + \sigma(a)^p + \cdots + \sigma^{n-1}(a)^p \equiv \mathrm{Tr}(a^p) \pmod{p}.$$

As a result, we have $\mathrm{Tr}(a^p) = \mathrm{Tr}(a)$. Finally putting everything together

$$g(\chi^p) = -\sum \chi(a^p)\zeta_p^{\mathrm{Tr}(a)} = -\sum \chi(a^p)\zeta_p^{\mathrm{Tr}(a^p)} = g(\chi).$$

■

2.7 Historical Remarks on Gauss and Jacobi Sums

Gauss sums over $\mathbb{F}_p$ were introduced by Lagrange and Vandermonde [5] for the purpose of solving algebraic equations and for this reason they were called *Lagrange resolvants* for a long time. Gauss used these sums in [8, Art. 356], and determined the sign of the quadratic Gauss sum in [7]. The above mentioned properties of Gauss and Jacobi sums can be found in his posthumously published [6, pg. 252]. These properties were also known to Cauchy, Jacobi, and Eisenstein.

Stickelberger [29] studied Gauss and Jacobi sums over arbitrary finite fields – we will discuss his results in detail in Chapter 2. In fact, Stickelberger was the first to suggest the minus sign in the definition of Gauss sums; in [29], he writes on pg. 358:

> besser noch ware es vielleicht, sowohl die gewöhnliche wie unsere allgemeine Resolvente mit -1 zu multiplizieren.[1]

For more information about Gauss and Jacobi sums as well as on related sums see the book of Lidl and Niederreiter [19], and the book of Ireland and Rosen [11].

[1] perhaps it would be even better if we multiplied both the usual as well as our general resolvent by -1.

There is an analogy (first noticed by Jacobi) between Gauss and Jacobi sums on one hand, and the Gamma and Beta functions on the other hand;

$$-g(\chi) = \sum_{a\in\mathbb{F}_q} \chi(a)\psi(a) \qquad \Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$$

$$-J(\chi,\lambda) = -\sum_{a\in\mathbb{F}_q} \chi(a)\lambda(1-a) \qquad B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}dt$$

$$g(\chi)g(\lambda) = g(\chi\lambda)J(\chi,\lambda) \qquad \Gamma(x)\Gamma(y) = \Gamma(x+y)B(x,y)$$

$$g(\chi)g(\overline{\chi}) = \chi(-1)q \qquad \Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin\pi x}$$

As we have seen earlier, the relations on the left side are valid if the occuring characters are $\neq \mathbb{1}$, whereas those on the right side make sense only if you stay away from the pole $x = 0$ of the Γ-function.

Finally we mention that Gauss sums have been generalized in various directions: Weber [33] and Jordan [14] considered Gauss sums in many variables, Thakur [31] defined Gauss sums to function fields of one variable over a finite field.

Chapter 3

Stickelberger Ideal

In this chapter, we define the Stickelberger ideal of an abelian number field E and show that it annihilates the ideal class group E. We use, in a fundamental way, the prime ideal decomposition of Gauss sums and some additional machinery.

3.1 Notation and Setup

Let m be a positive integer that is fixed throughout this chapter (unless mentioned otherwise). Let p be a rational prime *relatively prime* to m. Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{m}$. For any positive integer n we denote by ζ_n a primitive n-th root of unity. Putting $q = p^f$, we have the following diagram of the number fields and primes.

$$\begin{array}{cc} \mathbb{Q}(\zeta_{q-1},\zeta_p) & \mathfrak{P}_1^{p-1}\cdots\mathfrak{P}_g^{p-1} \\ | & | \\ \mathbb{Q}(\zeta_{q-1}) & \mathfrak{q}_1\cdots\mathfrak{q}_g \\ | & | \\ \mathbb{Q} & p \end{array}$$

Where the integral prime p splits into $g = \frac{\phi(q-1)}{f}$ many distinct prime ideals $\mathfrak{q}_1,\ldots,\mathfrak{q}_g$ of $\mathbb{Q}(\zeta_{q-1})$. We know that the primes $\mathfrak{q}_i$ do not split in $\mathbb{Q}(\zeta_{q-1},\zeta_p)$, so let $\mathfrak{P}_i$ be the unique prime of $\mathbb{Q}(\zeta_{q-1},\zeta_p)$ above $\mathfrak{q}_i$.

We fix a prime $\mathfrak{q}$ in $\mathbb{Q}(\zeta_{q-1})$ above p and let $\mathfrak{P}$ be its corresponding prime in $\mathbb{Q}(\zeta_{q-1},\zeta_p)$. The inertia degree of $\mathfrak{q}$ is f, therefore, we shall denote the residue field $\mathbb{Z}[\zeta_{q-1}]/\mathfrak{q}$ by $\mathbb{F}_q$.

We shall now define a character of $\mathbb{F}_q^*$ that is uniquely determined by $\mathfrak{q}$.

Proposition 3.1. *Denote by $\mu_{q-1} \subset \mathbb{Z}[\zeta_{q-1}]$ the group of $(q-1)$-th roots of unity in $\mathbb{Q}(\zeta_{q-1})$. Then the map*

$$u: \ \mu_{q-1} \to \mathbb{F}_q^*; \quad x \mapsto x \pmod{\mathfrak{q}}$$

is a group isomorphism.

Proof. Let $x, y \in \mu_{q-1}$, then

$$u(xy) = xy \mod \mathfrak{q} = (x \mod \mathfrak{q})(y \mod \mathfrak{q}) = u(x)u(y),$$

implies that u is a group homomorphism.

Since $\#\mu_{q-1} = \#\mathbb{F}_q^* = q-1$, it is sufficient to show that the $\ker(u)$ is trivial. Suppose $x = \zeta_{q-1}^k \in \ker(u)$, for some $1 \le k \le q-2$. Then $\zeta_{q-1}^k \equiv 1 \pmod{\mathfrak{q}}$, equivalently, $1 - \zeta_{q-1}^k \in \mathfrak{q}$. We know that

$$\prod_{1 \le j \le q-2} (x - \zeta_{q-1}^j) = 1 + x + x^2 + \cdots + x^{q-2}.$$

Substituting $x = 1$, we get $q - 1 \in \mathfrak{q}$. Since $q = p^f \in \mathfrak{q}$, $1 = q - (q-1) \in \mathfrak{q}$, which is absurd. ■

Let $\omega_{\mathfrak{q}}$ be the inverse of u, that is, $\omega_{\mathfrak{q}} := u^{-1}$, then

$$\omega_{\mathfrak{q}} : \mathbb{F}_q^* \to \mu_{q-1} \subset \mathbb{C},$$

is a unique isomorphism from $\mathbb{F}_q^*$ to μ_{q-1} satisfying the following property.

$$\omega_{\mathfrak{q}}(x) \mod \mathfrak{q} = x. \tag{3.1}$$

Since $\omega_{\mathfrak{q}}$ is a group homomorphism $\mathbb{F}_q^*$ to $\mathbb{C}$, $\omega_{\mathfrak{q}}$ is a character of $\mathbb{F}_q^*$. We extend $\omega_{\mathfrak{q}}$ to $\mathbb{F}_q$ by defining $\omega_{\mathfrak{q}}(0) = 0$ and call it *Teichmuller character* on $\mathbb{F}_q$. For our convenience, we write Equation 3.1 as follows:

$$\omega_{\mathfrak{q}}(x) \equiv x \pmod{\mathfrak{q}}. \tag{3.2}$$

Remark 1. It is easy to see that $\omega_{\mathfrak{q}}$ is uniquely determined by $\mathfrak{q}$.

Since $\omega_{\mathfrak{q}}$ is an isomorphism between $\mathbb{F}_q^*$ and μ_{q-1}, it is a character of order $q-1$. Therefore, any $\chi \in \hat{\mathbb{F}_q^*}$ is of the form $\chi = \omega_{\mathfrak{q}}^{-r}$ for some $0 \le r \le q-2$. As a result, the values

of the Gauss sums $g(\chi) = g(\omega_{\mathfrak{q}}^{-r})$ depend only on $(\mathfrak{q}, r)$. As mentioned above, the prime ideal $\mathfrak{q}$ is fixed, therefore, we omit the subscript $\mathfrak{q}$ from $\omega_{\mathfrak{q}}$ and write ω instead of $\omega_{\mathfrak{q}}$.

3.2 Prime Ideal Decomposition of Gauss Sums

We begin by proving the following congruence for Jacobi sums.

Proposition 3.2 (Jacobi Sum Congruence)**.** *Let $a, b \in \mathbb{Z}$ be such that $1 \leq a, b < q-1$. Then*

$$J(\omega^{-a}, \omega^{-b}) \equiv \begin{cases} 0 \pmod{\mathfrak{q}} & \text{if } a+b \geq q; \\ \binom{a+b}{a} \pmod{\mathfrak{q}} & \text{otherwise.} \end{cases} \tag{3.3}$$

We require the following lemma to prove the above congruence.

Lemma 3.3. *1. For $0 < m < q-1$ we have*

$$\sum_{a \in \mathbb{F}_q} a^m = 0.$$

2. For any $m \in \mathbb{Z}$ we have

$$\sum_{a \in \mathbb{F}_q^*} a^m = \begin{cases} 0 & (q-1) \nmid m, \\ -1 & (q-1) \mid m. \end{cases}$$

Proof. Define the following map:

$$\begin{aligned} \varphi : \mathbb{F}_q^* &\to \mathbb{F}_q^* \\ a &\mapsto a^m. \end{aligned}$$

It is clear that φ is a group homomorphism. We know that $\mathbb{F}_q^*$ is cyclic, so let g be a generator. We have,

$$\varphi(g) \sum_{a \in \mathbb{F}_q^*} \varphi(a) = \sum_{a \in \mathbb{F}_q^*} \varphi(ga) = \sum_{a \in \mathbb{F}_q^*} \varphi(a)$$

Since $0 < m < q-1$, $\varphi(g) \neq 1$, it follows that

$$\sum_{a \in \mathbb{F}_q^*} \varphi(a) = \sum_{a \in \mathbb{F}_q^*} a^m = 0.$$

Since $m \neq 0$ we have the followsing equality

$$\sum_{a \in \mathbb{F}_q^*} a^m = \sum_{a \in \mathbb{F}_q} a^m,$$

which proves Part (1) and Part (2) immediately follows from Part (1). ■

Proof of Proposition 3.2. For any $x \in \mathbb{F}_q^*$, choose $x' \in \mu_{q-1}$ such that $x' \equiv x \pmod{\mathfrak{q}}$, then $\omega(x) = x'$.

Let $c = q-1-b$, then $\omega^{-b} = \omega^c$ as the order of ω is $q-1$. If $x \neq 1$, then we have

$$\omega^{-b}(1-x) = \omega^c(1-x) \equiv (1-x')^c \pmod{\mathfrak{q}}.$$

Therefore,

$$\begin{aligned} J(\omega^{-a}, \omega^{-b}) &= -\sum_{x \in \mathbb{F}_q^*} \omega^{-a}(x)\omega^{-b}(1-x) \\ &\equiv -\sum_{x \in \mathbb{F}_q^*} (x')^{-a}(1-x')^c \\ &\equiv -\sum_{x \in \mathbb{F}_q^*} x^{-a}(1-x)^c \\ &\equiv -\sum_{x \in \mathbb{F}_q^*} x^{-a} \sum_{0 \leq j \leq c} \binom{c}{j} (-1)^j x^j \\ &\equiv -\sum_{0 \leq j \leq c} (-1)^j \binom{c}{j} \sum_{x \in \mathbb{F}_q^*} x^{j-a} \pmod{\mathfrak{q}}. \end{aligned}$$

Since $j, a < q-1$, $j \equiv a \pmod{q-1}$ if and only if $j = a$. From Lemma 3.3 we have

$$\sum_{x \in \mathbb{F}_q^*} x^{j-a} = \begin{cases} 0 & j \neq a, \\ -1 & j = a. \end{cases}$$

If $a+b \geq q$, then $a > c$. Therefore, $j \neq 0$ as $0 \leq j \leq c$. Hence,

$$J(\omega^{-a}, \omega^{-b}) \equiv 0 \pmod{\mathfrak{q}}.$$

Suppose $a+b \leq q-1$, equivalently $a \leq c$. Then the sum $\sum_{x \in \mathbb{F}_q^*} x^{j-a}$ vanishes except if $j = a$. Therefore,

$$J(\omega^{-a}, \omega^{-b}) \equiv (-1)^{a-2} \binom{c}{a} \pmod{\mathfrak{q}}.$$

We have,

$$\begin{aligned}\binom{c}{a} = \binom{q-1-b}{a} &= \frac{(q-1-b)(q-2-b)\cdots(q-a-b)}{a!} \pmod{p} \\ &\equiv (-1)^a \frac{(b+1)(b+2)\cdots(a+b)}{a!} \\ &\equiv (-1)^a \binom{a+b}{a} \pmod{p}.\end{aligned}$$

Since $\mathfrak{q}$ divides p, the above congruence of the binomial coefficients also holds modulo $\mathfrak{q}$. Thus,

$$J(\omega^{-a}, \omega^{-b}) \equiv (-1)^{a-2}\binom{c}{a} \equiv (-1)^{2a-2}\binom{a+b}{a} \pmod{\mathfrak{q}}.$$

This proves our claim. ■

Remark 2. If $a+b \geq q$, then $\binom{a+b}{a} \equiv 0 \pmod{p}$. Therefore, the second congruence is valid in all generalities.

Definition 3.4. Let $0 \leq r < q-1$ be an integer and $r = \sum_{0\leq i<f} r_i p^i$ be its p-adic expansion, with $0 \leq r_i \leq p-1$. Define

$$s_p(r) := \sum_{0\leq i<f} r_i \quad \text{and} \quad t_p(r) := \prod_{0\leq i<f} r_i!.$$

Let $r \in \mathbb{Z}$, then there exist $0 \leq r' < q-1$ and $k \in \mathbb{Z}$ such that $r = k(q-1)+r'$. Define

$$s(r) := s_p(r') \quad \text{and} \quad t(r) := t_p(r').$$

Clearly, s and t are $(q-1)$-periodic functions on $\mathbb{Z}$.

Theorem 3.5 (Stickelberger's Congruence)**.** *For all $r \in \mathbb{Z}$ we have*

$$\frac{g(\omega^{-r})}{\pi^{s(r)}} \equiv \frac{1}{t(r)} \pmod{\mathfrak{P}}, \tag{3.4}$$

where $\pi = \zeta_p - 1$, and $\mathfrak{P}$ is the unique prime ideal of $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ above $\mathfrak{q}$. Furthermore, $v_{\mathfrak{P}}(g(\omega^{-r})) = s(r)$, where $v_{\mathfrak{P}}$ is the $\mathfrak{P}$-adic evaluation of $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$.

Proof. By periodicity we can assume that $0 \leq r < q-1$. We prove the theorem by inducting on $s(r) = s_p(r)$. If $s(r) = 0$, the claim is trivial because $r = 0$ and $g(\mathbb{1}) = 1$. The

crucial case to be proved is the case $s(r) = 1$, in which case $r = p^k$ for some $0 \leq k < f$ and $t(r) = 1$. Since $g(\chi^p) = g(\chi)$ (see Proposition 2.24), we have

$$g(\omega^{-p^k}) = g(\omega^{-p^{k-1}}) = \cdots = g(\omega^{-1}),$$

it follows that we can assume $r = 1$. Since ω is a nontrivial character, we have

$$g(\omega^{-1}) = -\sum_{x \in \mathbb{F}_q} \omega^{-1}(x)\zeta_p^{\mathrm{Tr}(x)} = -\sum_{x \in \mathbb{F}_q} \omega^{-1}(x)(\zeta_p^{\mathrm{Tr}(x)} - 1),$$

as $\sum_{x \in \mathbb{F}_q^*} \omega^{-1}(x) = 0$. The last sum has the advantage that all summands are divisible by $\zeta_p - 1$. Since $\zeta_p^r \equiv 1 \pmod{\pi}$ for all $r \in \mathbb{Z}$, we have

$$\frac{\zeta_p^m - 1}{\zeta_p - 1} = 1 + \zeta_p + \cdots + \zeta_p^{m-1} \equiv m \pmod{\pi}.$$

We know that $\pi \in \mathfrak{P}$, which implies that the above congruence also holds modulo $\mathfrak{P}$. This shows that

$$\frac{g(\omega^{-1})}{\zeta_p - 1} \equiv -\sum_{x \in \mathbb{F}_q^*} \omega^{-1}(x)\,\mathrm{Tr}(x) \pmod{\mathfrak{P}}.$$

Now $\mathrm{Tr}(x) = \sum_{0 \leq i < f} x^{p^i} \in \mathbb{F}_p$, and on the other hand, by definition, $\omega^{-1}(x) \equiv x^{-1} \pmod{\mathfrak{P}}$. It follows that

$$\frac{g(\omega^{-1})}{\pi} \equiv -\sum_{0 \leq i < f} \sum_{x \in \mathbb{F}_q^*} x^{p^i - 1} \pmod{\mathfrak{P}}.$$

Now again by Lemma 3.3 the inner sum vanishes if $1 \leq i < f$, and it is congruent to -1 modulo p if $i = 0$. It follows that

$$\frac{g(\omega^{-1})}{\zeta_p - 1} \equiv 1 \pmod{\mathfrak{P}},$$

proving the theorem when $s(r) = 1$.

Now let $r = \sum_{0 \leq i < f} r_i p^i$ with $0 \leq r_i < p$ be such that $s(r) > 1$, and assume by induction that the theorem is true for all $r' < q - 1$ with $s(r') < s(r)$. Again, using the fact that $g(\chi^p) = g(\chi)$, we can assume that $r_0 \geq 1$. It follows in particular that $s(r-1) = s(r) - 1 \geq 1$ and $r - 1 \geq 1$.

Since the characters involved are nontrivial, by Proposition 2.21 we have

$$J(\omega^{-1},\omega^{-(r-1)})g(\omega^{-r}) = g(\omega^{-1})g(\omega^{-(r-1)}). \tag{3.5}$$

Using Proposition 3.2 we know that

$$J(\omega^{-1},\omega^{-(r-1)}) \equiv \binom{r}{1} = r \equiv r_0 \pmod{\mathfrak{P}}. \tag{3.6}$$

Combining equations 3.5 and 3.6 we get

$$r_0\frac{g(\omega^{-r})}{\pi^{s(r)}} \equiv \frac{g(\omega^{-1})g(\omega^{-(r-1)})}{\pi^{s(r)}} \pmod{\mathfrak{P}}. \tag{3.7}$$

Since $1 \leq r_0 \leq p-1$, r_0 is invertible modulo $\mathfrak{P}$, we can divide both sides of congruence 3.7 by r_0:

$$\frac{g(\omega^{-r})}{\pi^{s(r)}} \equiv \frac{1}{r_0}\frac{g(\omega^{-1})}{\pi}\frac{g(\omega^{-(r-1)})}{\pi^{s(r)-1}} \pmod{\mathfrak{P}}. \tag{3.8}$$

The induction hypothesis implies that $\frac{g(\omega^{-(r-1)})}{\pi^{s(r-1)}} \equiv \frac{1}{t(r-1)} \pmod{\mathfrak{P}}$ (recall that $s(r-1) = s(r)-1$), and the case $r=1$ implies that $\frac{g(\omega^{-1})}{\pi} \equiv 1 \pmod{\mathfrak{P}}$. Combining this with equation 3.8 we see that

$$\frac{g(\omega^{-r})}{(\zeta_p-1)^{s(r)}} \equiv \frac{1}{r_0}\cdot 1 \cdot \frac{1}{t(r-1)} \pmod{\mathfrak{P}}, \tag{3.9}$$

since $t(r) = r_0 t(r-1)$ when $r_0 \neq 0$. We have proved our induction hypothesis and hence the first statement.

It is well known that $p\mathbb{Z}[\zeta_p] = (\pi)^{p-1}$ and $p\mathbb{Z}[\zeta_{p(q-1}] = (\mathfrak{P}_1\cdots\mathfrak{P}_g)^{p-1}$, where $\mathfrak{P}_i$ are the prime ideals of $\mathbb{Q}(\zeta_p,\zeta_{q-1})$ above p. We have

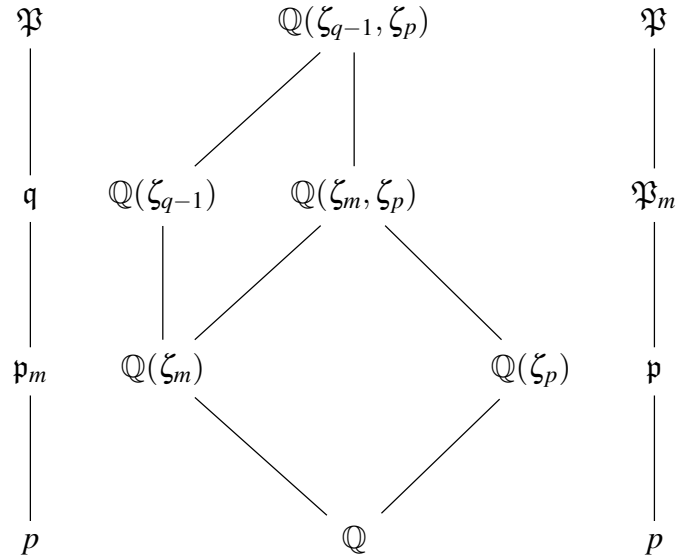
$$p\mathbb{Z}[\zeta_{p(q-1}] = (p\mathbb{Z}[\zeta_p])\mathbb{Z}[\zeta_{p(q-1}] = \pi^{p-1}\mathbb{Z}[\zeta_{p(q-1}] = (\mathfrak{P}_1\cdots\mathfrak{P}_g)^{p-1},$$

where, say, $\mathfrak{P} = \mathfrak{P}_1$. Hence $\pi\mathbb{Z}[\zeta_{p(q-1)}] = \mathfrak{P}_1\cdots\mathfrak{P}_g$, thus $v_{\mathfrak{P}}(\pi) = 1$. We know that $t(r)$ is coprime to p hence is invertible modulo $\mathfrak{P}$, so by the Stickelberger congruence:

$$v_{\mathfrak{P}}(g(\omega^{-r})) = s(r)v_{\mathfrak{P}}(\pi) = s(r).$$

This proves the second statement. ■

Let $\mathfrak{q}$ and $\mathfrak{P}$ be as above. Let $\mathfrak{p}_m$ be the *unique* prime ideal in $\mathbb{Q}(\zeta_m)$ below $\mathfrak{q}$, and $\mathfrak{P}_m$ be the *unique* prime ideal in $\mathbb{Q}(\zeta_m, \zeta_p)$ below $\mathfrak{P}$. Let $\mathfrak{p} = (\pi)$, where $\pi = \zeta_p - 1$, be the *unique* prime ideal in $\mathbb{Q}(\zeta_p)$ lying above p. The Hasse diagram for the fields and ideals occurring in this section is displayed in the following figure:



Let $d = \frac{q-1}{m}$ and r be any integer. Then $(\omega^{-rd})^m = \mathbb{1}$, which implies that $g(\omega^{-rd})$ is an algebraic integer in $\mathbb{Q}(\zeta_m, \zeta_p)$. Thus we can talk about the prime ideal decomposition of the principal ideal generated by $g(\omega^{-rd})$ in $\mathbb{Q}(\zeta_m, \zeta_p)$.

Let

$$\Gamma := \mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_p)/\mathbb{Q}(\zeta_p)).$$

For any b coprime to m, we define $\sigma_b \in \Gamma$ as

$$\sigma_b : \zeta_m \mapsto \zeta_m^b, \quad \zeta_p \mapsto \zeta_p.$$

It is well known that the map $b \mapsto \sigma_b$ from $(\mathbb{Z}/m\mathbb{Z})^*$ to Γ is an isomorphism. The following result gives the prime ideal decomposition of the principal ideal generated by the Gauss sum $g(\omega^{-rd})$ in $\mathbb{Q}(\zeta_m, \zeta_p)$.

Theorem 3.6. *For any $r \in \mathbb{Z}$ the prime ideal decomposition of the principal ideal $(g(\omega^{-rd}))$ in $\mathbb{Q}(\zeta_m, \zeta_p)$ is given by*

$$(g(\omega^{-rd})) = \prod_{t \in (\mathbb{Z}/m\mathbb{Z})^*/\langle p \rangle} \sigma_t^{-1}(\mathfrak{P}_m)^{s(rtd)},$$

where $\mathfrak{P}_m$ is the prime ideal of $\mathbb{Q}(\zeta_m, \zeta_p)$ lying below $\mathfrak{P}$.

Proof. The claim is trivially true when $r = 0$. To go further we first notice that the only prime ideals in $\mathbb{Q}(\zeta_m, \zeta_p)$ containing $g(\omega^{-rd})$ are those containing p, because for $r \not\equiv 0 \pmod{m}$, we have

$$g(\omega^{-rd})\overline{g(\omega^{-rd})} = |g(\omega^{-rd})|^2 = q = p^f.$$

Thus, the only prime ideals that divide $(g(\omega^{-rd}))$ in $\mathbb{Q}(\zeta_m, \zeta_p)$ are the prime ideals above p (equivalently, above $\mathfrak{p}$).

By Galois theory, we know that $\sigma_t^{-1}(\mathfrak{P}_m)$, for $t \in (\mathbb{Z}/m\mathbb{Z})^*$, are all the primes of $\mathbb{Q}(\zeta_m, \zeta_p)$ lying above $\mathfrak{p}$.

By the definition of the Guass sums we have $\sigma_t(g(\omega^{-rd})) = g(\omega^{-rtd})$. Therefore,

$$\begin{aligned} v_{\sigma_t^{-1}(\mathfrak{P}_m)}(g(\omega^{-rd})) &= v_{\mathfrak{P}_m}(\sigma_t(g(\omega^{-rd}))) \\ &= v_{\mathfrak{P}_m}(g(\omega^{-rtd})) \\ &= v_{\mathfrak{P}}(g(\omega^{-rtd})), \end{aligned}$$

where the second last equality is because the prime $\mathfrak{P}$ is unramified over the prime $\mathfrak{P}_m$. Thus by the second statement of Theorem 3.5 we have:

$$v_{\sigma_t^{-1}(\mathfrak{P}_m)}(g(\omega^{-rd})) = s(rtd).$$

Recall that $D_{\mathfrak{P}_m|\mathfrak{p}} = \{\sigma \in \Gamma : \sigma(\mathfrak{P}_m) = \mathfrak{P}_m\}$ is the *Decomposition Group* of $\mathfrak{P}_m$ over $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified in $\mathbb{Q}(\zeta_m, \zeta_p)$, $D_{\mathfrak{P}_m|\mathfrak{p}}$ is a cyclic subgroup of Γ of order f generated by the *Frobenius element* σ_p. This means that the prime ideals of $\mathbb{Q}(\zeta_m, \zeta_p)$ above $\mathfrak{p}$ are obtained once and only once as $\sigma_t^{-1}(\mathfrak{P}_m)$ for $\sigma_t \in \Gamma/D_{\mathfrak{P}_m|\mathfrak{p}}$, in other words for $t \in (\mathbb{Z}/m\mathbb{Z})^*/\langle p \rangle$. Consequently,

$$(g(\omega^{-rd})) = \prod_{t \in (\mathbb{Z}/m\mathbb{Z})^*/\langle p \rangle} \sigma_t^{-1}(\mathfrak{P}_m)^{s(rtd)}.$$

■

The restriction homomorphism from Γ to $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ induces an isomorphism from Γ to $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. We shall denote the image of $\sigma_t \in \Gamma$ under this isomorphism by σ_t. Let N be the relative ideal norm from $\mathbb{Q}(\zeta_m, \zeta_p)$ to $\mathbb{Q}(\zeta_m)$. From Proposition 2.23, we

know that $g(\omega^{-rd})^m \in \mathbb{Q}(\zeta_m)$. Since $\sigma(g(\omega^{-rd})^m) = g(\omega^{-rd})^m$ for all $\sigma \in \Gamma$, we have

$$N((g(\omega^{-rd})^m)) = g(\omega^{-rd})^{m(p-1)}\mathbb{Z}[\zeta_m].$$

We now give the prime ideal decomposition of the principal ideal generated by $g(\omega^{-rd})^m$ in $\mathbb{Q}(\zeta_m)$.

Theorem 3.7. *For any $r \in \mathbb{Z}$ the prime ideal decomposition of the principal ideal $(g(\omega^{-rd})^m)$ in $\mathbb{Q}(\zeta_m)$ is given by*

$$(g(\omega^{-rd})^m) = \prod_{t\in(\mathbb{Z}/m\mathbb{Z})^*/\langle p\rangle} \sigma_t^{-1}(\mathfrak{p}_m)^{\frac{m}{p-1}\cdot s(rtd)}.$$

Proof. Theorem 3.6 implies

$$(g(\omega^{-rd})^m) = \prod_{t\in(\mathbb{Z}/m\mathbb{Z})^*/\langle p\rangle} \sigma_t^{-1}(\mathfrak{P}_m)^{m\cdot s(rtd)}. \tag{3.10}$$

The primes $\sigma_t^{-1}(\mathfrak{P}_m)$ are totally ramified in $\mathbb{Q}(\zeta_m,\zeta_p)$. It follows that the ramification index of $\sigma_t^{-1}(\mathfrak{P}_m)$ over $\mathfrak{p}_m$ is equal to the full degree $p-1$, which in turn implies that the inertia degree of $\sigma_t^{-1}(\mathfrak{P}_m)$ over $\mathfrak{p}_m$ is equal to 1. Thus,

$$N(\sigma_t^{-1}(\mathfrak{P}_m)) = \sigma_t^{-1}(\mathfrak{p}_m).$$

We take the relative norm on both sides of the equation 3.10 and obtain the following:

$$\begin{aligned} g(\omega^{-rd})^{m(p-1)}\mathbb{Z}[\zeta_m] &= \prod_{t\in(\mathbb{Z}/m\mathbb{Z})^*/\langle p\rangle} \sigma_t^{-1}(\mathfrak{p}_m)^{m\cdot s(rtd)} \\ &= \prod_{t\in(\mathbb{Z}/m\mathbb{Z})^*/\langle p\rangle} \sigma_t^{-1}(\mathfrak{p}_m)^{\frac{m}{p-1}(p-1)\cdot s(rtd)}. \end{aligned}$$

Furthermore, in general, if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of a number field with the property that $\mathfrak{a}^k = \mathfrak{b}^k$, then $\mathfrak{a} = \mathfrak{b}$. Hence, we have

$$(g(\omega^{-rd})^m) = g(\omega^{-d})^m\mathbb{Z}[\zeta_m] = \prod_{t\in(\mathbb{Z}/m\mathbb{Z})^*/\langle p\rangle} \sigma_t^{-1}(\mathfrak{p}_m)^{\frac{m}{p-1}\cdot s(rtd)}.$$

■

Theorem 3.7 is an important result in the theory of cyclotomic fields. It is also the basis for

the proof of *Eisenstein reciprocity* (see [18]). In the last century the theory of cyclotomic fields has been dramatically advanced principally due to the efforts of Iwasawa. In his work Theorem 3.7 occupies a central position. It has also turned out to be of importance in arithmetic algebraic geometry.

3.3 Stickelberger's Element

The results of the last section can be expressed in a much more nice fashion using the language of group rings. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, $R = \mathbb{Z}[G]$. Then the *class group* Cl_m is a Galois module. We treat Cl_m as an R-module as described in §2.3.1. Any element of G is of the form $\sigma_a : \zeta_m \mapsto \zeta_m^a$, for some $a \in (\mathbb{Z}/m\mathbb{Z})^*$.

Definition 3.8. The **Stickelberger element** of $\mathbb{Q}(\zeta_m)$ is an element of $\mathbb{Q}[G]$ defined as

$$\Theta = \sum_{\substack{a \bmod m \\ (a,m)=1}} \left\{ \frac{a}{m} \right\} \sigma_a^{-1}.$$

Lemma 3.9. *1. For all $r \in \mathbb{Z}$ we have*

$$s(r) = (p-1) \sum_{0 \le i < f} \left\{ \frac{p^i r}{q-1} \right\}.$$

2. For $0 \le r < q-1$ we have

$$t(r) \equiv (-p)^{-v_p(r!)} r! \pmod{p}.$$

Proof. (1). Both sides of the formula are periodic of period dividing $q-1$; hence we may assume that $0 \le r < q-1$, so that $r = \sum_{0 \le j < f} r_j p^j$ with $0 \le r_j \le p-1$. For $0 \le i \le f-1$ we have

$$\begin{aligned} p^i r &= \sum_{0 \le j < f-i-1} r_j p^{j+i} + \sum_{f-i \le j < f} r_j p^{j+i} \\ &\equiv \sum_{0 \le j < f-i-1} r_j p^{j+i} + \sum_{f-i \le j < f} r_j p^{j+i-f} \pmod{q-1}, \end{aligned}$$

hence

$$\left\{ \frac{p^i r}{q-1} \right\} = \frac{1}{q-1} \left(\sum_{0 \le j < f-i-1} r_j p^{j+i} + \sum_{f-i \le j < f} r_j p^{j+i-f} \right).$$

It follows that

$$\sum_{0\le i<f}\left\{\frac{p^i r}{q-1}\right\} = \frac{1}{q-1}\sum_{0\le j<f} r_j A_j,$$

where

$$A_j = \sum_{0\le i<f-j-1} p^{j+i} + \sum_{f-j\le i<f} p^{j+i-f} = \sum_{0\le i<f} p^i = \frac{p^f-1}{p-1} = \frac{q-1}{p-1},$$

proving (1).

(2) is easily proved by induction on r: it is trivially true for $r \le 1$. Assume $r \ge 2$ and that the formula is true for $r-1$, and let $r = \sum_{k\le j\le f-1} r_j p^j$ be the p-adic decomposition of r, with $0 \le r_j \le p-1$ and $r_k \ne 0$. Since

$$r-1 = \sum_{0\le j\le k-1}(p-1)p^j + (r_k-1)p^k + \sum_{k+1\le j\le f-1} r_j p^j$$

it follows from Wilson's theorem that

$$t(r-1) \equiv (-1)^k (r_k-1)! \prod_{k+1\le j\le f-1}(r_j)! \pmod{p},$$

hence that

$$t(r) \equiv (-1)^k r_k t(r-1) \equiv \frac{r}{(-p)^{v_p(r)}} t(r-1) \pmod{p},$$

where $v_p(r)$ is the p-adic valuation of r. The result follows by induction. ■

We have the following restatement of Theorem 3.7.

Theorem 3.10. *Let Θ be the Stickelberger element of $\mathbb{Q}(\zeta_m)$. Then*

$$(g(\omega^{-d})^m) = \mathfrak{p}_m^{m\Theta}.$$

Proof. Let T be a system of representatives of $(\mathbb{Z}/mZ)^*/\langle p\rangle$. From Theorem 3.9, we have the following prime decomposition:

$$(g(\omega^{-d})^m) = \prod_{t\in(\mathbb{Z}/m\mathbb{Z})^*/\langle p\rangle} \sigma_t^{-1}(\mathfrak{p}_m)^{\frac{m}{p-1}\cdot s(td)}.$$

From Lemma 3.9 we have,

$$s(td) = (p-1)\sum_{0\le i<f}\left\{\frac{p^i t}{m}\right\}.$$

Therefore,

$$(g(\omega^{-d})^m) = \mathfrak{p}_m^{m\alpha},$$

where

$$\alpha = \sum_{t\in T}\sum_{0\le i<f}\left\{\frac{p^i t}{m}\right\}\sigma_t^{-1}.$$

As t varies in T and i ranges from 0 to $f-1$ the elements $p^i t$ modulo m range through $(Z/mZ)^*$, so that

$$\alpha = \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^*}\{t/m\}\sigma_{t'}^{-1},$$

where t' is a representative of the class of t modulo $\langle p\rangle$. Since the decomposition group of $\mathfrak{p}_m$ over p is a subgroup generated by σ_p, it follows that $\mathfrak{p}_m^{m\alpha} = \mathfrak{p}_m^{m\Theta}$. ■

Quick recap. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\zeta_m)$ which is coprime to m and Θ be the Stickelberger element of $\mathbb{Q}(\zeta_m)$. So far, we have shown that $\mathfrak{p}^{m\Theta}$ is a pricipal ideal in $\mathbb{Q}(\zeta_m)$. This innocent looking result is actually very strong, which we demonstrate below.

Lemma 3.11. *Let F be a number field and $\mathfrak{m}$ be an integral ideal of F. Then every ideal class of* $\mathrm{Cl}(F)$ *contains an integral ideal prime to* $\mathfrak{m}$.

Proof. Let $\mathfrak{a}$ be an ideal of $\mathscr{O}$ and let $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_t\}$ be the set of prime ideals dividing $\mathfrak{m}$ which do not divide $\mathfrak{a}$. If $\mathfrak{p}$ divides $\mathfrak{a}$ then let $a(\mathfrak{p})$ be the exponent of $\mathfrak{p}$ that occurs in the prime decomposition of $\mathfrak{a}$. Choose some

$$\pi(\mathfrak{p}) \in \mathfrak{p}^{a(\mathfrak{p})} - \mathfrak{p}^{a(\mathfrak{p})+1}.$$

By the Chinese Remainder Theorem there exists an α such that

$$\begin{aligned}\alpha &\equiv \pi(\mathfrak{p}) \mod \mathfrak{p}^{a(\mathfrak{p})+1} \quad \text{for } \mathfrak{p}|\mathfrak{a},\\ \alpha &\equiv 1 \mod \mathfrak{p}_i \quad \text{for } i = 1,2,\ldots,t.\end{aligned}$$

If $\mathfrak{p}|\mathfrak{a}$, then the above system of congruences implies that the exponent of $\mathfrak{p}$ that occurs in the prime decomposition of (α) is equal to $a(\mathfrak{p})$, and that $\mathfrak{p}_i$ does not divide (α) for

$i = 1, 2, \ldots, t$.

Thus we can write $(\alpha) = \mathfrak{a}\mathfrak{c}$ where $\mathfrak{c}$ is an ideal coprime to $\mathfrak{m}$. This shows that there is such an ideal, which is coprime to m, in the inverse of the ideal class of $\mathfrak{a}$, and because $\mathfrak{a}$ was arbitrary we deduce the result. ■

The above lemma implies that the set of prime ideals, coprime to m, completely generates the ideal class group. Since these prime ideals are annihilated by $m\Theta$, we conclude that the ideal class group is annihilated by $m\Theta$.

Theorem 3.12. *The m-th multiple of the Stickelberger element Θ of $\mathbb{Q}(\zeta_m)$ annihilates the ideal class group Cl_m of $\mathbb{Q}(\zeta_m)$, that is, for any fractional ideal $\mathfrak{a}$ of $\mathbb{Q}(\zeta_m)$ the ideal $\mathfrak{a}^{m\Theta}$ is principal.*

Proof. Let $\mathfrak{a}$ be a fractional ideal of $\mathbb{Q}(\zeta_m)$. Then there is $\alpha \in \mathbb{Q}(\zeta_m)$, such that $\mathfrak{b} = \alpha\mathfrak{a}$ is an integral ideal of $\mathbb{Q}(\zeta_m)$ coprime to m. Let $\mathfrak{p}_m$ be a prime of $\mathbb{Q}(\zeta_m)$ which divides $\mathfrak{b}$, choose a prime $\mathfrak{q}$ of $\mathbb{Q}(\zeta_{q-1})$, such that $\mathfrak{p}_m$ is the unique prime of $\mathbb{Q}(\zeta_m)$ lying below $\mathfrak{q}$. Theorem 3.10 implies that $\mathfrak{p}_m^{m\Theta}$ is principal, where Θ is the Stickelberger element of $\mathbb{Q}(\zeta_m)$. By multiplicativity, $\mathfrak{b}^{m\Theta}$ is principal in $\mathbb{Q}(\zeta_m)$. ■

3.4 Stickelberger Ideal of Cyclotomic Fields

We retain the notations from the previous sections. In this section, we will define the Stickelberger ideal of $\mathbb{Q}(\zeta_m)$ and show that this ideal annihilates the ideal class group Cl_m of $\mathbb{Q}(\zeta_m)$.

Definition 3.13. Let Θ be the Stickelberger element of $\mathbb{Q}(\zeta_m)$. We define the Stickelberger ideal I_S of $\mathbb{Q}(\zeta_m)$ by

$$I_S := R \cap \Theta R.$$

For any $b \in \mathbb{Z}$ with $\gcd(b, m) = 1$ we define $\Theta_b = (b - \sigma_b)\Theta \in \mathbb{Q}[G]$. Then we have

$$\Theta_b = (b - \sigma_b)\Theta = \sum_{\substack{a \bmod m \\ (a,m)=1}} \left[\frac{ba}{m}\right] \sigma_a^{-1}. \tag{3.11}$$

This implies that $\Theta_b \in R$ and hence $\Theta_b \in I_S$.

Example 3.1. If $m = p$ is an odd prime and $b = 2$ we have

$$\Theta_2 = -\sum_{(p+1)/2 \le t \le p-1} \sigma_t^{-1}.$$

Proposition 3.14. *The Stickelberger ideal I_S of $\mathbb{Q}(\zeta_m)$ is generated by the Θ_b as a $\mathbb{Z}$-module (hence also as an ideal). More precisely, it is generated over $\mathbb{Z}$ by Θ_b for $1 \le b \le m$ with $\gcd(b,m) = 1$, and Θ_{m+1}.*

Proof. By definition an element $\delta \in I_S$ has the form $\delta = \gamma\Theta$, where $\gamma\Theta \in R$ and $\gamma \in R$. Let $\sum_c = \sum_{\substack{1 \le c \le m \\ \gcd(c,m)=1}}$. If we write $\gamma = \sum_c x_c \sigma_c$, where $x_c \in \mathbb{Z}$, then

$$\gamma\Theta = \sum_{a,c} x_c \left\{ \frac{a}{m} \right\} \sigma_{ac^{-1}}^{-1} = \sum_b d_b \sigma_b^{-1}.$$

with

$$d_b = \sum_c x_c \left\{ \frac{bc}{m} \right\}.$$

Since $\gamma\Theta \in R$ we have $d_b \in \mathbb{Z}$ for $1 \le b \le m$ with $\gcd(b,m) = 1$, and in particular

$$d_1 = \sum_c x_c \left\{ \frac{c}{m} \right\} = \sum_c x_c \frac{c}{m} \in \mathbb{Z}.$$

We have

$$m\Theta = ((m+1) - \sigma_{m+1})\Theta = \Theta_{m+1} \in R. \tag{3.12}$$

Thus

$$\begin{aligned} \gamma\Theta &= \sum_c x_c \sigma_c \Theta = \sum_c x_c (\sigma_c - c)\Theta + \sum_c x_c c \Theta \\ &= \sum_c x_c (\sigma_c - c)\Theta + m d_1 \Theta = -\sum_c x_c \Theta_c + d_1 \Theta_{m+1}, \end{aligned}$$

which proves our claim. ∎

Proof of Theorem 1.1. As in the proof of Theorem 3.12, it is sufficient to show that $\mathfrak{p}_m^{\gamma}$ is a principal ideal for any $\gamma \in I_S$ and any prime ideal $\mathfrak{p}_m$ coprime to m. Recall from Theorem 3.10 that

$$(g(\omega^{-d})^m) = \mathfrak{p}_m^{m\Theta},$$

raise both sides to the power $b-\sigma_b$ for b coprime to m and obtain

$$\mathfrak{p}_m^{m\Theta_b} = (g(\omega^{-d})^{m(b-\sigma_b)}) = (\alpha^m),$$

where $\alpha = g(\omega^{-d})^{(b-\sigma_b)}$. From Proposition 2.23 $\alpha \in \mathbb{Z}[\zeta_m]$. Since $\mathfrak{p}_m^{\Theta_b}$ and (α) are ideals of $\mathbb{Z}[\zeta_m]$ whose m-th powers are equal, by uniqueness of the prime ideal decomposition in the Dedekind domain $\mathbb{Z}[\zeta_m]$ we deduce that they are equal and, in particular, $\mathfrak{p}_m^{\Theta_b}$ is a principal ideal. We know, from Proposition 3.14, that Θ_b generates I_S, thus $\mathfrak{p}_m^{\gamma}$ is a principal ideal for all $\gamma \in I_S$. ■

3.5 Stickelberger Ideal of Abelian Number Fields

In this section we define the Stickelberger element and the Stickelberger ideal of arbitrary abelian number fields. Let E be an abelian extension of $\mathbb{Q}$, $G = \mathrm{Gal}(E/\mathbb{Q})$, and $R = \mathbb{Z}[G]$. Then the *class group* $\mathrm{Cl}(E)$ of E is a Galois module. We treat $\mathrm{Cl}(E)$ as a R-module as described in §2.3.1.

The Kronecker-Weber theorem implies that $E \subset \mathbb{Q}(\zeta_m)$, we call the least such m the *conductor* of E. Thus, we can realize G as a quotient group of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Any element of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is of the form $\sigma_a : \zeta_m \mapsto \zeta_m^a$, for some $a \in (\mathbb{Z}/m\mathbb{Z})^*$. In what follows, we also denote by σ_a its restriction to E.

Definition 3.15. The Stickelberger element of E is an element of $\mathbb{Q}[G]$ defined as

$$\Theta(E) = \sum_{\substack{a \bmod m \\ (a,m)=1}} \left\{ \frac{a}{m} \right\} \sigma_a^{-1}.$$

Definition 3.16. The Stickelberger ideal $I_S(E)$ of E is an ideal of R defined as

$$I_S(E) = R \cap \Theta(E)R.$$

We define

$$\Theta_b(E) := (b-\sigma_b)\Theta(E),$$

then $\Theta_b(E) \in I_S(E)$ (analogous to Equation 3.11). We know from Proposition 3.14 that the Stickelberger ideal of cyclotomic fields is generated by Θ_b. However, the analog of Proposition 3.14 is not true in general for abelian number fields, as suggested by the

following example.

Example 3.2. Let $E = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\zeta_{12}^+) \subset \mathbb{Q}(\zeta_{12})$, with

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) = \{\sigma_1, \sigma_5, \sigma_7, \sigma_{11}\},$$

however, when restricted to E, $\sigma_1 = \sigma_{11} = 1$ and $\sigma_5 = \sigma_7 = \sigma$. Therefore, the Stickelberger element of E is $\Theta = 1 + \sigma$. Since $\Theta \in \mathbb{Z}[G]$, where $G = \mathrm{Gal}(E/\mathbb{Q})$, the Stickelberger ideal is equal to $I = \Theta\mathbb{Z}[G]$. The ideal generated by $(1 - \sigma_1 = 0)$, $(5 - \sigma)$, $(7 - \sigma)$, and $(11 - 1)$ is equal to $(2, 1 + \sigma = \Theta)$, therefore, J in this case is $(2\Theta, \Theta^2) = (2\Theta)$ which is properly contained in I.

We now proceed to give a proof of Stickelberger's theorem for arbitrary abelian number fields. For simplicity, let $\Theta = \Theta(E)$. Let $\mathfrak{a}$ be an integral ideal of E that is a co-prime to m, and let $\mathfrak{a}\mathbb{Z}[\zeta_m] = \prod_i \mathfrak{p}_i$ be its decomposition into primes in $\mathbb{Q}(\zeta_m)$. Then, from Theorem 3.10 we have

$$(\mathfrak{a}\mathbb{Z}[\zeta_m])^{m\Theta} = \prod_i \mathfrak{p}_i^{m\Theta} = (\prod_i g(\chi_{\mathfrak{p}_i})^m),$$

with $\chi_{\mathfrak{p}_i}^m = \mathbb{1}$, and we write $\chi_{\mathfrak{p}_i}$ to indicate that χ depends on $\mathfrak{p}_i$. Let $\beta \in R$ be such that $\beta\Theta \in R$. Then

$$\mathfrak{a}^{m\beta\Theta} = (\gamma^{\beta m}), \quad \text{where} \quad \gamma = \prod_i g(\chi_{\mathfrak{p}_i}) \in \mathbb{Q}(\zeta_{Pm}),$$

where $P = \prod_i p_i$ is the product of rational primes lying below $\mathfrak{p}_i$'s.

Proposition 3.17. *Let K be a number field, $a \in K^*$. and $n \in \mathbb{Z}$. Suppose $(a) = \mathfrak{a}^n$ for some ideal $\mathfrak{a}$ of K. Then $K(a^{\frac{1}{n}})/K$ is unramified outside of the primes dividing n.*

Proof. Let $\alpha = a^{\frac{1}{n}}$, $f(x) = x^n - a$ be the minimal polynomial of α, and $L = K(\alpha)$. Then

$$|\mathrm{disc}(f)| = |\mathrm{Norm}_{L/K} f'(\alpha)| = |\mathrm{Norm}_{L/K} b\alpha^{n-1}| = n^n a^{n-1}.$$

It is well known that a prime in L/K ramifies if and only if it divides $|\mathrm{disc}(f)|$. Therefore, the only ramified primes in the extension L/K are the factors of n and prime factors of a.

Since (a) is a n-th power of an ideal $\mathfrak{a}$, for a prime factor $\mathfrak{p}$ of a which is relatively prime to n, we have

$$K_{\mathfrak{p}}(a^{\frac{1}{n}}) = K_{\mathfrak{p}}(u^{\frac{1}{n}}),$$

for a unit u of the $\mathfrak{p}$-adic completion $K_{\mathfrak{p}}$ of K.

Since $\mathfrak{p} \nmid n$,

$$K_{\mathfrak{p}}(u^{\frac{1}{n}})/K_{\mathfrak{p}}$$

is unramified. To finally conclude that $\mathfrak{p}$ is unramified in $K(a^{\frac{1}{n}})/K$, we use [15, Theorem 4.8.5], which says that the ramification index of $\mathfrak{p}$ in $K(a^{\frac{1}{n}})/K$ is equal to the ramification index of $K_{\mathfrak{p}}(a^{\frac{1}{n}})/K_{\mathfrak{p}}$.

Since the ramification index of $K_{\mathfrak{p}}(a^{\frac{1}{n}})/K_{\mathfrak{p}}$ is 1, the prime $\mathfrak{p}$ is unramified in $K(a^{\frac{1}{n}})/K$. This proves our claim.

■

Since $\gamma^{m\beta} \in \mathbb{Q}(\zeta_m)$, and it is the m-th power of an ideal of $\mathbb{Q}(\zeta_m)$, namely $\mathfrak{a}^{\beta\Theta}$, from Proposition 3.17, it follows that the extension

$$\mathbb{Q}(\zeta_m, \gamma^{\beta})/\mathbb{Q}(\zeta_m)$$

can be ramified only at primes that divide m. But

$$\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_m, \gamma^{\beta}) \subseteq \mathbb{Q}(\zeta_m, \zeta_P)$$

which implies that ramification can occur only at the primes dividing P. But $\gcd(P,m) = 1$, thus the extension must be unramified. We need the following lemma which says that there does not exist a nontrivial unramified subextension between two cyclotomic fields.

Lemma 3.18. *Let $m,n \geq 1$ be such that m divides n. 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. If $m = n$, then it is trivial. Suppose $m \neq n$. Let p be a prime that divides n/m. Then $\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m)$ is totally ramified at the primes above p. Let $F = K \cap \mathbb{Q}(\zeta_{mp})$, then $\mathbb{Q}(\zeta_m) \subset F \subset K$, and since $K/\mathbb{Q}(\zeta_m)$ is unramified at primes above p, $F/\mathbb{Q}(\zeta_m)$ must also be unramified at primes above p.

Suppose that $F \neq \mathbb{Q}(\zeta_m)$, we have $\mathbb{Q}(\zeta_m) \subset F \subset \mathbb{Q}(\zeta_{mp})$. Let $\mathfrak{P}$ be a prime of $\mathbb{Q}(\zeta_{mp})$ above p, $\mathfrak{p} = \mathfrak{P} \cap \mathbb{Q}(\zeta_m)$, and $\mathfrak{q} = \mathfrak{P} \cap F$. Then we have $e(\mathfrak{P}|\mathfrak{p}) = p-1$, and $e(\mathfrak{q}|\mathfrak{p}) = 1$, which implies that $e(\mathfrak{P}|\mathfrak{q}) = p-1$. But $e(\mathfrak{P}|\mathfrak{q}) \leq [\mathbb{Q}(\zeta_{mp}) : F] < p-1$. Contradiction. Thus, $F = \mathbb{Q}(\zeta_m)$. So $[K(\zeta_{mp}) : \mathbb{Q}(\zeta_{mp})] = [K : \mathbb{Q}(\zeta_m)]$.

The lift of an unramified extension is still unramified, so now we are in the original situation, but with mp replacing m. Proceeding in this manner, we find that $[K(\zeta_n) : \mathbb{Q}(\zeta_n)] = [K : \mathbb{Q}(\zeta_m)]$. Since $K \subset \mathbb{Q}(\zeta_n)$, it follows that $K = \mathbb{Q}(\zeta_m)$. ■

Lemma 3.18 implies that $\mathbb{Q}(\zeta_m, \gamma^\beta) = \mathbb{Q}(\zeta_m)$, i.e., $\gamma^\beta \in \mathbb{Q}(\zeta_m)$. Therefore $\mathfrak{a}^{\beta\Theta} = (\gamma^\beta)$ is principal as an ideal of $\mathbb{Q}(\zeta_m)$. To show that it is also principal as an ideal of E, we prove that $\gamma^\beta \in E$.

Let $\mathfrak{q}$ be a prime of $\mathbb{Q}(\zeta_{q-1})$ lying over one of the prime factors $\mathfrak{p}_i$ of $\mathfrak{a}$. Recall that $\chi_{\mathfrak{p}_i}$ *a priori* depends on the choice of $\mathfrak{q}$, so we write $\chi_{\mathfrak{p}_i} = \chi_{\mathfrak{q}}$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}(\zeta_m))$, then σ induces a natural isomorphism between the following residue fields

$$\mathbb{Z}[\zeta_{q-1}]/\mathfrak{q} \backsimeq \mathbb{Z}[\zeta_{q-1}]/\mathfrak{q}^\sigma.$$

In what follows, we do not distinguish between these two fields, and we denote both of these fields by $\mathbb{F}_q$.

Let $a \in \mathbb{F}_q$, if $\chi_{\mathfrak{q}}(a) = \zeta$, then $\chi_{\mathfrak{q}^\sigma}(a) = \zeta^\sigma$. Therefore $\chi_{\mathfrak{q}}^\sigma = \chi_{\mathfrak{q}^\sigma}$, but $\chi_{\mathfrak{q}}^m = \mathbb{1}$, which implies that values of $\chi_{\mathfrak{q}}$ are m-th roots of unity. Since σ fixes $\mathbb{Q}(\zeta_m)$, we have $\chi_{\mathfrak{q}}^\sigma = \chi_{\mathfrak{q}}$, so $\chi_{\mathfrak{q}^\sigma} = \chi_{\mathfrak{q}}$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}(\zeta_m))$. Therefore, $\chi_{\mathfrak{q}}$ depends only on $\mathfrak{p}_i$, thus we can return to the notation $\chi_{\mathfrak{p}_i}$. Similar argument also implies that $\chi_{\mathfrak{p}_i}^\sigma = \chi_{\mathfrak{p}_i^\sigma}$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/E)$. Let us extend σ to $\mathbb{Q}(\zeta_m, \zeta_p)$, by letting $\sigma(\zeta_p) = \zeta_p$, where p is the rational prime lying below $\mathfrak{p}_i$, then $g(\chi_{\mathfrak{p}_i})^\sigma = g(\chi_{\mathfrak{p}_i}^\sigma) = g(\chi_{\mathfrak{p}_i^\sigma})$.

For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/E)$, we have $\mathfrak{a}^\sigma = \mathfrak{a}$, i.e., σ permutes the $\mathfrak{p}_i$'s. Therefore

$$\gamma^{\beta\sigma} = \prod_i g(\chi_{\mathfrak{p}_i})^{\beta\sigma} = \prod_i g(\chi_{\mathfrak{p}_i^\sigma})^\beta = \gamma^\beta.$$

Since, $\gamma^\beta \in \mathbb{Q}(\zeta_m)$, we have $\gamma^\beta \in E$. So $\mathfrak{a}^{\beta\Theta}$ is principal in E. We have proved the following.

Theorem 3.19. *Let $I_S(E)$ be the Stickelberger ideal of E. Then $I_S(E)$ annihilates the ideal class group $\mathrm{Cl}(E)$ of E.*

Remark 3. The Stickelberger theorem does not give any information in case of real abelian number fields. Let E be a real number field of conductor m. Then $\sigma_a = \sigma_{-a}$, and since $\{a/m\} + \{-a/m\} = 1$, we have

$$\Theta(E) = \frac{1}{2} \sum_{a \bmod m} \sigma_a = \frac{\phi(m)}{2\deg(E)} \mathrm{Norm}_{E/\mathbb{Q}}.$$

Thus a multiple of the norm annihilates the ideal class group of E, which is obviously true for any number field. This suggests that we can obtain nontrivial results only if we consider imaginary number fields.

In [30], Thaine used cyclotomic units to construct annihilators of ideal class groups of real abelian fields E: let m be the conductor of E, $G = \mathrm{Gal}(E/\mathbb{Q})$ its Galois group, put $K = \mathbb{Q}(\zeta_m)$, and let U_E be the group of units of E. Let C_E be the subgroup of U_E consisting of units of E of the form

$$\pm \mathrm{Norm}_{K/E}\left(\prod_a (\zeta_m^a - 1)^{b_a}\right),$$

where $b_a \in \mathbb{Z}$. The subgroup C_E is called the group of cyclotomic units (sometimes also called *circular*) units of E. Then Thaine proved that for any prime p that does not divide $[E:\mathbb{Q}]$, 2θ kills the p-class group $\mathrm{Cl}_p(E)$ of E whenever $\theta \in R$ kills the p-Sylow subgroup of U_E/C_E.

3.6 Some Natural Questions

Example 3.2 suggests that the analog of Proposition 3.14 does not hold in general for abelian fields which are not cycltomic fields. Therefore, it is natural to ask the following question.

Question 1. Are there abelian fields E of the conductor m that are not cyclotomic such that the Stickelberger ideal $I_S(E)$ is generated by $\Theta_b(E)$ for $1 \leq b \leq m$ with $\gcd(b,m) = 1$ and $\Theta_{m+1}(E)$?

We notice that in Example 3.2 the Stickelberger element of $\mathbb{Q}(\sqrt{3})$ has integer coefficients. Therefore, we ask the following natural question.

Question 2. For what abelian number fields E with Galois group G, the Stickelberger element $\Theta(E) \in \mathbb{Z}[G]$?

Example 3.2 suggests that there exist quadratic number fields such that the coefficients of their Stickelberger element are integers. This property is actually true for a wider class of abelian number fields, as we shall see now.

First, if E is a cyclotomic field of conductor m, then by the definition of the Stickelberger element $\Theta(E) \notin \mathbb{Z}[G]$. Therefore, we can only find abelian number fields with such a property if we consider abelian number fields E of conductor m with $E \neq \mathbb{Q}(\zeta_m)$.

Let us now consider a real quadratic number field E of discriminant $d > 0$, we know that

the conductor of E is d. From Remark 3 the Stickelberger element of is given by

$$\Theta(E) = \frac{\phi(d)}{4}\mathrm{Norm}_{K/\mathbb{Q}}.$$

Clearly, there are infinitely many real quadratic fields of discriminant d such that 4 divides $\phi(d)$. For example, take $E = \mathbb{Q}(\sqrt{d})$, where $d = 5m$ for some $m \in \mathbb{Z}_{>0}$, and $(5,m) = 1$, then $4|\phi(d)$.

Now consider an imaginary quadratic number field $E = \mathbb{Q}(\sqrt{d})$, with discriminant $d \neq -3,-4,-8$. Let $G = \mathrm{Gal}(E/\mathbb{Q})$, and $R = \mathbb{Z}[G]$. Recall that $f = |d|$ is the conductor of E, the field E embeds as a subfield of $\mathbb{Q}(\zeta_f)$. We have the following natural surjection.

$$\chi_E : (\mathbb{Z}/f\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \twoheadrightarrow G \cong \langle \pm 1 \rangle, \tag{3.13}$$

where the final equality is the unique isomorphism between cyclic groups of order 2. It is clear that χ_E is a character of $(\mathbb{Z}/f\mathbb{Z})^*$ of the order 2. Set

$$A = \sum_{\chi_E(a)=1} a, \quad B = \sum_{\chi_E(b)=-1} b,$$

then the Stickelberger element $\Theta := \Theta(E)$ of E is given by

$$\Theta = \frac{1}{f}(A + B\sigma),$$

where σ is the non-trivial automorphism of $E/\mathbb{Q}$. The definition of Θ implies that $f\Theta \in R$. Actually, much more is true; Schmid [23] proved the following.

Theorem 3.20 (Schmid)**.** *Let A and B be as above, then f divides A and B unless $d = -3,-4$ or -8. Equivalently, the Stickelberger element Θ is an element of $\mathbb{Z}[G]$ unless $d = -3,-4$ or -8.*

This implies that the Stickelberger ideal $I_S := I_S(E)$ of E is the principal ideal in R generated by Θ, that is, $I_S = \Theta R$. In particular, Θ annihilates the ideal class group of E. We know that the norm element $1+\sigma$ also annihilates the class group of E. In fact, in the next chapter we show that $1+\sigma \in I_S$ (see Proposition 4.12). Therefore,

$$\pm\left(\frac{1}{f}(A+B\sigma) - \frac{B}{f}(1+\sigma)\right) = \pm\left(\frac{1}{f}(A-B)\right) \in I_S.$$

If E is an abelian number field, then we know that the class number $h(E)$ annihilates the

ideal class group of E. Therefore, it is natural to ask the following question.

Question 3. Do there exist abelian number fields E for which $h(E) \in I_S(E)$?

Let $h := h(E)$ be the class number of E, then the analytic class number formula for imaginary quadratic fields implies that

$$h = -\frac{1}{f} \sum_{a \in (\mathbb{Z}/f\mathbb{Z})^*} \chi_E(a)a = \frac{1}{f}(B - A),$$

therefore, $h \in I_S$. If the class number of E is 1, then $1 \in I_S$ and $I_S = R$. We are not aware of any other examples of an abelian number field for which the ideal class number is an element of the Stickelberger ideal.

We have seen in Remark 3 that the Stickelberger theorem does not give any information on the annihilators of an ideal class group of real abelian fields. In [30], Thaine constructed annihilators of the ideal class group of real abelian fields that are clearly different from those given by the Stickelberger theorem.

Question 4. Let E be an imaginary cyclotomic field. Are there any annihilators of the ideal class group of E that are different from those given by the Stickelberger theorem?

This question has been answered positively in [20], where the authors have constructed annihilators of the ideal class group of E that are not contained in the Stickelberger ideal of E.

Chapter 4

Iwasawa's Class Number Formula

Let m be any positive integer and $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Let χ be a character of G, then χ is also a Dirichlet charater of modulus m, we denote by f_χ the conductor of χ. In what follows, we do not distinguish between $\chi(a)$ and $\chi(\sigma_a)$, for any a coprime to m. Let $j = \sigma_{-1} \in G$ be the complex conjugation, then $\chi(j) = \chi(-1)$ can be equal to 1 or -1. We say that χ is even (respectively, odd) if $\chi(j) = \chi(-1) = 1$ (respectively, if $\chi(j) = \chi(-1) = -1$).

4.1 Analytic Class Number Formula

In this section we briefly recall the analytic class number formula (for a full discussion, see Chapter 4 of [32]). We first prove a basic result from the theory of cyclotomic fields.

Proposition 4.1. *Let W be the group of roots of unity in $\mathbb{Q}(\zeta_m)$ and $w = \#W$. If m is even, the only roots of unity in K are the m-th roots of unity, so that $W \cong \mathbb{Z}/m\mathbb{Z}$. If m is odd, the only ones are the $2m$-th roots of unity, so that $W \cong \mathbb{Z}/2m\mathbb{Z}$. In particular, $w = m$ if m is even and $w = 2m$ if m is odd.*

Proof. If m is odd, then $(-\zeta_m)^{(m+1)/2}$ is a primitive $2m$-th root if unity. Therefore, $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$. It will, therefore, suffice to establish the statement for m even. Let $\alpha \in \mathbb{Q}(\zeta_m)$ be primitive k-th root of unity, $k \nmid m$. Then $\zeta_m \alpha$ is a primitive r-th root unity, where $r = \mathrm{lcm}(k,m) > m$. Thus $\mathbb{Q}(\zeta_r) \subseteq \mathbb{Q}(\zeta_m)$ and

$$\phi(r) = [\mathbb{Q}(\zeta_r) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m),$$

where ϕ denotes the Euler phi-funtion. But m is even and m properly divides r implies that

$\phi(m)$ properly divides $\phi(r)$, so that, in particular, $\phi(m) < \phi(r)$, which is a contradiction. Thus, the m-th roots of unity are the only roots of unity in $\mathbb{Q}(\zeta_m)$. ■

Lemma 4.2. *If α is an algebraic integer all of whose conjugates have absolute value 1, then α is a root of unity.*

Proof. We know that the minimal polynomial of α over $\mathbb{Z}$ is

$$p(x) = \prod_{i=1}^{d}(x - \alpha_i),$$

where d is the degree of α over $\mathbb{Q}$ and α_i are all the conjugates of α. Then

$$p_n(x) = \prod_{i=1}^{d}(x - \alpha_i^n)$$

is a polynomial over $\mathbb{Z}$ with α^n as a root. It also has degree d, and all the roots have absolute value 1. The coefficients of these polynomials are 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. ■

Proposition 4.3. *Let U be the unit group of $\mathbb{Q}(\zeta_m)$. Let U^+ be the unit group of $\mathbb{Q}(\zeta_m^+)$, W be the group of roots of unity in $\mathbb{Q}(\zeta_m)$, and $Q := [U : WU^+]$ be the Hasse unit index of $\mathbb{Q}(\zeta_m)$. Then $Q = 1$ if m is a prime power and $Q = 2$ is m is not a prime power.*

Proof. We show that $Q \in \{1,2\}$ and omit the proof of the second statement which is an easy but a lengthy computation. Let $\phi : U \to W$ be a group homomorphism defined by $\phi(u) = u/\overline{u}$. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and $\sigma \in G$, then $\overline{\sigma(u)} = \sigma(\overline{u})$ (because complex conjugation commutes with the other elements of the Galois group), we have $|\sigma(\phi(u))| = 1$ for all $\sigma \in G$. By Lemma 4.2 $\phi(u) \in W$.

Let $\psi : U \to W/W^2$ be the map induced by ϕ. We claim that $\ker(\psi) = WU^+$. Let $u = \zeta u_1$, where $\zeta \in W$ and $u_1 \in U^+$. Then

$$\phi(u) = \zeta u_1/\overline{\zeta u_1} = \zeta^2 u_1/\overline{u_1},$$

since $u_1 \in U^+$, $\overline{u_1} = u_1$. Thus, $\phi(u) = \zeta^2 \in W^2$, so $u \in \ker(\psi)$. Conversely, suppose $u \in U$ and $\phi(u) = \zeta^2 \in W^2$. Then $u/\overline{u} = \zeta^2$, which implies $\zeta^{-1}u = \zeta\overline{u}$. Therefore, $u_1 = \zeta^{-1}u$

is real. It follows that $\ker(\psi) = WU^+$. Since $[W : W^2] = 2$ and $[E : \ker(\psi)]$ must divide $[W : W^2]$, we are done. Note that if $\phi(U) = W$ then $Q = 2$; if $\phi(U) = W^2$ then $Q = 1$. ■

Let Cl_m and h_m (respectively, Cl_m^+ and h_m^+) be the ideal class group and the class number of $\mathbb{Q}(\zeta_m)$ (respectively, $\mathbb{Q}(\zeta_m^+)$). The class number h_m^+ is always a divisor of h_m. This numerical statement has an algebraic underpinning as follows:

Lemma 4.4. *The natural map (induced by the inclusion of fields)* $\mathrm{Cl}_m^+ \to \mathrm{Cl}_m$ *is injective. The quotient* h_m/h_m^+ *is the order of the cokernel of this natural map, and therefore an integer.*

Proof. We will show that the kernel of this natural map is trivial. Suppose I is an ideal of $\mathbb{Q}(\zeta_m^+)$ which becomes principal when lifted to $\mathbb{Q}(\zeta_m)$. We claim that I is principal in $\mathbb{Q}(\zeta_m^+)$.

Let $I = (\alpha)$, where $\alpha \in \mathbb{Q}(\zeta_m)$. Since I is real we have

$$(\bar{\alpha}/\alpha) = \bar{I}/I = (1).$$

Therefore, $\bar{\alpha}/\alpha$ is a unit. Also all its conjugates have abosulte value 1. By Lemma 4.2, $\bar{\alpha}/\alpha$ is a root of unity. If m is not a prime power, then $Q = 2$ and Proposition 4.3 implies that there is a unit u in $\mathbb{Q}(\zeta_m)$ such that

$$u/\bar{u} = \bar{\alpha}/\alpha.$$

This implies that αu is real, i.e., $\alpha u \in \mathbb{Q}(\zeta_m^+)$, and $I = (\alpha) = (\alpha u)$. It follows form the unique factorization of ideals in $\mathbb{Q}(\zeta_m^+)$ that $I = (\alpha u)$ in $\mathbb{Q}(\zeta_m^+)$, so I was originally principal.

Now suppose $m = p^n$ for some positive integer n. Let $\pi = \zeta_m - 1$. We have $\pi/\bar{\pi} = -\zeta_m$, which generates the roots of unity in $\mathbb{Q}(\zeta_m)$. Therefore $\bar{\alpha}/\alpha = (\pi/\bar{\pi})^d$ for some d. Since the π-adic valuation takes on only even values on $\mathbb{Q}(\zeta_m^+)$ 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 $\bar{\alpha}/\alpha = (-\zeta_m)^d \in W^2$. 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. ■

The quotient h_m/h_m^+ is written h_m^- and is known as *minus part of the class number* or simply the minus class number. We now recall the definition of *Bernoulli numbers* and some of their properties.

Definition 4.5. The Bernoulli numbers B_n are defined implicitly by the relation

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

Some of the initial Bernoulli numbers are: $B_0 = 1, B_1 = \frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}$ and so on.

Proposition 4.6. *If $n \geq 3$ is an odd integer greater than or equal to 3, then $B_n = 0$.*

Proof. It suffices to show that the formal power series $\frac{te^t}{e^t-1} - \frac{t}{2}$ does not have any odd-degree terms. Since we have

$$\frac{te^t}{e^t-1} - \frac{t}{2} = \frac{t(e^t-1+1)}{e^t-1} - \frac{t}{2} = \frac{t}{e^t-1} + \frac{t}{2}$$

and

$$\frac{(-t)e^{-t}}{e^{-t}-1} - \frac{(-t)}{2} = \frac{-t}{1-e^t} + \frac{t}{2} = \frac{t}{e^t-1} + \frac{t}{2},$$

$\frac{te^t}{e^t-1} - \frac{t}{2}$ is invariant under the substitution $t \to -t$. This shows that the coefficients of odd-degree terms are all 0. ■

Definition 4.7. Let χ be a Dirichlet character defined modulo m. Then the generalized Bernoulli numbers $B_{n,\chi}$ are defined implicitly by the relation

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

Clearly, $B_{n,\chi} = B_n$ for $\chi = \mathbb{1}$. Table 4.1 contains some Bernoulli numbers $B_{n,\chi}$ for characters χ defined modulo 3 and modulo 4.

For studying generalized Bernoulli numbers, the Bernoulli polynomials are an indispensable tool. They are defined by

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

n	$3B_{n,\chi}\quad(f_\chi=3)$	$2B_{n,\chi}\quad(f_\chi=4)$
1	-1	-1
3	2	3
5	$-2\cdot 5$	-5^2
7	$2\cdot 7^2$	$7\cdot 61$
9	$-2\cdot 809$	$-3^2\cdot 5\cdot 277$
11	$2\cdot 11\cdot 1847$	$11\cdot 19\cdot 2659$
13	$-2\cdot 7\cdot 13^3\cdot 47$	$-5\cdot 13^2\cdot 43\cdot 967$
15	$2\cdot 5\cdot 419\cdot 16519$	$3\cdot 5\cdot 47\cdot 4241723$

Table 4.1: Bernoulli Numbers

The following propertie of Bernoulli polynomials are easy to verify:

- $B_n(x)\in\mathbb{Q}[x]$;
- $B_n(1)=B_n$, $B_n(1-x)=(-1)^nB_n(x)$;
- $B_n(x)=\sum_{i=0}^n\binom{n}{i}B_ix^{n-i}$;
- $B_{n,\chi}=\frac{1}{m}\sum_{a=1}^{m-1}\chi(a)B_n\left(\frac{a}{m}\right)$.

Since $B_1(x)=x-\frac{1}{2}$, the last property immediately implies that

$$B_{1,\chi}=\frac{1}{m}\sum_{\substack{a=1\\(a,m)=1}}^{m}\chi(a)a$$

for any $\chi\neq\mathbb{1}$. We have seen that all the Bernoulli numbers with odd indices greater than 1 are 0. For generalized Bernoulli numbers we have the following.

Proposition 4.8. *Let χ be a non-trivial character. Then, for any n satisfying $(-1)^{n-1}=\chi(-1)$, we have $B_{n,\chi}=0$. In other words, if χ is an even character, then $B_{n,\chi}$ with odd indices n are 0; if χ is an odd character, then $B_{n,\chi}$ with even indices n are 0.*

Proof. Since χ is non-trivial, we can rewrite the generating function as follows:

$$\begin{aligned}\sum_{a=1}^{m-1}\frac{\chi(a)te^{at}}{e^{mt}-1}&=\sum_{a=1}^{m-1}\frac{\chi(m-a)te^{(m-a)t}}{e^{mt}-1}\\&=\chi(-1)\sum_{a=1}^{m-1}\frac{\chi(a)te^{-at}}{1-e^{-mt}}\\&=\chi(-1)\sum_{a=1}^{m-1}\frac{\chi(a)(-t)e^{a(-t)}}{e^{m(-t)}-1}.\end{aligned}$$

It follows immediately from this that the generating function is an even function if $\chi(-1) = 1$, and an odd function if $\chi(-1) = -1$. ■

We now state the analytic class number formula for the minus class number of $\mathbb{Q}(\zeta_m)$.

Proposition 4.9. *Let Q and w be defined as above. Then*

$$h_m^- = Qw \prod_{\chi \ odd} \left(-\frac{1}{2} B_{1,\chi} \right), \tag{4.1}$$

where the product extends over the odd Dirichlet characters defined modulo m.

Proof. See [32, Theorem 4.17]. ■

4.2 $\mathbb{Z}$-rank of Stickelberger Ideal

Let $m = p^n \neq 2$, where p is a prime and n is an arbitrary positive integer. Denote by Θ the Stickelberger element of $\mathbb{Q}(\zeta_m)$, by R the group ring $\mathbb{Z}[G]$, and by I_S the Stickelberger ideal of $\mathbb{Q}(\zeta_m)$. From Proposition 3.14 it is clear that the $\mathbb{Z}$-rank of I_S is bounded above by $\phi(m) + 1$.

Let χ be a character of G, then we can extend χ to $\mathbb{Q}[G]$ by linearity: let $\alpha = \sum_{\sigma \in G} x_\sigma \sigma \in \mathbb{Q}[G]$, then $\chi(\alpha) = \sum_{\sigma \in G} x_\sigma \chi(\sigma)$. It follows from the definition of generalized Bernoulli numbers that $\chi(\Theta) = B_{1,\chi^{-1}}$ whenever χ is non trivial.

Proposition 4.10. *Let χ be a character of G, then $\chi(\Theta) = 0$ if and only if χ is a non-trivial even character.*

Proof. We know that the character χ is even (respectively, odd) if and only if χ^{-1} is even (respectively, odd). If χ is odd, then Proposition 4.9 implies that $\chi(\theta) = B_{1,\chi^{-1}} \neq 0$. If χ is a trivial character, then clearly $\chi(\Theta) \neq 0$. If χ is a non-trivial even character, then from Proposition 4.8 $\chi(\Theta) = B_{1,\chi^{-1}} = 0$. ■

Proposition 4.11. *The $\mathbb{Z}$-rank of I_S is $\frac{\phi(m)}{2} + 1$.*

Proof. Let the $\mathbb{Z}$-rank of I_S be r, then

$$I_S = R \cap \Theta R = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r, \tag{4.2}$$

for some $v_1, v_2, \ldots, v_r \in I_S$. Let (I_S) be the ideal in $\mathbb{Q}[G]$ generated by I_S. Clearly, we have $(I_S) = \Theta\mathbb{Q}[G]$, and from equation 4.2 we have

$$\Theta\mathbb{Q}[G] = \mathbb{Q}v_1 \oplus \cdots \oplus \mathbb{Q}v_r.$$

Thus, r is equal to the $\mathbb{Q}$-dimension of the principal ideal $\Theta\mathbb{Q}[G]$ which is equal to the number of characters that do not vanish at Θ (by Equation 2.7). From Proposition 4.10 we know that there are exactly $\frac{\phi(m)}{2} + 1$ characters of G that do not vanish at Θ, which proves our claim. ■

Proposition 4.12. *Let $N = \sum_{\sigma \in G} \sigma$ be the norm element of G. Then*

$$N = (1 + j)\Theta.$$

In particular, N is an element of the Stickelberger ideal I_S.

Proof. Since $j = \sigma_{-1} = \sigma_{m-1}$, we have

$$j\Theta = \frac{1}{m}\sum a\sigma_{ma-a}^{-1} = \frac{1}{m}\sum a\sigma_{m-a}^{-1}$$
$$(1 + j\Theta) = \frac{1}{m}\sum (m - a + a)\sigma_{m-a}^{-1} = N.$$

Since $N \in \mathbb{Z}[G]$, the norm element $N \in I_S$. ■

In what follows, we shall be mainly dealing with the ideal $(1 - j)I_S$ instead of I_S.

Proposition 4.13. *The $\mathbb{Z}$-rank of $(1 - j)I_S$ is $\phi(m)/2$.*

Proof. We use a similar argument as in the proof of Proposition 4.11. The $\mathbb{Z}$-rank of $(1 - j)I_S$ is equal to the number of characters that do not vanish at $(1 - j)\Theta$. Let χ be a character of G. If $\chi(j) = 1$, then clearly $\chi((1 - j)\Theta) = 0$. If $\chi(j) = -1$, then $\chi((1 - j)\Theta) = 2\chi(\Theta)$, but $\chi(\Theta) \neq 0$ (by Proposition 4.10). Which implies that only the characters do not vanish at $(1 - j)\Theta$ are the odd characters and there are exactly $\phi(m)/2$ odd characters, which proves the claim. ■

4.3 Plus and Minus Part of I_S

Let M be an R-module. Recall that $M^+ = \{x \in M : j \cdot x = x\}$ is the *plus-part* and $M^- = \{x \in M : j \cdot x = -x\}$ is the *minus-part* of the R-module M.

Proposition 4.14. *Let R^+ and R^- be the plus and minus part of R respectively. Then,*

$$R^+ = (1+j)R, \quad R^- = (1-j)R.$$

Proof. Let $\alpha \in (1+j)R$, then we can write $\alpha = (1+j)\beta$ for some $\beta \in R$. We have

$$j \cdot \alpha = j \cdot (1+j)\beta = \alpha.$$

Conversely, if

$$\alpha = \sum_{\substack{a=1 \\ p \nmid a}}^{m} x_a \sigma_a \in R^+$$

then $j\alpha = \alpha$. By comparing the coefficients on both sides we have $x_a = x_{m-a}$. If

$$\beta = \sum_{\substack{a=1 \\ p \nmid a}}^{\lfloor m/2 \rfloor} x_a \sigma_a,$$

then $\alpha = (1+j)\beta \in (1+j)R$. Using a similar argument we can show that $R^- = (1-j)R$. ■

Let I be any arbitrary ideal of R, then

$$I^+ \supseteq (1+j)I \quad \text{and} \quad I^- \supseteq (1-j)I.$$

This section contains a detailed study of the plus part I_S^+ and the minus part I_S^- of the Stickelberger ideal of $\mathbb{Q}(\zeta_m)$. We first settle the simple case of plus part of I_S.

Proposition 4.15. *We have $I_S^+ = (1+j)I_S = N\mathbb{Z}$. In particular, the $\mathbb{Z}$-rank of I_S^+ is* 1.

Proof. Since $(1+j)\Theta = N$, we have $N\mathbb{Z} \subseteq (1+j)I_S \subseteq I_S^+$, and we have to show that $I_S^+ \subseteq N\mathbb{Z}$. Moreover, it suffices to verify that $I_S^+ \subseteq N\mathbb{Q}$, because $N\mathbb{Z} = \mathbb{N}\mathbb{Q} \cap R$.

For any $\alpha \in R^+$, we have $j\alpha = \alpha$, which implies $(1+j)\alpha = 2\alpha$. We obtain

$$2I_S^+ = (1+j)I_S^+ \subseteq (1+j)I_S \subseteq (1+j)\Theta R = NR = N\mathbb{Z}.$$

(Recall that $NR = N\mathbb{Z}$.) Thus, $I_S^+ \subseteq N\mathbb{Q}$, as wanted. ■

Recall from the proof of Proposition 4.14 that, if

$$\alpha = \sum_{\substack{a=1 \\ p\nmid a}}^{m} x_a \sigma_a \in R^+,$$

then $x_a = x_{m-a}$. Therefore, we can write

$$\alpha = \sum_{\substack{a=1 \\ p\nmid a}}^{\lfloor m/2 \rfloor} x_a(\sigma_a + \sigma_{m-a}) \in R.$$

From this we see that the $\mathbb{Z}$-rank of R^+ is $\frac{\phi(m)}{2}$. Similarly, the $\mathbb{Z}$-rank of R^- is also $\frac{\phi(m)}{2}$.

Proposition 4.16. *The index $[R^+ : I_S^+]$ is infinite except when $m = 3$ or 4, in which case it is equal to* 1.

Proof. If $m = 3$ or 4, then $R^+ = I_S^+ = (1+j)\mathbb{Z}$. Suppose that $m \neq 3$ and 4, then $\phi(m)/2 > 1$, and from Proposition 4.15 we know that $\mathbb{Z}$-rank of I_S^+ is 1, which implies that $[R^+ : I_S^+]$ is infinite. ■

The theory of the relative part I_S^- is much more substantial. We have the following inclusion

$$R^- \supset I_S^- \supset (1-j)I_S,$$

and the $\mathbb{Z}$-rank of R^- and $(1-j)I_S$ is $\phi(m)/2$, so is the ank of I_S^-. In particular, both the indices $[R^- : I_S^-]$ and $[I_S^- : (1-j)I_S]$ are finite.

Define $J := \{\alpha \in R : \alpha\Theta \in R\}$, so that $I_S = J\Theta$. Let $\Phi : R \to \mathbb{Z}/m\mathbb{Z}$ be defined by $\Phi : \sigma_a \mapsto a \mod m$. Then Φ extends to a surjective ring homomorphism.

Lemma 4.17. *The ideal J is the kernel of $\Phi : R \to \mathbb{Z}/m\mathbb{Z}$.*

Proof. Let

$$\alpha = \sum_{\substack{b=1 \\ (m,b)=1}}^{m} x_b \sigma_b \in R.$$

Then

$$m\alpha\Theta = \sum_{\substack{a=1 \\ (m,a)=1}}^{m} \sum_{\substack{b=1 \\ (m,b)=1}}^{m} a x_b \sigma_a^{-1} \sigma_b = \sum_{\substack{c=1 \\ (m,c)=1}}^{m} \sigma_c \sum_{\substack{a=1 \\ (a,c)=1}}^{m} a x_{ac}.$$

If $\alpha\Theta \in R$ then the coefficient of σ_1 in $m\alpha\Theta$ is divisible by m and so

$$\sum_{\substack{a=1\\(m,a)=1}}^{m} ax_a \equiv 0 \pmod{m}$$

or equivalently $\Phi(\alpha) = 0$. Conversely, if $\Phi(\alpha) = 0$ then the coefficient of σ_1 in $\alpha\Theta$ is an integer. But the coefficient of σ_c in $\alpha\Theta$ is also the coefficient of σ_1 in $\alpha\sigma_c^{-1}\Theta$. But as Φ is a homomorphism, $\Phi(\alpha) = 0$ implies that $\Phi(\alpha\sigma_c^{-1}) = 0$, and so the coefficient of σ_c in $\alpha\Theta$ is an integer. Hence $\alpha\Theta \in R$.

To summarize, $\alpha\Theta \in R$ if and only if $\Phi(\alpha) = 0$, as required. ■

Corollary 4.18. *We have* $[R : J] = m$.

Proof. The claim follows as $\Phi : R \to \mathbb{Z}/m\mathbb{Z}$ is surjective and $\ker(\Phi) = J$. ■

Let $\alpha \in (1-j)I_S$, then $\alpha = (1-j)\Theta\beta$ for some $\beta \in J$. This β may not be well-defined, to illustrate this, we note that $1 + j \in J$ and $(1-j)\Theta(1+j) = (1-j)\Theta(2+2j) = 0$. However, the parity of the weight $w(\beta)$ of β is well defined (see Definition 2.3.3).

Proposition 4.19. *Let* $\beta_1, \beta_2 \in J$ *be such that*

$$(1-j)\Theta\beta_1 = (1-j)\Theta\beta_2.$$

Then

$$w(\beta_1) \equiv w(\beta_2) \pmod{2}.$$

Proof. It suffices to show that $(1-j)\Theta\beta = 0$ implies $w(\beta) \equiv 0 \pmod{2}$.

If $(1-j)\Theta\beta = 0$, then $j\Theta\beta = \Theta\beta$. This implies $\Theta\beta \in I_S^+ = N\mathbb{Z}$, therefore, we can write $\Theta\beta = Nk$ for some $k \in \mathbb{Z}$. Taking weight of both sides, we obtain

$$w(\Theta)w(\beta) = w(N)w(k).$$

It is well known that

$$\sum_{\substack{a=1\\(a,m)=1}}^{m} a = \frac{m \cdot \phi(m)}{2}.$$

Thus,

$$w(\Theta) = \frac{1}{m} \sum_{\substack{a=1 \\ (a,m)=1}}^{m} a = \frac{m \cdot \phi(m)}{2m} = \frac{\phi(m)}{2}.$$

We also know that $w(N) = \phi(m)$. Therefore,

$$w(\beta) = 2w(k),$$

equivalently, $w(\beta) \equiv 0 \pmod 2$. ■

Definition 4.20. Let $\alpha = (1-j)\Theta\beta \in (1-j)I_S$. Then α is called *even* (respectively, *odd*) if $w(\beta)$ is even (respectively, odd).

Let $I_0 = \{\alpha \in (1-j)I_S : \alpha \text{ is even}\}$ be the subgroup of all even elements of $(1-j)I_S$. We know that the set of even elements form a subgroup of index 1 or 2.

Proposition 4.21. *If m is a odd prime power, then*

$$[(1-j)I_S : I_0] = 2.$$

However, if $m = 2^n$ for $n > 1$, then

$$[(1-j)I_S : I_0] = 1.$$

Proof. We know that $m \in J$. If m is an odd prime power, then $(1-j)\Theta m \in (1-j)I_S$ is an odd element of $(1-j)I_S$ because $w(m) = m$ is odd.

Suppose $m = 2^n$ for $n > 1$, then we show that $(1-j)I_S = I_0$, which is equivalent to show that $w(\beta) \equiv 0 \pmod 2$ for all $\beta \in J$. We observe that $(\sum x_b\sigma_b)\Theta = (\sum x_b b)\Theta$ for $\sum x_b\sigma_b \in R$; since the b's are all odd, we see that

$$\sum x_b b \equiv \sum x_b = w(\sum x_b\sigma_b) \pmod 2.$$

In particular, the existence of a $\beta \in J$ with odd $w(\beta)$ implies that the odd integer $w(\beta)$ is in J: but J also contains 2^n, and since J is an ideal, it must contain $\gcd(w(\beta), 2^n) = 1$, that is, J must be equal to R. But this is a contradiction because it woud imply that $\Theta \in R$, which is clearly not true in case of cyclotomic fields. This completes our proof. ■

We now determine the index $[I_S^- : (1-j)I_S]$.

Proposition 4.22. *We have*

$$I_S^- = \{\alpha \in I_S : w(\alpha) = 0\}.$$

If m is a odd prime power then

$$[I_S^- : (i-j)I_S] = 2^{\frac{\phi(m)}{2}-1}.$$

If m is a power of 2, then

$$[I_S^- : (i-j)I_S] = 2^{\frac{\phi(m)}{2}}.$$

Proof. Clearly, if $\alpha \in I_S^-$, then $w(\alpha) = 0$. Conversely, let $\alpha \in I_S$ be such that $w(\alpha) = 0$. We write $\alpha = \Theta\beta$ for some $\beta \in J$, since $w(\alpha) = 0$ and $w(\Theta) \neq 0$, we have $w(\beta) = 0$. Furthermore,

$$(1+j)\alpha = (1+j)\Theta\beta = N\beta = w(\beta)N = 0 \implies j\alpha = -\alpha,$$

which implies that $\alpha \in I_S \cap R^-$, which proves the first claim.

For any $\alpha \in R^-$, we have $j\alpha = -\alpha$, which implies $(1-j)\alpha = 2\alpha$. Hence for any ideal I of R, we have $2I^- = (1-j)I^-$. In particular,

$$2I_S^- = (1-j)I_S^- \subseteq (1-j)I_S.$$

As I_S^- is a free $\mathbb{Z}$-module of rank $\frac{\phi(m)}{2}$, we get $[I_S^- : 2I_S^-] = 2^{\phi(m)/2}$.

We claim that $2I_S^- = I_0$. Clearly, $2I_S^- \subseteq I_0$. Conversely, let $\alpha = (1-j)\Theta\beta$ be an even element and write $w(\beta) = 2k$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned}\alpha + 2kN &= (1-j)\Theta\beta + w(\beta)N \\ &= (1-j)\Theta\beta + \beta N \\ &= (1-j)\Theta\beta + (1+j)\Theta\beta \\ &= 2\Theta\beta,\end{aligned}$$

which implies that $\alpha + 2kN$ belongs to $2I_S$. Hence α itself belongs to $2I_S$. Since $\alpha \in R^-$, we obtain $\alpha \in 2I_S^-$. This proves the inclusion $I_0 \subseteq 2I_S^-$. Hence $I_0 = 2I_S^-$.

From Proposition 4.21 we know that if m is a power of an odd prime, then $[(1-j)I_S : I_0] = [(1-j)I_S : 2I_S^-] = 2$, which implies that $[I_S^- : (1-j)I_S] = 2^{\frac{\phi(m)}{2}-1}$. However, if m is

a power of 2, then $(1-j)I_S = I_0$, which implies that $[I_S^- : (1-j)I_S] = 2^{\frac{\phi(m)}{2}}$.

■

We recall a basic lemma from group theory.

Lemma 4.23. *Let $B \subseteq A$ be abelian groups and $f : A \to A$ be a group homomorphism. Then*

$$[A : B] = [f(A) : f(B)] \cdot [\ker(f) + B : B].$$

Proof. Define

$$\begin{aligned} \phi : A/B &\to f(A)/f(B) \\ a+B &\mapsto f(a)+f(B). \end{aligned}$$

Clearly ϕ is a surjective homomorphism. We claim that $\ker(\phi) = (\ker(f)+B)/B$. The inclusion $(\ker(f)+B)/B \subseteq \ker(\phi)$ is trivial. Let $a+B \in \ker(\phi)$, then

$$\phi(a+B) = f(a)+f(B) = f(B) \implies f(a) \in f(B).$$

Let $f(a) = f(b)$ for some $b \in B$, then $f(a-b) = 0$, which implies $a-b \in \ker(f)$, i.e., $a \in \ker(f)+B$. The claim follows. ■

Proposition 4.24. *We have $[R^- : (1-j)J] = m$. Furthermore, if m is a power of an odd prime then $J^- = (1-j)J$.*

Proof. Applying the previous lemma to the situation $A = R$, $B = J$ and $f = 1-j$, we find $[R : J] = [R^- : (1-j)J]$ because the kernel of $1-j : R \to R$ is $(1+j)R \subseteq J$. We know from Corrolary 4.18 that $[R : J] = m$. Thus $[R^- : (1-j)J] = m$.

Clearly, $(1-j)J \subseteq J^-$. Now suppose that m is a odd prime power. Let $\alpha \in J^- = J \cap R^-$, then we can write $\alpha = (1-j)\beta$ for some $\beta \in R$. Since $\alpha \in J$, we have

$$0 = \Phi(\alpha) = \Phi((1-j)\beta) = (1-\Phi(j))\Phi(\beta) = 2\Phi(\beta).$$

As m is odd, we obtain $\Phi(\beta) = 0$ and so $\beta \in J$. Therefore, $\alpha = (1-j)\beta \in (1-j)J$. ■

4.4 Index of the Stickelberger Ideal

Let V be a $\mathbb{Q}$-vector space of finite dimension n. A *lattice* in V is a free abelian subgroup of V of rank n. If L is a lattice, then we can write

$$L = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n,$$

where $\mathbf{B} = [u_1, u_2, \ldots, u_n]$ is a $\mathbb{Q}$-basis of V.

Definition 4.25. Let $\mathbf{B} = [u_1, u_2, \ldots, u_n]$ be a $\mathbb{Q}$-basis of V. The lattice generated by $\mathbf{B}$ is the set

$$\mathscr{L}(\mathbf{B}) = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n.$$

Proposition 4.26. *Let $\mathbf{B}_1$ and $\mathbf{B}_2$ be two $\mathbb{Q}$-bases of V. Then $\mathscr{L}(\mathbf{B}_1) = \mathscr{L}(\mathbf{B}_2)$ if and only if there exists a unimodular matrix U (i.e., a square matrix with integer entries and determinant ± 1) such that $\mathbf{B}_1 = \mathbf{B}_2 U$.*

Proof. First assume $\mathbf{B}_1 = \mathbf{B}_2 U$ for some unimodular matrix U. Notice that if U is unimodular then U^{-1} is also unimodular. In particular, both U and U^{-1} are integer matrices, and $\mathbf{B}_1 = \mathbf{B}_2 U$ and $\mathbf{B}_2 = \mathbf{B}_1 U^{-1}$. It follows that $\mathscr{L}(\mathbf{B}_1) \subseteq \mathscr{L}(\mathbf{B}_2)$ and $\mathscr{L}(\mathbf{B}_2) \subseteq \mathscr{L}(\mathbf{B}_1)$, i.e., the two matrices $\mathbf{B}_1$ and $\mathbf{B}_2$ generate the same lattice.

Now assume $\mathbf{B}_1$ and $\mathbf{B}_2$ are two bases for the same lattice $\mathscr{L}(\mathbf{B}_1) = \mathscr{L}(\mathbf{B}_2)$. Then, by definition of lattice, there exist integer square matices U_1 and U_2 such that $\mathbf{B}_1 = \mathbf{B}_2 U_1$ and $\mathbf{B}_2 = \mathbf{B}_1 U_2$. Combining these two equation we get $\mathbf{B}_1 = \mathbf{B}_1 U_1 U_2$, or equivalently, $\mathbf{B}_1(\mathbf{I} - U_1 U_2) = \mathbf{O}$. Since vectors $\mathbf{B}_1$ are linearly independent, it must be $\mathbf{I} - U_1 U_2 = \mathbf{O}$, i.e., $U_1 U_2 = \mathbf{I}$. In particular, $\det(U_1) \cdot \det(U_2) = \det(U_1 \cdot U_2) = \det(I) = 1$. Since matrices U_1 and U_2 have integer entries, $\det(U_1), \det(U_2) \in \mathbb{Z}$, and it must be $\det(U_1) = \det(U_2) = \pm 1$. ■

Let $L = \mathscr{L}(\mathbf{B}_1)$ and $M = \mathscr{L}(\mathbf{B}_2)$ be two lattices. Let $A \in \mathbb{Q}_{n\times n}$ be the base change matirx from $\mathbf{B}_1$ to $\mathbf{B}_2$, i.e., $\mathbf{B}_2 = \mathbf{B}_1 A$. We define

$$(L : M) = |\det(A)|. \tag{4.3}$$

Proposition 4.26 implies that $(L : M)$ is independent of the choice of the bases $\mathbf{B}_1$ and $\mathbf{B}_2$. The following lemma can be proved easily.

Lemma 4.27. *Let L, M, and N be lattices of V. Then*

1. *If $M \subseteq L$, then $(L:M)$ is defined if and only if $[L:M]$ is finite; if this is the case, $(L:M) = [L:M]$.*
2. $(L:N) = (L:M)(M:N)$.

We know that $I_S^- \subseteq R^-$ and the $\mathbb{Z}$-rank of I_S^- is equal to the $\mathbb{Z}$-rank of R^-. Therefore, we have

$$[R^- : I_S^-] = (R^- : I_S^-).$$

From Part (2) of Lemma 4.27 we have

$$[R^- : I_S^-] = (R^- : I_S^-) = \frac{(R^- : (1-j)J) \cdot ((1-j)J : (1-j)I_S)}{(I_S^- : (1-j)I_S)}. \tag{4.4}$$

Similar argument also implies that

$$(R^- : (1-j)J) = [R^- : (1-j)J],$$
$$(I_S^- : (1-j)I_S) = [I_S^- : (1-j)I_S].$$

Proposition 4.28. *We have*

$$((1-j)J : (1-j)I_S) = \prod_{\chi(j)=-1} B_{1,\chi^{-1}},$$

where the product is over all the odd characters of G.

Proof. Let $V = \mathbb{Q}[G]^- = (1-j)\mathbb{Q}[G]$ be a $\mathbb{Q}$-vector space of dimension $\frac{\phi(m)}{2}$, then $(1-j)J$ and $(1-j)I_S$ are lattices in V. Define

$$f : V \to V;$$
$$x \mapsto \Theta x.$$

Since $f((1-j)J) = (1-j)\Theta J = (1-j)I_S$, we have

$$((1-j)J : (1-j)I_S) = |\det(f)|.$$

We now compute the determinant of f. To do so we may extend the base field as we please and choose the most convenient basis. Let us extend the base field to $\mathbb{C}$. The ideal $\mathbb{C}[G]^-$ of the group algebra $\mathbb{C}[G]$ is the common kernel of the *even* characters. Thus, according

to Proposition 2.16 the ideal $\mathbb{C}[G]^-$ has a $\mathbb{C}$-basis consisting of idempotents ε_χ, where χ runs over the *odd* characters. Now

$$\begin{aligned} f(\varepsilon_\chi) = \Theta\varepsilon_\chi &= \chi(\Theta)\varepsilon_\chi \\ &= B_{1,\chi^{-1}}\varepsilon_\chi. \end{aligned}$$

Hence

$$|\det(f)| = \prod_{\chi(j)=-1} B_{1,\chi^{-1}}.$$

■

Theorem 4.29. *Let* $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ *and* $R = \mathbb{Z}[G]$. *Then* $[R^- : I_S^-] = h_m^-$.

Proof. From Proposition 4.9 we have

$$\prod_{\chi(j)=-1} B_{1,\chi^{-1}} = \frac{2^{\frac{\phi(m)}{2}} \cdot h_m^-}{Q \cdot w},$$

where $Q = 1$ (see Proposition 4.3), and $w = m$ if m is even and $w = 2m$ if m is odd (see Proposition 4.1).

First, assume that $m = 2^n$ for $n > 1$. From Proposition 4.24 we have $(R^- : (1-j)J) = m$, and from Proposition 4.22 we have $(I_S^- : (1-j)I_S) = 2^{\frac{\phi(m)}{2}}$. Therefore,

$$(R^- : I_S^-) = \frac{m \cdot \prod_{\chi(j)=-1} B_{1,\chi^{-1}}}{2^{\frac{\phi(m)}{2}}} = \frac{m \cdot h_m^-}{Q \cdot w}. \tag{4.5}$$

But $Q = 1$ and $w = m$. Thus, $(R^- : I_S^-) = h_m^-$.

Now suppose that m is an odd prime power. In this case, from Proposition 4.22 we have $(I_S^- : (1-j)I_S) = 2^{\frac{\phi(m)}{2}-1}$. Therefore,

$$(R^- : I_S^-) = \frac{m \cdot \prod_{\chi(j)=-1} B_{1,\chi^{-1}}}{2^{\frac{\phi(m)}{2}-1}} = \frac{2m \cdot h_m^-}{Q \cdot w}. \tag{4.6}$$

But $Q = 1$ and $w = 2m$. Thus, $(R^- : I_S^-) = h_m^-$. ■

Theorem 4.29 also implies that h_m^- is an integer: a direct integrality proof for general abelian extensions was given by Hasse [10].

Remark 4. Similar class number formula also holds for the plus part when the Stickelberger ideal is replaced by cyclotomic units (see [25]). In 1996, Anderson [1] discovered a unified approach that combined the plus and minus parts.

As an application of Theorem 4.29 we give an algebraic proof of the fact that h_m^- annihilates the odd part of Cl_m^-.

Proposition 4.30. *Let l be an odd prime and $m = l^n$, for some positive integer n. Let $\mathrm{Cl} = \mathrm{Cl}_m$ be the ideal class group of $\mathbb{Q}(\zeta_m)$ and let $h = h_m$ be the class number. Then the minus class number $h^- = h_m^-$ annihilates the minus part of the p-class group of $\mathbb{Q}(\zeta_m)$ for all odd primes p, i.e., h^- annihilates Cl_p^- for all odd primes p.*

Proof. We know $\mathrm{Cl}_p^- = \mathrm{Cl}_p^{1-j}$. Since $R^- = (1-j)R$, we have

$$\mathrm{Cl}_p^- = \mathrm{Cl}_p^{1-j} = \mathrm{Cl}_p^{R^-}.$$

Let $c \in \mathrm{Cl}_p^-$, then $c \in \mathrm{Cl}_p^{R^-}$. Since $h^- = (R^- : I_S^-)$, we find that $c^{h^-} \in \mathrm{Cl}_p^{I_S^-} \subset \mathrm{Cl}^{I_S^-}$, but I_S^- annihilates Cl as $I_S^- \subset I_S$. Therefore, h^- annihilates Cl_p^- for every odd prime p. ■

The fact that the index $[R^- : I_S^-]$ coincides with the minus class number $h_m^- = \#\mathrm{Cl}_m^-$ prompts the question whether there is an isomorphism $R^-/I_S^- \cong \mathrm{Cl}_m^-$ as abelian groups (or even as $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$-modules). The answer to both questions is no; see [32, p. 106-107] and [18, p. 382].

In the next chapter, we present generalizations of Iwasawa's class number formula to arbitrary cyclotmic fields. However, the situation is much more complicated; see Sinnott [25] and Kučera [17].

Chapter 5

Sinnott Ideal of Cycltomic Fields

Let K be an imaginary cyclotomic field. Then there is a unique integer $m > 2$, $m \not\equiv 2 \pmod 4$, such that $K = K$, we call m the conductor of K. Let $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, and $R = \mathbb{Z}[G]$.

In Chapter 3 we have defined the Stickelberger ideal I_S of K and proved that I_S annihilates the ideal class group of K. In Chapter 4 we considered the minus part I_S^- of the Stickelberger ideal I_S and proved Iwasawa's class number formula $[R^- : I_S^-] = h(K)^-$, in the special case when m is a power of a prime. A natural question that arises is whether a generalization of Iwasawa's theorem to the case of arbitrary cyclotomic fields is possible. Unfortunately, such a generalization is not possible with our current definition of the Stickelberger ideal of K.

The obstacle that prevents such a generalization is as follows. When the conductor m is composite and has at least 2 different prime factors, then the index $[R^- : I_S^-]$ is not finite in general. In fact, Kučera [17] proved the following.

Theorem 5.1 (Kučera)**.** *Let $m = p_1^{e_1} p_2^{e_2} \cdots p_g^{e_g}$ be such that $m \not\equiv 2 \pmod 4$. Put $m_i = \frac{m}{p_i^{e_i}}$ and let s_i be the order of p_i in $(\mathbb{Z}/m_i\mathbb{Z})^*$. Then the group R^-/I_S^- is finite if and only if s_i is even and*

$$p_i^{\frac{s_i}{2}} \equiv -1 \pmod{m_i},$$

for each $i = 1, 2, \ldots, g$, or if $g = 1$.

Example 5.1. Let $m = 2^3 3^2$, with $p_1 = 2$ and $p_2 = 3$. Then $s_1 = 6$ and $s_2 = 2$. We have

$$2^3 \equiv -1 \pmod 9,$$
$$3^1 \not\equiv -1 \pmod 8.$$

Theorem 5.1 implies that for $\mathbb{Q}(\zeta_{72})$ the index $[R^- : I_S^-]$ is not finite.

If the index $[R^- : I_S^-]$ is finite, then Kučera gave the following generalization of Iwasawa's class number formula.

Theorem 5.2 (Kucera)**.** *If the group R^-/I_S^- is finite, then*

$$[R^- : I_S^-] = 2^b \cdot h(K)^-,$$

where $b = 0$ if $g = 1$ and

$$b = -1 + \sum_{i=1}^{g} \frac{\phi(m_i)}{s_i}$$

if $g \geq 2$.

To overcome the obstacle mentioned above, Sinnott considered a new ideal, which we call the Sinnott ideal[1] of K and denote it by S. We are uncertain about the origin of the definition of the Sinnott ideal, whether it was first defined by Iwasawa or by Sinnott himself. However, the first mention of this definition in the literature is in Sinnott's 1978 article [25]. If I_S^- is replaced by S^-, then in [25] it is proved that the index $[R^- : S^-]$ is finite for any imaginary cyclotomic field (see Theorem 5.8). However, Sinnott attributes the proof of this finiteness property mentioned in [25] to Iwasawa.

We give a brief description of the remainder of the chapter. In Section 5.1, we give an equivalent definition of the Stickelberger ideal, which motivates the definition of the Sinnott ideal. In Section 5.2, we give Sinnott's generalization of Iwasawa's class number formula and present a brief outline of its proof. In Section 3, we show that the Sinnott ideal of K annihilates the ideal class group of K.

5.1 Definition of Sinnott Ideal

We now define the Sinnott ideal S of K. The motivation to define the Sinnott ideal comes from the following proposition, which suggests an equivalent definition of the Stickel-

[1] Sinnott in [25] calls S the Stickelberger ideal of K. However, to avoid confusion, we call this the Sinnott ideal of K

berger ideal. For any integer a, set

$$\Theta(a) := \sum_{\substack{t \bmod m \\ (t,m)=1}} \left\{ -\frac{at}{m} \right\} \sigma_t^{-1} \in \mathbb{Q}[G].$$

Proposition 5.3. *Let I' be the subgroup of $\mathbb{Q}[G]$ generated by the elements $\Theta(a)$, for all a from a complete set of integers coprime to m and distinct modulo m. Then the Stickelberger ideal I_S of K is the intersection of R with I'.*

Proof. For any integer a coprime to m we have

$$\Theta(a) = \sigma_{-a}\Theta(-1),$$

which implies that I' is an R-module and

$$I' = (\Theta(-1))R.$$

We know that $\Theta(-1)$ is the Stickelberger element of K, therefore, by definition $I' \cap R$ is the Stickelberger ideal of K. ■

Let S' be the subgroup of $\mathbb{Q}[G]$ generated by the elements $\Theta(a)$, for all a from the complete set of integers distinct modulo m. Note that to define I' we considered a from the complete set of integers *coprime* to m and distinct modulo m.

Definition 5.4 (Sinnott Ideal)**.** The Sinnott ideal S of K is defined as the intersection of S' and R:

$$S := S' \cap R.$$

5.2 Sinnott's Theorem

The following generalization of Iwasawa's class number formula to arbitrary cyclotomic fields is due to.

Theorem 5.5 (Sinnott)**.** *Let $m > 2$ be an integer, g be the number of distinct primes that divide m, and $G = \mathrm{Gal}(K/\mathbb{Q})$. Then*

$$[\mathbb{Z}[G]^- : S^-] = 2^a h(K)^-,$$

where $a = 0$ *if* $g = 1$, *and*

$$a = 2^{g-2} - 1, \quad \text{if } g > 1.$$

To justify that Sinnott's theorem 5.5 is indeed a generalization of Iwasawa's theorem, we claim that when m is a prime power then the minus part of the Stickelberger and Sinnott ideal of K coincide: $I_S^- = S^-$. By definition, $\Theta(-1)$ is the Stickelberger element of K, which implies that $I_S^- \subseteq S^-$.

However, when m is a prime power, Theorem 1.2 and Theorem 5.5 imply that

$$[R^- : I_S^-] = [R^- : S^-].$$

As $I_S^- \subseteq S^-$, we must have $I_S^- = S^-$.

In fact, Kučera proved that $S^- = I_S^-$ if and only if m is a prime power (see [17, Prop. 4.3]).

If χ is any character of G, then from the isomorphism $G \cong (\mathbb{Z}/m\mathbb{Z})^*$ it follows that χ is a Dirichlet character of modulus m (see Section 2.2). We also use the notation χ to denote the *primitive* Dirichlet character that induces the Dririchlet character χ.

For any prime p, define

$$\overline{\mu}_p = \sum_{\chi} \overline{\chi}(p)\varepsilon_\chi,$$

where $\overline{\chi}$ denotes the complex conjugate of the primitive Dirichlet character associated to χ, and ε_χ is the idempotent associated to χ in $\mathbb{C}[G]$:

$$\varepsilon_\chi = \frac{1}{\#G} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1};$$

here $\#G$ denotes the order of G.

Note that $\overline{\mu}_p$ actually lies in $\mathbb{Q}[G]$ (viewed as subring of $\mathbb{C}[G]$).

For any positive divisor f of m, let H_f denote the subgroup of G consisiting of the elements of σ_t, with $t \equiv 1 \pmod{f}$, $(t,m) = 1$. Let $s(H_f)$ denote the sum, in $\mathbb{C}[G]$, of the elements of H_f. The element $s(H_f)$ obviously lies in R.

Definition 5.6. Define U to be the R-submodule of $\mathbb{C}[G]$ generated by the elements

$$s(H_f) \prod_{p|f} (1 - \overline{\mu}_p),$$

as f varies over the divisors of m and the product is taken over the distinct primes p

dividing f.

Proposition 5.7. *U is contained in $\mathbb{Q}[G]$, and is isomorphic as an abelian group to $\mathbb{Z}^{\phi(m)}$.*

Proof. See [25, Proposition 2.2]. ■

Let $e^+ = (1+j)/2$, $e^- = (1-j)/2$. Then the following result was proved by Iwasawa.

Theorem 5.8 (Iwasawa)**.** *S^- has finite index in R^-, and*

$$[R^- : S^-] = h(K)^-(e^-R : e^-U)/Q,$$

where Q is the factor appearing in the analytic class number formula (see Theorem 4.9).

We remark that $(e^-R : e^-U)$ is defined, in the sense of Section 4.4. It follows immediately from Proposition 5.7 that e^-U is finitely generated as an abelian group and that its span in $\mathbb{Q}[G]$ is $e^-\mathbb{Q}[G]$. The same statements are obviously true of e^-R, hence $(e^-R : e^-U)$ is defined. In particular, this implies that $[R^- : S^-]$ is finite. For the proof of Theorem 5.8 see [25, Theorem 3.1].

The analytic class number formula played a crucial role in Sinnott's work, as did the Galois module U introduced by Iwasawa. An important technical advance made by Sinnott was his determination of the cohomology groups of U with respect to the action of complex conjugation; theses cohomology groups had to be determined in order to compute the factors of 2 in Sinnott's index formulas.

Theorem 5.9 (Sinnott)**.** *Let g be the number of primes dividing m. Then*

$$(e^-R : e^-U) = \begin{cases} 1 & \text{if } g = 1, \\ 2^{2^{g-2}} & \text{if } g > 1. \end{cases} \tag{5.1}$$

Proof. See [25, Section 6]. ■

Combining Theorem 5.8 and Theorem 5.9 and using the fact that $Q = 1$ if $g = 1$ and $Q = 2$ if $g > 1$ (see 4.3), we obtain Theorem 5.5.

5.3 Sinnott Ideal as Annihilators of Class Group

Let p be an integral prime relatively prime to m. Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{m}$, and $q = p^f$. Let $\mathfrak{q}$ be a prime ideal in $\mathbb{Q}(\zeta_{q-1})$ above p, and $\mathfrak{p}_m$

be the prime ideal of $\mathbb{Q}(\zeta_m)$ below $\mathfrak{q}$. Let $\mathscr{O} = \mathbb{Z}[\zeta_m]$. We have $q = p^f = N(\mathfrak{p}_m) = |\mathscr{O}/\mathfrak{p}_m|$.

Proposition 5.10. *We claim that* $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1} \in \mathscr{O}$ *are distinct modulo* $\mathfrak{p}_m$.

Proof. Observe that

$$\frac{x^m - 1}{x - 1} = 1 + x + \cdots + x^{m-1} = \prod_{i=1}^{m-1} (x - \zeta_m^i).$$

Substituting $x = 1$, we get

$$m = \prod_{i=1}^{m-1} (1 - \zeta_m^i).$$

If $\zeta_m^i \equiv \zeta_m^j \pmod{\mathfrak{p}_m}$, for some $i \neq j$, if $j > i$, then $\zeta_m^{j-i} \equiv 1 \pmod{\mathfrak{p}_m}$, so that $m \equiv 0 \pmod{\mathfrak{p}_m}$, which is a contradiction because $\mathfrak{p}_m$ is relatively prime to m. Thus, $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}$ are distinct $\pmod{\mathfrak{p}_m}$. ■

Proposition 5.11. *Let* $\alpha \in \mathscr{O}$, *and* $\alpha \notin \mathfrak{p}_m$. *Then there is a unique integer* i *modulo* m *such that*

$$\alpha^{(q-1)/m} \equiv \zeta_m^i \pmod{\mathfrak{p}_m}.$$

Proof. Since the order of $(\mathscr{O}/\mathfrak{p}_m)^*$ is $q - 1$, we have $\alpha^{q-1} \equiv 1 \pmod{\mathfrak{p}_m}$. Hence, $\alpha^{\frac{q-1}{m}} \pmod{\mathfrak{p}_m}$ is an m-th root of unity, and the claim follows. ■

For $\alpha \in \mathscr{O}$. Define

1. $\chi_{\mathfrak{p}_m}(\alpha) = 0$ if $\alpha \in \mathfrak{p}_m$; and
2. if $\alpha \notin \mathfrak{p}_m$, $\chi_{\mathfrak{p}_m}(\alpha)$ is the unique m-th root of unity such that

$$\alpha^{(q-1)/m} \equiv \chi_{\mathfrak{p}_m}(\alpha) \pmod{\mathfrak{p}_m}.$$

Then $\chi_{\mathfrak{p}_m}$ is a multiplicative character of order m of $\mathbb{F}_q = \mathscr{O}/\mathfrak{p}_m$. Let $\psi_{\mathfrak{p}_m}$ be the character of the additive group of $\mathbb{F}_q$, with values in the group of p-th roots on unity, defined by

$$\psi_{\mathfrak{p}_m}(x) := \zeta_p^{\mathrm{Tr}(x)}, \quad x \in \mathbb{F}_q;$$

where Tr denote the trace map $\mathbb{F}_q \to \mathbb{Z}/p\mathbb{Z}$.

Definition 5.12. For any integer a, we define the **generalized** Gauss sum $g(a,\mathfrak{p}_m)$ by

$$g(a,\mathfrak{p}_m) := -\sum_{x\in\mathbb{F}_q} \chi_{\mathfrak{p}_m}(x)^a \psi_{\mathfrak{p}_m}(x).$$

Clearly, $g(a,\mathfrak{p}_m)$ lies in $\mathbb{Q}(\zeta_m,\zeta_p)$. We know that $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m,\zeta_p)/\mathbb{Q}(\zeta_m))$ is defined by $\zeta_p \mapsto \zeta_p^t$, for some integer t prime to p. Then

$$g(a,\mathfrak{p}_m)^\sigma = -\sum_{x\in\mathbb{F}_q} \chi_{\mathfrak{p}_m}(x)^a \psi_{\mathfrak{p}_m}(x)^\sigma \tag{5.2}$$

$$= -\sum_{x\in\mathbb{F}_q} \chi_{\mathfrak{p}_m}(x)^a \psi_{\mathfrak{p}_m}(tx) \tag{5.3}$$

$$= \chi_{\mathfrak{p}_m}(t)^{-a} g(a,\mathfrak{p}_m). \tag{5.4}$$

Taking the m-th power of both sides of the above equation we conclude that $g(a,\mathfrak{p}_m)^m$ lies in $\mathbb{Q}(\zeta_m)$ as $\chi_{\mathfrak{p}_m}^m$ is the trivial character. Let $d = \frac{q-1}{m}$. Recall that the Teichmuller character ω of $\mathbb{F}_q$ is the *unique* character that satisfies

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

We have

$$\omega^d(\alpha) \equiv \alpha^d \pmod{\mathfrak{p}_m},$$

and $\chi_{\mathfrak{p}_m}(\alpha) \equiv \alpha^d \pmod{\mathfrak{p}_m}$. The uniqueness property implies that $\chi_{\mathfrak{p}_m} = \omega^d$. Therefore, we can write the generalized Gauss sums in terms of *ordinary* Gauss sums:

$$g(a,\mathfrak{p}_m) = g(\omega^{ad}).$$

For any $r \in \mathbb{Z}$, from Theorem 3.7 we have

$$(g(\omega^{-rd})^m) = \mathfrak{p}^{\theta_r},$$

where

$$\theta_r = \frac{m}{p-1} \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^*/\langle p\rangle} s(rtd)\sigma_t^{-1}.$$

Substitute $r = -a$. Then by using the same argument as in Theorem 3.10, we conclude

that

$$\theta_{-a} = m \cdot \sum_{\substack{t \bmod m \\ (t,m)=1}} \left\{ -\frac{at}{m} \right\} \sigma_t^{-1} = m\Theta(a).$$

We have thus proved the following proposition.

Proposition 5.13. $(g(a,\mathfrak{p}_m)^m) = g(\omega^{ad}) = \mathfrak{p}_m^{m\Theta(a)}$

If $a \equiv 0 \pmod{m}$, then $\Theta(a) = 0$. If $a \not\equiv 0 \pmod{m}$, then using $\{x\} + \{-x\} = 1$, we have $-\Theta(a) = \Theta(-a) - N$, where $N = \sum_{\sigma \in G} \sigma$. We may write any $\gamma \in S'$ in the form $\gamma = \sum_{i=1}^n \Theta(a_i) - rN$, with integers $n, r, a_1, \ldots, a_n$.

Proposition 5.14. *Let $\gamma = \sum_{i=1}^n \Theta(a_i) - rN \in S'$. Then $\gamma \in S$ if and only if $\sum_{i=1}^n a_i \equiv 0 \pmod{m}$.*

Proof. The coefficient of σ_t^{-1} in $\sum_{i=1}^n \Theta(a_i)$ is

$$c_t = \sum_{i=1}^n \left\{ -\frac{a_i t}{m} \right\}.$$

Using the congruence $\{x\} \equiv x \pmod{\mathbb{Z}}$, we see immediately that $c_t \in \mathbb{Z}$ if and only if $\sum -\frac{a_i t}{m} \in \mathbb{Z}$, equivalently, $\sum_{i=1}^n a_i \equiv 0 \pmod{m}$. This proves our claim. ∎

We will extend the definition of *generalized* Gauss sums $g(a,\mathfrak{p}_m)$ as follows, by defining $g(A,\mathfrak{a})$ whenever A is an n-tuple of integers and that $\mathfrak{a}$ is an integral ideal prime to m in $\mathbb{Q}(\zeta_m)$. This symbol is defined by Definition 5.12 when A is a sequence of a term and $\mathfrak{a}$ is a prime ideal; it will be defined in general by the conditions:

$$g((A,B),\mathfrak{a}) = g((A),\mathfrak{a}) \cdot g((B),\mathfrak{a}), \tag{5.5}$$

and

$$g(A,\mathfrak{ab}) = g(A,\mathfrak{a}) \cdot g(A,\mathfrak{b}), \tag{5.6}$$

where A, B are n-tuples of integers and $\mathfrak{a}, \mathfrak{b}$ are integral ideals of $\mathbb{Q}(\zeta_m)$ relatively prime to m.

Let $A = (a_1, a_2, \ldots, a_n)$ be an n-tuple of integers, and $\mathfrak{a}$ be an integral ideal relatively prime to m. Suppose $= \prod_{\mathfrak{p}} \mathfrak{p}$. Then we have

$$g(A,\mathfrak{a}) = \prod_{\mathfrak{p}} g(A,\mathfrak{p}).$$

Let $\mathfrak{p}_m$ be a prime of $\mathbb{Q}(\zeta_m)$ that divides $\mathfrak{a}$, choose a prime $\mathfrak{q}$ of $\mathbb{Q}(\zeta_{q-1})$, such that $\mathfrak{p}_m$ is the prime of $\mathbb{Q}(\zeta_m)$ lying below $\mathfrak{q}$. From Proposition 5.13 we have:

$$(g(A,\mathfrak{p}_m)^m) = \prod_{i=1}^{n} g(a_i,\mathfrak{p}_m)^m = \prod_{i=1}^{n} \mathfrak{p}_m^{m\Theta(a_i)} = \mathfrak{p}_m^{m\sum_i \Theta(a_i).} \tag{5.7}$$

Finally, using Equation 5.6 we have

$$(g(A,\mathfrak{a})^m) = \mathfrak{a}^{m\sum_i \Theta(a_i)}. \tag{5.8}$$

Let p be the prime of $\mathbb{Q}$ below $\mathfrak{q}$ and $|A| = \sum_{i=1}^{n} a_i$. Let

$$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m,\zeta_p)/\mathbb{Q}(\zeta_m))$$

be defined by $\zeta_p \mapsto \zeta_p^t$ for some t relatively prime to p, then using Equation 5.2 we get

$$g(A,\mathfrak{p}_m)^\sigma = \prod_{i=1}^{n} g(a_i,\mathfrak{p}_m)^\sigma = \prod_{i=1}^{n} \chi_{\mathfrak{p}_m}(t)^{-a_i} g(a_i,\mathfrak{p}_m) \tag{5.9}$$

$$= \chi_{\mathfrak{p}_m}(t)^{-|A|} g(A,\mathfrak{p}_m). \tag{5.10}$$

Theorem 5.15. *The Sinnott ideal S of $\mathbb{Q}(\zeta_m)$ annihilates the ideal class group Cl_m of $\mathbb{Q}(\zeta_m)$.*

Proof. relatively prime

Since γ *a priori* is an element of S', it is of the form $\gamma = \sum_{i=1}^{n} \Theta(a_i) - rN$ for integers $r,n,a_1,\ldots,a_n$. Let $A = (a_1,\ldots,a_n)$ and $|A| = \sum_{i=1}^{n} a_i$. Then from Proposition 5.14 $\gamma \in S$ if and ony if $|A| \equiv 0 \pmod{m}$. From Equation 5.9 we conclude that $g(A,\mathfrak{a}) \in \mathbb{Q}(\zeta_m)$.

From Equation 5.8 we have $(g(A,\mathfrak{a})^m) = \mathfrak{a}^{m\sum_i \Theta(a_i)}$. Thus

$$(g(A,\mathfrak{a})) = \mathfrak{a}^{\sum_i \Theta(a_i)}.$$

Let $N(\mathfrak{a})^{-r} = \mathfrak{a}^{-rN}$. Then

$$(g(A,\mathfrak{a})N(\mathfrak{a})^{-r}) = \mathfrak{a}^{\sum_i \Theta(a_i)-rN} = \mathfrak{a}^{\gamma}.$$

This proves our claim. ∎

We end our thesis by addressing an analogous question to Question 4.

Question 5. Let $K = \mathbb{Q}(\zeta_m)$, $G = \mathrm{Gal}(K/\mathbb{Q})$, and S be the Sinnott ideal of K. Can we find $\alpha \in \mathbb{Z}[G] \setminus S$, such that α annihilates the ideal class group of K?

This question has been answered positively by Greither and Kucěra in [9]. It turns out that in several frequently occurring situations there exist annihilators of K that are not contained in the Sinnott ideal.

Bibliography

[1] Greg W. Anderson, *Another look at the index formulas of cyclotomic number theory*, J. Number Theory **60** (1996), no. 1, 142–164. MR 1405731

[2] Emil Artin, *Galois Theory*, second ed., Notre Dame Mathematical Lectures, no. 2, University of Notre Dame, Notre Dame, Ind., 1944. MR 0009934

[3] Yuri F. Bilu, Yann Bugeaud, and Maurice Mignotte, *The problem of Catalan*, Springer, Cham, 2014. MR 3288807

[4] R. Chapman, *The Stickelberger Ideal*, unpublished manuscript, 1999.

[5] Joseph Louis de Lagrange, *Reflections on the algebraic resolution of equations*, `http://sites.mathdoc.fr/cgi-bin/oeitem?id=OE_LAGRANGE__3_205_0`, (Accessed on 03/09/2022).

[6] Carl Friedrich Gauss, *Disquisitionum circa aequationes puras*, Werke II.

[7] ———, *Summatio quarumdam serierum singularium*, Dieterich, 1808 (lat).

[8] ———, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. MR 837656

[9] Cornelius Greither and Radan Kučera, *Annihilators of minus class groups of imaginary abelian fields*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 5, 1623–1653. MR 2364145

[10] Helmut Hasse, *Über die Klassenzahl abelscher Zahlkörper*, first ed., Springer-Verlag, Berlin, 1985, With an introduction to the reprint edition by Jacques Martinet. MR 842666

[11] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 1070716

[12] Kenkichi Iwasawa, *A class number formula for cyclotomic fields*, Ann. of Math. (2) **76** (1962), 171–179. MR 154862

[13] Vijay Jha, *The Stickelberger ideal in the spirit of Kummer with application to the first case of Fermat's last theorem*, Queen's Papers in Pure and Applied Mathematics, vol. 93, Queen's University, Kingston, ON, 1993, Dissertation, Panjab University, Chandigarh, 1992. MR 1223999

[14] C. Jordan, *Sur les sommes de gauss à plusieurs variables.*, C. R. Acad. Sci. Paris **73**, 1316–1319.

[15] Helmut Koch, *Number theory*, Graduate Studies in Mathematics, vol. 24, American Mathematical Society, Providence, RI, 2000, Algebraic numbers and functions, Translated from the 1997 German original by David Kramer. MR 1760632

[16] Daniel S. Kubert and Serge Lang, *Stickelberger ideals*, Math. Ann. **237** (1978), no. 3, 203–212. MR 508752

[17] Radan Kučera, *On a certain subideal of the Stickelberger ideal of a cyclotomic field*, Arch. Math. (Brno) **22** (1986), no. 1, 7–19. MR 868116

[18] Franz Lemmermeyer, *Reciprocity laws*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000, From Euler to Eisenstein. MR 1761696

[19] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn. MR 1429394

[20] Nimish Kumar Mahapatra, Prem Prakash Pandey, and Mahesh Kumar Ram, *Prime ideals of higher residue degree and annihilators of class groups*, Submitted.

[21] M. Ram Murty and Jody Esmonde, *Problems in algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 190, Springer-Verlag, New York, 2005. MR 2090972

[22] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-

Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859

[23] Peter Schmid, *The Stickelberger element of an imaginary quadratic field*, Acta Arith. **91** (1999), no. 2, 165–169. MR 1726187

[24] René Schoof, *Catalan's conjecture*, Universitext, Springer-Verlag London, Ltd., London, 2008. MR 2459823

[25] W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. (2) **108** (1978), no. 1, 107–134. MR 485778

[26] ———, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980/81), no. 2, 181–234. MR 595586

[27] Ladislav Skula, *Another proof of Iwasawa's class number formula*, Acta Arith. **39** (1981), no. 1, 1–6. MR 638737

[28] ———, *Some bases of the Stickelberger ideal*, Math. Slovaca **43** (1993), no. 5, 541–571. MR 1273710

[29] Ludwig Stickelberger, *Ueber eine verallgemeinerung der kreistheilung*, Mathematische Annalen **37** (1890), 321–367.

[30] Francisco Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. (2) **128** (1988), no. 1, 1–18. MR 951505

[31] Dinesh S. Thakur, *Gauss sums for* $\mathbf{F}_q[T]$, Invent. Math. **94** (1988), no. 1, 105–112. MR 958591

[32] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575

[33] Heinrich Weber, *Ueber die mehrfachen gaussch ischen summen.*, (1872).

[34] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR 29393

[35] ———, *Jacobi sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. **73** (1952), 487–495. MR 51263

[36] ———, *Sommes de Jacobi et caractères de Hecke*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1974), no. 1, 1–14. MR 392859