On Ideal Class Groups of Cyclotomic Fields

Adolfo Rafael Alvaro Rúa Vargas

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy at
Concordia University
Montreal, Quebec, Canada

March 2006

Library and
Archives Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-16272-9
Our file Notre référence
ISBN: 978-0-494-16272-9

Abstract

On Ideal Class Groups of Cyclotomic Fields

Adolfo Rúa, Ph.D.

Concordia University, 2006

Let m be an integer $\geqslant 3$ and let F be one of the fields $\mathbb{Q}(\zeta_m)^+$ or $\mathbb{Q}(\zeta_m)$. Denote the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ by Δ and let p be an odd prime such that $p \nmid |\Delta|$, where $|\Delta|$ denotes the order of Δ. Let A denote the p-part of the ideal class group of F and $(E/C)_p$ denote the p-part of the group E of units of F modulo the subgroup C of cyclotomic units.

For $F = \mathbb{Q}(\zeta_m)^+$, the equality $|e_\rho A| = |e_\rho (E/C)_p|$ is proven, where e_ρ is the idempotent corresponding to an irreducible higher dimensional character ρ of Δ into $\mathbb{Z}_p$. Furthermore, it is shown that $e_\rho(E/C)_p$ is a principal $\mathbb{Z}_p[\Delta]$-module.

For $F = \mathbb{Q}(\zeta_m)$, assuming certain conditions for m and p, the equality $|e_\rho A| = (B_{1,\rho^{-1}})_p$ is obtained, where e_ρ is the idempotent corresponding to an irreducible higher dimensional odd character ρ of Δ into $\mathbb{Z}_p$ distinct from the Teichmüller character and $(B_{1,\rho^{-1}})_p$ is the highest power of p dividing the p-adic integer $B_{1,\rho^{-1}}$, which is defined in terms of generalized Bernoulli numbers.

The method applied is an extension of Rubin's early treatment of Kolyvagin's Euler systems.

Acknowledgements

I express my thanks to the Department of Mathematics of Concordia University and ISM for the financial support during my studies in the Ph.D. Program.

I also express my gratefulness to professors of the above-mentioned department and CICMA for transmitting to me fundamental knowledge in number theory.

I am specially grateful to Professor Francisco Thaine, who has supervised this thesis, for valuable guidance, willing help, and long-standing financial support.

My warmest thanks go to my family for their patience, affection, unconditional help, and constant encouragement.

Table of Contents

List of Symbols

$\lvert\cdot\rvert$	the order of a group or the cardinality of a set	
$(\cdot\,,\cdot)$	greatest common divisor of two integers	
$\Vert$	exactly divides	Section 1.2, page 9
$(\cdot)_p$	p-part of a number	Section 3.6, page 58
α		Section 2.1, page 15
$\alpha(L)$		Section 2.1, page 15
$\alpha(L,\mathcal{L})$		Section 3.1, page 30
A	p-part of the ideal class group of F	Introduction, page 3
$A(L)$	p-part of the ideal class group of $F(L)$	Chapter 3, page 28
β_L		Section 2.1, page 17
$B_{1,\chi}$	generalized Bernoulli number	Section 3.6, page 56
$B_{1,\rho^{-1}}$	$\prod_{\chi\in X_\rho} B_{1,\chi^{-1}}$	Section 3.6, page 58
C	group of cyclotomic units	Chapter 2, page 14
condition **C**		Section 3.5, page 50
$\delta(L)$		Section 3.1, page 34
Δ	$\mathrm{Gal}(F/\mathbb{Q})$	Introduction, page 3
$\Delta(L)$	$\mathrm{Gal}(F(L)/\mathbb{Q})$	Chapter 3, page 28
$\widehat{\Delta}$	group of p-adic characters of Δ	Section 1.2, page 6

D_ℓ		Section 2.1, page 16 Section 3.1, page 29
D_L	$\prod_{\ell \mid L} D_\ell$	Section 2.1, page 16 Section 3.1, page 29
e_χ	idempotent corresponding to χ	Section 1.2, page 6
e'_ρ	an element of $\mathbb{Z}[\Delta]$ satisfying $e'_\rho \equiv e_\rho \bmod M$	Chapter 2, page 14 Chapter 3, page 28
$\bar{e}_\rho$	reduction of e_ρ mod p	Section 1.2, page 8
E	group of units of F	Chapter 2, page 14
$(E/C)_p$	p-part of E/C	Chapter 2, page 14
φ_λ		Section 3.4, page 42
$\varphi_\mathcal{L}$		Section 3.4, page 41
F	$\mathbb{Q}(\zeta_m)^+$ $\mathbb{Q}(\zeta_m)$	Chapter 2, page 14 Chapter 3, page 28
$F(L)$	$F(\zeta_L)$	Section 2.1, page 15 Chapter 3, page 28
$\mathbb{F}_q$	finite field with q elements	
G_L	$\mathrm{Gal}(F(L)/F)$	Section 2.1, page 15 Chapter 3, page 29
$H^j(G, N)$	j th cohomology group of G with coefficients in N	
$\mathrm{Im}\,\chi$	image of χ	Section 2.4, page 25 Section 3.5, page 47
$\mathrm{ind}_\lambda, \mathrm{ind}_\mathcal{L}$		Section 3.4, page 41
$\kappa(L)$		Section 2.1, page 17

$\kappa(L,\lambda)$		Section 3.1, page 34
λ	a prime of F above ℓ	Section 2.2, page 18 Chapter 3, page 28
ℓ	an odd rational prime satisfying $\ell \equiv 1 \bmod mM$	Section 2.1, page 15 Chapter 3, page 28
$\mathcal{L}$	a prime of $F(\ell L)$ above λ a prime of $F(L)$ above λ	Section 2.2, page 18 Chapter 3, page 29
L	a product of distinct rational primes ℓ	Section 2.1, page 15 Chapter 3, page 28
$\mathbb{L}$	set of products L	Section 2.1, page 15 Chapter 3, page 28
μ_M	group of Mth roots of unity	Chapter 3, page 28
m	an integer satisfying $m \geqslant 3$, $m \not\equiv 2 \bmod 4$	Introduction, page 2
M	$p \cdot \lvert (E/C)_p \rvert \cdot \lvert A \rvert$ $p^{r(1)+1} \cdot \lvert e_\rho A \rvert$	Chapter 2, page 14 Section 3.6, page 53
N_ℓ		Section 2.1, page 16 Section 3.1, page 29
N_L	$\prod_{\ell \mid L} N_\ell$	Section 2.1, page 16 Section 3.1, page 29
ω	Teichmüller character of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathbb{Z}_p$	Section 1.2, page 6
Ω	set of irreducible higher dimensional characters ρ	Section 1.2, page 7
$\mathcal{O}_{X_\rho}$	integer ring of $\mathbb{Q}_p(X_\rho)$	Section 3.6, page 56
p	an odd rational prime not dividing $\lvert \Delta \rvert$	Introduction, page 3
$\mathbb{Q}_p$	field of p-adic numbers	

$\mathbb{Q}_p(X_\rho)$		Section 3.5, page 47
ρ	an irreducible higher dimensional character of Δ into $\mathbb{Z}_p$	Section 1.2, page 7 Chapter 2, page 14 Chapter 3, page 28
$r(L)$		Section 3.6, page 53
$\sigma_s = \sigma_{s_\ell}$	a generator of G_ℓ	Section 2.1, page 15 Section 3.1, page 29
$s = s_\ell$	a primitive root mod ℓ	Section 2.1, page 15 Section 3.1, page 29
$s(L)$		Section 3.1, page 31
$s'(L, \ell)$		Section 3.3, page 39
$S(\mathcal{L}, \zeta_\ell)$		Section 3.1, page 30
$S(\xi, {\zeta_\ell}^{\mathrm{T}r})$	a Gauss sum	Section 1.3, page 10
$\theta(L)$		Section 3.1, page 31
$\theta'(L, \ell)$		Section 3.3, page 39
Tr	trace of $\mathbb{F}_q/\mathbb{F}_\ell$	Section 1.3, page 10
v_λ , $v_{\mathcal{L}}$	valuation at λ, valuation at $\mathcal{L}$	
χ	a p-adic character of Δ	Section 1.2, page 6
X_ρ	orbit of ρ	Section 1.2, page 7
ζ_m	a primitive mth root of unity	
$\mathbb{Z}_p$	ring of p-adic integers	

Introduction

The purpose of this thesis is to study ideal class groups of cyclotomic fields by using higher dimensional p-adic characters of the corresponding Galois groups. Specifically, p being an odd prime, the order of the ρ-component of the p-part of the class group of a field F with Galois group Δ over $\mathbb{Q}$ is determined for an irreducible higher dimensional character ρ of Δ into $\mathbb{Z}_p$ in two situations: when F is the maximal real subfield of a cyclotomic field (Chapter 2), and when F is a cyclotomic field and the character ρ is odd (Chapter 3). Both situations are developed in the semisimple case, that is, assuming that p does not divide the order of Δ. In the second situation, an additional condition is adopted, which will be defined in Section 3.5. These results (without assuming the additional condition) were conjectured by Gras [G1] for abelian number fields in 1977.

Furthermore, in Chapter 2 the structure of the ρ-component of the p-part of the group of units of F modulo cyclotomic units is determined.

This work is detailed and based only on fundamental results in number theory, which are stated in Chapter 1.

The results mentioned in the first paragraph have counterparts in terms of one-dimensional p-adic Dirichlet characters χ. These analogous results, assuming that $p \nmid \operatorname{ord} \chi$, were obtained first as consequences of the main conjecture of Iwasawa theory for abelian number fields by Mazur-Wiles [MW] in 1984. In this manner, the Gras conjectures became proven. The methods used by Mazur and Wiles relied on modular constructions of unramified extensions of abelian number fields. In comparison, the methods in the present thesis are much simpler and the results are obtained directly.

In 1988, Kolyvagin [K2] introduced Euler systems, which have become a very important tool with several applications in number theory. Kolyvagin used Euler systems to provide direct proofs of the results mentioned in the first paragraph in the case $m = p$, among other advances. He also suggested that Euler systems could be used to obtain another proof of the main conjecture for abelian number fields.

Detailed versions of the results of Kolyvagin mentioned above were given by Rubin. The situation $F = \mathbb{Q}(\zeta_p)^+$ was presented in an appendix to [L] in 1990 and the situation $F = \mathbb{Q}(\zeta_p)$ was treated in [R1] in 1991. These works are generalized by the results referred in the first paragraph.

Besides relying on the works of Rubin mentioned above, the methods in this thesis require the repeated application of a congruence for elements in $\mathbb{Z}_p[\Delta]e_\rho$, given in Proposition 1.4. This application originated in an idea of Rubin, which appears in the appendix of the paper of Thaine [T] of 1988, where it is used to find annihilators for the p-part of the ideal class group of a real abelian number field.

In 1990, in the appendix to [L] already mentioned, Rubin used Euler systems to prove the main conjecture for $\mathbb{Q}(\zeta_{p^\infty})$ for an odd prime p. By the same means, in 1992, Greither [G2] proved the main conjecture for any abelian number field including the case $p = 2$. Moreover, Greither derived from the main conjecture the results for one-dimensional characters χ referred above, including the case $p = 2$ and dropping the condition $p \nmid \operatorname{ord} \chi$.

Direct proofs of the results for one-dimensional Dirichlet characters χ, maintaining the condition $p \nmid \operatorname{ord} \chi$ with p odd, were achieved by Rubin [R2] in 2000 by using Euler systems of cohomology classes of p-adic representations. By contrast, the method of higher dimensional characters presented in this thesis uses only one result in group cohomology (the inflation-restriction exact sequence).

Throughout this thesis, m is a fixed integer satisfying the conditions $m \geq 3$ and $m \not\equiv 2 \bmod 4$, and Δ denotes the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ in the two situations

$F = \mathbb{Q}(\zeta_m)^+$ and $F = \mathbb{Q}(\zeta_m)$. In addition, p represents an odd prime not dividing $|\Delta|$, and A denotes the p-part of the ideal class group of F.

This work is based on the following fundamental results: Proposition 1.4, results on unramified extensions of the p-adic field $\mathbb{Q}_p$, the inflation-restriction exact sequence, the Chebotarev density theorem, Stickelberger's theorem, properties of Gauss sums including the Davenport-Hasse distribution theorem, and the existence of Minkowski units. These results are taken from the books [C], [J], [K1], [L], [W1], [W2] and are presented briefly in Chapter 1.

In Chapter 2, where $F = \mathbb{Q}(\zeta_m)^+$, the equality $|e_\rho A| = |e_\rho(E/C)_p|$ is obtained, where ρ is an irreducible higher dimensional character of Δ into $\mathbb{Z}_p$, and $(E/C)_p$ denotes the p-part of the group E of units of F modulo the subgroup C of cyclotomic units. Furthermore, it is shown that the ρ-component of the p-part of the group of units of F modulo cyclotomic units is a principal $\mathbb{Z}_p[\Delta]$-module. The exposition is based on Chapter 15 of Washington's book [W1], where the particular case $m = p$ is considered.

Chapter 3, where $F = \mathbb{Q}(\zeta_m)$, is devoted to proving the equality $|e_\rho A| = (B_{1,\rho^{-1}})_p$, where ρ is an irreducible higher dimensional odd character of Δ into $\mathbb{Z}_p$ distinct from the Teichmüller character, and $(B_{1,\rho^{-1}})_p$ is the p-part of the number $B_{1,\rho^{-1}}$ to be defined in Section 3.6. This result is obtained assuming condition **C**, which will be defined in Section 3.5. The discussion generalizes and closely follows Rubin's paper [R1], which presents a detailed exposition of Kolyvagin's theory for Gauss sums and gives the equality above in the case $m = p$. Some difficulties had to be overcome in order to attain such generalization, as the handling of the group Δ when it is not cyclic and the extension of Theorem 3.1 in [R1] to Proposition 3.14.

Concerning notation, if H is a subgroup of an abelian group G, the class aH of an element a in G will sometimes be denoted simply by a. The congruence

$\alpha \equiv \beta \mod \wp$, where $\wp$ is a prime ideal of a number field K and $\alpha, \beta \in K^{\times}$, will mean that $\alpha\beta^{-1} \equiv 1 \mod \mathfrak{m}_{\wp}$, where $\mathfrak{m}_{\wp}$ is the maximal ideal of the local ring at $\wp$. Furthermore, group ring actions on multiplicative groups will often be written additively; for example $(\sigma - 1)\alpha$ will stand for $\alpha^{\sigma-1} = \sigma\alpha/\alpha$.

CHAPTER 1

Preliminaries

1.1 Unramified Extensions of the p-adic Field

The brief explanation that follows about finite unramified extensions of the p-adic field $\mathbb{Q}_p$ is relevant for Section 3.6. The results presented are fully developed in [C], Chapter 8, Section 2, and [K1], Chapter 3, Section 3.

Consider the extension $\mathbb{Q}_p(\zeta_d)$ of the p-adic field $\mathbb{Q}_p$. Denote the ring of integers of $\mathbb{Q}_p(\zeta_d)$ by $\mathcal{O}$. There is a unique prime $\wp$ of $\mathcal{O}$ above p. The prime $\wp$ is a maximal ideal, so the quotient $\mathcal{O}/\wp$ is a field. The degree $f = [\mathcal{O}/\wp : \mathbb{Z}_p/p\mathbb{Z}_p]$ is known as the residual degree of the extension $\mathbb{Q}_p(\zeta_d)/\mathbb{Q}_p$, while the ramification index e is defined by the equality $p\mathcal{O} = \wp^e$. Denoting $n = [\mathbb{Q}_p(\zeta_d) : \mathbb{Q}_p]$, an important relation is given by the equality $n = ef$.

In the case $p \nmid d$, the extension $\mathbb{Q}_p(\zeta_d)/\mathbb{Q}_p$ is unramified[†], that is, $e = 1$. Thus $n = f$, in view of the equality $n = ef$. This extension is clearly Galois, so the equality $n = f$ implies the group isomorphism $\mathrm{Gal}(\mathbb{Q}_p(\zeta_d)/\mathbb{Q}_p) \simeq \mathrm{Gal}((\mathcal{O}/\wp)\,/\,(\mathbb{Z}_p/p\mathbb{Z}_p))$. Hence the extension $\mathbb{Q}_p(\zeta_d)/\mathbb{Q}_p$ is cyclic.

Assuming that $p \nmid d$, the prime p is inert in the field $\mathbb{Q}_p(\zeta_d)$, that is, $p\mathcal{O} = \wp$. In consequence, p is also inert in any subfield K of $\mathbb{Q}_p(\zeta_d)$. Thus p is a prime element of the integer ring $\mathcal{O}_K$ of K and the quotient $\mathcal{O}_K/p\mathcal{O}_K$ is a field.

[†] Conversely, every finite unramified extension of $\mathbb{Q}_p$ is obtained by adjoining a root of unity of order prime to p.

1.2 p-adic Characters

Recall the notation defined in the Introduction: m is a fixed integer satisfying $m \geq 3$, $m \not\equiv 2 \bmod 4$, $F = \mathbb{Q}(\zeta_m)^+$ or $F = \mathbb{Q}(\zeta_m)$, $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, p represents an odd prime not dividing $|\Delta|$, and A denotes the p-part of the class group of F.

Some results in this section, as well as most results in the rest of this chapter, are given with references, where the corresponding sources and proofs can be found.

This section is based on Section 15.2 of [W1]. The properties of the idempotents presented below, especially Proposition 1.4, will be repeatedly applied in the next chapters.

Let χ be a p-adic character of Δ, that is, a character of Δ into $\mathbb{Z}_p[\zeta_{|\Delta|}]^\times$. Define the idempotent corresponding to χ by

$$e_\chi = \tfrac{1}{|\Delta|} \sum_{\sigma \in \Delta} \chi(\sigma)\, \sigma^{-1} \in \mathbb{Z}_p[\zeta_{|\Delta|}][\Delta].$$

The group of characters of Δ into $\mathbb{Z}_p[\zeta_{|\Delta|}]^\times$ will be denoted by $\widehat{\Delta}$. In the situation when $F = \mathbb{Q}(\zeta_m)$, it will be usual to identify characters in $\widehat{\Delta}$ with characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathbb{Z}_p[\zeta_{|\Delta|}]^\times$ by means of the isomorphism $\Delta \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.

If $F = \mathbb{Q}(\zeta_m)$, then the condition $p \nmid |\Delta| = \varphi(m)$ implies that $p \parallel m$ or $p \nmid m$. When $p \parallel m$, there exists a unique character $\omega : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ satisfying the congruence

$$\omega(a) \equiv a \mod p\,,$$

which is called the Teichmüller character of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathbb{Z}_p$.

Basic properties of characters in $\widehat{\Delta}$ are given in the following proposition.

Proposition 1.1.

(1) $e_\chi^2 = e_\chi$ *for every* $\chi \in \widehat{\Delta}$.

(2) $e_{\chi_1} e_{\chi_2} = 0$ *for any* $\chi_1, \chi_2 \in \widehat{\Delta}$, $\chi_1 \neq \chi_2$.

(3) $\sum_{\chi \in \widehat{\Delta}} e_\chi = 1$.

(4) $\sigma e_\chi = \chi(\sigma) e_\chi$ *for any* $\sigma \in \Delta$, $\chi \in \widehat{\Delta}$.

Proof. Item 4 is shown first and then used to prove the other items.

$$\begin{aligned}(4)\ \ \sigma e_\chi &= \tfrac{1}{|\Delta|}\textstyle\sum_{\tau\in\Delta} \chi(\tau)\,\sigma\tau^{-1} = \tfrac{1}{|\Delta|}\sum_{\tau} \chi(\sigma\tau)\,\tau^{-1}\\ &= \tfrac{\chi(\sigma)}{|\Delta|}\textstyle\sum_{\tau} \chi(\tau)\,\tau^{-1} = \chi(\sigma)e_\chi\,.\end{aligned}$$

$$\begin{aligned}(1)\ \ e_\chi^2 &= \tfrac{1}{|\Delta|}\textstyle\sum_{\sigma\in\Delta} \chi(\sigma)\,\sigma^{-1}e_\chi = \tfrac{1}{|\Delta|}\sum_{\sigma\in\Delta} \chi(\sigma)\,\chi(\sigma^{-1})\,e_\chi\\ &= \tfrac{1}{|\Delta|}\big(\textstyle\sum_{\sigma} 1\big)e_\chi = e_\chi\,.\end{aligned}$$

$$\begin{aligned}(2)\ \ e_{\chi_1}e_{\chi_2} &= \tfrac{1}{|\Delta|}\textstyle\sum_{\sigma\in\Delta} \chi_1(\sigma)\,\sigma^{-1}e_{\chi_2} = \tfrac{1}{|\Delta|}\big(\sum_{\sigma} \chi_1(\sigma)\,\chi_2(\sigma)^{-1}\big)e_{\chi_2}\\ &= \tfrac{1}{|\Delta|}\big(\textstyle\sum_{\sigma} \chi_1\,\chi_2^{-1}(\sigma)\big)e_{\chi_2} = 0\,.\end{aligned}$$

$$\begin{aligned}(3)\ \ \textstyle\sum_{\chi\in\widehat{\Delta}} e_\chi &= \textstyle\sum_{\chi\in\widehat{\Delta}} \tfrac{1}{|\Delta|}\sum_{\sigma\in\Delta} \chi(\sigma)\,\sigma^{-1} = \tfrac{1}{|\Delta|}\sum_{\sigma}\sum_{\chi} \chi(\sigma)\,\sigma^{-1}\\ &= \tfrac{1}{|\Delta|}\textstyle\sum_{\chi} 1 = 1. \quad \square\end{aligned}$$

The orbit of a character χ is a subset of $\widehat{\Delta}$ defined by

$$X = \{\tau\chi : \tau \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_{|\Delta|})/\mathbb{Q}_p)\},$$

where $\tau\chi$ denotes the composition of the character χ and the automorphism τ. Two distinct orbits as above are disjoint, so the set of all orbits is a partition of $\widehat{\Delta}$.

Let ρ be the sum of the characters in a given orbit X. It is said that the orbit X has sum ρ. By linear independence of characters, distinct orbits have distinct sums. Thus the orbit X is characterized by its sum ρ, so X will be conveniently denoted by X_ρ and ρ will be written as

$$\rho = \sum_{\chi\in X_\rho} \chi\,.$$

It is easily seen that the orbit X_ρ is preserved by $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{|\Delta|})/\mathbb{Q}_p)$. The same is true for the sum ρ. This implies that for $\sigma \in \Delta$, $\rho(\sigma) \in \mathbb{Q}_p$, so $\rho(\sigma) \in \mathbb{Z}_p$ as $\rho(\sigma)$ is integral over $\mathbb{Z}_p$.

Sums ρ as above will be called irreducible higher dimensional characters of Δ into $\mathbb{Z}_p$, and the set which they form will be denoted by Ω. The set of characters

$\{\chi^{-1} : \chi \in X_\rho\}$ is easily seen to be an orbit. The corresponding irreducible higher dimensional character will be denoted by ρ^{-1}.

It is clear that any two characters in the same orbit are either both even or both odd. An irreducible higher dimensional character is said to be even or odd according as the characters in its orbit are even or odd.

The idempotent corresponding to $\rho \in \Omega$ is given by

$$e_\rho = \sum_{\chi \in X_\rho} e_\chi = \tfrac{1}{|\Delta|} \sum_{\sigma \in \Delta} \rho(\sigma)\, \sigma^{-1} = \tfrac{1}{|\Delta|} \sum_{\chi \in X_\rho} \sum_{\sigma \in \Delta} \chi(\sigma)\, \sigma^{-1} \in \mathbb{Z}_p[\Delta].$$

The following properties of idempotents e_ρ, $\rho \in \Omega$, are analogous to properties 1, 2, and 3 in Proposition 1.1 for idempotents e_χ, $\chi \in \widehat{\Delta}$.

Proposition 1.2.

(1) $e_\rho^2 = e_\rho$ *for every* $\rho \in \Omega$.

(2) $e_{\rho_1} e_{\rho_2} = 0$ *for any* $\rho_1, \rho_2 \in \Omega$, $\rho_1 \neq \rho_2$.

(3) $\sum_{\rho \in \Omega} e_\rho = 1$.

Proof. Items 1, 2, and 3 of Proposition 1.1 are applied.

(1) $e_\rho^2 = \sum_{\chi \in X_\rho} e_\chi \sum_{\chi' \in X_\rho} e_{\chi'} = \sum_\chi e_\chi^2 = \sum_\chi e_\chi = e_\rho$.

(2) $e_{\rho_1} e_{\rho_2} = \sum_{\chi \in X_{\rho_1}} e_\chi \sum_{\chi' \in X_{\rho_2}} e_{\chi'} = \sum_{\chi, \chi'} e_\chi \, e_{\chi'} = 0$.

(3) $\sum_{\rho \in \Omega} e_\rho = \sum_{\rho \in \Omega} \sum_{\chi \in X_\rho} e_\chi = \sum_{\chi \in \widehat{\Delta}} e_\chi = 1$. □

Observe that there is no analogous of property $\sigma e_\chi = \chi(\sigma) e_\chi$ of idempotents e_χ for idempotents e_ρ. This deficiency will be rectified by Proposition 1.4.

The properties in Proposition 1.2 imply that a $\mathbb{Z}_p[\Delta]$-module N can be decomposed as a direct sum

$$N = \sum_{\rho \in \Omega} e_\rho N.$$

Denote the reduction of an element $\theta \in \mathbb{Z}_p[\Delta]$ mod p by $\bar{\theta}$. It is clear that $\bar{e}_\rho$ is an idempotent in $\mathbb{F}_p[\Delta]$, which satisfies properties analogous to those in Proposition 1.2.

Lemma 1.3 ([W1], Chapter 15, Proposition 15.5). $\mathbb{F}_p[\Delta]\bar{e}_\rho$ *is an irreducible* $\mathbb{F}_p[\Delta]$-*module.*

Observe that for $\theta = \sum_{\sigma\in\Delta} c_\sigma \sigma \in \mathbb{Z}_p[\Delta]$, $p^r \mid \theta$ means that $p^r \mid c_\sigma$ for every $\sigma \in \Delta$. The notation $p^r \parallel \theta$ will mean thoughout this thesis that $p^r \mid \theta$ but $p^{r+1} \nmid \theta$.

The proof of the following proposition differs from the proof in the reference given. See the reference for a proof using Nakayama's Lemma.

Proposition 1.4 ([W1], Chapter 15, Proposition 15.6). *If* $\theta \in \mathbb{Z}_p[\Delta]$ *and* $p^r \parallel \theta e_\rho$, *then there exists* $\theta' \in \mathbb{Z}_p[\Delta]$ *such that* $p^{-r}\theta\theta' e_\rho = e_\rho$. *Consequently, if* M *is a power of* p, $\theta \in \mathbb{Z}[\Delta]$ *and* $p^r \parallel \theta e_\rho$, *then there exists* $\theta' \in \mathbb{Z}[\Delta]$ *such that* $p^{-r}\theta\theta' e_\rho \equiv e_\rho \bmod M$.

Proof. In order to show the first part of the proposition, observe that by Lemma 1.3, $\overline{p^{-r}\theta e_\rho}\,\mathbb{F}_p[\Delta]\bar{e}_\rho = \mathbb{F}_p[\Delta]\bar{e}_\rho$. Then, if $\psi \in \mathbb{Z}_p[\Delta]$ is given, $\overline{p^{-r}\theta e_\rho}\,\overline{\phi}\,\bar{e}_\rho = \overline{\psi}\,\bar{e}_\rho$ for some $\phi \in \mathbb{Z}_p[\Delta]$, which can be written as

$$p^{-r}\theta\,\phi\, e_\rho = \psi\, e_\rho + p\,\psi' e_\rho\,,$$

where $\psi' \in \mathbb{Z}_p[\Delta]$.

Let $\psi_1 = 1$. Apply the observation above with $\psi = \psi_1, \psi_2, \dots, \psi_n$ consecutively to obtain the equalities

$$p^{-r}\theta\,\phi_i\, e_\rho = \psi_i\, e_\rho + p\,\psi_{i+1}\, e_\rho \quad \text{for} \quad i = 1, 2, \dots, n\,,$$

where $\phi_i, \psi_i \in \mathbb{Z}_p[\Delta]$. Multiplying the ith equality by $(-p)^{i-1}$ and summing over $1 \leqslant i \leqslant n$, there results that

$$p^{-r}\theta\,\theta'_n\, e_\rho = e_\rho - (-p)^n \psi_{n+1}\, e_\rho\,,$$

where $\theta'_n = \sum_{1\leqslant i\leqslant n} (-p)^{i-1}\phi_i$. Taking limits as $n \to \infty$ yields the equality $p^{-r}\theta\,\theta' e_\rho = e_\rho$, where $\theta' = \lim \theta'_n \in \mathbb{Z}_p[\Delta]$. This shows the first part. The second part then follows inmediately. □

1.3 Gauss Sums

Let ℓ be a rational prime and let $q = \ell^f$ with $f \geqslant 1$. Write Tr for the trace of the extension $\mathbb{F}_q/\mathbb{F}_\ell$. Define the Gauss sum

$$S(\xi, {\zeta_\ell}^{\mathrm{Tr}}) = \sum_{a \in \mathbb{F}_q} \xi(a)\, {\zeta_\ell}^{\mathrm{Tr}(a)} \in \mathbb{Z}[\zeta_{\ell(q-1)}]\,,$$

where ξ is a character of $\mathbb{F}_q^\times$.

Proposition 1.5, Theorem 1.7, and Proposition 1.8 below are used in the proof of Proposition 3.2. Proposition 1.6 is needed for Lemma 3.9 and Theorem 1.9 is applied in Theorem 3.20.

Proposition 1.5 ([L], Chapter 1, Section 1, **GS2**). $\left| S(\xi, {\zeta_\ell}^{\mathrm{Tr}}) \right| = \sqrt{q}$ *for* $\xi \neq 1$.

Assume that $m \mid q-1$. Let λ be a prime of $\mathbb{Q}(\zeta_m)$ above ℓ, Λ be a prime of $\mathbb{Q}(\zeta_{q-1})$ above λ, and $\widehat{\Lambda}$ be a prime of $\mathbb{Q}(\zeta_{\ell(q-1)})$ above Λ.

The residual degree of Λ over ℓ is f, so the residual field $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/\Lambda$, where $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ denotes the integer ring of $\mathbb{Q}(\zeta_{q-1})$, is isomorphic to $\mathbb{F}_q$. Since the $q-1$ st roots of unity in $\mathbb{Q}(\zeta_{q-1})$ are pairwise incongruent mod Λ, it follows that there is a unique character ω of $(\mathbb{F}_q)^\times \simeq (\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/\Lambda)^\times$ such that $\omega(a) \equiv a \bmod \Lambda$ for every $a \in \mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$. This character is called the Teichmüller character.

Let k be an integer satisfying $0 \leqslant k < q-1$. Let

$$k = k_0 + k_1\,\ell + \ldots + k_{f-1}\,\ell^{f-1}$$

be the ℓ-adic expansion of k with $0 \leqslant k_i < \ell$ for $0 \leqslant i \leqslant f-1$. Define

$$\beta(k) = k_0 + k_1 + \ldots + k_{f-1} \qquad \text{and} \qquad \gamma(k) = k_0!\, k_1! \ldots k_{f-1}!$$

Extend the definitions above to any integer k by $(q-1)$-periodicity, that is, $\beta(k) = \beta(\langle k \rangle)$ and $\gamma(k) = \gamma(\langle k \rangle)$, where $\langle k \rangle$ denotes the least nonnegative residue of k mod $q-1$.

Proposition 1.6 ([L], Chapter 1, Theorem 2.1). *For every integer k,*

$$S(\omega^{-k}, {\zeta_\ell}^{\mathrm{Tr}}) \,/\, (\zeta_\ell - 1)^{\beta(k)} \equiv -1 \,/\, \gamma(k) \mod \widehat{\Lambda}.$$

In particular, $v_{\widehat{\Lambda}}(S(\omega^{-k}, {\zeta_\ell}^{\mathrm{Tr}})) = \beta(k)$.

Theorem 1.7 (Davenport-Hasse distribution theorem, [L], Chapter 2, Theorem 10.1). *Let ξ and ϑ be characters of $\mathbb{F}_q^\times$. Then*

$$\prod_{\vartheta^m=1} S(\xi\vartheta, {\zeta_\ell}^{\mathrm{Tr}}) = S(\xi^m, {\zeta_\ell}^{\mathrm{Tr}})\, \xi(m^{-m}) \prod_{\vartheta^m=1} S(\vartheta, {\zeta_\ell}^{\mathrm{Tr}}).$$

Define the Stickelberger element by

$$\Theta = \tfrac{1}{m} \sum_{\substack{1 \leqslant a < m \\ (a,m)=1}} a\,\sigma_a^{-1} \in \mathbb{Q}[\Delta],$$

where $\sigma_a \in \Delta$ is defined by $\sigma_a(\zeta_m) = \zeta_m^a$. For every integer r satisfying $1 \leqslant r < m$, $(r, m) = 1$, define the element

$$\Theta_r = \sum_{\substack{1 \leqslant a < m \\ (a,m)=1}} \left\{\tfrac{ra}{m}\right\} \sigma_a^{-1} \in \mathbb{Q}[\Delta],$$

where $\{\cdot\}$ denotes the fractional part.

Proposition 1.8 ([L], Chapter 1, Theorem 2.2). *Assume that f is the order of ℓ mod m. Let r satisfy $1 \leqslant r < m$, $(r, m) = 1$, and let $k = (q-1)\,r/m$. Then the sum $S(\omega^{-k}, {\zeta_\ell}^{\mathrm{Tr}})$ can be factored as*

$$\big(S(\omega^{-k}, {\zeta_\ell}^{\mathrm{Tr}})\big) = \lambda^{\Theta_r}.$$

Define the Stickelberger ideal of $\mathbb{Z}[\Delta]$ as $\mathbb{Z}[\Delta] \cap \Theta\mathbb{Z}[\Delta]$.

Theorem 1.9 (Stickelberger's theorem, [W1], Chapter 6, Theorem 6.10). *The Stickelberger ideal annihilates the ideal class group of $\mathbb{Q}(\zeta_m)$.*

1.4 The Inflation-Restriction Exact Sequence

The following result of homological algebra is used in the proof of Lemma 3.5.

Proposition 1.10 (Inflation-restriction exact sequence, [W2], Chapter 6, Subsection 6.8.3). Let G be a group and let H be a normal subgroup of G. Let N be a G-module. The following sequence is exact:

$$0 \longrightarrow H^1(G/H, N^H) \xrightarrow{\text{inf}} H^1(G,N) \xrightarrow{\text{res}} H^1(H,N)^{G/H} \longrightarrow$$
$$\longrightarrow H^2(G/H, N^H) \xrightarrow{\text{inf}} H^2(G,N),$$

where inf and res denote the inflation map and the restriction map respectively.

1.5 Dirichlet Density

Let K be a number field. Let P be a set of nonzero prime ideals of K and denote the norm of an ideal $\mathcal{B}$ by $\mathcal{N}\mathcal{B}$. If the limit

$$\lim_{s\to 1^+} \frac{\sum_{\wp\in P}\frac{1}{\mathcal{N}\wp^s}}{\log\frac{1}{s-1}}$$

exists, then its value is called the Dirichlet density of P and is denoted by $\mathrm{Dd}(P)$. The Dirichlet density of a set of primes, if it exists, is a number in the interval $[0,1]$.

The following results are used in the proof of Theorem 3.14.

Proposition 1.11 ([J], Chapter 4, Subsection 4.6). *Let P and Q be sets of primes of K having Dirichlet densities. Let P_1 be the set of primes of K having absolute degree* 1.

(a) *If $Dd(P) > 0$, then P is an infinite set.*

(b) *$Dd(P) = Dd(P \cap P_1)$.*

(c) *If $P \subseteq Q$, then $Dd(P) \leqslant Dd(Q)$.*

Theorem 1.12 (Chebotarev density theorem, [J], Chapter 5, Theorem 10.4). *Let E/K be a Galois extension of a number field with Galois group G. Let $\sigma \in G$ and suppose that σ has c conjugates in G. The set of primes of K that are unramified in E and have a prime divisor in E whose Frobenius automorphism in G is equal to σ has Dirichlet density $c/|G|$.*

1.6 Minkowski Units

The following proposition is applied in the proof of Proposition 2.8.

Proposition 1.13 ([W1], Chapter 5, Lemma 5.27). *Let $K/\mathbb{Q}$ be a finite Galois extension. If K is real, write $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1\,, \dots, \sigma_{r+1}\}$. If K is complex, write $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1\,, \dots, \sigma_{r+1}\,, \bar{\sigma}_1\,, \dots, \bar{\sigma}_{r+1}\}$. Then there exists a unit ε of K such that the set $\{\sigma_i\,\varepsilon \,:\, 1 \leqslant i \leqslant r\}$ is multiplicatively independent, hence generates a subgroup of finite index in the group of all units. Such a unit is called a Minkowski unit.*

CHAPTER 2

On the Ideal Class Group of the Maximal Real Subfield of a Cyclotomic Field

Consider the maximal real subfield $F = \mathbb{Q}(\zeta_m)^+$ of the mth cyclotomic field for $m \geqslant 3$. Without loss of generality, it is assumed that $m \not\equiv 2 \bmod 4$. Denote $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ and let p be an odd prime not dividing $|\Delta| = \varphi(m)/2$.

Let E be the group of units of F and let C be the subgroup of cyclotomic units, i.e., units of the form $\pm\prod_{1\leqslant j\leqslant m-1}((1-\zeta_m^j)(1-\zeta_m^{-j}))^{a_j}$. The p-part of the quotient group E/C and the p-part of the ideal class group of F will be denoted by $(E/C)_p$ and A respectively.

Consider a nontrivial irreducible higher dimensional character ρ of Δ with values in $\mathbb{Z}_p$, and let e_ρ be the corresponding idempotent, defined in Section 1.2.

Let $M = p \cdot |(E/C)_p| \cdot |A|$. The notation e'_ρ will stand for a fixed element of the group ring $\mathbb{Z}[\Delta]$ satisfying the congruence $e'_\rho \equiv e_\rho \bmod M$.

2.1 Basic Elements

In this section, basic definitions and properties are given of elements appearing repeatedly in this chapter, such as the cyclotomic units $\alpha(L)$, the operators N_L and D_L, and the numbers $\kappa(L)$ and β_L for integer numbers L of a special form.

Let $\mathbb{L}$ denote the set of products (the empty product included) of distinct odd rational primes ℓ satisfying the congruence $\ell \equiv 1 \bmod mM$. Throughout this chapter, L and ℓ will denote a number in $\mathbb{L}$ and a prime in $\mathbb{L}$ respectively.

For every ℓ, fix a primitive ℓth root of unity ζ_ℓ. For every L, define a primitive Lth root of unity by $\zeta_L = \prod_{\ell \mid L} \zeta_\ell$ and denote $F(L) = F(\zeta_L)$. If $\ell \nmid L$, write $N_{\ell L/L}$ for the norm of $F(\ell L)/F(L)$. Furthermore, let

$\alpha = \pm \prod_{1 \leqslant j \leqslant m-1}((1-\zeta_m^j)(1-\zeta_m^{-j}))^{a_j}$ = a cyclotomic unit of F,

$\alpha(L) = \pm \prod_{1 \leqslant j \leqslant m-1}((1-\zeta_m^j\zeta_L)(1-\zeta_m^{-j}\zeta_L))^{a_j}$ with the same sign as α.

In this manner, $\alpha(L)$ is a cyclotomic unit of $F(L)$, since the number $1-\zeta_n$ in $\mathbb{Q}(\zeta_n)$ is a unit if n has at least two distinct prime factors. The cyclotomic units $\alpha(L)$ form an Euler system.

Lemma 2.1. *Let $\ell \nmid L$.*

(a) $N_{\ell L/L}\,\alpha(\ell L) = \alpha(L)^{\mathrm{Frob}_\ell - 1}$, *where* Frob_ℓ *is the Frobenius of ℓ in $F(L)/\mathbb{Q}$.*

(b) $\alpha(\ell L) \equiv \alpha(L)$ mod *all primes of $F(\ell L)$ above ℓ.*

Proof. (a) Since $N_{\ell L/L}(1-\zeta_m^j\zeta_{\ell L}) = \prod_{1 \leqslant b \leqslant \ell-1}(1-\zeta_m^j\zeta_L\zeta_\ell^b) = (1-\zeta_m^{j\ell}\zeta_L^\ell)/(1-\zeta_m^j\zeta_L) = (1-\zeta_m^j\zeta_L)^{\mathrm{Frob}_\ell - 1}$, the required equality follows.

(b) The congruence $\alpha(\ell L) \equiv \alpha(L) \bmod (1-\zeta_\ell)$ follows from the definition of $\alpha(\ell L)$. Then the stated congruences hold because the ideal $(1-\zeta_\ell)$ of $F(\ell L)$ equals the product of all primes above ℓ. □

Denote $G_L = \mathrm{Gal}(F(L)/F)$. Thus G_L is isomorphic to $\prod_{\ell \mid L} G_\ell$.

Fix a primitive root s_ℓ mod ℓ, define a generator σ_{s_ℓ} of the cyclic group G_ℓ by $\sigma_{s_\ell}(\zeta_\ell) = \zeta_\ell^{s_\ell}$, and extend σ_{s_ℓ} to fields $F(L)$ with $\ell \mid L$ so that σ_{s_ℓ} acts as the identity on roots of unity of order prime to ℓ. When there is no risk of confusion, s_ℓ will be denoted simply by s and correspondingly σ_{s_ℓ} will be denoted by σ_s.

Define elements in $\mathbb{Z}[G_\ell]$ by

$$N_\ell = \sum_{0 \leqslant j \leqslant \ell-2} \sigma_s^j\,, \quad D_\ell = \sum_{1 \leqslant j \leqslant \ell-2} j\,\sigma_s^j\,,$$

and elements in $\mathbb{Z}[G_L]$ by

$$N_L = \prod_{\ell \mid L} N_\ell\,, \quad D_L = \prod_{\ell \mid L} D_\ell\,.$$

Then, if $\ell \nmid L$, N_ℓ coincides with the norm $N_{\ell L/L}$. The elements N_ℓ and D_ℓ satisfy the equality $(\sigma_s - 1)\, D_\ell = \ell - 1 - N_\ell$. Indeed,

$$\begin{aligned}(\sigma_s - 1)\, D_\ell = (\sigma_s - 1) \sum_{1 \leqslant j \leqslant \ell-2} j\,\sigma_s^j &= \sum_{2 \leqslant j \leqslant \ell-1} (j-1)\,\sigma_s^j - \sum_{1 \leqslant j \leqslant \ell-2} j\,\sigma_s^j \\ &= \ell - 2 - \sum_{1 \leqslant j \leqslant \ell-2} \sigma_s^j = \ell - 1 - N_\ell\,.\end{aligned}$$

Lemma 2.2.

(a) $(\sigma - 1)\, D_L\, \alpha(L) \in (F(L)^\times)^M$ *for all* $\sigma \in G_L$.

(b) *The function* $c : G_L \to F(L)^\times$ *given by* $c(\sigma) = ((\sigma - 1)\, D_L\, \alpha(L))^{1/M}$ *is well defined and satisfies the cocycle relation* $c(\tau\sigma) = c(\tau) \cdot \tau(c(\sigma))$.

Proof. (a) The case $L = 1$ is trivial because $G_1 = 1$. Assume by induction that $L > 1$ and that the statement is true for all proper divisors of L. Let ℓ be a prime factor of L and $L = \ell L'$. Then, for $s = s_\ell$,

$$\begin{aligned}(\sigma_s - 1)\, D_L\, \alpha(L) &= (\sigma_s - 1)\, D_{\ell L'}\, \alpha(\ell L') \\ &= (\ell - 1 - N_\ell)\, D_{L'} \alpha(\ell L') \quad \text{because} \quad (\sigma_s - 1)\, D_\ell = \ell - 1 - N_\ell \\ &= D_{L'}\, \alpha(\ell L')^{\ell - 1} / (\mathrm{Frob}_\ell - 1)\, D_{L'}\, \alpha(L') \text{ by item (a) of Lemma 2.1,}\end{aligned}$$

so $(\sigma_s - 1)\, D_L\, \alpha(L) \in (F(L)^\times)^M$ by induction hypothesis and because $M \mid \ell - 1$. Since G_L is generated by the $\sigma_s = \sigma_{s_\ell}$ with $\ell \mid L$, the statement is valid for all $\sigma \in G_L$.

(b) Since $\mathbb{Q}(\zeta_p, \zeta_m) \cap \mathbb{Q}(\zeta_L) = \mathbb{Q}$ (because L is prime to pm) and $F \subseteq F(\zeta_p) \subseteq \mathbb{Q}(\zeta_p, \zeta_m)$, $F(\zeta_p) \cap \mathbb{Q}(\zeta_L) = \mathbb{Q}$ and $F \cap \mathbb{Q}(\zeta_L) = \mathbb{Q}$. Then $[F(L)(\zeta_p) : \mathbb{Q}(\zeta_L)] = [F(\zeta_p) : \mathbb{Q}]$ and $[F(L) : \mathbb{Q}(\zeta_L)] = [F : \mathbb{Q}]$, so $[F(L)(\zeta_p) : F(L)] = [F(\zeta_p) : F]$, whence $\zeta_p \notin F(L)$ (as $\zeta_p \notin F$). Hence the pth root of a number in $F(L)$ is unique if exists, and so is the Mth root. Thus $c(\sigma) = ((\sigma - 1)\, D_L\, \alpha(L))^{1/M}$ is well defined.

The cocycle relation $c(\tau\sigma) = c(\tau) \cdot \tau(c(\sigma))$ follows from the equalities

$$\begin{aligned} c(\tau\sigma)^M &= (\tau\sigma - 1)\, D_L\, \alpha(L) = (\tau - 1 + \tau(\sigma - 1))\, D_L\, \alpha(L) \\ &= (\tau - 1)\, D_L\, \alpha(L) \cdot \tau(\sigma - 1)\, D_L\, \alpha(L) = c(\tau)^M \cdot \tau(c(\sigma))^M. \end{aligned}$$

This concludes the proof. □

The following proposition defines the numbers $\kappa(L)$ and β_L.

Proposition 2.3. *There exist $\kappa(L) \in F^\times$ and $\beta_L \in F(L)^\times$ such that*

(a) $((\sigma - 1)\, D_L\, \alpha(L))^{1/M} = (\sigma - 1)\, \beta_L$ *for all* $\sigma \in G_L$;

(b) $D_L\, \alpha(L) = \kappa(L)\, \beta_L^M$.

Proof. (a) By the linear independence of characters, there exists $\delta \in F(L)^\times$ such that $\gamma = \sum_\sigma c(\sigma)\, \sigma(\delta) \neq 0$, where c is the function of Lemma 2.2. Thus, by item (b) of the same lemma,

$$\tau\gamma = \sum_\sigma c(\tau\sigma)\, c(\tau)^{-1} \tau\sigma(\delta) = c(\tau)^{-1}\gamma \quad \text{for all} \quad \tau \in G_L\,.$$

Setting $\beta_L = \gamma^{-1}$, it follows that $c(\tau) = (\tau - 1)\beta_L$ with $\beta_L \in F(L)^\times$, which amounts to the required equality.

(b) The equality shown in item (a) implies that

$$(\sigma - 1) \left(\frac{D_L\, \alpha(L)}{\beta_L^M} \right) = 1 \quad \text{for all} \quad \sigma \in G_L\,.$$

This means that $\kappa(L) = D_L\, \alpha(L) \,/\, \beta_L^M \in F^\times$, which yields the result. This concludes the proof. □

2.2 The Induction Property

This section consists of Propositions 2.4 and 2.5. Proposition 2.4 presents the induction property of the numbers $\kappa(L)$ and serves to prove Proposition 2.5. The latter proposition will be used in Proposition 2.8 as an essential element to obtain the main results.

Let λ be a prime of F above ℓ and $\mathcal{L}$ be a prime of $F(\ell L)$ above λ. This notation will be used in the rest of this chapter.

Observe that if $\ell \equiv 1 \bmod mML$, then ℓ splits completely in $F(L)$ and ramifies totally in $F(\ell L)/F(L)$. Then, since $s = s_\ell$ is a primitive root mod ℓ, s is also a primitive root mod λ and mod $\mathcal{L}$.

Proposition 2.4. *Let* $\ell \equiv 1 \bmod mML$. *If* $\kappa(L) \equiv s^a \bmod \lambda$, $a \in \mathbb{Z}$, *then*

$$v_\lambda(\kappa(\ell L)) \equiv -a \bmod M.$$

Proof. Assume that $\kappa(L) \equiv s^a \bmod \lambda$ with $a \in \mathbb{Z}$. $D_L\, \alpha(L)$ being a unit, $D_L\, \alpha(L)$ $\equiv s^{a'} \bmod \mathcal{L}$ for some $a' \in \mathbb{Z}$. In general, if $s^i \equiv s^j \bmod \mathcal{L}$, then $s^i \equiv s^j \bmod \ell$ and $i \equiv j \bmod \ell - 1$. Thus $a' \equiv a \bmod M$ by item (b) of Proposition 2.3.

Since $\ell \equiv 1 \bmod mML$, the Frobenius of ℓ in $F(L)/\mathbb{Q}$ is equal to the identity. Then $N_\ell\, \alpha(\ell L) = 1$ in view of item (a) of Lemma 2.1. Hence, item (a) of Proposition 2.3 and item (b) of Lemma 2.1 imply that

$$\begin{aligned}(\sigma_s - 1)\, \beta_{\ell L} &= ((\sigma_s - 1)\, D_{\ell L}\, \alpha(\ell L))^{1/M} = ((\ell - 1 - N_\ell)\, D_L\, \alpha(\ell L))^{1/M} \\ &= D_L\, \alpha(\ell L)^{(\ell-1)/M} \equiv D_L\, \alpha(L)^{(\ell-1)/M} \equiv s^{a'(\ell-1)/M} \bmod \mathcal{L}\end{aligned}$$

Thus, if $(\sigma_s - 1)\, \beta_{\ell L} \equiv s^b \bmod \mathcal{L}$, $b \in \mathbb{Z}$, there results the congruence

$$b \equiv a'\, \tfrac{\ell-1}{M} \equiv a\, \tfrac{\ell-1}{M} \bmod \ell - 1.$$

Let $c = v_{\mathcal{L}}(\beta_{\ell L})$. Since $v_{\mathcal{L}}(1 - \zeta_\ell) = 1$, $\beta_{\ell L}$ can be expressed as $\beta_{\ell L} = (1 - \zeta_\ell)^c\, \gamma$ with $\gamma \in F(\ell L)^\times$, $v_{\mathcal{L}}(\gamma) = 0$. Also, since $\mathcal{L}$ is totally ramified in $F(\ell L)/F(L)$, σ_s

is in the inertia group of $\mathcal{L}$, so $\sigma_s\gamma \equiv \gamma \bmod \mathcal{L}$. On the other hand, the congruence $\zeta_\ell \equiv 1 \bmod \mathcal{L}$ implies that

$$\frac{1-\zeta_\ell^s}{1-\zeta_\ell} = 1 + \zeta_\ell + \ldots + \zeta_\ell^{s-1} \equiv s \bmod \mathcal{L}.$$

Therefore

$$s^b \equiv (\sigma_s - 1)\,\beta_{\ell L} = \left(\frac{1-\zeta_\ell^s}{1-\zeta_\ell}\right)^c \frac{\sigma_s\gamma}{\gamma} \equiv s^c \bmod \mathcal{L},$$

so $b \equiv c \bmod \ell - 1$. It then follows that $c \equiv a\,\frac{\ell-1}{M} \bmod \ell - 1$, that is,

$$v_{\mathcal{L}}(\beta_{\ell L}) \equiv a\,\tfrac{\ell-1}{M} \bmod \ell - 1.$$

Since the ramification index of $\mathcal{L}$ over λ is equal to $\ell - 1$ and $D_{\ell L}\,\alpha(\ell L)$ is a unit, by item (b) of Proposition 2.3 there results that

$$v_\lambda(\kappa(\ell L)) = \tfrac{1}{\ell-1}\,v_{\mathcal{L}}(\kappa(\ell L)) = -\tfrac{1}{\ell-1}\,v_{\mathcal{L}}(\beta_{\ell L}^M) = -\tfrac{M}{\ell-1} v_{\mathcal{L}}(\beta_{\ell L}) \equiv -a \bmod M,$$

as required. □

Recall that e'_ρ is an element in $\mathbb{Z}[\Delta]$ satisfying $e'_\rho \equiv e_\rho \bmod M$, where $M = p \cdot |(E/C)_p| \cdot |A|$.

Proposition 2.5. *Let $\ell \equiv 1 \bmod mML$. Suppose that the class $\mathfrak{C}$ of λ is in $e_\rho A$ and that*

(1) *the group B generated by the classes of the primes of F dividing L is included in $e_\rho A$;*
(2) *$e'_\rho\kappa(\ell L) \in (F^\times)^{p^r}$ with $p^r \leqslant M$ and $p^{-r}M$ annihilates A;*
(3) *if $\kappa(L)$ is a unit at $\sigma\lambda$ for every $\sigma \in \Delta$ and $e'_\rho\kappa(L) \equiv s^a \bmod \lambda$ with $p^{r'} \parallel a$, then $p^{r'} < M$.*

Then $r \leqslant r'$ and $p^{r'-r}$ annihilates $\mathfrak{C}$ in $e_\rho A/B$.

Proof. Let $e'_\rho = \sum_{\sigma\in\Delta} c_\sigma\,\sigma^{-1}$, $c_\sigma \in \mathbb{Z}$. For every $\sigma \in \Delta$, s is a primitive root $\bmod\, \sigma\lambda$, so $\kappa(L) \equiv s^{a_\sigma} \bmod \sigma\lambda$ for some $a_\sigma \in \mathbb{Z}$. Thus $\sigma^{-1}\kappa(L) \equiv s^{a_\sigma} \bmod \lambda$ and $e'_\rho\kappa(L) \equiv s^a \bmod \lambda$, where $a = \sum_\sigma a_\sigma c_\sigma$.

In view of Proposition 2.4, the congruence $\kappa(L) \equiv s^{a_\sigma} \bmod \sigma\lambda$ implies that $v_{\sigma\lambda}(\kappa(\ell L)) \equiv -a_\sigma \bmod M$. Hence,

$$\begin{aligned} v_\lambda(e'_\rho\kappa(\ell L)) &= \sum_\sigma c_\sigma\, v_\lambda(\sigma^{-1}\kappa(\ell L)) = \sum_\sigma c_\sigma\, v_{\sigma\lambda}(\kappa(\ell L)) \\ &\equiv -\sum_\sigma a_\sigma c_\sigma = -a \mod M. \end{aligned}$$

If $\mathfrak{q}$ is a prime of F not dividing ℓL, then $\mathfrak{q}$ does not ramify in $F(\ell L)$. Thus, since $D_{\ell L}\,\alpha(\ell L)$ is a unit of $F(\ell L)$ and $D_{\ell L}\,\alpha(\ell L) = \kappa(\ell L)\,\beta_{\ell L}^M$ by item (b) of Proposition 2.3, $(\kappa(\ell L)) = (\beta_{\ell L}^{-1})^M$ as ideals of $F(\ell L)$, so $M \mid v_\mathfrak{q}(\kappa(\ell L))$. Therefore,

$$(\kappa(\ell L)) = \lambda^\theta \cdot (\,\text{primes dividing } L\,) \cdot \mathcal{B}^M,$$

where $\theta \in \mathbb{Z}[\Delta]$ and $\mathcal{B}$ is an ideal of F whose class is in A (this follows from the stated equality). Applying e'_ρ yields the equality

$$(e'_\rho\kappa(\ell L)) = \lambda^{\theta e'_\rho} \cdot (\,\text{primes dividing } L\,) \cdot \mathcal{B}'^M,$$

where the ideal $\mathcal{B}' = \mathcal{B}^{e'_\rho}$ has its class in A.

Since the left side is a p^rth power, the exponent of every prime on the right side is a multiple of p^r, so the p^rth root of the equality can be taken. The ideal $\mathcal{B}'^{p^{-r}M}$ being principal as $p^{-r}M$ annihilates A, there results that $\mathfrak{C}^{p^{-r}\theta e'_\rho} \in B$.

Let $p^{r'} \parallel a$, $p^t \parallel \theta e'_\rho$, and write $\theta e'_\rho = \sum_\sigma b_\sigma \sigma^{-1}$. Then $r \leqslant t$ because $p^r \mid \theta e'_\rho$, and $t \leqslant r'$ because $b_1 = v_\lambda(e'_\rho\kappa(\ell L)) \equiv -a \bmod M$. Thus $r \leqslant r'$.

By Proposition 1.4, there exists $\theta' \in \mathbb{Z}[\Delta]$ such that $p^{-t}\theta\theta' e'_\rho \equiv e'_\rho \bmod M$. Since $\mathfrak{C} \in e_\rho A$, e_ρ preserves $\mathfrak{C}$, and so does e'_ρ. Hence,

$$\mathfrak{C}^{p^{t-r}} = \mathfrak{C}^{p^{t-r}e'_\rho} = (\mathfrak{C}^{p^{-r}\theta e'_\rho})^{\theta'} \in B,$$

as B is preserved by Δ. This means that p^{t-r} annihilates $\mathfrak{C}$. Thus, since $t \leqslant r'$, there results that $p^{r'-r}$ annihilates $\mathfrak{C}$, as required. □

2.3 First Application of the Chebotarev Density Theorem

The only result in this section, Theorem 2.6, is an application of the Chebotarev density theorem (Theorem 1.12) and is, as Proposition 2.5, an important element to obtain the main results in the next section. Theorem 2.6 is Proposition 15.4 in [W1], Chapter 15, and is presented here for convenience of the reader. Theorem 2.6 is stated for a generalized case in which the field F is a real abelian extension of $\mathbb{Q}$. This is the only exception to the notation $F = \mathbb{Q}(\zeta_m)^+$ adopted in this chapter.

Theorem 2.6. *Let F be a real abelian extension of $\mathbb{Q}$ and let $\mathfrak{C}$ be an ideal class of F of order prime to $[F : \mathbb{Q}]$. Let b and c be positive integers such that $c \mid b$. Suppose that $\beta \in F^\times$ is a* cth power mod λ *for all except possibly a finite set of the prime ideals $\lambda \in \mathfrak{C}$ of absolute degree 1, lying over rational primes $\ell \equiv 1 \bmod b$. Then $\beta \in (F^\times)^c$ if c is odd, and $\beta \in \pm(F^\times)^{c/2}$ if c is even.*

2.4 Main Results

The main results of this chapter are presented in Theorems 2.9 and 2.11. An important prelude to these theorems is Proposition 2.8, which applies all the material in previous sections.

The following easy lemma is used in Proposition 2.8 and Theorem 2.11.

Lemma 2.7. *Let B be a submodule of the $\mathbb{Z}_p[\Delta]$-module $e_\rho(E/C)_p$ (resp. $e_\rho A$) and $\xi \in e_\rho(E/C)_p$ (resp. $\xi \in e_\rho A$). Let f be the order of ξ in $e_\rho(E/C)_p/B$ (resp. $e_\rho A/B$). Then for $\theta \in \mathbb{Z}_p[\Delta]e_\rho$, $\xi^\theta \in B$ if and only if $f \mid \theta$.*

Proof. Suppose that $\xi^\theta \in B$. By Proposition 1.4, there is $\theta' \in \mathbb{Z}_p[\Delta]$ such that $p^{-t}\theta\theta' e_\rho \equiv e_\rho \bmod M$ with $p^t \parallel \theta$. Thus,

$$\xi^{p^t} = \xi^{p^t e_\rho} = \xi^{\theta\theta' e_\rho} = \xi^{\theta\theta'} \in B.$$

It follows that $f \mid p^t$ by definition of f, so $f \mid \theta$. This shows one implication. The other implication is clear. This concludes the proof. $\square$

In the rest of this chapter, the following notation will be adopted: $\langle \eta \rangle$ will denote the cyclic group generated by η, and $(\mathfrak{C}_1, \ldots, \mathfrak{C}_i)$ will denote the multiplicative module generated over $\mathbb{Z}_p[\Delta]$ by $\mathfrak{C}_1, \ldots, \mathfrak{C}_i$.

Proposition 2.8. *Let H be a maximal principal submodule of $e_\rho(E/C)_p$ over $\mathbb{Z}_p[\Delta]$. Then $|e_\rho A| \mid |H|$.*

Proof. Let $H = (\eta C)$ with $\eta \in E$. It will be shown that $\langle \eta C \rangle$ is a maximal cyclic subgroup of $e_\rho(E/C)_p$. Suppose the contrary, that is, $\langle \eta C \rangle \subsetneqq \langle \varepsilon C \rangle \subseteq e_\rho(E/C)_p$ for some $\varepsilon \in E$. This clearly implies that $\eta C = (\varepsilon C)^a$ with $p \mid a$ and that $(\eta C) \subseteq (\varepsilon C)$. From the last relation it follows that $(\eta C) = (\varepsilon C)$, as (ηC) is a maximal principal submodule of $e_\rho(E/C)_p$. Thus, $\varepsilon C = (\eta C)^\theta$ with $\theta \in \mathbb{Z}_p[\Delta]$, whence $\eta C = (\varepsilon C)^a = (\eta C)^{a\theta}$. Since $p \mid a$, the order of ηC must be 1, so $\eta C = C$. Hence, $\varepsilon C = (\eta C)^\theta = \eta C$, which contradicts that $\langle \eta C \rangle \neq \langle \varepsilon C \rangle$. This shows the claim.

Let p^{r_0} be the order of $\langle \eta C \rangle$ and let $\alpha = \eta^{p^{r_0}} \in C$. Since $\eta C \in e_\rho(E/C)_p$, $e_\rho(\eta C) = \eta C$, and since M annihilates $(E/C)_p$, $e_\rho(\eta C) = e'_\rho(\eta C)$, so $\eta C = e_\rho(\eta C) = e'_\rho(\eta C) = (e'_\rho \eta)C$. The unit η will be chosen so that r_0 is the largest integer verifying $e'_\rho \alpha \in (F^\times)^{p^{r_0}}$. First assume that $e_\rho(E/C)_p$ is nontrivial. In this case, take any $\eta \in E$ such that $H = (\eta C)$. Clearly $e'_\rho \alpha = (e'_\rho \eta)^{p^{r_0}} \in (F^\times)^{p^{r_0}}$. Suppose that $e'_\rho \alpha = \varepsilon^{p^{r_0+1}}$ with $\varepsilon \in E$. Then $e'_\rho \eta = \varepsilon^p$ (as the pth root in F is unique if exists), so $((e'_\rho \varepsilon)C)^p = (e'_\rho \varepsilon^p)C = (e'_\rho \eta)C = \eta C$ with $(e'_\rho \varepsilon)C = e_\rho(\varepsilon C) \in e_\rho(E/C)_p$ ($\varepsilon C \in (E/C)_p$ as $(\varepsilon C)^p = (e'_\rho \eta)C \in (E/C)_p$). Thus $\langle (e'_\rho \varepsilon)C \rangle$ is a cyclic subgroup of $e_\rho(E/C)_p$ of order p^{r_0+1} containing $\langle \eta C \rangle$ properly, which contradicts the maximality of $\langle \eta C \rangle$. Now assume that $e_\rho(E/C)_p$ is trivial. In this case, $r_0 = 0$, $\alpha = \eta \in C$, and it is enough to find a unit $\eta \in C$ such that $e'_\rho \eta \notin (F^\times)^p$. By Proposition 1.13, there exists a Minkowski unit $\varepsilon \in E$. It is not difficult to show that $E^{p^n} \cap \mathbb{Z}[\Delta]\varepsilon \subseteq \mathbb{Z}[\Delta]\varepsilon^p$ for n sufficiently large. Choose $\hat{e}_\rho \in \mathbb{Z}[\Delta]$ such that $\hat{e}_\rho \equiv e_\rho \bmod p^n$. If for every

$\gamma \in E$, $\hat{e}_\rho\gamma \in E^p$, then $\hat{e}_\rho\gamma \in E^{p^n}$ (by applying $\hat{e}_\rho$ repeatedly), so in particular $\hat{e}_\rho\varepsilon \in E^{p^n}$. This implies that $\hat{e}_\rho\varepsilon \in E^{p^n} \cap \mathbb{Z}[\Delta]\varepsilon \subseteq \mathbb{Z}[\Delta]\varepsilon^p$, whence $\varepsilon^{\hat{e}_\rho} = \varepsilon^{p\theta}$ for some $\theta \in \mathbb{Z}[\Delta]$, so $\hat{e}_\rho = p\theta + be_1$ for some $b \in \mathbb{Z}$. Since $\rho \neq 1$, multiplying this equality by e_ρ yields $p \bigm| e_\rho$, which is impossible. Hence, there exists $\gamma \in E$ such that $\hat{e}_\rho\gamma \notin E^p$, or equivalently $e'_\rho\gamma \notin E^p$. Let $\eta = e'_\rho\gamma^{p^{-a}[E:C]}$ with $p^a \parallel [E:C]$. Thus $\eta C = e_\rho(\eta C) \in e_\rho(E/C)_p$ (as $\eta^{p^a} \in C$). Since $e_\rho(E/C)_p$ is trivial, there results that $\eta \in C$. Moreover, $e'_\rho\eta \notin E^p$ because $e'_\rho\gamma \notin E^p$. It then follows easily that $e'_\rho\eta \notin (F^\times)^p$, as needed.

Choose classes $\mathfrak{C}_1, \dots, \mathfrak{C}_k$ in $e_\rho A$ such that $e_\rho A = (\mathfrak{C}_1, \dots, \mathfrak{C}_k)$ and $\mathfrak{C}_i$ has order $f_i > 1$ in the group $e_\rho A / (\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})$ for $1 \leqslant i \leqslant k$.

Starting with $\kappa(L_0) = \alpha$ ($L_0 = 1$), the elements $\kappa(L_1), \dots, \kappa(L_k)$ of $F^\times$ will be obtained, where $L_i = \ell_1 \cdots \ell_i \in \mathbb{L}$ with $\ell_i \equiv 1 \bmod mML_{i-1}$. In addition, the prime λ_i of F above ℓ_i will be in the class $\mathfrak{C}_i$.

For $1 \leqslant i \leqslant k$, write r'_{i-1} for the largest integer such that $e'_\rho\kappa(L_{i-1})$ is a $p^{r'_{i-1}}$th power mod λ_i, and r_i for the largest integer such that $e'_\rho\kappa(L_i) \in (F^\times)^{p^{r_i}}$. It will be shown inductively that $r_i \leqslant r'_{i-1} \leqslant r_{i-1} \leqslant r_0$ and $f_i \bigm| p^{r_{i-1}-r_i}$ for $1 \leqslant i \leqslant k$, by choosing the primes $\lambda_1, \dots, \lambda_k$ suitably.

Fix i, $1 \leqslant i \leqslant k$, and assume $r_{i-1} \leqslant r_0$, which is trivial for $i = 1$. Apply Theorem 2.6 with $\mathfrak{C} = \mathfrak{C}_i$, $b = mML_{i-1}$, $c = p^{r_{i-1}+1}$, and $\beta = e'_\rho\kappa(L_{i-1})$, considering the prime ideals in $\mathfrak{C}_i$ at whose conjugates $\kappa(L_{i-1})$ is a unit, to show by absurd that there exists a prime $\lambda_i \in \mathfrak{C}_i$ of absolute degree 1, lying over a rational prime $\ell_i \equiv 1 \bmod mML_{i-1}$, and such that $r'_{i-1} \leqslant r_{i-1}$ and $\kappa(L_{i-1})$ is a unit at $\sigma\lambda_i$ for every $\sigma \in \Delta$. Since obviously $r'_{i-1} \geqslant r_{i-1}$, it follows that $r'_{i-1} = r_{i-1}$.

Let $\bar{r}_i$ be the largest integer $\leqslant r_0 + 1$ such that $e'_\rho\kappa(L_i) \in (F^\times)^{p^{\bar{r}_i}}$. The hypotheses of Proposition 2.5 are satisfied by $\ell = \ell_i$, $L = L_{i-1}$, $B = (\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})$, $r = \bar{r}_i$, and $r' = r'_{i-1}$. Indeed, the subgroup generated by the classes of the primes dividing L_{i-1} equals $(\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})$, which is included in $e_\rho A$ (condition

(1)); $p^{\bar{r}_i} \leqslant p^{r_0+1} \leqslant p \cdot |(E/C)_p| \leqslant M$, and $p^{-\bar{r}_i}M \geqslant p^{-r_0-1}M \geqslant |A|$, so $p^{-\bar{r}_i}M$ annihilates A (condition (2)); $e'_\rho \kappa(L_{i-1}) \equiv s^a \bmod \lambda_i$ implies $p^{r'_{i-1}} \parallel a$ by definition of r'_{i-1}, and $r_{i-1} \leqslant r_0$ (induction hypothesis) and $r'_{i-1} = r_{i-1}$ imply $p^{r'_{i-1}} \leqslant p^{r_0} \leqslant |(E/C)_p| < M$ (condition (3)). In consequence, $\bar{r}_i \leqslant r'_{i-1}$ and $p^{r'_{i-1}-\bar{r}_i}$ annihilates $\mathfrak{C}_i$ in $e_\rho A/(\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})$, so $f_i \mid p^{r'_{i-1}-\bar{r}_i}$. Since $r'_{i-1} = r_{i-1} \leqslant r_0$, $\bar{r}_i \leqslant r_0$. Then $r_i \leqslant r_0$ because $r_i \geqslant r_0 + 1$ would imply $\bar{r}_i = r_0 + 1$, which is impossible. Hence, $\bar{r}_i = r_i$, and so $r_i \leqslant r'_{i-1} = r_{i-1} \leqslant r_0$ and $f_i \mid p^{r_{i-1}-r_i}$.

As a consequence of the last relation, it will be obtained in the next paragraphs that $[(\mathfrak{C}_1, \dots, \mathfrak{C}_i) : (\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})] \mid [((\eta C)^{p^{r_i}}) : ((\eta C)^{p^{r_{i-1}}})]$.

It is easy to show that $(\eta C)^{p^{r_i}}$ has order $p^{r_{i-1}-r_i}$ in $e_\rho(E/C)_p/((\eta C)^{p^{r_{i-1}}})$. This amounts to showing that the least integer t such that $(\eta C)^{p^{r_i+t}} \in ((\eta C)^{p^{r_{i-1}}})$ equals $r_{i-1}-r_i$. Indeed, $t \leqslant r_{i-1}-r_i$ obviously, and since $|\langle \eta C \rangle| = p^{r_0}$, $(\eta C)^{p^{r_i+t+r_0-r_{i-1}}} = C$, and so $r_i+t+r_0-r_{i-1} \geqslant r_0$, i.e., $t \geqslant r_{i-1}-r_i$. In this manner, Lemma 2.7 can be used to show that the kernel of the surjective $\mathbb{Z}_p[\Delta]$-homomorphism from $\mathbb{Z}_p[\Delta]e_\rho$ to $((\eta C)^{p^{r_i}})/((\eta C)^{p^{r_{i-1}}})$ defined by $\theta \mapsto (\eta C)^{p^{r_i}\theta}$ is equal to $p^{r_{i-1}-r_i}\mathbb{Z}_p[\Delta]e_\rho$. Hence, $\mathbb{Z}_p[\Delta]e_\rho/p^{r_{i-1}-r_i}\mathbb{Z}_p[\Delta]e_\rho \simeq ((\eta C)^{p^{r_i}})/((\eta C)^{p^{r_{i-1}}})$.

Analogously, the kernel of the surjective $\mathbb{Z}_p[\Delta]$-homomorphism from $\mathbb{Z}_p[\Delta]e_\rho$ to $(\mathfrak{C}_1, \dots, \mathfrak{C}_i)/(\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})$ given by $\theta \mapsto \mathfrak{C}_i^\theta$ equals $f_i\,\mathbb{Z}_p[\Delta]e_\rho$, as f_i is the order of $\mathfrak{C}_i$ in $e_\rho A/(\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})$. Thus $\mathbb{Z}_p[\Delta]e_\rho/f_i\,\mathbb{Z}_p[\Delta]e_\rho \simeq (\mathfrak{C}_1, \dots, \mathfrak{C}_i)/(\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})$.

The relation $f_i \mid p^{r_{i-1}-r_i}$ obtained above implies that

$$\big|\mathbb{Z}_p[\Delta]e_\rho \,/\, f_i\,\mathbb{Z}_p[\Delta]e_\rho\big| \;\Big|\; \big|\mathbb{Z}_p[\Delta]e_\rho \,/\, p^{r_{i-1}-r_i}\mathbb{Z}_p[\Delta]e_\rho\big| .$$

Thus, by the stated isomorphisms, it follows that

$$[(\mathfrak{C}_1, \dots, \mathfrak{C}_i) : (\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})] \;\Big|\; [((\eta C)^{p^{r_i}}) : ((\eta C)^{p^{r_{i-1}}})] .$$

Finally, since

$$|e_\rho A| = \big|\,(\mathfrak{C}_1, \dots, \mathfrak{C}_k)\,\big| = \prod_{1 \leqslant i \leqslant k} [(\mathfrak{C}_1, \dots, \mathfrak{C}_i) : (\mathfrak{C}_1, \dots, \mathfrak{C}_{i-1})],$$

there results that

$$|e_\rho A| \;\Big|\; \prod_{1\leqslant i\leqslant k} [\,((\eta C)^{p^{r_i}}) : ((\eta C)^{p^{r_{i-1}}})\,] = |((\eta C)^{p^{r_k}})| \;\Big|\; |(\eta C)| = |H|\,,$$

as required. □

Theorem 2.9. *$|e_\rho A| = |e_\rho(E/C)_p|$ and $e_\rho(E/C)_p$ is a principal module over $\mathbb{Z}_p[\Delta]$.*

Proof. For every nontrivial irreducible higher dimensional character ρ of Δ with values in $\mathbb{Z}_p$, take a maximal principal submodule H_ρ of $e_\rho(E/C)_p$. Then $|e_\rho A| \mid |H_\rho|$ by Proposition 2.8, so $|e_\rho A| \leqslant |H_\rho| \leqslant |e_\rho(E/C)_p|$. Since $e_1 A = 1$ and $e_1(E/C)_p = C$, the group decompositions $A \simeq \prod_\rho e_\rho A$ and $(E/C)_p \simeq \prod_\rho e_\rho(E/C)_p$ hold. Hence,

$$|A| = \prod_\rho |e_\rho A| \leqslant \prod_\rho |H_\rho| \leqslant \prod_\rho |e_\rho(E/C)_p| = |(E/C)_p|.$$

Furthermore, the equality $|A| = |(E/C)_p|$ follows from the formula $[E : C] = 2^b h$, where h is the ideal class number of F, $b = 0$ if $g = 1$, $b = 2^{g-2} + 1 - g$ if $g \geqslant 2$, and g is the number of distinct prime factors of m (cf. [S], Theorem on p. 107).

There results that for every ρ, $|e_\rho A| = |H_\rho| = |e_\rho(E/C)_p|$, and $e_\rho(E/C)_p$ is a principal module as $e_\rho(E/C)_p = H_\rho$. This concludes the proof. □

Let $\operatorname{Im}\chi$ denote the image of $\chi \in X_\rho$. Observe that if $\chi_1, \chi_2 \in X_\rho$, then $\mathbb{Q}_p(\operatorname{Im}\chi_1) = \mathbb{Q}_p(\operatorname{Im}\chi_2)$. Indeed, the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{\varphi(m)/2})/\mathbb{Q}_p)$ acts transitively on the orbit X_ρ, so this group contains an automorphism τ such that $\tau\chi_1 = \chi_2$, and hence $\tau\mathbb{Q}_p(\operatorname{Im}\chi_1) = \mathbb{Q}_p(\operatorname{Im}\chi_2)$. But since $\mathbb{Q}_p(\operatorname{Im}\chi_1)/\mathbb{Q}_p$ is a subextension of the abelian (in fact cyclic) extension $\mathbb{Q}_p(\zeta_{\varphi(m)/2})/\mathbb{Q}_p$, $\mathbb{Q}_p(\operatorname{Im}\chi_1)/\mathbb{Q}_p$ is Galois (in fact cyclic), so $\tau\mathbb{Q}_p(\operatorname{Im}\chi_1) = \mathbb{Q}_p(\operatorname{Im}\chi_1)$. Thus the claimed equality follows.

Fix a character χ_0 in the orbit X_ρ, and denote $G = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{\varphi(m)/2})/\mathbb{Q}_p)$ and $H = \{\tau \in G : \tau\chi_0 = \chi_0\}$. It is clear that H is a subgroup of G and $|X_\rho| = [G : H]$ (orbit stabilizer theorem). Note that $\tau \in G$ fixes $\mathbb{Q}_p(\operatorname{Im}\chi_0)$ pointwise if and only if $\tau \in H$, so $H = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{\varphi(m)/2})/\mathbb{Q}_p(\mathrm{Im}\,\chi_0))$. Hence, by Galois theory, $|X_\rho| = [\mathbb{Q}_p(\mathrm{Im}\,\chi_0) : \mathbb{Q}_p]$.

Since the image $\mathrm{Im}\,\chi_0$ is a subgroup of the cyclic group generated by $\zeta_{\varphi(m)/2}$, it is also a cyclic group. Fix $\sigma_0 \in \Delta$ such that $\chi_0(\sigma_0)$ generates $\mathrm{Im}\,\chi_0$. Then $\mathbb{Q}_p(\mathrm{Im}\,\chi_0) = \mathbb{Q}_p(\chi_0(\sigma_0))$.

The next proposition will permit to determine the structure and the order of the groups $e_\rho(E/C)_p$ and $(\mathfrak{C})$ with $\mathfrak{C} \in e_\rho A$ in terms of their exponents.

Proposition 2.10. *$\mathbb{Z}_p[\Delta]e_\rho$ is a free $\mathbb{Z}_p$-module with base $\sigma_0{}^j e_\rho$ for $0 \leqslant j < |X_\rho|$.*

Proof. It is enough to show that every element in $\mathbb{Z}_p[\Delta]e_\rho$ can be uniquely written in the form $\sum_{0\leqslant j<|X_\rho|} c_j\, \sigma_0{}^j e_\rho$ with $c_j \in \mathbb{Z}_p$.

Let $\theta = \sum_{\sigma\in\Delta} b_\sigma\, \sigma \in \mathbb{Z}_p[\Delta]$. Then

$$\theta e_\rho = \sum_{\sigma\in\Delta} b_\sigma\, \sigma \sum_{\chi\in X_\rho} e_\chi = \sum_\chi \sum_\sigma b_\sigma \chi(\sigma) e_\chi\,,$$

because $\sigma e_\chi = \chi(\sigma)e_\chi$ for all $\sigma \in \Delta$ and $\chi \in X_\rho$. Since $\sum_\sigma b_\sigma \chi_0(\sigma) \in \mathbb{Q}_p(\mathrm{Im}\,\chi_0) = \mathbb{Q}_p(\chi_0(\sigma_0))$ and $[\mathbb{Q}_p(\mathrm{Im}\,\chi_0) : \mathbb{Q}_p] = |X_\rho|$, $\sum_\sigma b_\sigma \chi_0(\sigma)$ can be written as a polynomial in $\chi_0(\sigma_0)$ of degree less than $|X_\rho|$ with coefficients in $\mathbb{Z}_p$, say $\sum_\sigma b_\sigma \chi_0(\sigma) = \sum_{0\leqslant j<|X_\rho|} c_j \chi_0(\sigma_0)^j$. This equality is then valid for any χ in X_ρ, that is,

$$\sum_{\sigma\in\Delta} b_\sigma \chi(\sigma) = \sum_{0\leqslant j<|X_\rho|} c_j \chi(\sigma_0)^j,$$

by applying the automorphism that takes χ_0 into χ. As $\chi(\sigma_0)^j e_\chi = \chi(\sigma_0{}^j) e_\chi = \sigma_0{}^j e_\chi$, it follows that

$$\theta e_\rho = \sum_\chi \sum_j c_j \chi(\sigma_0)^j e_\chi = \sum_\chi \sum_j c_j\, \sigma_0{}^j e_\chi = \sum_j c_j\, \sigma_0{}^j e_\rho\,,$$

as required.

To show uniqueness, assume that $\sum_{0\leqslant j<|X_\rho|} c_j \sigma_0{}^j e_\rho = 0$. Then, by applying e_{χ_0}, it follows that $\sum_j c_j \sigma_0{}^j e_{\chi_0} = 0$, which amounts to writing $\sum_j c_j \chi_0(\sigma_0)^j e_{\chi_0} = 0$. Thus $\sum_j c_j \chi_0(\sigma_0)^j = 0$, whence all the c_j are 0, since $\chi_0(\sigma_0)$ has degree $|X_\rho|$ over $\mathbb{Q}_p$. This concludes the proof. □

Theorem 2.11. *The following group decompositions and formulas hold:*

(a) $e_\rho(E/C)_p \simeq \prod_{0 \leqslant j < |X_\rho|} \langle \sigma_0{}^j \eta C \rangle$, *where* ηC *is a generator of* $e_\rho(E/C)_p$ *as* $\mathbb{Z}_p[\Delta]$*-module, and* $|e_\rho(E/C)_p| = |\langle \eta C \rangle|^{|X_\rho|}$;

(b) $(\mathfrak{C}) \simeq \prod_{0 \leqslant j < |X_\rho|} \langle \sigma_0{}^j \mathfrak{C} \rangle$ *for every* $\mathfrak{C} \in e_\rho A$, *and* $|(\mathfrak{C})| = |\langle \mathfrak{C} \rangle|^{|X_\rho|}$.

Proof. (a) By Proposition 2.9 there is a generator ηC of $e_\rho(E/C)_p$ as $\mathbb{Z}_p[\Delta]$-module. Thus it will be enough to show that the classes $\sigma_0{}^j \eta C$ for $0 \leqslant j < |X_\rho|$ are multiplicatively independent. For this purpose, assume that

$$(\eta C)^{\sum_{0 \leqslant j < |X_\rho|} c_j \sigma_0{}^j} = C \quad \text{with} \quad c_j \in \mathbb{Z}_p\,.$$

Then $\sum_j c_j \sigma_0{}^j e_\rho$ is an annihilator in $\mathbb{Z}_p[\Delta]e_\rho$ of ηC, so it is divisible by $|\langle \eta C \rangle|$ by Lemma 2.7 with $B = (1)$ as submodule of $e_\rho(E/C)_p$. Hence the coefficients c_j are all divisible by $|\langle \eta C \rangle|$ in view of their uniqueness in Proposition 2.10. It then follows that

$$(\eta C)^{c_j \sigma_0{}^j} = C \quad \text{for every } j\,, \ 0 \leqslant j < |X_\rho|\,,$$

as required.

The equality $|e_\rho(E/C)_p| = |\langle \eta C \rangle|^{|X_\rho|}$ follows readily from the group decomposition shown above, because $|\langle \sigma_0{}^j \eta C \rangle| = |\langle \eta C \rangle|$ for every j, $0 \leqslant j < |X_\rho|$.

(b) The proof is analogous to that of item (a). This concludes the proof of the theorem. □

CHAPTER 3

The Minus Part of the Ideal Class Group of a Cyclotomic Field

Consider the mth cyclotomic field $F = \mathbb{Q}(\zeta_m)$ for $m \geqslant 3$. Without lost of generality, it is assumed that $m \not\equiv 2 \bmod 4$. Denote $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ and let p be an odd prime not dividing $|\Delta| = \varphi(m)$. This assumption implies that $p \parallel m$ or $p \nmid m$.

Characters of Δ will be defined on $(\mathbb{Z}/m\mathbb{Z})^\times$ via the canonical isomorphism $\Delta \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.

Fix an irreducible higher dimensional odd character ρ of $(\mathbb{Z}/m\mathbb{Z})^\times$ with values in $\mathbb{Z}_p$, and assume, if $p \parallel m$, that $\rho \neq \omega$, where ω is the Teichmüller character of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathbb{Z}_p^\times$. Let e_ρ be the idempotent corresponding to ρ, defined in Section 1.2.

In general, the group of bth roots of unity will be denoted by μ_b and ζ_b will stand for a primitive bth root of unity. Denote $F(L) = F(\zeta_L)$ and $\Delta(L) = \mathrm{Gal}(F(L)/\mathbb{Q})$. Write $A(L)$ for the p-part of the ideal class group of $F(L)$ and let $A = A(1)$.

Let M be a power of p greater than 1 to be defined in Section 3.6. The notation e'_ρ will stand for a fixed element of the group ring $\mathbb{Z}[\Delta]$ such that $e'_\rho \equiv e_\rho \bmod M$. Let $\mathbb{L}$ denote the set of products (the empty product included) of distinct odd rational primes ℓ satisfying the congruence $\ell \equiv 1 \bmod mM$. Henceforth L and ℓ will denote an integer and a prime in $\mathbb{L}$ respectively. In addition, λ will denote a prime of F

above ℓ, and $\mathcal{L}$ a prime of $F(L)$ above λ.

Let $G_L = \mathrm{Gal}(F(L)/F)$. Thus G_L is isomorphic to $\prod_{\ell \mid L} G_\ell$ and to $\mathrm{Gal}(\mathbb{Q}(\zeta_L)/\mathbb{Q})$, and $\Delta(L)$ is isomorphic to ΔG_L.

Any automorphism in Δ, $\Delta(L)$, and G_L will be extended as necessary so that it acts as the identity on roots of unity of order prime to m, mL, and L respectively.

When the notation for an automorphism over $\mathbb{Q}$ carries a subindex, it will be understood that the automorphism raises the appropriate root of unity to the index. For example, $\tau_b \in \Delta(L)$ will mean that τ_b is defined by $\tau_b(\zeta_{mL}) = \zeta_{mL}^b$. However, this convention will not stand for extensions of automorphisms.

3.1 Basic Elements

In this section, definitions are stated and basic properties are shown of important elements, such as Gauss sums $S(\mathcal{L}, \zeta_\ell)$, numbers $\alpha(L, \mathcal{L})$, and operators N_L, D_L, $s(L)$, $\theta(L)$, and $\delta(L)$, which will be utilized repeatedly in this chapter. Proposition 3.2 applies the Davenport-Hasse distribution theorem (Theorem 1.7).

Fix a primitive root s_ℓ mod ℓ. Then $\sigma_{s_\ell} \in G_\ell$ generates G_ℓ. When there is no risk of confusion, s_ℓ will be denoted simply by s. Define elements in $\mathbb{Z}[G_\ell]$ by

$$N_\ell = \sum_{0 \leqslant j \leqslant \ell-2} \sigma_s^j \,, \quad D_\ell = \sum_{1 \leqslant j \leqslant \ell-2} j\sigma_s^j \,,$$

and elements in $\mathbb{Z}[G_L]$ by

$$N_L = \prod_{\ell \mid L} N_\ell \,, \quad D_L = \prod_{\ell \mid L} D_\ell \,.$$

It is easily shown, as in Chapter 2, that N_ℓ and D_ℓ verify the equality $(\sigma_s - 1)D_\ell = \ell - 1 - N_\ell$.

Let $\ell \equiv 1$ mod mML. Consider the Gauss sum

$$S(\xi, \zeta_\ell) = \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \xi(a)\, \zeta_\ell^a \in \mathbb{Z}[\zeta_{\ell(\ell-1)}],$$

where ξ is a character of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ into $\mu_{\ell-1}$. Define

$$S(\mathcal{L},\zeta_\ell) = S(\varepsilon,\zeta_\ell) = \sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^\times} \varepsilon(a)\,\zeta_\ell^a \in F(\ell L),$$

where $\varepsilon : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mu_{mL}$ is the character satisfying $\varepsilon(a) \equiv a^{-(\ell-1)/mL} \bmod \mathcal{L}$ for all $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$. The uniqueness of this character follows from the pairwise incongruence of the mLth roots of unity mod $\mathcal{L}$, which derives from the relation $\ell \nmid mL$ (as $\ell \equiv 1 \bmod mML$).

The first simple properties of the sum $S(\mathcal{L},\zeta_\ell)$ are given in the next lemma.

Lemma 3.1. *Let $\ell \equiv 1 \bmod mML$ and let $\varepsilon : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mu_{mL}$ be the character satisfying $\varepsilon(a) \equiv a^{-(\ell-1)/mL} \bmod \mathcal{L}$ for all $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$. Then*

(a) *$\sigma S(\mathcal{L},\zeta_\ell) = S(\mathcal{L},\sigma\zeta_\ell) = \varepsilon(b)^{-1}S(\mathcal{L},\zeta_\ell)$ for every $\sigma = \sigma_b \in G_\ell$;*

(b) *$\sigma S(\mathcal{L},\zeta_\ell) = S(\sigma\mathcal{L},\zeta_\ell)$ for every $\sigma \in G_L$.*

Proof. (a) Let $\sigma = \sigma_b \in G_\ell$. Thus $\sigma S(\mathcal{L},\zeta_\ell) = \sigma(\sum_a \varepsilon(a)\zeta_\ell^a) = \sum_a \varepsilon(a)(\sigma\zeta_\ell)^a = \sum_a \varepsilon(a)\zeta_\ell^{ab} = \varepsilon(b)^{-1}\sum_a \varepsilon(ab)\zeta_\ell^{ab} = \varepsilon(b)^{-1}S(\mathcal{L},\zeta_\ell)$.

(b) Let $\sigma \in G_L$. Then $\sigma\varepsilon(a) \equiv a^{-(\ell-1)/mL} \bmod \sigma\mathcal{L}$ for all $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, so $\sigma S(\mathcal{L},\zeta_\ell) = \sigma(\sum_a \varepsilon(a)\zeta_\ell^a) = \sum_a \sigma\varepsilon(a)\zeta_\ell^a = S(\sigma\mathcal{L},\zeta_\ell)$. □

For $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, extend the automorphism $\sigma_a \in \Delta$ to $F(\zeta_{ML})$ so that $\sigma_a\zeta_M = \zeta_M^{\omega(a)}$ if $p \parallel m$, $\sigma_a\zeta_M = \zeta_M$ if $p \nmid m$, and $\sigma_a\zeta_L = \zeta_L$. This extension will be standard throughout this chapter except in a part of the proof of Theorem 3.14. Let $n \in (\mathbb{Z}/m\mathbb{Z})^\times$ satisfy $n \not\equiv 1 \bmod m$, and for every n, fix an integer n_L such that $\sigma_n\zeta_{mML} = \zeta_{mML}^{n_L}$. Thus, $n_L \equiv n \bmod m$; $n_L \equiv \omega(n) \bmod M$ if $p \parallel m$, $n_L \equiv 1 \bmod M$ if $p \nmid m$; and $n_L \equiv 1 \bmod L$. (The integer n will be suitably chosen in the proof of Proposition 3.19.)

For L and ℓ satisfying $\ell \equiv 1 \bmod mML$, define

$$\alpha(L,\mathcal{L}) = (\sigma_n - n_L)\,S(\mathcal{L},\zeta_\ell).$$

Since $\sigma_n - n_L$ annihilates μ_{mL}, item (a) of Lemma 3.1 implies that $\alpha(L, \mathcal{L})$ is in $F(L)^\times$ and does not depend on the choice of ζ_ℓ. The numbers $\alpha(L, \mathcal{L})$ form an Euler system of Gauss sums.

Define elements in $\mathbb{Z}[\Delta(L)]$ by

$$s(L) = \sum_{\substack{1 \leqslant a < mL \\ (a, mL)=1}} a \, \tau_a^{-1}, \quad \theta(L) = \tfrac{1}{mL} \, (\sigma_n - n_L) \, s(L).$$

It is easily shown that $\theta(L) \in \mathbb{Z}[\Delta(L)]$. Indeed, $\langle \cdot \rangle$ standing for the least nonnegative residue mod mL,

$$\begin{aligned}(\sigma_n - n_L) \sum_a a \, \tau_a^{-1} &= \sum_a a \, \tau_{n_L} \tau_a^{-1} - \sum_a a \, n_L \tau_a^{-1} \\ &= \sum_a (\langle a n_L \rangle - a n_L) \, \tau_a^{-1} \in mL \, \mathbb{Z}[\Delta(L)],\end{aligned}$$

so the claim follows.

Proposition 3.2. *Let $\ell \equiv 1$ mod mML.*

(a) *If $L = \ell' L'$, then $N_{\ell'} \, \alpha(L, \mathcal{L}) = (1 - \mathrm{Frob}_{\ell'}^{-1}) \, \alpha(L', N_{\ell'} \mathcal{L}) \, \beta^M$, where* $\mathrm{Frob}_{\ell'}$ *is the Frobenius of ℓ' in $F(L')/\mathbb{Q}$, and $\beta \in F(L')^\times$.*

(b) $(\alpha(L, \mathcal{L})) = \mathcal{L}^{\theta(L)}$.

Proof. (a) In order to prove the required equality, $N_{\ell'} \, S(\mathcal{L}, \zeta_l)$ will be expressed in terms of $S(N_{\ell'} \, \mathcal{L}, \zeta_\ell)$.

By definition of $S(\mathcal{L}, \zeta_l)$,

$$N_{\ell'} \, S(\mathcal{L}, \zeta_l) = N_{\ell'} \Big(\sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \varepsilon(a) \, \zeta_\ell^a \Big) = \prod_{\sigma \in G_{\ell'}} \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \sigma \, \varepsilon(a) \, \zeta_\ell^a \,,$$

where $\varepsilon : (\mathbb{Z}/m\mathbb{Z})^\times \to \mu_{mL}$ is the character satisfying $\varepsilon(a) \equiv a^{-(\ell-1)/mL}$ mod $\mathcal{L}$ for all $a \in (\mathbb{Z}/\ell \, \mathbb{Z})^\times$.

There exists a generator g of $(\mathbb{Z}/\ell \, \mathbb{Z})^\times$ such that $\varepsilon(g) = \zeta_{mL'} \, \zeta_{\ell'}$. Define a character $\psi : (\mathbb{Z}/\ell \, \mathbb{Z})^\times \to \mu_{\ell'}$ by $\psi(g) = \zeta_{\ell'}$. It follows that $\sigma\varepsilon(g) = \zeta_{mL'} \, \sigma\zeta_{\ell'} =$

$\zeta_{mL'}\,\zeta_{\ell'}\,\zeta_{\ell'}^{\sigma-1} = \varepsilon(g)\,\psi(g)^{\sigma-1}$, and so $\sigma\varepsilon(a) = \varepsilon(a)\,\psi(a)^{\sigma-1}$ for all $\sigma \in G_{\ell'}$ and $a \in (\mathbb{Z}/\ell\mathbb{Z})^{\times}$. Hence

$$\begin{aligned} N_{\ell'}\,S(\mathcal{L},\zeta_l) &= \prod_{\sigma}\sum_{a}\varepsilon(a)\,\psi(a)^{\sigma-1}\zeta_\ell^a = \prod_{0\leqslant j\leqslant \ell'-2}\Bigl(\sum_a \varepsilon(a)\,\psi(a)^j\zeta_\ell^a\Bigr) \\ &= \Bigl(\sum_a \varepsilon(a)\,\psi(a)^{-1}\zeta_\ell^a\Bigr)^{-1}\prod_{0\leqslant j\leqslant \ell'-1}\Bigl(\sum_a \varepsilon(a)\,\psi(a)^j\zeta_\ell^a\Bigr). \end{aligned}$$

The character $\varepsilon\,\psi^{-1}$ of $(\mathbb{Z}/\ell\mathbb{Z})^{\times}$ takes values in $\mu_{mL'}$, so $\mathrm{Frob}_{\ell'}$ can be applied to it, yielding $\mathrm{Frob}_{\ell'}(\varepsilon\,\psi^{-1}) = \varepsilon^{\ell'}$. This character satisfies the congruence $\varepsilon^{\ell'}(a) \equiv a^{-(\ell-1)/mL'} \bmod N_{\ell'}\mathcal{L}$ for all $a \in (\mathbb{Z}/\ell\mathbb{Z})^{\times}$, because it satisfies the same congruence $\bmod\,\mathcal{L}$ and $\varepsilon^{\ell'}(a) \in \mu_{mL'} \subseteq F(L')$. Thus,

$$\sum_a \varepsilon(a)\,\psi(a)^{-1}\zeta_\ell^a = \mathrm{Frob}_{\ell'}^{-1}\Bigl(\sum_a \varepsilon^{\ell'}(a)\,\zeta_\ell^{a\ell'}\Bigr) = \mathrm{Frob}_{\ell'}^{-1}\,S(N_\ell'\mathcal{L},\zeta_\ell^{\ell'}).$$

On the other hand, the Davenport-Hasse distribution theorem (Theorem 1.7) yields the equality

$$\prod_{0\leqslant j\leqslant \ell'-1} S(\varepsilon\,\psi^j,\zeta_\ell) = -S(\varepsilon^{\ell'},\zeta_\ell)\,\varepsilon(\ell'^{-\ell'})\prod_{0\leqslant j\leqslant \ell'-1} S(\psi^j,\zeta_\ell)\,.$$

The product on the right side can be evaluated by applying Proposition 1.5:

$$\begin{aligned} \prod_{0\leqslant j\leqslant \ell'-1} S(\psi^j,\zeta_\ell) &= S(1,\zeta_\ell)\prod_{1\leqslant j\leqslant (\ell'-1)/2} S(\psi^j,\zeta_\ell)\,S(\psi^{-j},\zeta_\ell) \\ &= \Bigl(\sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^{\times}}\zeta_l^a\Bigr)\prod_{1\leqslant j\leqslant (\ell'-1)/2} S(\psi^j,\zeta_\ell)\,\psi^j(-1)\,\overline{S(\psi^j,\zeta_\ell)} \\ &= -\prod_{1\leqslant j\leqslant (\ell'-1)/2}\bigl|S(\psi^j,\zeta_\ell)\bigr|^2 \\ &= -\prod_{1\leqslant j\leqslant (\ell'-1)/2}\ell \;=\; -\ell^{(\ell'-1)/2}. \end{aligned}$$

Thus,

$$\begin{aligned} \prod_{0\leqslant j\leqslant \ell'-1}\sum_a \varepsilon(a)\,\psi^j(a)\,\zeta_\ell^a &= \prod_j S(\varepsilon\,\psi^j,\zeta_\ell) \\ &= S(\varepsilon^{\ell'},\zeta_\ell)\,\varepsilon(\ell')^{-\ell'}\,\ell^{(\ell'-1)/2} \\ &= S(N_{\ell'}\mathcal{L},\zeta_\ell)\,\varepsilon(\ell')^{-\ell'}\,\ell^{(\ell'-1)/2}. \end{aligned}$$

Replacing the results of the last two paragraphs in the previous formula for $N_{\ell'} S(\mathcal{L}, \zeta_\ell)$ leads to

$$N_{\ell'} S(\mathcal{L}, \zeta_\ell) = S(N_{\ell'}\mathcal{L}, \zeta_\ell)\, \varepsilon(\ell')^{-\ell' \ell(\ell'-1)/2} \,/\, \mathrm{Frob}_{\ell'}^{-1}\, S(N_{\ell'}\mathcal{L}, \zeta_\ell^{\ell'}).$$

The required equality follows by applying $\sigma_n - n_L$, as $(\sigma_n - n_L)\, S(\mathcal{L}, \zeta_\ell) = \alpha(L, \mathcal{L})$, $(\sigma_n - n_L)\, S(N_{\ell'}\mathcal{L}, \zeta_\ell) = \alpha(L', N_{\ell'}\mathcal{L})\, S(N_{\ell'}\mathcal{L}, \zeta_\ell)^{n_{L'} - n_L}$, $(\sigma_n - n_L)\, S(N_{\ell'}\mathcal{L}, \zeta_\ell^{\ell'}) = \alpha(L', N_{\ell'}\mathcal{L})\, S(N_{\ell'}\mathcal{L}, \zeta_\ell^{\ell'})^{n_{L'} - n_L}$, $(\sigma_n - n_L)\, \varepsilon(\ell') = 1$, $M \mid n_{L'} - n_L$, and $M \mid (\ell' - 1)/2$.

(b) By Proposition 1.8, the principal ideal generated by the Gauss sum $S(\mathcal{L}, \zeta_\ell)$ can be factored as

$$(S(\mathcal{L}, \zeta_\ell)) = \mathcal{L}^{\frac{1}{m_L} s(L)}.$$

Then applying $\sigma_n - n_L$ yields the factorization

$$(\alpha(L, \mathcal{L})) = \mathcal{L}^{\theta(L)},$$

as required. □

Lemma 3.3. *Let $\ell \equiv 1 \bmod mML$.*

(a) $(\sigma - 1)\, D_L\, \alpha(L, \mathcal{L}) \in (F(L)^\times)^M$ *for every* $\sigma \in G_L$.

(b) $(\sigma - 1)\, D_L\, \theta(L) \in M\mathbb{Z}[\Delta(L)]$ *for every* $\sigma \in G_L$.

(c) $D_L\, \theta(L) \in N_L (\mathbb{Z}/M\mathbb{Z})[\Delta]$.

Proof. (a) The case $L = 1$ is trivial because $G_1 = 1$. Assume by induction that $L > 1$ and that the statement is true for all proper divisors of L. Let ℓ' be a prime factor of L and $L = \ell' L'$. Then, considering the equality $(\sigma_{\ell'} - 1)\, D_{\ell'} = \ell' - 1 - N_{\ell'}$ and item (a) of Proposition 3.2,

$$\begin{aligned}(\sigma_{\ell'} - 1)\, D_L\, \alpha(L, \mathcal{L}) &= (\sigma_{\ell'} - 1)\, D_{\ell'} D_{L'}\, \alpha(L, \mathcal{L}) \\ &= (\ell' - 1 - N_{\ell'})\, D_{L'}\, \alpha(L, \mathcal{L}) \\ &= D_{L'}\, \alpha(L, \mathcal{L})^{\ell' - 1} / (1 - \mathrm{Frob}_{\ell'}^{-1})\, D_{L'}\, \alpha(L', N_{\ell'}\mathcal{L})\, \beta^M,\end{aligned}$$

where $\mathrm{Frob}_{\ell'}$ is the Frobenius of ℓ' in $F(L')/\mathbb{Q}$ and $\beta \in F(L')^\times$. It follows that $(\sigma_{\ell'} - 1)\, D_L\, \alpha(L, \mathcal{L}) \in (F(L)^\times)^M$ by induction hypothesis and because $M \mid \ell' - 1$. Since G_L is generated by the $\sigma_{\ell'}$ with $\ell' \mid L$, the statement is valid for all $\sigma \in G_L$.

(b) By item (a), the principal ideal $(\sigma - 1)\, D_L\, (\alpha(L, \mathcal{L}))$ is the Mth power of an ideal of $F(L)$, and by item (b) of Proposition 3.2, $(\alpha(L, \mathcal{L})) = \mathcal{L}^{\theta(L)}$. Hence $\mathcal{L}^{(\sigma-1)\, D_L\, \theta(L)}$ is the Mth power of an ideal of $F(L)$. Since ℓ splits completely in $F(L)$, $(\sigma - 1)\, D_L\, \theta(L)$ must be divisible by M. This shows the result.

(c) Since $\Delta(L) \simeq \Delta G_L$, $D_L\, \theta(L) \in \mathbb{Z}[\Delta(L)]$ can be written in the form

$$D_L\, \theta(L) = \sum_{\sigma \in \Delta} \sum_{\tau \in G_L} a_{\sigma\tau}\, \sigma\tau \quad \text{with} \quad a_{\sigma\tau} \in \mathbb{Z}.$$

Thus item (b) implies that for σ fixed, all the coefficients $a_{\sigma\tau}$ for $\tau \in G_L$ are congruent mod M. Choosing a representative a_σ of their common class mod M, it follows that

$$D_L\, \theta(L) \equiv \sum_\sigma \sum_\tau a_\sigma\, \sigma\tau = \sum_\tau \tau \sum_\sigma a_\sigma\, \sigma = N_L \sum_\sigma a_\sigma\, \sigma \mod M,$$

which means that $D_L\, \theta(L) \in N_L\, (\mathbb{Z}/M\mathbb{Z})[\Delta]$. This concludes the proof. □

Define $\delta(1) = \theta(1)\, e_\rho \in \mathbb{Z}[\Delta]e_\rho$. For $L > 1$, define $\delta(L)$ to be the element in $(\mathbb{Z}/M\mathbb{Z})[\Delta]e_\rho$ satisfying the congruence

$$N_L\, \delta(L) \equiv D_L\, \theta(L)\, e_\rho \mod M. \qquad (*)$$

The existence of $\delta(L)$ is guaranteed by item (c) of Lemma 3.3, and its uniqueness is clearly seen. It is also clear that $\delta(1)$ satisfies the congruence above with $L = 1$.

3.2 An Application of the Inflation-Restriction Exact Sequence

This section consists of Lemmas 3.4 and 3.5, the definition of the numbers $\kappa(L, \lambda)$, and Proposition 3.6. Lemma 3.4 is a basic tool in this chapter; it is used in Lemma

3.5 and in later sections. Lemma 3.5 is an application of the inflation-restriction exact sequence (Proposition 1.10) and is the unique result in this thesis requiring methods of homological algebra. This lemma is needed to define the numbers $\kappa(L,\lambda)$. Proposition 3.6 gives a fundamental relationship between the numbers $\kappa(L,\lambda)$ and the operators $\delta(L)$, and will be utilized in Theorem 3.12 and Proposition 3.15.

Lemma 3.4. $e_\rho\,\zeta_M = 1$.

Proof. Let $p \parallel m$. Then the Teichmüller character ω is defined but is not contained in X_ρ, so $\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}\chi^{-1}(a)\,\omega(a) = 0$ for every $\chi\in X_\rho$. Thus, a and χ running over $(\mathbb{Z}/m\mathbb{Z})^\times$ and X_ρ respectively, and writing $e_\rho = \varphi(m)^{-1}\sum_a\sum_\chi\chi^{-1}(a)\,\sigma_a$, it follows that

$$e_\rho\,\zeta_M^{\varphi(m)} = \left(\textstyle\sum_a\sum_\chi\chi^{-1}(a)\,\sigma_a\right)\zeta_M = \left(\textstyle\sum_\chi\sum_a\chi^{-1}(a)\,\omega(a)\right)\zeta_M = 1.$$

Let $p\nmid m$. Then $\sum_a\chi^{-1}(a) = 0$ for every $\chi\in X_\rho$, as ρ is odd. Thus,

$$e_\rho\,\zeta_M^{\varphi(m)} = \left(\textstyle\sum_a\sum_\chi\chi^{-1}(a)\,\sigma_a\right)\zeta_M = \left(\textstyle\sum_\chi\sum_a\chi^{-1}(a)\right)\zeta_M = 1.$$

In both cases, there results that $e_\rho\,\zeta_M = 1$, as required. □

Lemma 3.5. *Let F' be an abelian number field containing F. Then the canonical map*

$$e_\rho\,(F^\times/(F^\times)^M) \longrightarrow e_\rho\left[F'^\times/(F'^\times)^M\right]^{\mathrm{Gal}(F'/F)}$$

is an isomorphism.

Proof. Let $\bar{F}$ be an algebraic closure of F containing F'. Consider the partial inflation-restriction exact sequence

$$H^1(G/H,\mu_M^H) \longrightarrow H^1(G,\mu_M) \longrightarrow H^1(H,\mu_M)^{G/H} \longrightarrow H^2(G/H,\mu_M^H)\,,$$

where $G = \mathrm{Gal}(\bar{F}/F)$ and $H = \mathrm{Gal}(\bar{F}/F')$ (see Proposition 1.10). The cohomology groups in this sequence will be evaluated.

It is clear that $G/H \simeq \mathrm{Gal}(F'/F)$ and $\mu_M^H = \mu_M \cap F'$. The short exact sequence of G-modules

$$1 \longrightarrow \mu_M \longrightarrow \bar{F}^\times \xrightarrow{M} \bar{F}^\times \longrightarrow 1\,,$$

where the map $\bar{F}^\times \xrightarrow{M} \bar{F}^\times$ rises to the Mth power, yields the long exact sequence

$$\begin{aligned} 1 \longrightarrow & H^0(G,\mu_M) \longrightarrow H^0(G,\bar{F}^\times) \xrightarrow{M} H^0(G,\bar{F}^\times) \longrightarrow \\ & H^1(G,\mu_M) \longrightarrow H^1(G,\bar{F}^\times) \xrightarrow{M} H^1(G,\bar{F}^\times) \longrightarrow \;\ldots\;. \end{aligned}$$

Thus, since $H^0(G,\bar{F}^\times) = (\bar{F}^\times)^G = F^\times$, and $H^1(G,\bar{F}^\times) = 1$ by Hilbert's Theorem 90, it follows that $H^1(G,\mu_M) \simeq F^\times/(F^\times)^M$. Similarly it is obtained that $H^1(H,\mu_M) \simeq F'^\times/(F'^\times)^M$.

Therefore, the partial inflation-restriction exact sequence becomes

$$\begin{aligned} H^1(\mathrm{Gal}(F'/F),\mu_M \cap F') \longrightarrow F^\times/(F^\times)^M \longrightarrow \big[F'^\times/(F'^\times)^M\big]^{\mathrm{Gal}(F'/F)} \longrightarrow \\ \longrightarrow H^2(\mathrm{Gal}(F'/F),\mu_M \cap F'). \end{aligned}$$

Let $\mathrm{Gal}(F'/F) = \prod_j C_j$ be a decomposition in cyclic groups. Then

$$H^i(\mathrm{Gal}(F'/F),\mu_M \cap F') \simeq \prod_j H^i(C_j\,,\mu_M \cap F') \quad \text{for} \quad i = 1,2.$$

Since for a cyclic group C,

$$H^1(C,\mu_M \cap F') = \frac{\ker N\,\big|_{\mu_M \cap F'}}{(\mu_M \cap F')^{\sigma-1}}\,, \quad H^2(C,\mu_M \cap F') = \frac{(\mu_M \cap F')^C}{N(\mu_M \cap F')},$$

where σ is a generator of C and $N = 1+\sigma+\ldots+\sigma^{|C|-1}$, these cohomology groups are quotients of subgroups of $\mu_M \cap F'$. Thus, by Lemma 3.4, $e_\rho\, H^i(\mathrm{Gal}(F'/F),\mu_M) = 1$ for $i = 1,2$.

Hence, applying e_ρ to the exact sequence above concludes the proof. □

Let $\ell \equiv 1 \bmod mML$. As a consequence of item (a) of Lemma 3.3, $D_L\,\alpha(L,\mathcal{L}) \in \big[F(L)^\times/(F(L)^\times)^M\big]^{G_L}$. Thus, in view of Lemma 3.5 with $F' = F(L)$, there exists a unique $\kappa(L,\lambda) \in e_\rho(F^\times/(F^\times)^M)$ satisfying the congruence

$$\kappa(L,\lambda) \equiv D_L\,\alpha(L,\mathcal{L})\,e_\rho \mod (F(L)^\times)^M. \qquad (**)$$

The relation $\sigma\,\alpha(L,\mathcal{L}) = \alpha(L,\sigma\mathcal{L})$ for every $\sigma \in G_L$, which follows from item (b) of Lemma 3.1, justifies the notation $\kappa(L,\lambda)$, indicating dependence on L and λ but not on $\mathcal{L}$.

Proposition 3.6. *Let $\ell \equiv 1 \bmod mML$. Then*

$$(\kappa(L,\lambda)) = \lambda^{\delta(L)} \cdot (\textit{primes dividing } L) \cdot \mathcal{B}^M,$$

where $\mathcal{B}$ is an ideal of F.

Proof. Applying $D_L\, e'_p$ to the equality in item (b) of Proposition 3.2 and using congruence $(*)$ of Section 3.1 and congruence $(**)$ above, the principal ideal $(\kappa(L,\lambda))$ of $F(L)$ can be factored in the form

$$(\kappa(L,\lambda)) = \mathcal{L}^{N_L\,\delta(L)} \cdot \mathcal{B}'^M,$$

where $\mathcal{B}'$ is an ideal of $F(L)$ such that $\mathcal{B}'^M$ is the lift of an ideal of F.

If $\mathfrak{q}$ is a prime of F not dividing L, then $\mathfrak{q}$ does not ramify in $F(L)$. Thus, if $\mathfrak{q} \neq \lambda$, $v_{\mathfrak{q}}(\kappa(L,\lambda)) \equiv 0 \bmod M$. Since $\mathcal{L}^{N_L} = \lambda$, the prime factorization of $\kappa(L,\lambda)$ in F must have the form

$$(\kappa(L,\lambda)) = \lambda^{\delta(L)} \cdot (\text{primes dividing } L) \cdot \mathcal{B}^M,$$

where $\mathcal{B}$ is an ideal of F, as required. □

3.3 Kolyvagin's Lemma

In this section, the map ind_ℓ is defined and a notable property of it is given in Lemma 3.7. In addition, the operators $s'(L,\ell)$ and $\theta'(L,\ell)$ are introduced, and an important relationship between the operators N_ℓ, D_ℓ, $\theta(\ell L)$, and $\theta'(L,\ell)$ is presented in Proposition 3.8.

Lemma 3.7, proven first by Kolyvagin in [K2], is a generalization of the case $m = p$ given by Rubin in [R1]. This lemma serves to prove Proposition 3.8.

Proposition 3.8 will be used in the next section to prove Proposition 3.10, which leads to the important induction property given in Theorem 3.12.

For $b \in \mathbb{Z}$ satisfying $v_\ell(b) = 0$, define $\mathrm{ind}_\ell(b) \in \mathbb{Z}/(\ell-1)\mathbb{Z}$ by the congruence

$$b \equiv s^{\mathrm{ind}_\ell(b)} \mod \ell.$$

Lemma 3.7. *Let $\ell \equiv 1 \bmod mML$ and $t = (\ell-1)/mL$. Then for every a, $1 \leqslant a < mL$, $(a, mL) = 1$, the congruence*

$$\sum_{\substack{1 \leqslant b \leqslant m\ell L \\ b \equiv a \bmod mL \\ \ell \nmid b}} b\, ind_\ell(b) \equiv u + mL\, ind_\ell(-1/(at)!) \mod (\ell-1)/2$$

holds with u independent of a.

Proof. The notation $\langle \cdot \rangle$ will stand for the least nonnegative residue mod mL. Since $mL \mid \ell - 1$, $\{1 \leqslant b \leqslant m\ell L : b \equiv a \bmod mL,\ \ell \nmid b\} = \{c + \ell\langle a - c\rangle : 1 \leqslant c \leqslant \ell - 1\}$. Thus,

$$\sum_{\substack{1 \leqslant b \leqslant m\ell L \\ b \equiv a \bmod mL \\ \ell \nmid b}} b\,\mathrm{ind}_\ell(b) \equiv \mathrm{ind}_\ell\Big(\prod_b b^b\Big) \equiv \mathrm{ind}_\ell\Big(\prod_{1 \leqslant c \leqslant \ell-1} (c + \ell\langle a-c\rangle)^{c+\ell\langle a-c\rangle}\Big)$$

$$\equiv \mathrm{ind}_\ell\Big(\prod_{1 \leqslant c \leqslant \ell-1} c^{c+\langle a-c\rangle}\Big) \mod \ell - 1.$$

It is easy to see that

$$\langle a - c\rangle - (a - \langle c\rangle) = \begin{cases} 0 & \text{if } a \geqslant \langle c\rangle, \\ mL & \text{if } a < \langle c\rangle. \end{cases}$$

Hence, c running over the interval $1 \leqslant c \leqslant \ell - 1$,

$$\prod_c c^{c+\langle a-c\rangle} \equiv \prod_c c^{c-\langle c\rangle} \prod_c c^a \prod_{\langle c\rangle > a} c^{mL} \mod \ell.$$

The first product on the right side is independent of a. The second is $(\ell-1)!^a \equiv (-1)^a \bmod \ell$ by Wilson's Theorem, so its valuation is $\mathrm{ind}_\ell((-1)^a) = a(\ell-1)/2 \equiv 0 \bmod (\ell-1)/2$. In order to evaluate the third product, consider the sets

$$C = \{ c : 1 \leqslant c \leqslant \ell-1,\ \langle c \rangle > a \} = \{ j + kmL : a < j < mL,\ 0 \leqslant k < t \},$$
$$C' = \{ c' : at < c' \leqslant \ell - 1 - t \} = \{ jt - k : a < j < mL,\ 0 \leqslant k < t \}.$$

Multiplication by t gives a bijection from C to C' mod ℓ. Thus,

$$\prod_{\langle c \rangle > a} c = \prod_{c \in C} c \equiv t^{-t(mL-1-a)} \prod_{c' \in C'} c' = t^{-t(mL-1-a)} (\ell - 1 - t)!/(at)! \mod \ell.$$

Hence, up to a constant independent of a, $\mathrm{ind}_\ell\big(\prod_{\langle c \rangle > a} c^{mL}\big)$ is

$$\begin{aligned} mL\,\mathrm{ind}_\ell(t^{at}/(at)!) &\equiv a\,(\ell-1)\,\mathrm{ind}_\ell(t) + mL\,\mathrm{ind}_\ell(1/(at)!) \\ &\equiv mL\,\mathrm{ind}_\ell(-1/(at)!) \mod (\ell-1)/2. \end{aligned}$$

This concludes the proof. □

For $\ell \equiv 1 \bmod mML$, define elements in $(\mathbb{Z}/M\mathbb{Z})[\Delta(L)]$ by

$$\begin{aligned} s'(L,\ell) &\equiv \sum_{\substack{1 \leqslant a < mL \\ (a,mL)=1}} \mathrm{ind}_\ell(-1/(at)!)\, \tau_a^{-1} \mod M, \\ \theta'(L,\ell) &\equiv (\sigma_n - n_L)\, s'(L,\ell) \mod M, \end{aligned}$$

where $t = (\ell-1)/mL$.

Proposition 3.8. *Let $\ell \equiv 1 \bmod 2mML$. Then*

$$D_\ell\, \theta(\ell L)\, e_\rho \equiv N_\ell\, \theta'(L,\ell)\, e_\rho \mod M.$$

Proof. The element $D_\ell = \sum_{1 \leqslant j \leqslant \ell-2} j\, \sigma_s^j \in \mathbb{Z}[G_\ell]$, satisfies the congruence $D_\ell \equiv \sum_{b \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \mathrm{ind}_\ell(b)\, \sigma_b \mod \ell - 1$. Denoting the usual extension of σ_b to $F(\ell L)$ by $\tau_{b'}$, the congruence becomes

$$D_\ell \equiv \sum_{\substack{b' \in (\mathbb{Z}/m\ell L\mathbb{Z})^\times \\ b' \equiv 1 \bmod mL}} \mathrm{ind}_\ell(b')\, \tau_{b'} \mod \ell - 1.$$

In the rest of the proof, a and b will run over the set $\{c : 1 \leqslant c < m\ell L, (c, m\ell L) = 1\}$ with additional conditions indicated. Thus,

$$D_\ell\, s(\ell L) \equiv \sum_{b\equiv 1 \bmod mL} \operatorname{ind}_\ell(b)\, \tau_b \sum_a a\, \tau_a^{-1} \equiv \sum_a \sum_{b\equiv 1 \bmod mL} \langle ab\rangle \operatorname{ind}_\ell(b)\, \tau_a^{-1} \mod \ell{-}1,$$

where $\tau_a, \tau_b \in \Delta(\ell L)$, and $\langle\,\cdot\,\rangle$ stands for the least nonnegative residue mod $m\ell L$. The inner sum can be evaluated as follows.

$$\begin{aligned}\sum_{b\equiv 1 \bmod mL} \langle ab\rangle \operatorname{ind}_\ell(b) &\equiv \sum_{b\equiv 1 \bmod mL} b \operatorname{ind}_\ell(a^{-1}b)\\ &\equiv \operatorname{ind}_\ell(a^{-1}) \sum_{b\equiv 1 \bmod mL} b + \sum_{b\equiv 1 \bmod mL} b \operatorname{ind}_\ell(b) \mod \ell - 1,\end{aligned}$$

where a^{-1} denotes the inverse of a mod $m\ell L$. Furthermore, it is elementary to show that $\sum_{b\equiv 1 \bmod mL} b = m\ell L(\ell - 1)/2$. Hence

$$\sum_{b\equiv 1 \bmod mL} \langle ab\rangle \operatorname{ind}_\ell(b) \equiv \sum_{b\equiv 1 \bmod mL} b \operatorname{ind}_\ell(b) \mod (\ell - 1)/2.$$

Therefore

$$D_\ell\, s(\ell L) \equiv \sum_a \sum_{b\equiv 1 \bmod mL} b \operatorname{ind}_\ell(b)\, \tau_a^{-1} \mod (\ell - 1)/2.$$

Applying Lemma 3.7, it follows that

$$D_\ell\, s(\ell L) \equiv \sum_a \left(u + mL \operatorname{ind}_\ell(-1/(\langle a\rangle t)!\right) \tau_a^{-1} \mod (\ell - 1)/2,$$

where u is independent of a, $t = (\ell{-}1)/mL$, and $\langle\,\cdot\,\rangle$ stands for the least nonnegative residue mod mL. Then

$$D_\ell\, s(\ell L) \equiv u\, N_{\ell L} \sum_{\sigma\in\Delta} \sigma + mL\, N_\ell\, s'(L, \ell) \mod mML.$$

Since $1 \notin X_\rho$ (for ρ is odd), $e_\rho \sum_{\sigma\in\Delta} \sigma = \varphi(m)\, e_\rho\, e_1 = 0$. Thus, as $\theta(\ell L) = \frac{1}{m\ell L}(\sigma_n - n_{\ell L})\, s(\ell L)$, applying $\frac{1}{m\ell L}(\sigma_n - n_{\ell L})\, e_\rho$ yields

$$D_\ell\, \theta(\ell L)\, e_\rho \equiv \tfrac{1}{\ell} N_\ell\, (\sigma_n - n_{\ell L})\, s'(L, \ell)\, e_\rho \mod M.$$

Since $\ell \equiv 1 \bmod M$, $n_{\ell L} \equiv n_L \bmod M$, and $\theta'(L, \ell) \equiv (\sigma_n - n_L)\, s'(L, \ell) \bmod M$, it follows that

$$D_\ell\, \theta(\ell L)\, e_\rho \equiv N_\ell\, \theta'(L, \ell)\, e_\rho \mod M,$$

as required. □

3.4 The Induction Property

The induction property of the operators $\delta(L)$ is presented in Theorem 3.12, which is utilized in Proposition 3.15 as an essential element to obtain the main result.

The map $\varphi_{\mathcal{L}}$ is introduced in the following paragraphs and its basic properties are stated in Lemma 3.9. This lemma and the subsequent two propositions serve to prove Theorem 3.12.

Observe that if ℓ has degree 1 in $F(L)$, then the primitive root s mod ℓ is also a primitive root mod $\tau\mathcal{L}$ for every $\tau \in \Delta(L)$.

Suppose that ℓ has degree 1 in $F(L)$ and $\beta_0 \in F(L)^{\times}$ is a unit at $\mathcal{L}$, i.e., $v_{\mathcal{L}}(\beta_0) = 0$. Then $\beta_0 \equiv s^a \bmod \mathcal{L}$ for a unique $a \in \mathbb{Z}/(\ell-1)\mathbb{Z}$. Thus, one can define $\mathrm{ind}_{\mathcal{L}}(\beta_0) \in \mathbb{Z}/M\mathbb{Z}$ by the congruence $\mathrm{ind}_{\mathcal{L}}(\beta_0) \equiv a \bmod M$. If $\beta \in F(L)^{\times}$ satisfies that $v_{\mathcal{L}}(\beta) \equiv 0 \bmod M$, then there is $\beta_0 \in F(L)^{\times}$ such that $\beta \equiv \beta_0 \bmod (F(L)^{\times})^M$ and $v_{\mathcal{L}}(\beta_0) = 0$. Thus, one can define $\mathrm{ind}_{\mathcal{L}}(\beta) \in \mathbb{Z}/M\mathbb{Z}$ by the congruence

$$\mathrm{ind}_{\mathcal{L}}(\beta) \equiv \mathrm{ind}_{\mathcal{L}}(\beta_0) \bmod M.$$

Extend this definition to the class of β mod $(F(L)^{\times})^M$ in the obvious manner. It is clear that the map $\mathrm{ind}_{\mathcal{L}}$ has the property

$$\mathrm{ind}_{\mathcal{L}}(\beta\beta') \equiv \mathrm{ind}_{\mathcal{L}}(\beta) + \mathrm{ind}_{\mathcal{L}}(\beta') \quad \bmod M,$$

and that the definition of $\mathrm{ind}_{\mathcal{L}}$ includes that of ind_{λ} by taking $L = 1$.

Suppose that ℓ has degree 1 in $F(L)$ and $\beta \in F(L)^{\times}$ verifies that $v_{\tau\mathcal{L}}(\beta) \equiv 0 \bmod M$ for every $\tau \in \Delta(L)$. Then there is $\beta_0 \in F(L)^{\times}$ such that $\beta \equiv \beta_0 \bmod (F(L)^{\times})^M$ and $v_{\tau\mathcal{L}}(\beta_0) = 0$ for every $\tau \in \Delta(L)$. Thus, one can define $\varphi_{\mathcal{L}}(\beta) \in (\mathbb{Z}/M\mathbb{Z})[\Delta(L)]$ by

$$\varphi_{\mathcal{L}}(\beta) \equiv \sum_{\tau \in \Delta(L)} \mathrm{ind}_{\tau\mathcal{L}}(\beta)\,\tau \quad \bmod M.$$

The map $\varphi_{\mathcal{L}}$ will be said to be defined at β if the condition $v_{\tau\mathcal{L}}(\beta) \equiv 0 \bmod M$ for every $\tau \in \Delta(L)$ is satisfied. Extend this definition to the class of β mod $(F(L)^{\times})^M$

in the obvious manner. It is easily seen that the map $\varphi_{\mathcal{L}}$ has the property

$$\varphi_{\mathcal{L}}(\beta,\beta') \equiv \varphi_{\mathcal{L}}(\beta) + \varphi_{\mathcal{L}}(\beta') \mod M,$$

and that the definition of $\varphi_{\mathcal{L}}$ includes that of φ_{λ} by taking $L = 1$.

Lemma 3.9. *Let $\varphi_{\mathcal{L}}$ be defined at $\beta \in F(L)^{\times}$.*

(a) *For $\theta \in \mathbb{Z}[\Delta(L)]$, φ is defined at $\theta\beta$ and $\varphi_{\mathcal{L}}(\theta\beta) \equiv \theta\, \varphi_{\mathcal{L}}(\beta)$ mod M.*

(b) *Let $L' \mid L$ and let $\mathcal{L}'$ be the ideal of $F(L')$ below $\mathcal{L}$. If $\beta \in F(L')^{\times}$ and $\varphi_{\mathcal{L}'}$ is defined at β, then $\varphi_{\mathcal{L}}(\beta) \equiv N_{L/L'}\, \varphi_{\mathcal{L}'}(\beta)$ mod M.*

Proof. Since $\varphi_{\mathcal{L}}$ is defined at β, $v_{\tau\mathcal{L}}(\beta) \equiv 0$ mod M for every $\tau \in \Delta(L)$.

(a) Let $\theta = \sum_{\tau\in\Delta(L)} c_\tau\, \tau$ with $c_\tau \in \mathbb{Z}$. For $\tau' \in \Delta(L)$,

$$v_{\tau'\mathcal{L}}(\theta\beta) = v_{\tau'\mathcal{L}}(\prod_{\tau} \tau\beta^{c_\tau}) = \sum_{\tau} c_\tau\, v_{\tau'\mathcal{L}}(\tau\beta) = \sum_{\tau} c_\tau\, v_{\tau^{-1}\tau'\mathcal{L}}(\beta).$$

Then $v_{\tau'\mathcal{L}}(\theta\beta) \equiv 0$ mod M for every $\tau' \in \Delta(L)$, so $\varphi_{\mathcal{L}}$ is defined at $\theta\beta$. Thus, τ and τ' running over $\Delta(L)$,

$$\begin{aligned}
\varphi_{\mathcal{L}}(\theta\beta) &\equiv \varphi_{\mathcal{L}}\Big(\prod_{\tau} \tau\beta^{c_\tau}\Big) \equiv \sum_{\tau} c_\tau\, \varphi_{\mathcal{L}}(\tau\beta) \\
&\equiv \sum_{\tau} c_\tau \sum_{\tau'} \mathrm{ind}_{\tau'\mathcal{L}}(\tau\beta)\, \tau' \equiv \sum_{\tau} c_\tau \sum_{\tau'} \mathrm{ind}_{\tau^{-1}\tau'\mathcal{L}}(\beta)\, \tau' \\
&\equiv \sum_{\tau} c_\tau \sum_{\tau'} \mathrm{ind}_{\tau'\mathcal{L}}(\beta)\, \tau\tau' \equiv \sum_{\tau} c_\tau\, \tau \sum_{\tau'} \mathrm{ind}_{\tau'\mathcal{L}}(\beta)\, \tau' \\
&\equiv \theta\, \varphi_{\mathcal{L}}(\beta) \mod M.
\end{aligned}$$

(b) Considering the isomorphism $\Delta(L) \simeq G_{L/L'}\, \Delta(L')$, it follows that

$$\begin{aligned}
\varphi_{\mathcal{L}}(\beta) &\equiv \sum_{\tau\in\Delta(L)} \mathrm{ind}_{\tau\mathcal{L}}(\beta)\, \tau \equiv \sum_{\sigma'\in G_{L/L'}} \sum_{\sigma\in\Delta(L')} \mathrm{ind}_{\sigma'\sigma\mathcal{L}}(\beta)\, \sigma'\, \sigma \\
&\equiv \sum_{\sigma'} \sum_{\sigma} \mathrm{ind}_{\sigma\mathcal{L}'}(\beta).\sigma'\, \sigma \equiv \sum_{\sigma'} \sigma' \sum_{\sigma} \mathrm{ind}_{\sigma\mathcal{L}'}(\beta)\, \sigma \\
&\equiv N_{L/L'}\, \varphi_{\mathcal{L}'}(\beta) \mod M.
\end{aligned}$$

This completes the proof. □

The following proposition is due to Kolyvagin [K2].

Proposition 3.10. *Let $\ell \equiv 1 \bmod 2mML$. There exists $\pi \in F^\times$ satisfying the congruence*

$$\varphi_\lambda\big(\kappa(L,\lambda)\,/\,\delta(L)\,\pi\big) \equiv \delta(\ell L) \quad \text{mod } M.$$

Proof. It will be assumed throughout this proof that the integer a satisfies the conditions $1 \leqslant a < mL$ and $(a, mL) = 1$. Let $\tau_a \in \Delta(L)$ and extend τ_a to $F(\ell L)$ with the same notation. Let $\widehat{\mathcal{L}}$ be the prime ideal of $F(\ell L)$ above $\mathcal{L}$.

Choose a number $\Pi \in F(\ell L)^\times$ satisfying

$$\Pi \equiv \zeta_\ell - 1 \quad \text{mod } \widehat{\mathcal{L}}^2, \qquad \Pi \equiv 1 \quad \text{mod } \tau_a\widehat{\mathcal{L}} \quad \text{for every} \quad a \neq 1\,.$$

Setting $t = (\ell - 1)/mL$, the property of Gauss sums in Proposition 1.6 yields

$$S(\varepsilon^a, \zeta_\ell)\,/\,(\zeta_\ell - 1)^{at} \equiv -1/(at)! \quad \text{mod } \widehat{\mathcal{L}} \quad \text{for every} \quad a\,,$$

where $\varepsilon : (\mathbb{Z}/m\mathbb{Z})^\times \to \mu_{mL}$ is the character satisfying $\varepsilon(b) \equiv b^{-(\ell-1)/mL} \bmod \mathcal{L}$ for all b. Then

$$S(\varepsilon^a, \zeta_\ell)\,/\,\Pi^{at} \equiv -1/(at)! \quad \text{mod } \widehat{\mathcal{L}},$$

because $(\zeta_\ell - 1)/\Pi \equiv 1 \bmod \widehat{\mathcal{L}}$. Applying τ_a^{-1}, considering item (b) of Lemma 3.1, and using the congruences $\Pi \equiv 1 \bmod \tau_a\widehat{\mathcal{L}}$ for $a \neq 1$, it follows that

$$S(\mathcal{L}, \zeta_\ell)\,/\,s(L)\,\Pi^t \equiv \tau_a^{-1}\big(S(\varepsilon^a, \zeta_\ell)\,/\,\Pi^{at}\big) \equiv -1/(at)! \quad \text{mod } \tau_a^{-1}\widehat{\mathcal{L}} \quad \text{for every} \quad a\,.$$

Thus, since $\mathcal{L}$ is totally ramified in $F(\ell L)$, ℓ is unramified in $F(L)$, and $1 \leqslant at < \ell - 1$,

$$\begin{aligned} v_{\tau_a^{-1}\widehat{\mathcal{L}}}\big(S(\mathcal{L}, \zeta_\ell)\,/\,s(L)\,\Pi^t\big) &= v_{\tau_a^{-1}\widehat{\mathcal{L}}}(-1/(at)!) = (\ell - 1)\,v_{\tau_a^{-1}\mathcal{L}}(-1/(at)!) \\ &= (\ell - 1)\,v_\ell(-1/(at)!) = 0. \end{aligned}$$

This implies that $\varphi_{\widehat{\mathcal{L}}}$ is defined at $S(\mathcal{L}, \zeta_\ell)\,/\,s(L)\,\Pi^t$, as ℓ has degree 1 in $F(\ell L)$ and the primes $\tau_a^{-1}\widehat{\mathcal{L}}$ are all the conjugates of $\widehat{\mathcal{L}}$.

Considering the isomorphism $\Delta(\ell L) \simeq G_\ell\,\Delta(L)$, from the last congruence it follows that

$$\begin{aligned}\varphi_{\widehat{\mathcal{L}}}\big(S(\mathcal{L},\zeta_\ell)\,/\,s(L)\,\Pi^t\big) &\equiv N_\ell \sum_{\substack{1\leqslant a<mL\\(a,mL)=1}} \operatorname{ind}_{\tau_a^{-1}\widehat{\mathcal{L}}}(-1/(at)!)\,\tau_a^{-1}\\ &\equiv N_\ell \sum_a \operatorname{ind}_\ell(-1/(at)!)\,\tau_a^{-1} \equiv N_\ell\, s'(L,\ell) \mod M.\end{aligned}$$

By item (a) of Lemma 3.9, multiplying by $\sigma_n - n_L$ yields

$$\varphi_{\widehat{\mathcal{L}}}\big(\alpha(L,\mathcal{L})\,/\,\theta(L)\,\Pi^{\ell-1}\big) \equiv N_\ell\,\theta'(L,\ell) \mod M.$$

A number $\Pi_0 \in F(L)^\times$ satisfying $\Pi_0/\Pi^{\ell-1} \equiv 1 \bmod \tau_a\widehat{\mathcal{L}}$ for every a will be determined. Let $\Pi_1 \in F(L)^\times$ satisfy

$$\Pi_1 \equiv \ell \mod \mathcal{L}^2 \quad\text{and}\quad \Pi_1 \equiv 1 \mod \tau_a\mathcal{L} \quad\text{for every}\quad a \neq 1.$$

Then $v_{\mathcal{L}}(\Pi_1) = 1$, so $v_{\widehat{\mathcal{L}}}(\Pi_1) = \ell - 1$, $v_{\widehat{\mathcal{L}}}(\Pi_1/\Pi^{\ell-1}) = 0$ (for $v_{\widehat{\mathcal{L}}}(\Pi) = 1$), and $\Pi_1/\Pi^{\ell-1} \equiv c \not\equiv 0 \bmod \widehat{\mathcal{L}}$ with $c \in \mathbb{Z}$. In addition for every $a \neq 1$, $\Pi_1 \equiv 1 \bmod \tau_a\widehat{\mathcal{L}}$, so $\Pi_1/\Pi^{\ell-1} \equiv 1 \bmod \tau_a\widehat{\mathcal{L}}$. Choosing $\Pi_2 \in F(L)^\times$ such that $\Pi_2 \equiv c^{-1} \bmod \mathcal{L}$ and $\Pi_2 \equiv 1 \bmod \tau_a\mathcal{L}$ for every $a \neq 1$, the number $\Pi_0 = \Pi_1\Pi_2 \in F(L)^\times$ satisfies the desired congruences. Therefore,

$$\varphi_{\widehat{\mathcal{L}}}\big(\alpha(L,\mathcal{L})\,/\,\theta(L)\,\Pi_0\big) \equiv N_\ell\,\theta'(L,\ell) \mod M.$$

Since for every $\tau \in \Delta(\ell L)$, $v_{\tau\widehat{\mathcal{L}}}\big(S(\mathcal{L},\zeta_\ell)\,/\,s(L)\,\Pi^t\big) = 0$ and $v_{\tau\widehat{\mathcal{L}}}\big(\Pi_0/\Pi^{\ell-1}\big) = 0$, it follows that $v_{\tau\widehat{\mathcal{L}}}\big(\alpha(L,\mathcal{L})\,/\,\theta(L)\,\Pi_0\big) = 0$. Then $v_{\tau\mathcal{L}}\big(\alpha(L,\mathcal{L})\,/\,\theta(L)\,\Pi_0\big) = 0$ for every τ, as $\alpha(L,\mathcal{L})\,/\,\theta(L)\,\Pi_0 \in F(L)^\times$, so $\varphi_{\mathcal{L}}$ is defined at this number. Using item (b) of Lemma 3.9, there results the congruence

$$N_\ell\,\varphi_{\mathcal{L}}\big(\alpha(L,\mathcal{L})\,/\,\theta(L)\,\Pi_0\big) \equiv N_\ell\,\theta'(L,\ell) \mod M.$$

By item (a) of Lemma 3.9, congruence $(*)$ of Section 3.1, congruence $(**)$ of Section 3.2, and Proposition 3.8, multiplying by $D_L\,e'_\rho$ yields

$$N_\ell\,\varphi_{\mathcal{L}}\big(\kappa(L,\lambda)\,/\,N_L\,\delta(L)\,\Pi_0\big) \equiv D_{\ell L}\,\theta(\ell L)\,e'_\rho \equiv N_{\ell L}\,\delta(\ell L) \mod M.$$

Let $\pi = N_L \mathit{\Pi}_0 \in F^\times$. Since λ is unramified in $F(L)$, φ_λ is defined at $\kappa(L,\lambda) \,/\, \delta(L)\, \pi \in F(L)^\times$. Then item (b) of Lemma 3.9 implies that

$$N_{\ell L}\, \varphi_\lambda\big(\kappa(L,\lambda) \,/\, \delta(L)\, \pi\big) \equiv N_{\ell L}\, \delta(\ell L) \mod M.$$

Finally, on cancelling $N_{\ell L}$ there results the congruence in $\mathbb{Z}[\Delta]$

$$\varphi_\lambda\big(\kappa(L,\lambda) \,/\, \delta(L)\, \pi\big) \equiv \delta(\ell L) \mod M,$$

as required. □

Proposition 3.11. *Let $\ell \equiv 1 \bmod 2mML$. Let $\ell' \neq \ell$ be a rational prime satisfying the same congruence $\ell' \equiv 1 \bmod 2mML$. Let λ' be a prime of F above ℓ', and $\mathcal{L}'$ be a prime of $F(L)$ above λ'. Assume that the projections of $\mathcal{L}$ and $\mathcal{L}'$ into $e_\rho\, A(L)$ are equal. Then*

$$\kappa(L,\lambda') \,/\, \kappa(L,\lambda) \equiv \delta(L)\, \beta \mod (F^\times)^M$$

for some $\beta \in F^\times$.

Proof. The equality of the projections of $\mathcal{L}$ and $\mathcal{L}'$ in $e_\rho\, A(L)$ can be expressed as $e_\rho[\mathcal{L}]_p = e_\rho[\mathcal{L}']_p$, where the ideal class is denoted by $[\,\cdot\,]$, and its p-part, by $[\,\cdot\,]_p$. Let $\hat{e}_\rho$ denote a fixed element in $\mathbb{Z}[\Delta]$ satisfying the congruence $\hat{e}_\rho \equiv e_\rho \bmod Mh_L$ with $h_L = \big|A(L)\big|$. Thus $\big[\hat{e}_\rho(\mathcal{L}/\mathcal{L}')\big]_p = 1$, so $\big[\hat{e}_\rho(\mathcal{L}/\mathcal{L}')\big]$ is an Mh_Lth power in the class group of $F(L)$. Then there is $\beta_L \in F(L)^\times$ such that $(\beta_L)\, \hat{e}_\rho(\mathcal{L}/\mathcal{L}')$ is an Mh_Lth power in the ideal group of $F(L)$, and so is $\hat{e}_\rho\big((\beta_L)\mathcal{L}/\mathcal{L}'\big)$. Applying $\theta(L)$ and using item (b) of Proposition 3.2, it follows that the principal ideal $\big(\hat{e}_\rho\big(\theta(L)\, \beta_L\, \alpha(L,\mathcal{L}) \,/\, \alpha(L,\mathcal{L}')\big)\big)$ is the Mh_Lth power of an ideal of $F(L)$, and it is then the Mth power of a principal ideal of $F(L)$. Hence

$$\hat{e}_\rho\big(\theta(L)\, \beta_L\, \alpha(L,\mathcal{L}) \,/\, \alpha(L,\mathcal{L}')\big) \equiv \eta \mod (F(L)^\times)^M$$

for some unit η in $F(L)$.

It will be shown that $e'_\rho \eta \in (F(L)^\times)^M$. Write $e'_\rho = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} c_a \, \sigma_a^{-1}$ with $c_a \in \mathbb{Z}$. Then $c_a \equiv \rho(a)/\varphi(m) \bmod M$, so $c_{-a} \equiv -c_a \bmod M$ as ρ is odd. Thus $e'_\rho \eta = \left(\sum_a c_a \, \sigma_a^{-1}\right) \eta \equiv \left(\sum'_a c_a \, \sigma_a^{-1}\right) (\eta/\bar{\eta}) \bmod (F(L)^\times)^M$, where $\sum_a$ and $\sum'_a$ denote summation as a runs over $(\mathbb{Z}/m\mathbb{Z})^\times$ and over $(\mathbb{Z}/m\mathbb{Z})^\times/\langle -1 \rangle$ respectively. It will then be enough to show that $e'_\rho(\eta/\bar{\eta}) \in (F(L)^\times)^M$. Since all the conjugates of $\eta/\bar{\eta}$ have absolute value 1, $\eta/\bar{\eta}$ is a root of unity. Thus $\eta/\bar{\eta} = \pm\zeta_{mL} \equiv \zeta_{p^r}^b \bmod (F(L)^\times)^M$ with $p^r \parallel m$, $b \in \mathbb{Z}$. Hence, by Lemma 3.4, $e'_\rho(\eta/\bar{\eta}) \equiv e'_\rho \zeta_{p^r}^b \equiv 1 \bmod (F(L)^\times)^M$. This means that $e'_\rho(\eta/\bar{\eta}) \in (F(L)^\times)^M$, which shows the claim.

Therefore,

$$e'_\rho\big(\theta(L) \, \beta_L \, \alpha(L, \mathcal{L}) \, / \, \alpha(L, \mathcal{L}')\big) \in (F(L)^\times)^M.$$

Thus, by definition of $\kappa(L, \lambda)$ and $\delta(L)$,

$$\begin{aligned} \kappa(L, \lambda') \, / \, \kappa(L, \lambda) &\equiv D_L \, e'_\rho\big(\alpha(L, \mathcal{L}') \, / \, \alpha(L, \mathcal{L})\big) \\ &\equiv D_L \, \theta(L) \, e'_\rho \, \beta_L \equiv N_L \, \delta(L) \, \beta_L \mod (F(L)^\times)^M. \end{aligned}$$

Setting $\beta = N_L \, \beta_L \in F^\times$, by Lemma 3.5 there results that

$$\kappa(L, \lambda') \, / \, \kappa(L, \lambda) \equiv \delta(L) \, \beta \mod (F^\times)^M,$$

as required. □

Theorem 3.12. *Let $\ell \equiv 1 \bmod 2mML$. Let $\ell' \neq \ell$ be a rational prime satisfying the same congruence $\ell' \equiv 1 \bmod 2mML$. Let λ' be a prime of F above ℓ', and $\mathcal{L}'$ be a prime of $F(L)$ above λ'. Assume that the projections of $\mathcal{L}$ and $\mathcal{L}'$ into $e_\rho \, A(L)$ are equal. Then*

$$\varphi_\lambda(\kappa(L, \lambda')) \equiv \delta(\ell L) \mod \delta(L)(\mathbb{Z}/M\mathbb{Z})[\Delta].$$

Proof. By Proposition 3.10,

$$\varphi_\lambda\big(\kappa(L, \lambda) \, / \, \delta(L) \, \pi\big) \equiv \delta(\ell L) \mod M$$

for some $\pi \in F^\times$. Since $\lambda \neq \sigma\lambda'$ for every $\sigma \in \Delta$ and $\lambda \nmid L$ (as $\ell \neq \ell'$ and $\ell \nmid L$), the map φ_λ is defined at $\kappa(L, \lambda')$ by Proposition 3.6, so it is defined at $\delta(L)\,\pi\,\kappa(L,\lambda') \,/\, \kappa(L,\lambda)$. Thus, by Proposition 3.11 and Lemma 3.9,

$$\varphi_\lambda\big(\delta(L)\,\pi\,\kappa(L,\lambda') \,/\, \kappa(L,\lambda)\big) \equiv \varphi_\lambda\big(\delta(L)\,\pi \cdot \delta(L)\,\beta\big) \equiv \delta(L)\,\varphi_\lambda(\beta\pi) \mod M,$$

where $\beta \in F^\times$. Hence

$$\begin{aligned}\varphi_\lambda(\kappa(L,\lambda')) &\equiv \varphi_\lambda\big(\big(\kappa(L,\lambda) \,/\, \delta(L)\,\pi\big) \cdot \big(\delta(L)\,\pi\,\kappa(L,\lambda') \,/\, \kappa(L,\lambda)\big)\big)\\ &\equiv \varphi_\lambda\big(\kappa(L,\lambda) \,/\, \delta(L)\,\pi\big) + \varphi_\lambda\big(\delta(L)\,\pi\,\kappa(L,\lambda') \,/\, \kappa(L,\lambda)\big)\\ &\equiv \delta(\ell L) + \delta(L)\,\varphi_\lambda(\beta\pi) \mod M,\end{aligned}$$

so

$$\varphi_\lambda(\kappa(L,\lambda')) \equiv \delta(\ell L) \mod \delta(L)(\mathbb{Z}/M\mathbb{Z})[\Delta],$$

as required. □

3.5 Second Application of the Chebotarev Density Theorem

This section is dedicated to Theorem 3.14, which is an extension of Theorem 3.1 in [R1] and includes an application of the Chebotarev density theorem (Theorem 1.12). Theorem 3.14, as well as Theorem 3.12, will be crucial in the proof of Proposition 3.15 to obtain the main result. Lemma 3.13, stated in order to abbreviate the proof of Theorem 3.14, reveals the purpose of condition **C**, which is defined after the lemma.

In a similar manner as in Chapter 2 before Proposition 2.10, it can be shown that $|X_\rho| = [\mathbb{Q}_p(\operatorname{Im}\chi) : \mathbb{Q}_p]$ for every character $\chi \in X_\rho$, where $\operatorname{Im}\chi$ is the image of χ. Moreover, $\mathbb{Q}_p(\operatorname{Im}\chi_1) = \mathbb{Q}_p(\operatorname{Im}\chi_2)$ for any characters $\chi_1, \chi_2 \in X_\rho$. Denote this field by $\mathbb{Q}_p(X_\rho)$. Thus $|X_\rho| = [\mathbb{Q}_p(X_\rho) : \mathbb{Q}_p]$.

Lemma 3.13. *If m is not a power of a prime congruent to* $5 \bmod 8$ *or if* $(\varphi(m), p-1) > 2$, *then there exists a character* $\phi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ *such that* $X_\rho \neq X_{\phi\rho^{-1}}$. *Conversely, if m is a power of a prime congruent to* $5 \bmod 8$ *and* $(\varphi(m), p-1) = 2$, *then there exists an irreducible higher dimensional odd character* ρ_0 *of* $(\mathbb{Z}/m\mathbb{Z})^\times$ *into* $\mathbb{Z}_p$ *such that* $X_{\rho_0} = X_{\phi\rho_0^{-1}}$ *for every character* $\phi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}_p^\times$.

Proof. In order to prove the contrapositive of the first part of the lemma, assume that $X_\rho = X_{\phi\rho^{-1}}$ for every character $\phi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}_p^\times$.

For a character ϕ as above (with values in $\mathbb{Z}_p^\times$) and a fixed character $\chi_0 \in X_\rho$, $\phi\chi_0^{-1} \in X_{\phi\rho^{-1}} = X_\rho$, so $\phi\chi_0^{-1} = \tau_\phi \chi_0$ for some $\tau_\phi \in \mathrm{Gal}(\mathbb{Q}_p(X_\rho)/\mathbb{Q}_p)$. Applying the automorphisms in $\mathrm{Gal}(\mathbb{Q}_p(X_\rho)/\mathbb{Q}_p)$ to the last equality, it follows that for every $\chi \in X_\rho$,

$$\phi\chi^{-1} = \tau_\phi \chi .$$

The equality above implies that $\tau_\phi^2 = 1$, because $\tau_\phi^2\chi = \phi(\tau_\phi\chi)^{-1} = \phi(\phi\chi^{-1})^{-1} = \chi$ for every $\chi \in X_\rho$. In addition, it is easily seen that ϕ is even. Thus there are only two possible values for τ_ϕ, as $\mathrm{Gal}(\mathbb{Q}_p(X_\rho)/\mathbb{Q}_p)$ is cyclic. Since it is clear that there is a character $\phi \neq 1$ and the map $\phi \to \tau_\phi$ is injective, it follows that there are exactly two distinct characters ϕ.

Let $m = \prod_{1 \leqslant i \leqslant k} q_i^{a_i}$ be the prime factorization of m. If $4 \mid m$, then $\langle -1 \rangle$ is a direct factor of $(\mathbb{Z}/m\mathbb{Z})^\times$, so there is an odd character ϕ defined as -1 at -1 and as 1 at the other direct factors, which is absurd. The same result is obtained if $q_j \equiv 3 \bmod 4$ for some j, $1 \leqslant j \leqslant k$. In this case, $(\mathbb{Z}/m\mathbb{Z})^\times$ has the direct factor $(\mathbb{Z}/q_j^{a_j}\mathbb{Z})^\times \simeq \langle g_j \rangle$, where g_j is a primitive root mod $q_j^{a_j}$, so the character ϕ defined as -1 at g_j and as 1 at the other direct factors is odd, since $\phi(-1) = \phi\left(g_j^{q_j^{a_j-1}(q_j-1)/2}\right) = (-1)^{(q_j-1)/2} = -1$. Hence, every prime q_i has the form $q_i \equiv 1 \bmod 4$.

If $k \geqslant 2$, then $(\mathbb{Z}/m\mathbb{Z})^\times$ has at least two non-trivial direct factors, so at least four characters ϕ with values 1 and -1 can be defined, which is absurd. Thus m

has the form $m = q^a$ for some prime $q \equiv 1 \bmod 4$.

If $(\varphi(m), p-1) > 2$, then, setting $\zeta = \zeta_{(\varphi(m),p-1)} \in \mathbb{Z}_p^\times$ and g being a primitive root mod q^a, more than two characters ϕ can be defined by $\phi(g) = \zeta^j$ for $0 \leqslant j < (\varphi(m), p-1)$, which is absurd. Thus $(\varphi(m), p-1) = 2$.

Suppose that $\tau_\phi = 1$ for $\phi = 1$. It then follows from the equation $\phi\chi^{-1} = \tau_\phi\chi$ that $\chi^{-1} = \chi$, i.e., $\chi^2 = 1$, for every $\chi \in X_\rho$. Thus $\operatorname{Im}\chi \subseteq \mathbb{Z}_p^\times$, so the odd character $\phi = \chi$ is defined, which is absurd. Hence $\tau_\phi \neq \mathrm{id}$ for $\phi = 1$, so for $\phi \neq 1$, $\tau_\phi = 1$ and $\phi = \chi^2$ for any $\chi \in X_\rho$.

Let g be a generator of $(\mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}/q^a\mathbb{Z})^\times$. Suppose that $q \equiv 1 \bmod 8$ and consider the character $\phi \neq 1$. On the one hand $\phi(g) = -1$ as $(\varphi(m), p-1) = 2$, so $\phi(g^{(q-1)/4}) = (-1)^{(q-1)/4} = 1$. On the other hand $\phi = \chi^2$ for any $\chi \in X_\rho$, so $\phi(g^{(q-1)/4}) = \chi(g^{(q-1)/2}) = \chi(-1) = -1$, which is absurd. Hence $q \equiv 5 \bmod 8$.

It has been shown that $m = q^a$ for a prime $q \equiv 5 \bmod 8$, and $(\varphi(m), p-1) = 2$. This proves the first part of the lemma.

Conversely, assume that $m = q^a$ for a prime $q \equiv 5 \bmod 8$, and $(\varphi(m), p-1) = 2$. Define a character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}_p[\zeta_{\varphi(m)}]^\times$ by $\chi(g) = \zeta_4$, where g is a generator of $(\mathbb{Z}/m\mathbb{Z})^\times$. This character is well defined as $4 \mid \varphi(m) = q^{a-1}(q-1)$, and it is odd because $\chi(-1) = \chi(g^{\varphi(m)/2}) = \zeta_4^{q^{a-1}(q-1)/2} = (\pm\zeta_4)^2 = -1$. Since $\mathrm{Gal}(\mathbb{Q}_p(\zeta_4)/\mathbb{Q}_p) = \{1, \tau\}$ with $\tau(\zeta_4) = \zeta_4^{-1}$, the other character in the orbit of χ is given by $\tau\chi(g) = \tau(\zeta_4) = \zeta_4^{-1} = \chi^{-1}(g)$, so it is χ^{-1}. Thus the higher dimensional character ρ_0 with orbit $X_{\rho_0} = \{\chi, \chi^{-1}\}$ is odd and irreducible.

Since $(\varphi(m), p-1) = 2$, the only possible values for a character ϕ are 1 and -1. Then 1 and the character ϕ_* defined by $\phi_*(g) = -1$ are the only characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathbb{Z}_p^\times$. In addition, $\chi^2(g) = \zeta_4^2 = -1 = \phi_*(g)$, so $\phi_* = \chi^2$. Thus the characters 1 and ϕ_* satisfy the required equalities

$$X_{\rho_0^{-1}} = \{\chi^{-1}, \chi\} = X_{\rho_0}, \quad X_{\phi_*\rho_0^{-1}} = \{\phi_*\chi^{-1}, \phi_*\chi\} = \{\chi, \chi^3\} = \{\chi, \chi^{-1}\} = X_{\rho_0}.$$

This concludes the proof. □

If m is not a power of a prime congruent to $5 \bmod 8$ or if $(\varphi(m), p-1) > 2$, m and p will be said to satisfy condition **C**.

Theorem 3.14. *Assume that m and p satisfy condition* **C**. *Let $\mathfrak{C} \in e_\rho A(L)$, $k \in \mathbb{Z}$, $k \geqslant 1$, and $\beta \in e_\rho(F^\times/(F^\times)^M)$. Let t be the largest integer such that $\beta \in (F^\times)^{p^t}/(F^\times)^M$ and suppose that $p^t < M$. Then there exist infinitely many primes λ of F such that*

1. *there is a prime $\mathcal{L}$ of $F(L)$ above λ whose projection into $e_\rho A(L)$ equals $\mathfrak{C}$;*
2. *the rational prime ℓ below λ has the form $\ell \equiv 1 \bmod kmML$;*
3. *$v_\lambda(\beta) \equiv 0 \bmod M$ and $p^t \parallel \operatorname{ind}_\lambda(\beta)$.*

Proof. Let d be the order of β in $F^\times/(F^\times)^M$. It will be shown that $d = p^{-t}M$. From the condition $\beta \in (F^\times)^{p^t}/(F^\times)^M$, it follows that $\beta^{p^{-t}M} \in (F^\times)^M$, so $d \mid p^{-t}M$. Since $\beta^d \in (F^\times)^M$, $\beta = \gamma^{M/d}\zeta_d^b$ with $\gamma \in F^\times$, $b \in \mathbb{Z}$. Applying e'_ρ and using Lemma 3.4 yields $\beta \in e'_\rho\gamma^{M/d}(F^\times)^M$, whence $M/d \leqslant p^t$ by the maximality of t. Since $d \mid p^{-t}M$, there results that $d = p^{-t}M$, as claimed.

Let H be the subfield of the Hilbert class field of $F(L)$ such that $\mathrm{Gal}(H/F(L))$ is isomorphic to $e_\rho A(L)$ by class field theory, and denote $F' = F(\zeta_{kML})$. Consider the extension $F'(\beta^{1/M})/F'$ and let $G = \mathrm{Gal}(F'(\beta^{1/M})/F')$. By Kummer theory and Lemma 3.5, $G \simeq \langle\beta\rangle$, where $\langle\beta\rangle$ denotes the subgroup of $F^\times/(F^\times)^M$ generated by β. Thus G is a cyclic group of order $p^{-t}M$. In addition, a nondegenerate pairing $G \times \langle\beta\rangle \to \mu_M$ is given by $(\tau, \beta) \mapsto \langle\tau, \beta\rangle = \tau\alpha/\alpha$, where α is an Mth root of β.

If $p \parallel m$, then the Teichmüller character ω verifies $X_\rho \neq X_{\omega\rho^{-1}}$, because ρ is odd while $\omega\rho^{-1}$ is even. In this case, let $\phi = \omega$. If $p \nmid m$, then by Lemma 3.13 there exists a character $\phi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ such that $X_\rho \neq X_{\phi\rho^{-1}}$. For $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, extend $\sigma_a \in \Delta$ to F' so that $\sigma_a\zeta_M = \zeta_M^{\phi(a)}$ and $\sigma_a\zeta_L = \zeta_L$. This extension coincides on $F(L)$ with the standard extension, defined after Proposition 3.1, and will be used only to obtain the equality $H \cap F'(\beta^{1/M}) = F(L)$ in the next paragraphs. Extend σ_a further to $HF' \cap F'(\beta^{1/M})$, and then to HF' and $F'(\beta^{1/M})$ separately. Thus Δ acts on $\mathrm{Gal}(HF'/F')$ and G by the same formula $\sigma_a \cdot \tau = \sigma_a\, \tau\, \sigma_a^{-1}$. Adopting the notation $(\sigma_a + \sigma_b) \cdot \tau = (\sigma_a \cdot \tau)\,(\sigma_b \cdot \tau)$, since $\mathrm{Gal}(HF'/F') \hookrightarrow \mathrm{Gal}(H/F(L)) \simeq e_\rho A(L)$, it follows that $e_\rho \cdot \tau = \tau$ for every $\tau \in \mathrm{Gal}(HF'/F')$.

The pairing $G \times \langle\beta\rangle \to \mu_M$ is easily shown to have the property $\sigma_a\langle\tau,\beta\rangle = \langle\sigma_a \cdot \tau, \sigma_a\,\beta\rangle$. (Recall that $\beta \in F^\times/(F^\times)^M$, so the notation $\langle\tau,\beta^c\rangle$ is well defined for $\tau \in G$, $c \in \mathbb{Z}_p$.) Then, a running over $(\mathbb{Z}/m\mathbb{Z})^\times$,

$$\begin{aligned}\big\langle\big(\textstyle\sum_a \phi(a)\rho^{-1}(a)\,\sigma_a^{-1}\big)\cdot\tau,\beta\big\rangle &= \langle\textstyle\prod_a \sigma_a^{-1}\cdot\tau^{\phi(a)\rho^{-1}(a)},\beta\rangle = \prod_a \big\langle\sigma_a^{-1}\cdot\tau,\beta^{\phi(a)\rho^{-1}(a)}\big\rangle \\ &= \prod_a \sigma_a^{-1}\big\langle\tau,\sigma_a\beta^{\phi(a)\rho^{-1}(a)}\big\rangle = \prod_a \big\langle\tau,\sigma_a\beta^{\phi(a)\rho^{-1}(a)}\big\rangle^{\phi^{-1}(a)} \\ &= \prod_a \big\langle\tau,\sigma_a\beta^{\rho^{-1}(a)}\big\rangle = \big\langle\tau,\textstyle\prod_a \sigma_a\beta^{\rho^{-1}(a)}\big\rangle \\ &= \big\langle\tau,\big(\textstyle\sum_a \rho^{-1}(a)\,\sigma_a\big)\,\beta\big\rangle = \big\langle\tau,\big(\textstyle\sum_a \rho(a)\,\sigma_a^{-1}\big)\,\beta\big\rangle,\end{aligned}$$

whence $\langle e_{\phi\rho^{-1}}\cdot\tau,\beta\rangle = \langle\tau,e_\rho\beta\rangle$. Thus $\langle e_{\phi\rho^{-1}}\cdot\tau,\beta\rangle = \langle\tau,\beta\rangle$ as $\beta \in e_\rho(F^\times/(F^\times)^M)$, which implies that $e_{\phi\rho^{-1}}\cdot\tau = \tau$ for every $\tau \in G$.

Since the extension of $\sigma_a \in \Delta$ to $F'(\beta^{1/M})$ satisfies the equality $\sigma_a\,\sigma_b\,\zeta_M = \sigma_{ab}\,\zeta_M$ (as ϕ is a homomorphism), $\sigma_{ab}^{-1}\,\sigma_a\,\sigma_b$ commutes with every $\tau \in G$, so $\sigma_a\,\sigma_b\cdot\tau = \sigma_{ab}\cdot\tau$. This equality then holds for every $\tau \in \mathrm{Gal}(HF' \cap F'(\beta^{1/M})/F')$. Hence, for such τ, $e_\rho\, e_{\phi\rho^{-1}}\cdot\tau = 1$, as $X_\rho \neq X_{\phi\rho^{-1}}$. Thus the equalities $e_\rho\cdot\tau = \tau$ and $e_{\phi\rho^{-1}}\cdot\tau = \tau$ for $\tau \in \mathrm{Gal}(HF' \cap F'(\beta^{1/M})/F')$ imply that

$$\tau = e_\rho\cdot\tau = e_\rho\, e_{\phi\rho^{-1}}\cdot\tau = 1,$$

so $HF' \cap F'(\beta^{1/M}) = F'$. On the other hand, since $\mathrm{Gal}(F'/F(L))$ is generated by inertia groups, there is no nontrivial unramified extension of $F(L)$ in F', so $H \cap F' = F(L)$. Hence,

$$H \cap F'(\beta^{1/M}) = H \cap HF' \cap F'(\beta^{1/M}) = H \cap F' = F(L).$$

Choose $\tilde{\tau} \in \mathrm{Gal}(HF'(\beta^{1/M})/F(L))$ that restricts to the Artin symbol $[\mathfrak{C}, H/F(L)]$ on H and to a generator of G on $F'(\beta^{1/M})$. By the Chebotarev density theorem (Theorem 1.12), there are infinitely many primes $\mathcal{L}$ of $F(L)$ of absolute degree 1, unramified in $HF'(\beta^{1/M})/\mathbb{Q}$, whose Frobenius conjugacy class in $\mathrm{Gal}(HF'(\beta^{1/M})/F(L))$ contains $\tilde{\tau}$. Then the Frobenius of such a prime $\mathcal{L}$ in $H/F(L)$ equals $[\mathfrak{C}, H/F(L)]$, which means that $\mathcal{L} \in \mathfrak{C}$, so the projection of $\mathcal{L}$ into $e_\rho A(L)$ equals $\mathfrak{C}$. This shows item (1).

Let $\widetilde{\mathcal{L}}$ be a prime of $HF'(\beta^{1/M})$ above $\mathcal{L}$ whose Frobenius in $HF'(\beta^{1/M})/F(L)$ equals $\tilde{\tau}$. Denote the prime of $F'(\beta^{1/M})$ below $\widetilde{\mathcal{L}}$ by $\mathcal{L}''$, and the prime of F' below $\mathcal{L}''$ by $\mathcal{L}'$. Since the Frobenius of $\mathcal{L}''$ in $F'(\beta^{1/M})/F(L)$ is the restriction of $\tilde{\tau}$ to $F'(\beta^{1/M})$, it generates G, so it restricts to the identity on F' and it is also the Frobenius of $\mathcal{L}''$ in $F'(\beta^{1/M})/F'$; in addition, the Frobenius of $\mathcal{L}'$ in $F'/F(L)$ is the identity. Denoting the prime of F below $\mathcal{L}$ by λ, and the rational prime below λ by ℓ, it follows that the Frobenius of ℓ in $F'/\mathbb{Q}$ is the identity, as $\mathcal{L}$ has absolute degree 1. Hence, ℓ splits completely in $F' = \mathbb{Q}(\zeta_{kmML})$, which means that $\ell \equiv 1 \bmod kmML$. This shows item (2).

Since $\mathcal{L}''$ is unramified in $F'(\beta^{1/M})/\mathbb{Q}$, λ is unramified in $F'(\beta^{1/M})$, so $v_\lambda(\beta) \equiv 0 \bmod M$. In view that the Frobenius of $\mathcal{L}''$ in $F'(\beta^{1/M})/F'$ generates G and this group is cyclic of order $p^{-t}M$, the extension

$$(O_{F'(\beta^{1/M})}/\mathcal{L}'')/(O_{F'}/\mathcal{L}') = (O_{F'}/\mathcal{L}')(\beta^{1/M})/(O_{F'}/\mathcal{L}')$$

is cyclic of degree $p^{-t}M$. In addition, $O_{F'}/\mathcal{L}' \simeq O_F/\lambda$ because ℓ splits completely in F', and it is clear that $\mathrm{char}(O_{F'}/\mathcal{L}') = \ell \nmid p$. Then, by Kummer theory, β has order $p^{-t}M$ in $(O_F/\lambda)^\times/((O_F/\lambda)^\times)^M$. Hence $\mathrm{ind}_\lambda(\beta) \equiv p^t u \bmod M$ with $p \nmid u$. As $p^t < M$, it follows that $p^t \parallel \mathrm{ind}_\lambda(\beta)$, which shows item (3). This concludes the proof. $\square$

3.6 The Main Result

Propositions 3.15 to 3.19 in this section are aimed to obtain Theorem 3.20, which presents the main result of this chapter. Initially, the integers $r(L)$ and the constant M are defined. In addition, the generalized Bernoulli numbers $B_{1,\chi}$ are defined before Proposition 3.19 and the numbers $B_{1,\rho^{-1}}$ are introduced before Theorem 3.20.

Define $r(L)$ as the integer satisfying $p^{r(L)} \parallel \delta(L)$ and let $M = p^{r(1)+1} \cdot |e_\rho A|$.

Proposition 3.15. *Assume that m and p satisfy condition* **C** *and that $r(L) \leqslant r(1)$. Let B be the subgroup of $e_\rho A$ generated by the projections of the primes of F dividing L. If $\mathfrak{C} \in e_\rho A - B$, then there exists a prime λ of F whose projection into $e_\rho A$ equals $\mathfrak{C}$ and that lies above a rational prime $\ell \equiv 1 \bmod mML$ such that $r(\ell L) < r(L)$ and $p^{r(L)-r(\ell L)}$ annihilates $\mathfrak{C}$ in $e_\rho A/B$.*

Proof. By Theorem 3.14, there exists a prime λ' of F whose projection into $e_\rho A$ equals $\mathfrak{C}$ and that lies above a rational prime $\ell' \equiv 1 \bmod 2mML$.

Let t be the largest integer such that $\kappa(L, \lambda') \in (F^\times)^{p^t}/(F^\times)^M$. By Proposition 3.6,

$$(\kappa(L, \lambda')) = {\lambda'}^{\delta(L)} \cdot (\text{primes dividing } L) \cdot \mathcal{B}^M,$$

where $\mathcal{B}$ is an ideal of F. Since the left side is a p^tth power, the p^tth root of the equality can be taken. Then $p^t \mid \delta(L)$, so $t \leqslant r(L) \leqslant r(1)$ (as $p^{r(L)} \parallel \delta(L)$) and $p^{-t}M$ annihilates $e_\rho A$. Projecting the primes in the equality into $e_\rho A$, it follows that $\mathfrak{C}^{p^{-t}\delta(L)} \in B$.

By Proposition 1.4, there exists $\delta' \in (\mathbb{Z}/M\mathbb{Z})[\Delta]$ such that $p^{-r(L)}\delta(L)\,\delta' e_\rho \equiv e_\rho \bmod M$. Thus,

$$\mathfrak{C}^{p^{r(L)-t}} = \mathfrak{C}^{p^{r(L)-t} e_\rho} = \mathfrak{C}^{p^{-t}\delta(L)\,\delta' e_\rho} \in B,$$

that is, $p^{r(L)-t}$ annihilates $\mathfrak{C}$ in $e_\rho A/B$. Since $\mathfrak{C} \notin B$, it follows that $t < r(L)$.

Let $\mathcal{L}'$ be a prime of $F(L)$ above λ'. Express the projection of $\mathcal{L}'$ into $e_\rho A(L)$ by $e_\rho[\mathcal{L}']_p$, where the p-part of the ideal class is denoted by $[\cdot]_p$. By Theorem 3.14

with $\mathfrak{C} = e_\rho[\mathcal{L}']_p$, $k = 2$, $\beta = \kappa(L, \lambda')$, having that $p^t < M$ as $t \leqslant r(1)$, there exists a prime λ of F such that a prime $\mathcal{L}$ of $F(L)$ above λ satisfies the equality $e_\rho[\mathcal{L}]_p = e_\rho[\mathcal{L}']_p$, the rational prime ℓ below λ is distinct from ℓ' and has the form $\ell \equiv 1 \bmod 2mML$, $v_\lambda(\kappa(L, \lambda')) \equiv 0 \bmod M$, and $p^t \parallel \mathrm{ind}_\lambda(\kappa(L, \lambda'))$. Thus the prime ℓ satisfies the required congruence $\ell \equiv 1 \bmod mML$.

By Theorem 3.12, $\varphi_\lambda(\kappa(L, \lambda')) \equiv \delta(\ell L) \bmod \delta(L)(\mathbb{Z}/M\mathbb{Z})[\Delta]$, so $\mathrm{ind}_\lambda(\kappa(L, \lambda')) \equiv d(\ell L) \bmod p^{r(L)}$, where $d(\ell L)$ denotes the coefficient of the identity in $\delta(\ell L)$. Since $p^t \parallel \mathrm{ind}_\lambda(\kappa(L, \lambda'))$ and $t < r(L)$, it follows that $p^t \parallel d(\ell L)$. Thus $r(\ell L) \leqslant t$ because $p^{r(\ell L)} \mid d(\ell L)$ (as $p^{r(\ell L)} \mid \delta(\ell L)$). Therefore $r(\ell L) < r(L)$, and $p^{r(L)-r(\ell L)}$ annihilates $\mathfrak{C}$ in $e_\rho A/B$ as so does $p^{r(L)-t}$.

Finally, since the projection of λ' into $e_\rho A$ equals $\mathfrak{C}$, applying N_L to the equality $e_\rho[\mathcal{L}]_p = e_\rho[\mathcal{L}']_p$ yields $e_\rho[\lambda]_p = e_\rho[\lambda']_p = \mathfrak{C}$. This concludes the proof. □

Fix $\chi_o \in X_\rho$. The image $\mathrm{Im}\,\chi_o$ is a cyclic group, as it is a subgroup of $\mu_{\varphi(m)}$. Let $\chi_o(\sigma_o)$ with $\sigma_o \in \Delta$ be a generator of $\mathrm{Im}\,\chi_o$. Then $\mathbb{Q}_p(X_\rho) = \mathbb{Q}_p(\mathrm{Im}\,\chi_o) = \mathbb{Q}_p(\chi_o(\sigma_o))$.

The next two propositions are analogous to Propositions 2.7, 2.10, 2.11 of the previous chapter.

Proposition 3.16. *$\mathbb{Z}_p[\Delta]e_\rho$ is a free $\mathbb{Z}_p$-module with base $\sigma_o^j e_\rho$ for $0 \leqslant j < |X_\rho|$.*

Proof. The same as the proof of Proposition 2.10 with necessary changes related to the isomorphism $\Delta \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. □

In the rest of this chapter, $(\mathfrak{C}_1, \dots, \mathfrak{C}_i)$ will denote the multiplicative module over $\mathbb{Z}_p[\Delta]$ generated by $\mathfrak{C}_1, \dots, \mathfrak{C}_i$.

Proposition 3.17. *Suppose that B is a submodule of the $\mathbb{Z}_p[\Delta]$-module $e_\rho A$. Let $\mathfrak{C} \in e_\rho A$ and let f be the order of $\mathfrak{C}$ in $e_\rho A/B$.*

(a) *$\theta \in \mathbb{Z}_p[\Delta]e_\rho$ annihilates $\mathfrak{C}$ in $e_\rho A/B$ if and only if $\theta \in f\,\mathbb{Z}_p[\Delta]e_\rho$.*

(b) $[B\cdot(\mathfrak{C}) : B] = f^{\,|X_\rho|}$.

Proof. (a) Assume that $\theta \in \mathbb{Z}_p[\Delta]e_\rho$ annihilates $\mathfrak{C}$ in $e_\rho A/B$, that is, $\mathfrak{C}^\theta \in B$. Let $p^t \parallel \theta$. By Proposition 1.4, there exists $\theta' \in \mathbb{Z}[\Delta]$ such that $\theta\theta' e_\rho \equiv p^t e_\rho \bmod M$. As M annihilates $e_\rho A$, it follows that $\mathfrak{C}^{p^t} = \mathfrak{C}^{p^t e_\rho} = \mathfrak{C}^{\theta\theta' e_\rho} \in B$. Then $f \mid p^t$, so $f \mid \theta$. Hence $\theta \in f\,\mathbb{Z}_p[\Delta]e_\rho$. This shows one implication. The converse is clear.

(b) The kernel of the surjective $\mathbb{Z}_p[\Delta]$-homomorphism from $\mathbb{Z}_p[\Delta]e_\rho$ to $B\cdot(\mathfrak{C})/B$ defined by $\theta \mapsto \mathfrak{C}^\theta$ is equal to $f\,\mathbb{Z}_p[\Delta]e_\rho$ by item (a). Hence

$$B\cdot(\mathfrak{C})\,/\,B \simeq \mathbb{Z}_p[\Delta]e_\rho\,/\,f\,\mathbb{Z}_p[\Delta]e_\rho\,.$$

This isomorphism implies by Proposition 3.16 that

$$\begin{aligned}[][B\cdot(\mathfrak{C}) : B] &= [\,\mathbb{Z}_p[\Delta]e_\rho : f\,\mathbb{Z}_p[\Delta]e_\rho\,] \\ &= \Bigg[\sum_{0\leqslant j<|X_\rho|} \mathbb{Z}_p\,\sigma_0^j e_\rho : f \sum_{0\leqslant j<|X_\rho|} \mathbb{Z}_p\,\sigma_0^j e_\rho\Bigg] \\ &= \big[\,\mathbb{Z}_p^{|X_\rho|} : f\,\mathbb{Z}_p^{|X_\rho|}\,\big] = [\,\mathbb{Z}_p : f\,\mathbb{Z}_p\,]^{|X_\rho|} = f^{\,|X_\rho|},\end{aligned}$$

as required. □

Proposition 3.18. *If m and p satisfy condition* **C**, *then* $|e_\rho A| \mid p^{r(1)\,|X_\rho|}$.

Proof. Choose classes $\mathfrak{C}_1, \ldots, \mathfrak{C}_k$ in $e_\rho A$ such that $e_\rho A = (\,\mathfrak{C}_1, \ldots, \mathfrak{C}_k)$ and $\mathfrak{C}_i$ has order $f_i > 1$ in the group $e_\rho A/(\,\mathfrak{C}_1, \ldots, \mathfrak{C}_{i-1})$ for $1 \leqslant i \leqslant k$.

Applying Proposition 3.15, suitable primes λ_i of F will be obtained for $1 \leqslant i \leqslant k$ so that the projection of λ_i into $e_\rho A$ equals $\mathfrak{C}_i$ and the rational prime ℓ_i below λ_i satisfies $\ell_i \equiv 1 \bmod mML_{i-1}$ with $L_i = \ell_1 \cdots \ell_i$ and $L_0 = 1$. In addition, it will be shown inductively that $r(L_i) < r(L_{i-1}) \leqslant r(1)$ and $f_i \mid p^{r(L_{i-1})-r(L_i)}$ for $1 \leqslant i \leqslant k$.

Fix i, $1 \leqslant i \leqslant k$, and assume that $r(L_{i-1}) \leqslant r(1)$, which is trivial for $i = 1$ (as $L_0 = 1$). According to the notation introduced above, the subgroup of $e_\rho A$ generated by the projections of the primes of F dividing L_{i-1} equals $(\,\mathfrak{C}_1, \ldots, \mathfrak{C}_{i-1})$. Apply Proposition 3.15 with $L = L_{i-1} \in \mathbb{L}$, $B = (\,\mathfrak{C}_1, \ldots, \mathfrak{C}_{i-1})$, and $\mathfrak{C} = \mathfrak{C}_i$ to show that there exists a prime λ_i of F whose projection into $e_\rho A$ equals $\mathfrak{C}_i$ and that lies above a rational prime $\ell_i \equiv 1 \bmod mML_{i-1}$ such that $r(L_i) = r(\ell_i L_{i-1}) < r(L_{i-1})$ and $p^{r(L_{i-1})-r(L_i)}$ annihilates $\mathfrak{C}_i$ in $e_\rho A/(\mathfrak{C}_1, \ldots, \mathfrak{C}_{i-1})$. Thus $r(L_i) < r(L_{i-1}) \leqslant r(1)$ and $f_i \mid p^{r(L_{i-1})-r(L_i)}$, as claimed.

Since $\mathfrak{C}_i$ has order f_i in $e_\rho A/(\mathfrak{C}_1, \ldots, \mathfrak{C}_{i-1})$, by item (b) of Proposition 3.17 it follows that

$$[(\mathfrak{C}_1, \ldots, \mathfrak{C}_i) : (\mathfrak{C}_1, \ldots, \mathfrak{C}_{i-1})] = f_i^{|X_\rho|}.$$

Therefore

$$\begin{aligned} |e_\rho A| &= \prod_{1 \leqslant i \leqslant k} [(\mathfrak{C}_1, \ldots, \mathfrak{C}_i) : (\mathfrak{C}_1, \ldots, \mathfrak{C}_{i-1})] \\ &= \prod_i f_i^{|X_\rho|} \Bigm| \prod_i p^{(r(L_{i-1})-r(L_i))\,|X_\rho|} \\ &= p^{(r(1)-r(L_k))\,|X_\rho|} \bigm| p^{r(1)\,|X_\rho|}, \end{aligned}$$

as required. □

Denote the integer ring of the field $\mathbb{Q}_p(X_\rho)$ by $\mathcal{O}_{X_\rho}$ or simply by $\mathcal{O}$. Then, since the extension $\mathbb{Q}_p(\zeta_{\varphi(m)})/\mathbb{Q}_p$ is unramified (as $p \nmid \varphi(m)$), so is the subextension $\mathbb{Q}_p(X_\rho)/\mathbb{Q}_p$. Thus $p\mathcal{O}_{X_\rho}$ is a prime ideal and $\mathcal{O}_{X_\rho}/p\mathcal{O}_{X_\rho}$ is a field (see Section 1.1).

For a character χ of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathbb{Z}_p[\zeta_{\varphi(m)}]^\times$ define the generalized Bernoulli number

$$B_{1,\chi} = \tfrac{1}{m} \sum_{\substack{1 \leqslant a < m \\ (a,m)=1}} a\,\chi(a).$$

It is not difficult to show that $B_{1,\chi} \in \mathcal{O}_{X_\rho}$ except when $\chi = \omega^{-1}$. In particular, $B_{1,\chi^{-1}} \in \mathcal{O}_{X_\rho}$ for every $\chi \in X_\rho$.

If $\chi_1, \chi_2 \in X_\rho$, then $\chi_2 = \tau\chi_1$ with $\tau \in \mathrm{Gal}(\mathbb{Q}_p(X_\rho)/\mathbb{Q}_p)$, and thus $B_{1,\chi_2^{-1}} = \tau B_{1,\chi_1^{-1}}$, which means that $B_{1,\chi_1^{-1}}$ and $B_{1,\chi_2^{-1}}$ are conjugate over $\mathbb{Q}_p$.

Proposition 3.19. *$p^{r(1)} \parallel B_{1,\chi^{-1}}$ for every $\chi \in X_\rho$.*

Proof. The next computation, where the relation $\sigma_a e_\chi = \chi(a) e_\chi$ is applied, gives an expresion for $\delta(1)$ in terms of the generalized Bernoulli numbers $B_{1,\chi^{-1}}$ for $\chi \in X_\rho$:

$$\begin{aligned}\delta(1) = \theta(1)\, e_\rho &= \tfrac{1}{m}\,(\sigma_n - n_1)\, s(1)\, e_\rho \\ &= \tfrac{1}{m}\,(\sigma_n - n_1) \sum_{\substack{1 \leqslant a < m \\ (a,m)=1}} a\,\sigma_a^{-1} \sum_{\chi \in X_\rho} e_\chi \\ &= \tfrac{1}{m} \sum_{\chi} (\chi(n) - n_1) \sum_{a} a\,\chi^{-1}(a)\, e_\chi \\ &= \tfrac{1}{\varphi(m)} \sum_{\chi} (\chi(n) - n_1)\, B_{1,\chi^{-1}} \sum_{a} \chi(a)\, \sigma_a^{-1} \\ &= \tfrac{1}{\varphi(m)} \sum_{a} \sum_{\chi} B_{1,\chi^{-1}} (\chi(n) - n_1)\, \chi(a)\, \sigma_a^{-1} .\end{aligned}$$

Setting $c_\chi = B_{1,\chi^{-1}}(\chi(n) - n_1)$ for $\chi \in X_\rho$, the last equality can be written as

$$\delta(1) = \tfrac{1}{\varphi(m)} \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \sum_{\chi \in X_\rho} c_\chi\, \chi(a)\, \sigma_a^{-1} .$$

Let $p^r \parallel B_{1,\chi_0^{-1}}$ for some $\chi_0 \in X_\rho$. This notation is well defined because $p\mathcal{O}$ is a prime ideal, so p is a prime element in $\mathcal{O}$. Then $p^r \parallel B_{1,\chi^{-1}}$ for every $\chi \in X_\rho$, since the numbers $B_{1,\chi^{-1}}$ are conjugate over $\mathbb{Q}_p$. Hence $p^r \mid c_\chi$ for every χ, so $p^r \mid \sum_\chi c_\chi\, \chi(a)$ for every a. It will thus be enough to show that $p^r \parallel \sum_\chi c_\chi\, \chi(b)$ for some $b \in (\mathbb{Z}/m\mathbb{Z})^\times$, as this implies that $p^r \parallel \delta(1)$ and $p^{r(1)} \parallel \delta(1)$ by definition.

Write $\overline{y}$ for the class of $y \in \mathcal{O}$ mod p, that is, for the image of y by the canonical homomorphism $\mathcal{O} \to \mathcal{O}/p\mathcal{O}$. Similarly, write $\overline{\chi}$ for the composition of a character χ of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathcal{O}^\times$ and the canonical homomorphism $\mathcal{O}^\times \to (\mathcal{O}/p\mathcal{O})^\times$. Thus $\overline{\chi}$ is a character of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $(\mathcal{O}/p\mathcal{O})^\times$.

It will be shown that $\overline{\chi}_1 = \overline{\chi}_2$ implies $\chi_1 = \chi_2$ for characters χ_1, χ_2 of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathcal{O}^\times$. Suppose that $\overline{\chi}_1 = \overline{\chi}_2$ and $\chi_1 \neq \chi_2$. Then there is $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $\chi_1(a) \neq \chi_2(a)$ and $\chi_1(a) \equiv \chi_2(a) \bmod p$. Multiplying these relations by $\chi_2(a)^{-1}$, it follows that $\zeta \equiv 1 \bmod p$ for some $\varphi(m)$ th root of unity $\zeta \neq 1$. Applying the polynomial function $x^{\varphi(m)} - 1 \,/\, x - 1 = x^{\varphi(m)-1} + \ldots + x + 1$ to the last congruence, there results that $0 \equiv \varphi(m) \bmod p$, whence $p \mid \varphi(m)$, which contradicts the general hypothesis $p \nmid |\Delta| = \varphi(m)$. This shows the claim.

Since the characters $\overline{\chi}$ for $\chi \in X_\rho$ are distinct, they are linearly independent over $\mathcal{O}/p\mathcal{O}$. Thus $\sum_{\chi \in X_\rho} \overline{p^{-r}c_\chi}\;\overline{\chi} \neq 0$ provided that $\overline{p^{-r}c_{\chi_0}} \neq 0$, i.e., $p^r \parallel c_{\chi_0}$, for some $\chi_0 \in (\mathbb{Z}/m\mathbb{Z})^\times$. It will be shown that this is the case when the integer n is suitably chosen.

Fix $\chi_0 \in X_\rho$. If $p \parallel m$, then $n_1 \equiv n \bmod p$, the Teichmüller character ω is defined, and $\chi_0 \neq \omega$. Thus $\overline{\chi}_0 \neq \overline{\omega}$ and n can be chosen so that $\overline{\chi}_0(n) \neq \overline{\omega}(n)$. It follows that $\chi_0(n) - n_1 \equiv \chi_0(n) - n \equiv \chi_0(n) - \omega(n) \not\equiv 0 \bmod p$. If $p \nmid m$, then $n_1 \equiv 1 \bmod p$. Choosing $n = -1$, it equally follows that $\chi_0(n) - n_1 \equiv \chi_0(-1) - 1 \equiv -2 \not\equiv 0 \bmod p$. Hence $p \nmid \chi_0(n) - n_1$, so $p^r \parallel B_{1,\chi_0^{-1}}(\chi_0(n) - n_1) = c_{\chi_0}$.

It has been shown that $\sum_{\chi \in X_\rho} \overline{p^{-r}c_\chi}\;\overline{\chi} \neq 0$. Then $\sum_\chi \overline{p^{-r}c_\chi\,\chi(b)} \neq 0$ for some $b \in (\mathbb{Z}/m\mathbb{Z})^\times$, which means that $p^r \parallel \sum_\chi c_\chi\,\chi(b)$. This concludes the proof. □

Define the number

$$B_{1,\rho^{-1}} = \prod_{\chi \in X_\rho} B_{1,\chi^{-1}}\,.$$

Since the numbers $B_{1,\chi^{-1}}$ with $\chi \in X_\rho$ are conjugate over $\mathbb{Q}_p$ and $|X_\rho| = [\mathbb{Q}_p(X_\rho) : \mathbb{Q}_p]$, it follows that $B_{1,\rho^{-1}} = \prod_{\chi \in X_\rho} B_{1,\chi^{-1}} = N_{\mathbb{Q}_p(X_\rho)/\mathbb{Q}_p} B_{1,\chi_*^{-1}}$, where $N_{\mathbb{Q}_p(X_\rho)/\mathbb{Q}_p}$ denotes the norm of $\mathbb{Q}_p(X_\rho)$ over $\mathbb{Q}_p$ and χ_* is any character in X_ρ. Moreover, $B_{1,\rho^{-1}} \in \mathbb{Z}_p$ as $B_{1,\chi^{-1}} \in \mathcal{O}_{X_\rho}$ for every $\chi \in X_\rho$.

Denote the p-part of $\beta \in \mathbb{Q}_p(X_\rho)$ by $(\beta)_p$, that is,

$$(\beta)_p = p^{\operatorname{ord}_p(\beta)}.$$

Theorem 3.20. *If m and p satisfy condition* **C**, *then* $|e_\rho A| = (B_{1,\rho^{-1}})_p$.

Proof. Consider the analytic formula for the minus part of the class number of $F = \mathbb{Q}(\zeta_m)$,

$$h^- = Qw \prod_{\chi\,\text{odd}} \left(-\tfrac{1}{2}B_{1,\chi}\right),$$

where $Q = 1$ if m is a prime power and $Q = 2$ otherwise; w denotes the number of roots of unity in F, so $w = m$ if m is even and $w = 2m$ if m is odd; and the product extends over the odd characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ into $\mathbb{Z}_p[\zeta_{\varphi(m)}]^\times$ (cf. [L], Chapter 3, Section 3, CNF$^-$). Taking the p-part of the formula above yields

$$(h^-)_p = (m)_p \prod_{\chi\,\mathrm{odd}} (B_{1,\chi})_p \,.$$

In the rest of the proof, the sum $\sum_a$ is taken over the integers a satisfying $1 \leqslant a < m$, $(a, m) = 1$, and the product $\prod_\rho$ will extend over the irreducible higher dimensional odd characters ρ of Δ with values in $\mathbb{Z}_p$ excluding the Teichmüller character ω if $p \parallel m$.

It will be shown that $\prod_\rho |e_\rho A| = \prod_\rho (B_{1,\rho^{-1}})_p$ considering the two cases $p \parallel m$ and $p \nmid m$ separately.

Assume that $p \parallel m$. Then $(h^-)_p = |e_\omega A| \prod_\rho |e_\rho A|$, $(m)_p = p$, and $\prod_{\chi\,\mathrm{odd}}(B_{1,\chi})_p$ $= (B_{1,\omega^{-1}})_p \prod_\rho \prod_{\chi\in X_\rho} (B_{1,\chi^{-1}})_p = (B_{1,\omega^{-1}})_p \prod_\rho (B_{1,\rho^{-1}})_p$. Thus, the equality $(h^-)_p = (m)_p \prod_{\chi\,\mathrm{odd}}(B_{1,\chi})_p$ becomes

$$|e_\omega A| \prod_\rho |e_\rho A| = p\,(B_{1,\omega^{-1}})_p \prod_\rho (B_{1,\rho^{-1}})_p \,.$$

Let $\mathfrak{C} \in e_\omega A$. By Stickelberger's theorem (Theorem 1.9), $(\sum_a a\,\sigma_a^{-1})\,\mathfrak{C} = 1$. Thus,

$$\mathfrak{C}^{\varphi(m)} = \mathfrak{C}^{\varphi(m)e_\omega} = (\textstyle\sum_a \omega(a)\,\sigma_a^{-1})\,\mathfrak{C} = (\sum_a a\,\sigma_a^{-1} + p\,\theta)\,\mathfrak{C} = \mathfrak{C}^{p\theta},$$

where $\theta \in \mathbb{Z}_p[\Delta]$. Since $\mathrm{ord}(\mathfrak{C}^{\varphi(m)}) = \mathrm{ord}(\mathfrak{C})$ (as $p \nmid \varphi(m)$), and $\mathrm{ord}(\mathfrak{C}) > 1$ would imply $\mathrm{ord}(\mathfrak{C}^{p\theta}) < \mathrm{ord}(\mathfrak{C})$, which is absurd, it follows that $\mathrm{ord}(\mathfrak{C}) = 1$, so $\mathfrak{C} = 1$. Hence $e_\omega A = 1$, so $|e_\omega A| = 1$.

By definition, $B_{1,\omega^{-1}} = \frac{1}{m}\sum_a a\,\omega^{-1}(a)$. Since $\sum_a a\,\omega^{-1}(a) \equiv \sum_a 1 \equiv \varphi(m)$ $\not\equiv 0 \bmod p$, it follows that $(B_{1,\omega^{-1}})_p = p^{-1}$. Hence, there results the equality

$$\prod_\rho |e_\rho A| = \prod_\rho (B_{1,\rho^{-1}})_p \,,$$

as claimed.

Assume that $p \nmid m$. Then $(h^-)_p = \prod_\rho |e_\rho A|$, $(m)_p = 1$, and $\prod_{\chi \text{ odd}}(B_{1,\chi})_p = \prod_\rho \prod_{\chi \in X_\rho}(B_{1,\chi^{-1}})_p = \prod_\rho (B_{1,\rho^{-1}})_p$. Thus the equality $(h^-)_p = (m)_p \prod_{\chi \text{ odd}}(B_{1,\chi})_p$ can be written as

$$\prod_\rho |e_\rho A| = \prod_\rho (B_{1,\rho^{-1}})_p \,,$$

so the claim follows.

Finally, from Propositions 3.18 and 3.19 it is obtained that $|e_\rho A| \leqslant (B_{1,\rho^{-1}})_p$ for every ρ, so the equality shown above implies

$$|e_\rho A| = (B_{1,\rho^{-1}})_p \,,$$

as required. □

References

[C] Cassels, J.W.S., *Local Fields,* Cambridge University Press, Cambridge, 1986.

[G1] Gras, G., Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, *Annales de l'Institut Fourier* 27, p. 1–66, 1977.

[G2] Greither, C., Class groups of abelian fields and the main conjecture, *Annales de l'Institut Fourier* 42, no. 3, p. 449–499, 1992.

[J] Janusz, G.J., *Algebraic Number Fields,* Academic Press, New York, London, 1973

[K1] Koblitz, N., *p-adic Numbers, p-adic Analysis, and Zeta-Functions,* Graduate Texts in Mathematics 58, Second Edition, Springer-Verlag, New York, 1984.

[K2] Kolyvagin, V., Euler systems, *The Grothendieck Festschrift,* vol. 2, P. Cartier et al., eds., Progress in Mathematics 87, Birkhäuser, Boston, p. 435–483, 1990.

[L] Lang, S., *Cyclotomic Fields I and II,* Graduate Texts in Mathematics 121, Springer-Verlag, New York, 1990.

[MW] Mazur, B. and Wiles, A., Class fields of abelian extensions of $\mathbb{Q}$, *Inventiones Mathematicae* 76, p. 179–330, 1984.

[R1] Rubin, K., Kolyvagin's system of Gauss sums, *Arithmetic Algebraic Geometry (Texel, 1989),* G. van der Geer et al., eds., Progress in Mathematics 89, Birkhäuser, Boston, p. 309–324, 1991.

[R2] Rubin, K., *Euler systems,* Annals of Mathematics Studies 147, Princeton University Press, Princeton, 2000.

[S] Sinnott, W., On the Stickelberger ideal and the circular units of a cyclotomic field, *Annals of Mathematics* 108, p. 107–134, 1978.

[T] Thaine, F., On the ideal class groups of real abelian number fields, *Annals of Mathematics* 128, p. 1–18, 1988.

[W1] Washington, L., *Introduction to Cyclotomic Fields,* Graduate Texts in Mathematics 83, Second Edition, Springer, Berlin, New York, 1997.

[W2] Weibel, C.A., *An Introduction to Homological Algebra,* Cambridge University Press, Cambridge, 1994.