ON THE GALOIS MODULE STRUCTURE OF THE UNITS AND RAY CLASSES OF A REAL ABELIAN NUMBER FIELD

DISSERTATION

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of the Ohio State University

By

Timothy J. All, BA

Graduate Program in Mathematics

The Ohio State University

2013

Dissertation Committee:

Warren Sinnott, Advisor

James Cogdell

David Goss

ABSTRACT

We study the Galois module structure of the ideal ray class group and the group of units of a real abelian number field. Specifically, we derive explicit annihilators of the ideal ray class groups in the vein of the classical Stickelberger theorems. This is made possible by generalizing a theorem of Rubin which in turn allows us to describe a relationship between the Galois module structure of certain explicit quotients of units and the Galois module structure of the ray class group. Along the way, we're compelled to study the Galois module structure of the p-adic completion of the units. We derive numerous conditions under which we may conclude that this module is cyclic some of which allow for p to divide the order of the Galois group. Under those conditions, we are able to relate the annihilators of the p-parts of various explicit quotients of units to annihilators of the p-parts of the ray class groups in many cases. This is a generalization of a theorem of Thaine.

to Mandy

ACKNOWLEDGMENTS

I remember a faculty member once described my advisor, Warren Sinnott, as a "real renaissance man". I've known Dr. Sinnott for many years now and I'm forced to agree. An actual gentleman and scholar, Dr. Sinnott's perspective and kindness have simply made me better. So my first thanks is to him. Thank you.

I'd also like to thank Dr. James Cogdell and Dr. David Goss not only for their participation in my doctoral committee, but also for their mentorship over the years.

I want to thank my friends for making this whole experience all the more humane, and for magnifying my enthusiasm for mathematics through conversation (and spirits). Particularly I want to thank my office mate, Kyle Joecken, and my mathematical brother, Brad Waller, and also Nick Peterson and my function field analogue, Rudy Perkins. Thanks, guys.

I want to thank my mom and dad for their unwavering support in this endeavor. It would have been easy to pass criticism on a son who was in school for over a decade, but I've never detected the slightest hint of it, and it has always meant a lot to me. Thanks.

Finally, I want to thank my wife, Mandy, to whom this dissertation is dedicated. You've given me: a son, a daughter, and a home. I'm happier than I have any right to be because of you. I love you.

VITA

2006	BA Mathematics, The Ohio State University
2006-Present	Graduate Research/Teaching Associate, The Ohio State University

PUBLICATIONS

All, Timothy; *On* p*-adic annihilators of real ideal classes*, J. Number Theory, 133(7): 2324-2338, 2013

FIELDS OF STUDY

Major Field: Mathematics

Specialization: Algebraic Number Theory

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 History

Let k be an abelian number field of conductor m. Let $\zeta_m = e^{2\pi i/m}$ and let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ be defined by $\sigma_a : \zeta_m \mapsto \zeta_m^a$. For any real x, let $\{x\}$ denote the unique real number such that $x - \{x\} \in \mathbb{Z}$ and $0 \leqslant \{x\} < 1$. Define

$$\theta_k = \sum_{\substack{a \bmod m \\ (a,m)=1}} \left\{\frac{a}{m}\right\} \sigma_a^{-1} \in \mathbb{Q}[G],$$

where we view $\sigma_a \in G$ by restriction. The element θ_k is called the *Stickelberger element* of k. We have the following classical theorem:

Theorem 1.1 (Stickelberger, [18]). *The Stickelberger ideal* $S_k := \mathbb{Z}[G]\theta_k \cap \mathbb{Z}[G]$ *annihilates* Cl_k*, the ideal class group of* k*.*

Stickelberger's theorem follows by studying the factorization of Gauss sums in $\mathbb{Q}(\zeta_m)$. This theorem is surprising (and useful) since it gives explicit information about the ideal class group. Perhaps even more surprising is the following theorem due to Iwasawa:

Theorem 1.2 (Iwasawa [7]). *Suppose* $k = \mathbb{Q}(\zeta_{p^n})$ *and let* $R^- = (1 - \sigma_{-1})\mathbb{Z}[G]$*. The index of the subgroup* $S_k^- = \theta_k\mathbb{Z}[G] \cap R^-$ *in* R^-*, denoted* $[R^- : S_k^-]$*, is finite. In fact,* $[R^- : S_k^-] = h_{p^n}^-$ *where* $h_{p^n}^-$ *is the relative class number of* $\mathbb{Q}(\zeta_{p^n})$*.*

For general abelian number fields, Sinnott [16, Theorem 2.1 and Theorem 3.1] has defined a larger ideal S'_k (which is essentially equivalent to S_k in the $k = \mathbb{Q}(\zeta_{p^n})$ case) whose members annihilate the ideal class group and satisfies an analogous index formula. Similarly, for $d \in \mathbb{N}$, Schmidt [15, Satz 1 and Satz 2] has defined an ideal $S'_k(d)$ (equivalent to Sinnott's S'_k if $d = 1$) whose members annihilate the ray class group $Cl_k(d)$ of k of modulus d, moreover, whose index $[R^- : S'^-_k(d)]$ is finite and related to $\#Cl_k(d)$. Unfortunately, if k is real, then the Stickelberger elements thus far mentioned devolve into multiples of the norm. For example, if $k = \mathbb{Q}(\zeta_m)^+$ then $\sigma_a|_k = \sigma_{-a}|_k$ and $\{a/m\} + \{-a/m\} = 1$. This means that

$$\theta_k = \frac{\phi(m)}{2[k : \mathbb{Q}]} \sum_{\sigma \in G} \sigma,$$

where $\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$. And since θ_k is a multiple of the norm, no useful information can be obtained.

Now, consider the following classical theorem due to Kummer.

Theorem 1.3 (Kummer [8]). *For $k = \mathbb{Q}(\zeta_{p^n})^+$, define the cyclotomic units C_k of k to be the $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})^+/\mathbb{Q})$-module generated by -1 and*

$$\zeta_{p^n}^{(1-s)/2} \frac{\zeta_{p^n}^s - 1}{\zeta_{p^n} - 1},$$

where $\langle s \rangle = (\mathbb{Z}/p^n\mathbb{Z})^\times$. Then C_k is a subgroup of finite index in the group of units E_k of k, in fact, $[E_k : C_k] = h^+_{p^n}$ where $h^+_{p^n}$ is the class number of k.

Once again, for general abelian number fields, Sinnott [16, Theorem 4.1] has defined a larger group of explicit units C'_k (which is essentially equivalent to C_k in the $k = \mathbb{Q}(\zeta_{p^n})^+$ case) and obtained an analogous index formula. Similarly, for $d \in \mathbb{N}$, Schmidt [15, Satz 3] has defined an explicit group of units $C'_k(d)$ (equivalent to Sinnott's C'_k when $d = 1$) congruent to 1 modulo d whose index in the full group of units congruent to 1 modulo d is finite and related to $\#\,Cl_k(d)$.

The next question to ask is now plain: If k is a real abelian number field, then is the relationship between $C'_k(d)$ and $Cl_k(d)$ purely combinatorial, or is it a symptom of a deeper algebraic relationship? It is, in fact, the latter case. When $d = 1$ this relationship is reflected in the work of Thaine [19], Rubin [14], and most spectacularly in the work of Mazur and Wiles [11]. One of the main goals of this dissertation is to establish similar relationships when $d \neq 1$.

We now discuss the work of Thaine and Rubin as it applies to this dissertation. From here on out, k denotes a real abelian number field with Galois group G and unit group E_k. We have the following theorem due to Thaine.

Theorem 1.4 (Thaine [19]). *Let p be an odd prime not dividing $[k : \mathbb{Q}]$. If $\theta \in \mathbb{Z}[G]$ such that θ annihilates $\mathrm{Syl}_p(E_k/C'_k)$, then θ annihilates $\mathrm{Syl}_p(Cl_k)$.*

Thaine's theorem follows by noticing that the units of C'_k satisfy the following property: for every $\delta \in C'_k$, for all but finitely many rational primes ℓ that split completely in k, there exists a $k(\zeta_\ell)/k$-norm 1 unit of $k(\zeta_\ell)$ that is congruent to δ modulo the primes of $k(\zeta_\ell)$ above ℓ. The fact that this unit is norm 1 allows us to construct various principal ideals (α) that are invariant under the $\mathrm{Gal}(k(\zeta_\ell)/k)$-action, or principal "ambiguous ideals" as Hilbert calls them. From the factorization of $(N_k^{k(\zeta_\ell)}(\alpha))$ we derive annihilators of $\mathrm{Syl}_p(Cl_k)$ much in the same way that Stickelberger elements are derived from the factorization of Gauss sums. The fact that ϵ satisfies the aforementioned congruence relation with δ allows us to relate the annihilators of $\mathrm{Syl}_p(Cl_k)$ with those of $\mathrm{Syl}_p(E_k/C'_k)$.

Using a "wild variant" of Thaine's method, Solomon [17, Proposition 4.1] was able to prove the following theorem.

Theorem 1.5 (Solomon [17]). *Fix an embedding so that we may view $\mathbb{Q}^{alg} \subseteq \mathbb{Q}_p^{alg}$. Suppose p is unramified in k, let m be the conductor of k, and let Dl_k denote the set of*

ideal classes of k *supported by the primes above* p. *Let* $\mathcal{O}_k$ *denote the ring of integers of the topological closure of* k, *and set*

$$\mathrm{sol}_k := \frac{1}{p} \sum_{\sigma \in G} \log_p \left((N_k^{\mathbb{Q}(\zeta_m)}(1-\zeta_m))^{\sigma} \right) \sigma^{-1}.$$

Then sol_k *annihilates* $D\mathfrak{l}_k \otimes_{\mathbb{Z}} \mathcal{O}_k$.

Naturally, this led Solomon to the following conjecture [17, Conjecture 4.1].

Conjecture (Solomon [17]). *If* p *is unramifed in* k, *then* sol_k *annihilates* $\mathrm{Cl}_k \otimes_{\mathbb{Z}} \mathcal{O}_k$.

The above conjecture is an analog of Stickelberger's theorem for real abelian number fields. Recently, Belliard and Quang Do [1, Theorem 5.4] were able to prove a modified version of Solomon's conjecture under the additional hypothesis that p is totally split in k.

Theorem 1.6 (Belliard and Quang Do [1]). *Assume* p *is totally split in* k. *If the conductor of* k *is a prime power, then* $(1-\tau)\,\mathrm{sol}_k$ *annihilates* $\mathrm{Syl}_p(\mathrm{Cl}_k)$ *where* τ *is a generator for* G; *otherwise,* sol_k *annihilates* $\mathrm{Syl}_p(\mathrm{Cl}_k)$.

If p is totally split in k, then $\mathcal{O}_k = \mathbb{Z}_p$, $\mathrm{sol}_k \in \mathbb{Z}_p[G]$ and $\mathrm{Cl}_k \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathrm{Syl}_p(\mathrm{Cl}_k)$. In this setting, Belliard and Quang Do were able to prove the above theorem by utilizing the following broad generalization of Thaine's method obtained by Rubin [14, Theorem 1.3].

Theorem 1.7 (Rubin [14]). *Let* $\alpha : E_k \to \mathbb{Z}_p[G]$ *be a* G*-module map. Then* $\alpha(C'_k)$ *annihilates* $\mathrm{Gal}(H/(k(\zeta_{p^\infty}) \cap H))$ *where* $\mathrm{Gal}(H/k) \simeq \mathrm{Syl}_p(\mathrm{Cl}_k)$ *via the Artin map and* ζ_{p^∞} *is the group of all* p*-power roots of unity.*

This dissertation is motivated by generalizing the approach of Belliard and Quang Do to arbitrary odd primes p, and extending all the annihilation results to the ideal ray class groups. So we have two principal objectives. For an ideal $\mathfrak{a}$ of the ring of integers of k:

- Define an explicit subgroup of units $C_k(\mathfrak{a})$ such that the G-module structure of $E_k/C_k(\mathfrak{a})$ is related to $Cl_k(\mathfrak{a})$ akin to the relationship between Cl_k and E_k/C_k' as seen in Theorem 1.7 and Theorem 1.4.

- Derive explicit annihilators of $Cl_k(\mathfrak{a}) \otimes_{\mathbb{Z}} \mathcal{O}_k$ (which in turn generate annihilators of $\mathrm{Syl}_p(Cl_k(\mathfrak{a}))$) in the vein of Theorem 1.1.

Along the way, we discover some interesting results regarding the structure of $E_k \otimes_{\mathbb{Z}} \mathbb{F}_p$ as an $\mathbb{F}_p[G]$-module. Consequently, we can prove a ray class analog of Thaine's theorem (which subsumes Thaine's theorem itself) that is applicable in some non semi-simple cases, surprisingly enough.

1.2 Outline of Results

Chapter 2 of this dissertation is devoted to proving the following generalization of Theorem 1.7.

Theorem 1.8. *Let $\mathfrak{a}$ be an ideal of the ring of integers of k, and let α be a G-module map from the S-units of k to $\mathcal{O}_k[G]$ where S contains all the Archimedean places. There is a subgroup of S-units $\mathcal{C}_S(\mathfrak{a})$ of k, whose definition (see Definition 2.8) does not involve the ray class group $Cl_k(\mathfrak{a})$, such that*

$$R_0 \cdot \alpha(\mathcal{C}_S(\mathfrak{a})) \qquad \textit{annihilates} \qquad Cl_k(\mathfrak{a}) \otimes_{\mathbb{Z}} \mathcal{O}_k$$

where R_0 is the augmentation ideal of $\mathcal{O}_k[G]$.

We end Chapter 2 by analyzing the G-module

$$\mathrm{Gal}\left(k(\zeta_{p^\infty}) \cap H(\mathfrak{a}) \Big/ k\right).$$

We derive sufficient conditions to conclude that this module is trivial. Under these conditions, it turns out we can remove the contribution from R_0 in Theorem 1.8.

In order to establish explicit annihilators of $\mathrm{Cl}_k(\mathfrak{a}) \otimes_{\mathbb{Z}} \mathcal{O}_k$ á la Stickelberger, we'd like to take advantage of Theorem 1.8. This will require:

- an explicit G-module map from the S-units E_S of k to $\mathcal{O}_k[G]$
- explicit examples of S-units of the type $\mathcal{C}_S(\mathfrak{a})$.

Chapter 3 is devoted to the latter in which we study an explicit subgroup of S-units $C_S(\mathfrak{a})$ of k which we call the $\mathfrak{a}$-cyclotomic S-units (equivalent to Schmidt's d-cyclotomic S-units for certain d depending on $\mathfrak{a}$) where $\mathfrak{a}$ is an ideal of the ring of integers of k (see Definition 3.1). In particular, we prove the following theorem.

Theorem 1.9. $C_S(\mathfrak{a}) \subseteq \mathcal{C}_S(\mathfrak{a})$.

We then show that the index $[E : C(\mathfrak{a})]$[1] is finite, and we compute it when $\mathfrak{a} = d \in \mathbb{N}$. In this case we prove the following generalization of Theorem 1.3.

Theorem 1.10. *The index* $[E : C(d)]$ *is finite and* $[E : C(d)] = \#\mathrm{Cl}_k(d) \cdot c_k(d)$ *where the explicit definition of* $c_k(d)$ *does not depend on* $\mathrm{Cl}_k(d)$.

As for G-module maps from $E \to \mathcal{O}_k[G]$, these are easiest to describe when $E \otimes_{\mathbb{Z}} \mathbb{F}_p$ is a cyclic module. Consequently, in Chapter 4 we study the G-module structure of $E \otimes_{\mathbb{Z}} \mathbb{F}_p$. In certain cases, we show that the cyclicality of $E \otimes_{\mathbb{Z}} \mathbb{F}_p$ is influenced by the capitulation of ideals and the number of primes ramifying in the p-part of the extension $k/\mathbb{Q}$. In particular, we have the following theorem.

Theorem 1.11. *If* $p \nmid \#G$, *then* $E \otimes_{\mathbb{Z}} \mathbb{F}_p$ *is a cyclic* $\mathbb{F}_p[G]$*-module.*

Things are, predictably, more complicated when $p \mid \#G$. We give necessary and sufficient conditions for the cyclicality of $E \otimes_{\mathbb{Z}} \mathbb{F}_p$ as a G-module when G is cyclic and $k/k^{\mathrm{Syl}_p(G)}$ is part of the $\mathbb{Z}_p$-extension of $k^{\mathrm{Syl}_p(G)}$. The clearest result we have in this vein is the following slightly more general result.

[1] We omit subscripts when S consists solely the Archimedean places.

Theorem 1.12. *Suppose* G *is cyclic and there is only one prime ideal of* $k^{\mathrm{Syl}_p(G)}$ *ramifying in* $k/k^{\mathrm{Syl}_p(G)}$. *Then* $E \otimes_{\mathbb{Z}} \mathbb{F}_p$ *is a cyclic* $\mathbb{F}_p[G]$*-module if and only if the natural map* $\mathrm{Cl}_{k^{\mathrm{Syl}_p(G)}} \to \mathrm{Cl}_k$ *is injective.*

Using a wholly different approach, we can also show that the G-module structure of $E \otimes_{\mathbb{Z}} \mathbb{F}_p$ is restricted by $\#\mathrm{Syl}_p(G)$ to a large extent. In fact, we get the following theorem.

Theorem 1.13. *If* $\#G = p$, *then* $E \otimes \mathbb{F}_p$ *is a cyclic* $\mathbb{F}_p[G]$*-module.*

As $\#\mathrm{Syl}_p(G)$ gets larger, this last approach becomes less useful. On the other hand, we did notice something unrelated but curious. Comparing results across Chapter 4, we get the following for a very attractive price. If $[k : \mathbb{Q}] = p^e m$ and $s > e$ rational primes ramify in k whose ramification indices are divisible by p, then the p-rank of Cl_k is at least $s - e$. This result is surprising, if anything, because it requires no class field theory to prove.

Chapter 5 is devoted to applications of the previous chapters. As mentioned before, one of our main goals is to find explicit annihilators of $\mathrm{Cl}_k(\mathfrak{a}) \otimes_{\mathbb{Z}} \mathcal{O}_k$. We can now do this by using Theorems 1.8 and 1.9 and the explicit G-module map $\vartheta : E_S \to \mathcal{K}[G]$ defined by

$$\vartheta(x) = \sum_{\sigma \in G} \log_p(x^\sigma)\sigma^{-1},$$

where $\mathcal{K}$ is the topological closure of k and $\log_p$ is the Iwasawa logarithm. In general, this map is not integral, so we must "integralize" it, i.e., we must find $\beta \in \mathcal{K}[G]$ such that $\beta\vartheta(E_S) \subseteq \mathcal{O}_k[G]$. We find explicit examples of such integralizers and therefore are able to derive explicit annihilators. In general, we have the following theorem.

Theorem 1.14. *Let* $\beta \in \mathcal{K}[G]$ *such that* $\beta\vartheta(E_S) \subseteq \mathcal{O}_k[G]$. *Then*

$$R_0 \cdot \beta\vartheta(C_S(\mathfrak{a})) \qquad \textit{annihilates} \qquad \mathrm{Cl}_k(\mathfrak{a}) \otimes_{\mathbb{Z}} \mathcal{O}_k.$$

This is gives the first full proof (of a much strengthened version) of Solomon's [17, Conjecture 4.1] (again, under certain conditions we can remove the contribution from R_0, the augmentation ideal of $\mathcal{O}_k[G]$).

We also show that any G-module map from $E \to \mathcal{O}_k[G]$ is a $\mathcal{K}[G]$-multiple of the map ϑ defined above. This gives us to describe the $\mathcal{O}_k[G]$ ideal $S_0(\mathfrak{a})$ defined by

$$S_0(\mathfrak{a}) := \langle \alpha(C(\mathfrak{a})) : \alpha \in \mathrm{Hom}_G(E, \mathcal{O}_k[G]) \rangle_{\mathcal{O}_k[G]}$$

in terms of the map ϑ defined above. This ideal (or possibly the product of this ideal with R_0) annihilates $\mathrm{Cl}_k(\mathfrak{a}) \otimes_{\mathbb{Z}} \mathcal{O}$ and is analogous to the ideal $\mathbb{Z}[G] \cap \mathbb{Z}[G]\theta_k$ of Theorem 1.1.

Under the additional assumption that $E \otimes_{\mathbb{Z}} \mathbb{F}_p$ is a cyclic module (and thus the content of Chapter 4 comes into the fold), we show that $S_0(\mathfrak{a})$ is essentially equal to the annihilator of $(E/C(\mathfrak{a})) \otimes_{\mathbb{Z}} \mathcal{O}_k$. This is a generalization of Theorem 1.4. Moreover, if we also assume $\mathfrak{a} = 1$ and $\mathrm{Syl}_p(G)$ is cyclic, we show that the index $[R_0 : S_0(1)]$ is finite equal to $\#(\mathrm{Cl}_k \otimes_{\mathbb{Z}} \mathcal{O}_k)$. This is a generalization of Theorem 1.2. In summary, we have the following theorem.

Theorem 1.15. *If* $E \otimes \mathbb{F}_p$ *is a cyclic* $\mathbb{F}_p[G]$ *module, then*

$$S_0(\mathfrak{a}) = R_0 \cdot \mathrm{Ann}_{\mathcal{O}_k[G]}(E/C(\mathfrak{a})) \otimes_{\mathbb{Z}} \mathcal{O}_k.$$

If, in addition, we have $\mathrm{Syl}_p(G)$ *is cyclic, then*

$$R_0/S_0(\mathfrak{a}) \simeq (E/C(\mathfrak{a})) \otimes_{\mathbb{Z}} \mathcal{O}_k.$$

In particular, if $\mathfrak{a} = 1$ *and* $p \nmid \#G$*, then*

$$\#(R_0/S_0(1)) = \#(\mathrm{Cl}_k \otimes_{\mathbb{Z}} \mathcal{O}_k).$$

1.3 Common Notation

We collect the common notations used throughout this dissertation here for the convenience of the reader. Throughout we let k denote a real abelian number field with Galois group G. For a number field K we set

$$\mathfrak{o}_K = \text{the ring of algebraic integers of } K$$
$$\mathrm{Cl}_K(\mathfrak{a}) = \text{the ray class group of } K \text{ of modulus } \mathfrak{a} \subseteq \mathfrak{o}_k.$$

If $K = k$, then we generally omit subscripts, and if $\mathfrak{a} = \mathfrak{o}$, then we generally omit parentheses (e.g., $\mathrm{Cl} = \mathrm{Cl}_k(\mathfrak{o})$). For a prime $\mathfrak{p} \subset \mathfrak{o}_K$, we use $\nu_\mathfrak{p}(x)$ to denote the p-adic valuation of $x \in K$. Further, we let

$$S = \text{a } G\text{-stable set of places of } k \text{ containing all the Archimedean places.}$$

For any $n \in \mathbb{N}$, we set

$$\zeta_n = e^{2\pi i/n}$$
$$W_n = \text{the group of } n\text{-th roots of unity.}$$

We fix an odd prime p, and an embedding of $k \hookrightarrow \mathbb{Q}_p^{\mathrm{alg}}$. We consider $k \subset \mathbb{Q}_p^{\mathrm{alg}}$ from here on out and omit any mention of the embedding for the sake of brevity.

For primes $\lambda \subset \mathfrak{o}_k$, we use the notation $(\lambda,\ K/k)$ to denote a Frobenius automorphism of λ in $\mathrm{Gal}(K/k)$. Note that $(\lambda, K/k)$ is only defined modulo the inertia subgroup for λ. We let $[\lambda, K/k]$ denote the conjugacy class of $(\lambda, K/k)$ in $\mathrm{Gal}(K/k)$.

Throughout we use $\otimes$ as an abbreviation for $\otimes_{\mathbb{Z}}$. We make a $\mathbb{Z}[G]$-module M into an $R[G]$-module $M \otimes R$ (where R is any commutative ring) in the obvious way: for $m \in M$, $r \in R$, and $\sum r_\sigma \sigma \in R[G]$ we set

$$(m \otimes r)^{\sum r_\sigma \sigma} := \sum m^\sigma \otimes r r_\sigma.$$

We let $\widehat{G}$ denote the character group of G. For each $\chi \in \widehat{G}$, we let e_χ denote the idempotent associated to χ:

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

We may view $e_\chi \in K[G]$ where K is any field whose characteristic does not divide $\#G$ and contains the $\#G$-th roots of unity.

CHAPTER 2

ON THE GALOIS MODULE STRUCTURE OF THE RAY CLASS GROUP

2.1 Preliminaries

In this chapter, we write E_S to denote the S-units of k, and we let $\mathfrak{a} \subseteq \mathfrak{o}$ be an ideal. For a natural number n, we write k_n for $k \cap \mathbb{Q}(\zeta_n)$. We also fix the following notations.

$$\begin{aligned}
\mathcal{K} &= \text{the topological closure of } k \text{ in } \mathbb{Q}_p^{alg} \\
\mathcal{O} &= \text{the valuation integers of } \mathcal{K} \\
\varpi &= \text{a uniformizer of } \mathcal{O} \\
A_n(\mathfrak{a}) &= Cl(\mathfrak{a})/p^n\, Cl(\mathfrak{a}) \\
A(\mathfrak{a}) &= Syl_p(Cl(\mathfrak{a})) \\
H_n(\mathfrak{a}) &= \text{the ray class field over } k \text{ associate to } A_n(\mathfrak{a}). \\
H(\mathfrak{a}) &= \text{the ray class field over } k \text{ associate to } A(\mathfrak{a}).
\end{aligned}$$

Note that $Gal(H_n(\mathfrak{a})/k) \simeq A_n(\mathfrak{a})$ and $Gal(H(\mathfrak{a})/k) \simeq A(\mathfrak{a})$ via the Artin map.

The proof of the main result of this chapter relies on the linear disjointness of $H_n(\mathfrak{a})$ and certain Kummer extensions of $k(\zeta_{p^n})$. For this reason, we will find the following proposition, essentially from [14], very helpful.

Proposition 2.1. *Let* $V \leqslant k^\times$ *such that* $Vk^{\times p^n}/k^{\times p^n}$ *is finite. Then*

$$H_n(\mathfrak{a}) \cap k(\zeta_{p^n}, V^{1/p^n}) = H_n(\mathfrak{a}) \cap k(\zeta_{p^n}).$$

Proof. Let K be the composite of $k(\zeta_{p^n})$ and $H_n(\mathfrak{a}) \cap k(\zeta_{p^n}, V^{1/p^n})$. Then we have a natural isomorphism of Galois groups

$$\mathrm{Gal}\left(\left(H_n(\mathfrak{a}) \cap k(\zeta_{p^n}, V^{1/p^n})\right)\right) \Big/ \mathrm{Gal}\left(H_n(\mathfrak{a}) \cap k(\zeta_{p^n})\right) \simeq \mathrm{Gal}(K/k(\zeta_{p^n})),$$

moreover, Kummer theory gives us an isomorphism of $\mathrm{Gal}(k(\zeta_{p^n})/k)$-modules

$$\mathrm{Gal}(K/k(\zeta_{p^n})) \simeq \mathrm{Hom}_{\mathbb{Z}}(B, W_{p^n}),$$

where $B \leqslant Vk^{\times p^n}/k^{\times p^n}$ such that $K = k(B^{1/p^n})$. Since $\mathrm{Gal}(K/k(\zeta_{p^n}))$ is abelian, we have that $\mathrm{Gal}(k(\zeta_{p^n})/k)$ acts trivially on $\mathrm{Gal}(K/k)$. So $\mathrm{Gal}(k(\zeta_{p^n})/k)$ acts trivially on $\mathrm{Hom}(B, W_{p^n})$. This means that for all $\tau \in \mathrm{Gal}(k(\zeta_{p^n})/k)$, for all $\psi \in \mathrm{Hom}(B, W_{p^n})$ we have

$$\psi(\tau b) = \tau\psi(b), \quad \text{for all } b \in B.$$

But $B \leqslant k^\times/k^{\times p^n}$, so $\tau\psi(b) = \psi(b)$ for all $b \in B$. It follows that $\psi(b) \in k$ for all $b \in B$. Since k is real and p is an odd prime, it must be that $\psi(b) = 1$ for all $b \in B$. So $\mathrm{Hom}(B, W_{p^n}) \simeq \mathrm{Gal}(K/k)$ is trivial. This completes the proof of the proposition. □

Let M be an $R[G]$-module where R is a commutative ring with 1. We make $\mathrm{Hom}_G(M, R[G])$ and $\mathrm{Hom}_R(M, R)$ into $R[G]$-modules in the usual way: for $\alpha \in \mathrm{Hom}_G(M, R[G])$, $a \in \mathrm{Hom}_R(M, R)$, and $\theta \in R[G]$ we define

$$(\theta \cdot \alpha)(m) := \theta\alpha(m) \quad \text{and} \quad (\theta \cdot a)(m) := a(\theta m).$$

We need the following lemma that relates these two modules.

Lemma 2.2. *Let* R *be a commutative ring with* 1*, and let* M *be an* $R[G]$*-module. The map* $\Phi : \mathrm{Hom}_G(M, R[G]) \to \mathrm{Hom}_R(M, R)$ *defined by*

$$\left(\alpha : m \to \sum_{\sigma \in G} m_\sigma \sigma^{-1}\right) \mapsto (a : m \to m_{\mathrm{id}})$$
$$\left(\alpha : m \to \sum_{\sigma \in G} a(m^\sigma)\sigma^{-1}\right) \leftarrow\!\shortmid (a : m \to a(m)),$$

is a G*-module isomorphism.*

Proof. This is a straight-forward verification. □

We will also need the following proposition regarding the injectivity of $R[G]$ when $R = {}^{\mathcal{O}}/_{\mathfrak{p}^n\mathcal{O}}$.

Proposition 2.3. *Let* $R = {}^{\mathcal{O}}/_{\mathfrak{p}^n\mathcal{O}}$*, and let* $N \subseteq M$ *be finite* $R[G]$*-modules. The natural map*

$$\mathrm{Hom}_G(M, R[G]) \to \mathrm{Hom}_G(N, R[G])$$

is surjective.

Proof. In lieu of the above lemma, it suffices to show that the natural map

$$\mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(N, R)$$

is surjective. Let $m \in M \setminus N$, and let $f \in \mathrm{Hom}_R(N, R)$. We wish to extend f to a homomorphism from $N + Rm \to R$. Let j be the least positive integer such that $\varpi^j m \in N$. Let e be the ramification index of $\mathfrak{p}$ in k so that $\mathfrak{p} = \varpi^e$. Define $f' : (\varpi^j) \to R$ by

$$f'(r) := f(rm).$$

Note that $0 < j \leqslant en$, so

$$\varpi^{en-j} f'(\varpi^j) = \varpi^{en-j} f(\varpi^j m) = f(\varpi^{en} m) = 0.$$

It follows that $f'(\varpi^j) \subseteq (\varpi)$. Let $u \in R$ such that $u\varpi = f'(\varpi^j)$.

Now, suppose $x_1, x_2 \in (\varpi^j)$ and $r_1, r_2 \in R$ such that

$$x_1 + r_1\varpi^{j-1} = x_2 + r_2\varpi^{j-1}.$$

Then

$$x_1 - x_2 = (r_2 - r_1)\varpi^{j-1}.$$

It follows that $r_2 - r_1 \in (\varpi)$. Let $v \in R$ such that $r_2 = r_1 + v\varpi$. Then

$$\begin{aligned} f'(x_2) + r_2u &= f'(x_1 + r_1\varpi^{j-1} - (r_1 + v\varpi)\varpi^{j-1}) + (r_1 + v\varpi)u \\ &= f'(x_1) + r_1u - f'(v\varpi^j) + uv\varpi \\ &= f'(x_1) + r_1u, \end{aligned}$$

since $f'(v\varpi^j) = vf'(\varpi^j) = uv\varpi$. It follows that the map $f'' : (\varpi^{j-1}) \to R$ defined by

$$x + r\varpi^{j-1} \mapsto f'(x) + ru$$

is well-defined, moreover, $f''|_{(\varpi^j)} = f'$. Similarly, we can lift f'' to a map $f''' : (\varpi^{j-2}) \to R$ such that $f'''|_{(\varpi^{j-1})} = f''$. Lifting j times successively, we construct a map $f^{(j+1)} : R \to R$ such that $f^{(j+1)}|_{(\varpi^j)} = f'$.

Now, suppose $y_1, y_2 \in N$ and $r_1, r_2 \in R$ such that

$$y_1 + r_1m = y_2 + r_2m.$$

Then

$$y_1 - y_2 = (r_2 - r_1)m.$$

It follows that $r_2 - r_1 \in (\varpi^j)$ by the minimality of j. Let $v \in R$ such that $r_2 = r_1 + v\varpi^j$. Then

$$\begin{aligned} f(y_2) + f^{(j+1)}(r_2) &= f(y_1 + r_1m - (r_1 + v\varpi^j)m) + f^{(j+1)}(r_1 + v\varpi^j) \\ &= f(y_1) + f^{(j+1)}(r_1) - f(v\varpi^j m) + f^{(j+1)}(v\varpi^j). \end{aligned}$$

By construction, we have

$$f^{(j+1)}(v\varpi^j) = f'(v\varpi^j) = f(v\varpi^j m),$$

so

$$f(y_2) + f^{(j+1)}(r_2) = f(y_1) + f^{(j+1)}(r_1).$$

It follows that the map $F : N + Rm \to R$ defined by

$$F(y + rm) := f(y) + f^{(j+1)}(r),$$

is well-defined, moreover, $F|_N = f$. □

2.2 Proof of the Main Theorem

For odd primes ℓ, let

$$E(\ell, a) := \{\epsilon \in E_{k(\zeta_\ell)} : N_k^{k(\zeta_\ell)}(\epsilon) = 1 \quad \text{and} \quad \epsilon \equiv 1 \bmod a\}.$$

The following lemma will act as a sort of explicit version of Hilbert's Theorem 90 for our purposes.

Lemma 2.4. *For any $\epsilon \in E_{k(\zeta_\ell)}$ such that $N_k^{k(\zeta_\ell)}(\epsilon) = 1$, we have that the element*

$$\alpha := \zeta_\ell^a + \zeta_\ell^{a\tau}\epsilon + \cdots + \zeta_\ell^{a\tau^{\ell-2}}\epsilon^{1+\tau+\cdots+\tau^{\ell-3}}$$

is non-zero for some choice of $0 \leqslant a \leqslant \ell - 1$.

Proof. Let $\alpha(x) \in \mathbb{C}(x)$ be the rational function defined by

$$x \mapsto \frac{\zeta_\ell}{1 - x\zeta_\ell} + \frac{\zeta_\ell^\tau}{1 - x\zeta_\ell^\tau} \cdot \epsilon + \cdots + \frac{\zeta_\ell^{\tau^{\ell-2}}}{1 - x\zeta_\ell^{\tau^{\ell-2}}} \cdot \epsilon^{1+\tau+\cdots+\tau^{\ell-3}}.$$

Since $\alpha(x)$ has distinct poles, it follows that $\alpha(x)$ is not identically zero. On the other hand, we may view $\alpha(x) \in \mathbb{C}[[x]]$ and write

$$\alpha(x) = \sum_{a=0}^{\infty} \left(\zeta_\ell^{a+1} + \zeta_\ell^{(a+1)\tau}\epsilon + \cdots + \zeta_\ell^{(a+1)\tau^{\ell-2}}\epsilon^{1+\tau+\cdots+\tau^{\ell-3}}\right)x^a.$$

Note that the power series form of $\alpha(x)$ has periodic coefficients of the form of the claim. Since $\alpha(x)$ is not identically zero, the claim follows. $\square$

The following theorem is crucial for what follows. It is a generalization of a theorem of Rubin which itself is a generalization of a theorem of Thaine (see [19] and [14]).

Theorem 2.5. *Let $n \in \mathbb{N}$ and ℓ be an odd prime split completely in k such that $\ell \equiv 1 \bmod n$. Fix a prime λ of k above ℓ, and let $\mathcal{A} \subseteq \mathbb{Z}/n\mathbb{Z}[G]$ be the annihilator of the cokernel of the natural map*

$$\phi : E(\ell, \mathfrak{a}) \to \left(\mathfrak{o}_{k(\zeta_\ell)}/L\right)^\times \otimes \mathbb{Z}/n\mathbb{Z}\,,$$

where L is the product of all primes of $\mathfrak{o}_{k(\zeta_\ell)}$ above ℓ. Then $\mathcal{A}$ annihilates the class of λ in $\mathrm{Cl}(\mathfrak{a})/n\,\mathrm{Cl}(\mathfrak{a})$.

Proof. Let $\theta \in \mathcal{A}$, and let $u \in \mathfrak{o}_{k(\zeta_\ell)}$ such that

$$u \equiv s^{-1} \bmod \mathcal{L} \qquad \text{and} \qquad u \equiv 1 \bmod \mathcal{L}^\sigma \quad \text{for all } \sigma \neq \mathrm{id},$$

where $\mathcal{L}$ is the prime of $\mathfrak{o}_{k(\zeta_\ell)}$ above λ and $\langle s \rangle = \mathbb{Z}/\ell\mathbb{Z}^\times$. The element u has been chosen so that

$$\left(\mathfrak{o}_{k(\zeta_\ell)}/L\right)^\times = \langle u \bmod L \rangle_{\mathbb{Z}/(\ell-1)\mathbb{Z}[G]}.$$

Now, $u^\theta \equiv \eta^n \epsilon \bmod L$ for some $\eta \in k(\zeta_\ell)^\times$ coprime to ℓ and $\epsilon \in E(\ell, \mathfrak{a})$. Let $\langle \tau \rangle = \mathrm{Gal}(k(\zeta_\ell)/k)$ and

$$\alpha := \zeta_\ell + \zeta_\ell^\tau \epsilon + \zeta_\ell^{\tau^2} \epsilon^{1+\tau} + \cdots + \zeta_\ell^{\tau^{\ell-2}} \epsilon^{1+\tau+\cdots+\tau^{\ell-3}}.$$

By Lemma 2.4, we may assume $\alpha \neq 0$ (allowing for a small abuse of notation). Notice that

$$\begin{aligned}\epsilon\alpha^{\tau} &= \zeta_{\ell}^{\tau}\epsilon + \zeta_{\ell}^{\tau^2}\epsilon^{1+\tau} + \cdots + \zeta_{\ell}^{\tau^{\ell-1}}\epsilon^{1+\tau+\cdots+\tau^{\ell-2}} \\ &= \zeta_{\ell}^{\tau}\epsilon + \zeta_{\ell}^{\tau^2}\epsilon^{1+\tau} + \cdots + \zeta_{\ell} \\ &= \alpha,\end{aligned}$$

since $\tau^{\ell-1} = \mathrm{id}$ and $1 + \tau + \cdots + \tau^{\ell-2} = N_k^{k(\zeta_\ell)}$. Since $\epsilon \in E(\ell, \mathfrak{a})$ we have

$$\begin{aligned}\alpha &\equiv \zeta_{\ell} + \zeta_{\ell}^{\tau^2} + \cdots + \zeta_{\ell}^{\tau^{\ell-2}} \bmod \mathfrak{a} \\ &\equiv -1 \bmod \mathfrak{a}.\end{aligned}$$

Now, (α) is a non-zero ideal inert under $\mathrm{Gal}(k(\zeta_\ell)/k)$. Given a prime ideal $\mathfrak{p} \subset \mathfrak{o}$, the Galois group of $k(\zeta_\ell)/k$ acts transitively on the primes above $\mathfrak{p}$ in $\mathfrak{o}_{k(\zeta_\ell)}$. It follows that

$$(\alpha) = \mathfrak{b} \cdot \prod_{\sigma \in G} \mathcal{L}^{a_\sigma \sigma^{-1}},$$

where $0 \leqslant a_\sigma < \ell - 1$ and $\mathfrak{b}$ is an ideal of $\mathfrak{o}$. Taking norms of both sides of the above we get

$$\left(N_k^{k(\zeta_\ell)}(\alpha)\right) = \mathfrak{b}^{\ell-1} \cdot \lambda^{\sum a_\sigma \sigma^{-1}}.$$

Since $\alpha \equiv -1 \bmod \mathfrak{a}$, we have that $N_k^{k(\zeta_\ell)}(\alpha) \equiv 1 \bmod \mathfrak{a}$. By assumption we have $n \mid (\ell - 1)$, so $\sum a_\sigma \sigma^{-1} \bmod n\mathbb{Z}[G]$ annihilates the class of λ in $\mathrm{Cl}(\mathfrak{a})/n\,\mathrm{Cl}(\mathfrak{a})$.

It remains to relate the coefficients a_σ to θ. To that end, note that

$$a_\sigma = \mathrm{ord}_{\mathcal{L}^{\sigma^{-1}}}(\alpha) = \mathrm{ord}_{\mathcal{L}^{\sigma^{-1}}}(1 - \zeta_\ell)^{a_\sigma}.$$

Write $\alpha = \beta(1 - \zeta_\ell)^{a_\sigma}$ where β is a $\mathcal{L}^{\sigma^{-1}}$-unit. Without loss of generality, let's

suppose $\tau : \zeta_\ell \to \zeta_\ell^s$. The primes above ℓ are totally ramified in $k(\zeta_\ell)/k$. So τ acts trivially on $\mathcal{L}^{\sigma^{-1}}$-units modulo $\mathcal{L}^{\sigma^{-1}}$. Hence

$$\begin{aligned}\epsilon = \frac{\alpha}{\alpha^\tau} &= \frac{\beta(1-\zeta_\ell)^{a_\sigma}}{\beta^\tau(1-\zeta_\ell^\tau)^{a_\sigma}} \\ &\equiv \left(\frac{1-\zeta_\ell}{1-\zeta_\ell^\tau}\right)^{a_\sigma} \bmod \mathcal{L}^{\sigma^{-1}} \\ &\equiv (s^{-1})^{a_\sigma} \bmod \mathcal{L}^{\sigma^{-1}},\end{aligned}$$

the last equivalence holding because $\zeta_\ell \equiv 1 \bmod \mathcal{L}^{\sigma^{-1}}$. So

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

This gives us that $\epsilon \equiv u^{a_\sigma \sigma^{-1}} \bmod \mathcal{L}^{\sigma^{-1}}$, so

$$\epsilon \equiv u^{\sum a_\sigma \sigma^{-1}} \equiv \eta^{-n} u^\theta \mod L.$$

Hence $\sum a_\sigma \sigma^{-1} \equiv \theta \bmod n\mathbb{Z}[G]$. □

Remark 2.6. *Note that* $N_k^{k(\zeta_\ell)}(\alpha)$ *is totally positive. So more precisely we have* A *annihilates the class of* λ *in the narrow ray class group* $\mathrm{Cl}(\mathfrak{a}_\infty)/n\,\mathrm{Cl}(\mathfrak{a}_\infty)$ *where* $\mathfrak{a}_\infty$ *is the cycle* $\mathfrak{a}\prod_{v|\infty} v$.

Now, we set $A'_n(\mathfrak{a}) \leqslant A_n(\mathfrak{a})$ such that $A'_n(\mathfrak{a}) \simeq \mathrm{Gal}(H_n(\mathfrak{a})/(H_n(\mathfrak{a}) \cap k(\zeta_{p^n})))$. Let $\rho : \mathcal{O}/p^n\mathcal{O}[G] \otimes \mathcal{O} \to \mathcal{O}/p^n\mathcal{O}[G]$ be defined by $\theta \otimes x \mapsto \theta x$. The following theorem is essentially from Rubin [14]. The use of multiple primes is necessary to accommodate the larger ring of coefficients.

Theorem 2.7. *Assume that* S *is finite, fix* $\mathfrak{c} \in A'_n(\mathfrak{a})$*, and let*

$$\alpha : E_S/E_S^{p^n} \to (\mathcal{O}/p^n\mathcal{O})[G]$$

be a G*-module map. There exists infinitely many non-conjugate* j*-tuples of degree* 1 *primes* $\lambda_1, \ldots, \lambda_j \notin S$ *of* $\mathfrak{o}$ *such that* $(\lambda_i, \mathfrak{a}) = 1$ *and*

(i) the class of λ_i *in* $A_n(\mathfrak{a})$ *is* $\mathfrak{c}$*,*

(ii) $p^n \mid \ell_i - 1$ *where* $\ell_i = \lambda_i \cap \mathbb{Z}$*, and*

(iii) there exists an $\mathcal{O}/p^n\mathcal{O}[G]$*-module map*

$$f : \left((\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}/p^n\mathbb{Z}\right) \otimes \mathcal{O} \to \left(\mathcal{O}/p^n\mathcal{O}\right)[G]$$

such that the diagram

$$\begin{array}{ccc} E_S/E_S^{p^n} \otimes \mathcal{O} & \xrightarrow{\rho \circ (\alpha \otimes \mathrm{id})} & \left(\mathcal{O}/p^n\mathcal{O}\right)[G] \\ {\scriptstyle \phi \otimes \mathrm{id}}\downarrow & \nearrow_{f} & \\ \left((\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}/p^n\mathbb{Z}\right) \otimes \mathcal{O} & & \end{array}$$

commutes where $\mathfrak{L} = \prod_i \ell_i$ *and* $\phi : E_S/E_S^{p^n} \to (\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}/p^n\mathbb{Z}$ *is the natural map.*

Proof. Let $\mathcal{G} = \mathrm{Gal}\left(k(\zeta_{p^n})/\mathbb{Q}\right)$ and

$$\Gamma = \mathrm{Gal}\left(k(\zeta_{p^n}, E_S^{1/p^n}) \Big/ k(\zeta_{p^n}, (\ker \alpha)^{1/p^n})\right).$$

Let $\mathcal{G}$ act on Γ in the natural way: for $g \in \mathcal{G}$, $\gamma \in \Gamma$, define

$$g \cdot \gamma := \tilde{g}\gamma\tilde{g}^{-1},$$

where $\tilde{g}$ is a lift of g to $\mathrm{Gal}\left(k(\zeta_{p^n}, E_S^{1/p^n})/\mathbb{Q}\right)$. This action is well-defined since $\mathrm{Gal}\left(k(\zeta_{p^n}, E_S^{1/p^n})/k(\zeta_{p^n})\right)$ is abelian. Let $\gamma_1, \ldots, \gamma_j$ be a complete system of unique representatives of $\Gamma/\mathcal{G}$.

Since $H_n(\mathfrak{a})$ and $k(\zeta_{p^n}, E_S^{1/p^n})$ are linearly disjoint over $H_n(\mathfrak{a}) \cap k(\zeta_{p^n})$ by Proposition 2.1, we may choose $\beta_i \in \mathrm{Gal}\left(H_n(\mathfrak{a})k(\zeta_{p^n}, E_S^{1/p^n})/k\right)$ such that

$$\beta_i|_{H_n(\mathfrak{a})} = \mathfrak{c} \quad \text{and} \quad \beta_i|_{k(\zeta_{p^n}, E_S^{1/p^n})} = \gamma_i.$$

By the Chebotarev Density Theorem [9, Chap VIII §4 Theorem 10], there exists infinitely many degree 1 non-conjugate j-tuples of primes $\lambda_1, \ldots, \lambda_j \notin S$ such that $(\lambda_i, \mathfrak{a}) = 1$ and

$$\beta_i \in \left[\lambda_i,\ H_n(\mathfrak{a})k(\zeta_{p^n}, E_S^{1/p^n})\Big/k\right].$$

Since $\beta_i|_{k(\zeta_{p^n})} = \mathrm{id}$, we have $(\lambda_i,\ k(\zeta_{p^n})/k) = \mathrm{id}$. So ℓ_i splits completely in $k(\zeta_{p^n})$, hence $\ell_i \equiv 1 \bmod p^n$. We also have $(\lambda_i,\ H_n(\mathfrak{a})/k) = \mathfrak{c}$, so $\lambda_i \in \mathfrak{c}$. This proves (i) and (ii).

Now, let $\epsilon \in E_S/E_S^{p^n}$ such that $\epsilon^{1/p^n} \in k(\zeta_{p^n}, (\ker\alpha)^{1/p^n})$. Then

$$\langle\epsilon\rangle k(\zeta_{p^n})^{\times p^n}\Big/k(\zeta_{p^n})^{\times p^n} \subseteq (\ker\alpha)k(\zeta_{p^n})^{\times p^n}\Big/k(\zeta_{p^n})^{\times p^n}.$$

So $\epsilon = \beta^{p^n}u$ where $u \in \ker\alpha$ and $\beta \in k(\zeta_{p^n})^\times$. From the exact sequence of $\mathcal{H} := \mathrm{Gal}(k(\zeta_{p^n})/k)$-modules

$$1 \to W_{p^n} \to k(\zeta_{p^n})^\times \xrightarrow{p^n} k(\zeta_{p^n})^{\times p^n} \to 1$$

we obtain the exact sequence of $\mathcal{H}$-invariants

$$1 \to W_n^{\mathcal{H}} \to k(\zeta_{p^n})^{\times\mathcal{H}} \to k(\zeta_{p^n})^{\times p^n\mathcal{H}} \to H^1(\mathcal{H}, W_{p^n}).$$

Since F is real and p^n an odd prime power, we have

$$W_{p^n}^{\mathcal{H}} = 1$$
$$k(\zeta_{p^n})^{\times\mathcal{H}} = k^\times$$
$$k(\zeta_{p^n})^{\times p^n\mathcal{H}} = k \cap k(\zeta_{p^n})^{\times p^n}.$$

Since $\mathcal{H}$ is cyclic, say generated by σ, and $\ker(\sigma - 1)|_{W_{p^n}} = 1$, we also have

$$H^1(\mathcal{H}, W_{p^n}) = \ker(W_{p^n} \xrightarrow{N_k^{k(\zeta_\ell)}} W_{p^n})\Big/\mathrm{im}(W_{p^n} \xrightarrow{\sigma-1} W_{p^n}) = W_{p^n}\Big/W_{p^n} = 1,$$

hence $[k \cap k(\zeta_{p^n})^{\times p^n} : k^{\times p^n}] = 1$. It follows that $\beta \in k^\times$, and since $\beta^{p^n} \in E_S$, it must be that $\beta \in E_S$. So we have that $\epsilon \in \ker \alpha$. This allows us to make the following chain of equivalences:

$$\begin{aligned}
\epsilon \in \ker \alpha \text{ iff } & \epsilon^{1/p^n} \in k(\zeta_{p^n}, (\ker \alpha)^{1/p^n}) \\
& \text{iff } \Gamma \text{ fixes } k(\zeta_{p^n}, \epsilon^{1/p^n}) \\
& \text{iff } g \cdot \gamma_i \text{ fixes } k(\zeta_{p^n}, \epsilon^{1/p^n}) \text{ for all } g \in \mathcal{G}, i = 1, \ldots, j \\
& \text{iff } \lambda^\sigma \text{ splits completely in } k(\epsilon^{1/p^n}) \text{ for all } \sigma \in G, i = 1, \ldots, j \\
& \text{iff } x^{p^n} - \epsilon \text{ splits completely } \bmod \lambda_i^\sigma \text{ for all } \sigma \in G, i = 1, \ldots, j \\
& \text{iff } \epsilon \in \ker \phi.
\end{aligned}$$

Now, since $\mathcal{O}$ is a flat $\mathbb{Z}$-module, we get the following exact sequences

$$\begin{aligned}
1 \to (\ker \alpha) \otimes \mathcal{O} \to E_S/E_S^{p^n} \otimes \mathcal{O} &\xrightarrow{\alpha \otimes \mathrm{id}} \left(\mathcal{O}/p^n\mathcal{O}\right)[G] \otimes \mathcal{O} \\
1 \to (\ker \alpha) \otimes \mathcal{O} \to E_S/E_S^{p^n} \otimes \mathcal{O} &\xrightarrow{\phi \otimes \mathrm{id}} \left((\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}/p^n\mathbb{Z}\right) \otimes \mathcal{O}.
\end{aligned}$$

So the G-module map

$$\tilde{f} : \rho \circ (\alpha \otimes \mathrm{id}) \circ (\phi \otimes \mathrm{id})^{-1} : \mathrm{im}(\phi \otimes \mathrm{id}) \to \left(\mathcal{O}/p^n\mathcal{O}\right)[G].$$

is well-defined. By Proposition 2.3, $\tilde{f}$ lifts to a G-module map

$$f : \left((\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}/p^n\mathbb{Z}\right) \otimes \mathcal{O} \to \left(\mathcal{O}/p^n\mathcal{O}\right)[G]$$

such that $f \circ (\phi \otimes \mathrm{id}) = \rho \circ (\alpha \otimes \mathrm{id})$. □

Now we make the following definition.

Definition 2.8. *For an ideal $\mathfrak{a} \subseteq \mathfrak{o}$, let $\mathcal{D}(\mathfrak{a})$ denote the set of numbers $\delta \in k^\times$ such that for all but finitely many primes ℓ split completely in k, we have that there is an $\epsilon \in E(\ell, \mathfrak{a})$ such that for all $\sigma \in G$,*

$$\epsilon \equiv \delta \mod \mathcal{L}^\sigma$$

where $\mathcal{L} \subset \mathfrak{o}_{k(\zeta_\ell)}$ *is a prime ideal such that* $\mathcal{L} \mid \ell$*. We call* $\mathcal{D}(\mathfrak{a})$ *the* $\mathfrak{a}$*-special numbers of* k*. Let*

$$\mathcal{C}(\mathfrak{a}) := \mathcal{D}(\mathfrak{a}) \cap E \qquad \textit{and} \qquad \mathcal{C}_S(\mathfrak{a}) := \mathcal{D}(\mathfrak{a}) \cap E_S.$$

We call $\mathcal{C}(\mathfrak{a})$ *and* $\mathcal{C}_S(\mathfrak{a})$ *the* $\mathfrak{a}$*-special units of* k *and the* $\mathfrak{a}$*-special* S*-units of* k*, respectively.*

Note that $\mathcal{D}(\mathfrak{o})$ is precisely Rubin's special numbers (see [14]). We may now prove the main theorem of this chapter. It is the ray class analogue of theorem of Rubin [14].

Theorem 2.9. *Suppose* S *is finite, and let* $\alpha : E_S/E_S^{p^n} \to \left(\mathcal{O}/p^n\mathcal{O}\right)[G]$ *be a* G*-module map. Then*

$$\alpha\left(\mathcal{C}_S(\mathfrak{a})E_S^{p^n}/E_S^{p^n}\right) \quad \textit{annihilates} \quad A_n'(\mathfrak{a}) \otimes \mathcal{O}.$$

Proof. Let $\delta \in \mathcal{C}_S(\mathfrak{a})$ and $\mathfrak{c} \in A_n'(\mathfrak{a})$. Let $\lambda_1, \ldots, \lambda_j \notin S$ be as in Theorem 2.7 such that for each i, there exists $\epsilon_i \in E(\ell_i, \mathfrak{a})$ such that

$$\epsilon_i \equiv \delta \bmod \mathcal{L}_i^\sigma \quad \text{for all } \sigma \in G,$$

where $\mathcal{L}_i \subset \mathfrak{o}_{k(\zeta_{\ell_i})}$ is the prime above λ_i. Set

$$\mathfrak{L} := \prod_{i=1}^{j} \ell_i \qquad \text{and} \qquad L_i := \prod_{\sigma \in G} \mathcal{L}_i^\sigma.$$

Since the primes of $\mathfrak{o}$ above ℓ_i are totally ramified in $k(\zeta_{\ell_i})$, we have that

$$(\mathfrak{o}/\mathfrak{L})^\times \simeq \prod_{i=1}^{j} (\mathfrak{o}/\ell_i)^\times \simeq \prod_{i=1}^{j} \left(\mathfrak{o}_{k(\zeta_{\ell_i})}/L_i\right)^\times.$$

Let $u_i \in \mathfrak{o}$ such that

$$u_i \equiv s_i^{-1} \bmod \lambda_i \qquad \text{and} \qquad u_i \equiv 1 \bmod \lambda_i^\sigma \quad \text{for all } \sigma \in G, \sigma \neq \mathrm{id},$$

where $\langle s_i \rangle = \mathbb{Z}/\ell_i\mathbb{Z}^\times$, as in Theorem 2.5. Note that

$$\langle u_i \bmod L_i \rangle_{(\mathbb{Z}/(\ell_i - 1)\mathbb{Z})[G]} \simeq \left(\mathfrak{o}_{k(\zeta_{\ell_i})}/L_i\right)^\times.$$

Let $\theta_i \in \mathbb{Z}/p^n\mathbb{Z}\,[G]$ such that

$$\begin{aligned}(\delta \bmod L_i) \otimes 1 &= (\epsilon_i \bmod L_i) \otimes 1 \\ &= (u_i^{\theta_i} \bmod L_i) \otimes 1 \in \left(\mathfrak{o}_{k(\zeta_{\ell_i})}/L_i\right)^\times \otimes \mathbb{Z}/p^n\mathbb{Z}\,.\end{aligned}$$

Notice that θ_i is an annihilator of the cokernel of the map

$$E(\ell_i, \mathfrak{a}) \to \left(\mathfrak{o}_{k(\zeta_{\ell_i})}/L_i\right)^\times \otimes \mathbb{Z}/p^n\mathbb{Z}\,.$$

So θ_i annihilates the class of λ_i in $\mathrm{Cl}(\mathfrak{a})/p^n\,\mathrm{Cl}(\mathfrak{a})$ by Theorem 2.5. But $\lambda_i \in \mathfrak{c}$ by Theorem 2.7, so θ_i annihilates $\mathfrak{c}$. Also,

$$\begin{aligned}\rho \circ (\alpha \otimes \mathrm{id})((\delta \bmod E_S^{p^n}) \otimes 1) &= f\big((\delta \bmod \ell_i) \otimes 1 \otimes 1\big) && \text{by Theorem 2.7} \\ &= f \circ \left(\prod_{i=1}^{j} (u_i^{\theta_i} \bmod L_i) \otimes 1 \otimes 1\right) \\ &= \sum_{i=1}^{j} \theta_i f\big((u_i \bmod L_i) \otimes 1 \otimes 1\big).\end{aligned}$$

Hence, for any $x \in \mathcal{O}$, we have $\alpha(\delta \bmod E_S^{p^n}) = \rho \circ (\alpha \otimes \mathrm{id})((\delta \bmod E_S^{p^n}) \otimes 1)$ so

$$\begin{aligned}(\mathfrak{c} \otimes x)^{\alpha(\delta \bmod E_S^{p^n})} &= (\mathfrak{c} \otimes x)^{\sum \theta_i f((u_i \bmod L_i) \otimes 1 \otimes 1)} \\ &= \sum \mathfrak{c}^{\theta_i} \otimes x \cdot f((u_i \bmod L_i) \otimes 1 \otimes 1) \\ &= 0.\end{aligned}$$

This completes the proof of the theorem. □

Now, let $A'(\mathfrak{a}) := \varinjlim A'_n(\mathfrak{a})$. We easily obtain the following more general corollary.

Corollary 2.10. *Let $\alpha : E_S \to \mathcal{O}[G]$ be a G-module map. Then*

$$\alpha(\mathcal{C}_S(\mathfrak{a})) \quad \textit{annihilates} \quad A'(\mathfrak{a}) \otimes \mathcal{O}.$$

Proof. If the corollary is true for every finite subset of S, then it's true for S itself. So we might as well assume S is finite. The corollary now follows immediately from Theorem 2.9 by letting $n \to \infty$. □

2.3 On the Defect $A'(\mathfrak{a})$

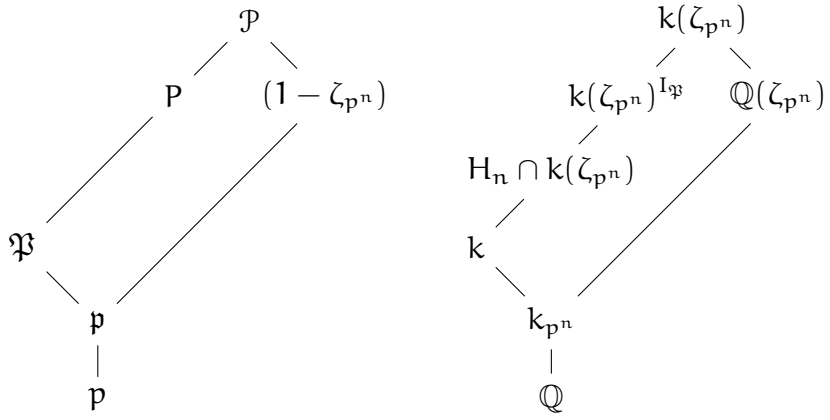
We'd like to know conditions under which $A'(\mathfrak{a}) = A(\mathfrak{a})$ to get a fuller annihilation result. We almost immediately obtain the following.

Proof of Theorem 1.8. Let $H'_n(\mathfrak{a})$ and $H'(\mathfrak{a})$ be the fixed fields of $A'_n(\mathfrak{a})$ and $A'(\mathfrak{a})$, respectively. From the start, we notice that $H'(\mathfrak{a})/\mathbb{Q}$ is abelian. So G acts trivially on $A(\mathfrak{a})/A'(\mathfrak{a})$. It follows from Corollary 2.10 that

$$R_0 \cdot \alpha(\mathcal{C}_S(\mathfrak{a})) \qquad \text{annihilates} \qquad A(\mathfrak{a}) \otimes \mathcal{O} = \mathrm{Cl}(\mathfrak{a}) \otimes \mathcal{O},$$

where $\alpha : E_S \to \mathcal{O}[G]$ is a G-module map and R_0 is the augmentation ideal of $\mathcal{O}[G]$. □

Now, let $\mathcal{P}$ be a fixed prime of $k(\zeta_{p^n})$ above p, $\mathfrak{P} = \mathcal{P} \cap k$, and $I_{\mathfrak{P}}$ the inertia subgroup for $\mathfrak{P}$ in $\mathrm{Gal}(k(\zeta_{p^n})/k)$. We have the following field diagram with corresponding diagram of prime ideals below $\mathcal{P}$ on the left:



Proposition 2.11. *Let $e(\mathfrak{P} : \mathfrak{p})$ denote the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, and likewise for the other primes below $\mathcal{P}$. We have the following divisibilities:*

$$[H_n \cap k(\zeta_{p^n}) : k] \mid \textit{p-part of } e(\mathfrak{P} : \mathfrak{p}) \mid \textit{p-part of } e(\mathfrak{P} : p).$$

Proof. Since p is totally ramified in $\mathbb{Q}(\zeta_{p^n})$ and $e(P : \mathfrak{P}) = 1$, we have

$$e(\mathcal{P} : p) = e(\mathcal{P} : P)e(\mathfrak{P} : p) \geqslant e((1 - \zeta_{p^n}) : p).$$

So

$$\frac{e((1 - \zeta_{p^n}) : p)}{e(\mathfrak{P} : p)} \leqslant e(\mathcal{P} : P).$$

On the other hand, we could solely consider degrees and obtain

$$[H_n \cap k(\zeta_{p^n}) : k]e(\mathcal{P} : P) \leqslant [k(\zeta_{p^n}) : k] = \frac{e((1 - \zeta_{p^n}) : p)}{e(\mathfrak{p} : p)}.$$

Combining the above inequalities we have

$$\frac{e((1 - \zeta_{p^n}) : p)}{e(\mathfrak{P} : p)} \leqslant e(\mathcal{P} : P) \leqslant \frac{e((1 - \zeta_{p^n}) : p)}{e(\mathfrak{p} : p)[H_n \cap k(\zeta_{p^n}) : k]}$$

whence

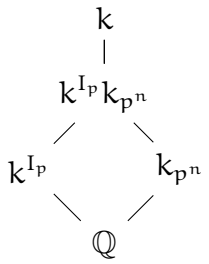
$$[H_n \cap k(\zeta_{p^n}) : k] \leqslant \frac{e(\mathfrak{P} : p)}{e(\mathfrak{p} : p)} = e(\mathfrak{P} : \mathfrak{p}).$$

Now, since $[H_n : k]$ is a p-power, so is $[H_n \cap k(\zeta_{p^n}) : k]$. On the other hand, $e(\mathfrak{P} : \mathfrak{p}) = p^l m$ for some integers $l \geqslant 0$ and $m \geqslant 1$ where $(m, p) = 1$. In fact, $m \mid p-1$ since $e(\mathfrak{P} : \mathfrak{p})$ divides the ramification index of p in $\mathbb{Q}(\zeta_m)$ where m is the conductor of k. It follows that $[H_n \cap k(\zeta_{p^n}) : k] \leqslant p^l$, so $[H_n \cap k(\zeta_{p^n}) : k] \mid e(\mathfrak{P} : \mathfrak{p})$. This completes the proof of the proposition. □

The second divisibility of the above proposition tells us that if p is tamely ramified in k, then $A'_n = A_n$ for all n. We use the first divisibility in the proposition to obtain

Proposition 2.12. *Suppose* $k = k'k''$ *where* $k' \subseteq \mathbb{Q}(\zeta_{p^m})^+$ *and* $k'' \subseteq \mathbb{Q}(\zeta_d)^+$ *where* $(p, d) = 1$. *Then* $A'_n = A_n$ *for all* n.

Proof. Let $I_p \leqslant G$ be the inertia subgroup for p. Consider the following diagram:



Let $n \geqslant m$, then $k' = k_{p^n}$ and $k'' \subseteq k^{I_p}$. So $k = k^{I_p}k_{p^n}$. Since the prime of k_{p^n} above p is unramified in $k^{I_p}k_{p^n}$, it follows that $e(\mathfrak{P} : \mathfrak{p}) = 1$. □

Lemma 2.13. *Let* $T_{\mathfrak{P}} \leqslant \mathrm{Gal}\,(H'_n(\mathfrak{a})/k)$ *be the inertia subgroup for* $\mathfrak{P}$. *Then* $T_{\mathfrak{P}} = \mathrm{Gal}\,(H'_n(\mathfrak{a})/H'_n)$.

Proof. The primes above p are the only primes ramifying in $H'_n(\mathfrak{a})/k$, moreover, since $H'_n(\mathfrak{a})/\mathbb{Q}$ is abelian, it follows that $T_{\mathfrak{P}} = T_{\mathfrak{P}'}$ where $\mathfrak{P}'$ is any prime of k over p. Hence

$$H'_n = H'_n(\mathfrak{a})^{T_p},$$

and the lemma follows. □

Combining all the above gives a sufficient condition for $A'_n(\mathfrak{a}) = A_n(\mathfrak{a})$:

Corollary 2.14. *If* k *satisfies any one of the following*

(i) p *is tamely ramified, or*

(ii) $k = k'k''$ *where* $k' \subseteq \mathbb{Q}(\zeta_{p^j})^+$, $k'' \subseteq \mathbb{Q}(\zeta_d)^+$, *and* $(p, d) = 1$,

and the product of the primes of k *dividing* p *does not divide* $\mathfrak{a}$, *then* $\alpha(\mathcal{C}_S(\mathfrak{a}))$ *annihilates* $A(\mathfrak{a}) \otimes \mathcal{O}$. *Otherwise* $R_0 \cdot \alpha(\mathcal{C}_S(\mathfrak{a}))$ *annihilates* $A(\mathfrak{a}) \otimes \mathcal{O}$.

Proof. Given the condition on $\mathfrak{a}$, Lemma 2.13 gives us that $H'_n(\mathfrak{a}) = H'_n$. If k satisfies (i) or (ii), then $H'_n = k$ by Proposition 2.11 or Proposition 2.12, respectively. So $H'_n(\mathfrak{a}) = k$, and the corollary follows by Corollary 2.10. □

CHAPTER 3

ON $\mathfrak{A}$-CYCLOTOMIC NUMBERS

Given the results of Chapter 2, a natural question arises: Can we find explicit examples of $\mathfrak{a}$-special numbers? To answer this question, we begin with a definition for $\mathfrak{a}$-cyclotomic numbers which were originally discovered by Schmidt [15].

Definition 3.1. *Let $\mathfrak{a} \subseteq \mathfrak{o}_k$ be an ideal. Let $d(\mathfrak{a}) = d \in \mathbb{N}$ be the minimal integer such that $\mathfrak{a} \mid d$, and let $\overline{d}$ denote the product of all prime divisors of d. For $n > 1$, $n \nmid \overline{d}$ we define*

$$\delta_{n,d} := N_{k_n}^{\mathbb{Q}(\zeta_n)} \prod_{t \mid \overline{d}} (1 - \zeta_n^t)^{\mu(t)d/t},$$

where μ is the Möbius function:

$$\mu(t) = \begin{cases} (-1)^j & \text{if } t = p_1 \cdots p_j,\ p_i \text{ primes} \\ 1 & \text{if } t = 1 \\ 0 & \text{else.} \end{cases}$$

Let $D(\mathfrak{a}) := \langle \delta_{n,d} : n > 1, n \nmid \overline{d} \rangle_{\mathbb{Z}[G]}$. We call $D(\mathfrak{a})$ the $\mathfrak{a}$-cyclotomic numbers of k, and $C_S(\mathfrak{a}) := D(\mathfrak{a}) \cap E_S$ the $\mathfrak{a}$-cyclotomic S-units.

Remark 3.2. *Note that $\pm D(1)$ and $\pm C(1)$ are precisely the sets of cyclotomic numbers and units, respectively, as defined by Sinnott [16]. Also, since $D(\mathfrak{a}) = D(d(\mathfrak{a}))$, these modules are most precise when $\mathfrak{a} \in \mathbb{N}$.*

Theorem 3.3. *If $\delta \in D(\mathfrak{a})$, then $\pm\delta \in \mathcal{D}(\mathfrak{a})$, i.e., $\pm D(\mathfrak{a}) \subseteq \mathcal{D}(\mathfrak{a})$.*

Proof. It suffices to show that $\pm\delta_{n,d} \in \mathcal{D}(\mathfrak{a})$ for all $n > 1$ and $n \nmid d = d(\mathfrak{a})$ since these numbers generate $D(\mathfrak{a})$. Let ℓ be a rational prime split completely in k such that $(\ell, nd) = 1$. Define

$$\pm\epsilon_{n,d} = N_{k_n(\zeta_\ell)}^{\mathbb{Q}(\zeta_{n\ell})} \prod_{t|\overline{d}} (\zeta_\ell^t - \zeta_n^t)^{\mu(t)d/t} \in k(\zeta_\ell).$$

Let λ be a prime of k above ℓ and $\mathcal{L}$ the prime of $k(\zeta_\ell)$ above λ. Since

$$(1-\zeta_\ell)\mathfrak{o}_{k(\zeta_\ell)} = \prod_{\sigma\in G} \mathcal{L}^\sigma,$$

it follows that $\zeta_\ell \equiv 1 \bmod \mathcal{L}^\sigma$ for all $\sigma \in G$, hence $\pm\epsilon_{n,d} \equiv \pm\delta_{n,d} \bmod \mathcal{L}^\sigma$ for all $\sigma \in G$. Now, we note

$$\begin{aligned} N_{k_n}^{k_n(\zeta_\ell)}(\pm\epsilon_{n,d}) &= N_{k_n}^{\mathbb{Q}(\zeta_n)} N_{\mathbb{Q}(\zeta_n)}^{\mathbb{Q}(\zeta_{n\ell})} \prod_{t|\overline{d}} (\zeta_\ell^t - \zeta_n^t)^{\mu(t)d/t} \\ &= N_{k_n}^{\mathbb{Q}(\zeta_n)} \prod_{t|\overline{d}} \left(\frac{\zeta_n^{t\ell}-1}{\zeta_n^t - 1}\right)^{\mu(t)d/t} \\ &= \delta_{n,d}^{[\ell,k]-1}. \end{aligned}$$

Since ℓ splits completely in k, it follows that $[\ell, k] = 1$ hence $N_{k_n}^{k_n(\zeta_\ell)}(\epsilon_{n,d}) = N_k^{k(\zeta_\ell)}(\epsilon_{n,d}) = 1$.

Now, let $p \mid d$ be a prime, let p^j be the p-primary part of d, and let $d_p = d/p^j$. Then

$$\epsilon_{n,d} = N_{k_n(\zeta_\ell)}^{\mathbb{Q}(\zeta_{n\ell})} \prod_{t|\frac{\overline{d}}{p}} \left[\frac{(\zeta_\ell^t - \zeta_n^t)^p}{(\zeta_\ell^{tp} - \zeta_n^{tp})}\right]^{p^{j-1}\mu(t)d_p/t}.$$

For all $t \mid \overline{d}/p$ we have that ζ_ℓ^t and ζ_ℓ^{tp} are primitive ℓ-th roots of unity since $(\ell, nd) = 1$, moreover, ζ_n^t and ζ_n^{tp} are not equal to 1 since $n \nmid \overline{d}$. It follows that $(\zeta_\ell^t - \zeta_n^t)$ and $(\zeta_\ell^{tp} - \zeta_n^{tp})$ are units in $\mathbb{Z}[\zeta_{n\ell}]$, hence $\epsilon_{n,d} \in E_{k(\zeta_\ell)}$. We also have

$$\frac{(\zeta_\ell^t - \zeta_n^t)^p}{\zeta_\ell^{tp} - \zeta_n^{tp}} \equiv 1 \bmod p$$

from which it follows that

$$\left[\frac{(\zeta_\ell^t - \zeta_n^t)^p}{\zeta_\ell^{tp} - \zeta_n^{tp}}\right]^{p^{j-1}} \equiv 1 \bmod p^j,$$

whence $\epsilon_{n,d} \equiv 1 \bmod p^j$. Since p was an arbitrary divisor of d, it follows that $\epsilon_{n,d} \equiv 1 \bmod d$, hence $\epsilon_{n,d} \equiv 1 \bmod \mathfrak{a}$. Therefore, we have $\epsilon_{n,d} \in E(\ell, \mathfrak{a})$, as desired. □

Remark 3.4. *Note that this proves Theorem 1.9.*

Let $E_{(d)}$ denote the group of units of k congruent to 1 modulo d, and let $C_{(d)} = D(d) \cap E_{(d)}$. Schmidt [15, Satz 3] has computed the index $[E_{(d)} : C_{(d)}]$ by using the methods of Sinnott [16, Theorem 4.1] to compute $[E : C]$. By the same means, we intend to compute the index $[E : C(d)]$ since it is related to the index of annihilators of $A(d) \otimes \mathcal{O}$ generated by the images of $C(d)$ via G-module maps (which we intend to compute in the sequel). This index is, in general, larger than the index computed in [15, Satz 3], but has the advantage of being somewhat more simple.

For the remainder of this chapter, we adopt some notation common to [16] and [15] since we follow these arguments very closely. Nevertheless, this section will be largely self-contained since there are some subtle differences in this setting that would be difficult to separate from [16] and [15]. Let $l : k^\times \to \mathbb{R}[G]$ be the map defined by

$$\alpha \mapsto -\frac{1}{2} \sum_{\sigma \in G} \log |\alpha^\sigma| \sigma^{-1}.$$

We let

$$\omega' = \sum_{\chi \neq 1} L'(0, \overline{\chi}) e_\chi,$$

where $L'(s, \overline{\chi})$ is the first derivative of the Dirichlet L-function attached to $\overline{\chi}$, the complex conjugate of χ. For a Galois extension of number fields K/k, we let

$G(K/k) = \mathrm{Gal}(K/k)$. For a finite subset X of G, we let $s(X)$ denote the sum of the elements of X in the group ring $\mathbb{Z}[G]$. For every prime p, we let

$$e_p = \frac{1}{\#T_p} s(T_p)$$

where T_p is the inertia subgroup for p in G.

We also adopt the following generalized index notation from Sinnott [16]. Suppose L and M are free $\mathbb{Z}$-modules of equal rank in $\mathbb{R}[G]$. Let T be an automorphism of the $\mathbb{R}$-vector space $\mathbb{R}[G]$ such that $T(L) = M$. Define

$$(L : M) := |\det(T)|,$$

and note that this index is independent of T. If $M \subseteq L$, then the index $(L : M)$ coincides with the usual subgroup index $[L : M]$.

We need the following result due to Sinnott [16, Proposition 4.2]:

Proposition 3.5 (Sinnott). *For $n > 1$ and t a positive proper divisor of n,*

$$(1 - e_1)l(N_{k_n}^{\mathbb{Q}(\zeta_n)}(1 - \zeta_n^t)) = \omega' \cdot \alpha_{\frac{n}{t},n}$$

where

$$\alpha_{\frac{n}{t},n} := [\mathbb{Q}(\zeta_n) : k_n\mathbb{Q}(\zeta_{\frac{n}{t}})] \cdot s(\mathrm{Gal}(k/k_{n/t})) \cdot \prod_{p|\frac{n}{t}} (1 - (p, k/\mathbb{Q})^{-1} e_p).$$

The product runs over all prime divisors p of n/t.

Suppose $p \mid \overline{d}/(\overline{d}, n)$ so that

$$\delta_{n,d} = N_{k_n}^{\mathbb{Q}(\zeta_n)} \prod_{t|\frac{\overline{d}}{p}} \left[\frac{(1 - \zeta_n^t)^p}{1 - \zeta_n^{tp}}\right]^{\mu(t)\frac{d}{tp}} = \delta_{n,\overline{d}/p}^{(d/\overline{d})\cdot(p-(p,k/\mathbb{Q})e_p)}.$$

Note that $(p, k/\mathbb{Q})e_p = (p, k_n/\mathbb{Q})$ since $(p, n) = 1$. By repeated application, we get the following lemma.

Lemma 3.6. *If* $n > 1$ *and* $n \nmid \overline{d}$*, then*

$$\delta_{n,d} = \delta_{n,(\overline{d},n)}^{(d/\overline{d})\cdot\gamma_{\overline{d}/(\overline{d},n)}} \quad \textit{where} \quad \gamma_t := \prod_{p|t}(p - (p, k/\mathbb{Q})e_p).$$

The product in γ_t *runs over all prime divisors* p *of* t*.*

This is essentially [15, Lemma 3.5]. Combining Lemma 3.6 and Proposition 3.5 we get the following proposition.

Proposition 3.7. *If* $n \geqslant 1$ *and* $n \nmid \overline{d}$*, then*

$$(1 - e_1)l(\delta_{n,d}) = \omega' \cdot v_{n,d},$$

where

$$v_{n,d} := \frac{d}{\overline{d}} \cdot \gamma_{\overline{d}/(\overline{d},n)} \cdot \sum_{t|(\overline{d},n)} \mu(t) \cdot \frac{(\overline{d},n)}{t} \cdot \alpha_{\frac{n}{t},n}.$$

We define $U(d)$ *to be the* $\mathbb{Z}[G]$*-module generated by* $v_{1,d}$ *and* $v_{n,d}$ *for all* $n > 1$*,* $n \nmid \overline{d}$*.*

Remark 3.8. *Note that* $U(d)$ *coincides with Sinnott's* U *if* $d = 1$ *(see [16, Corollary to Proposition 2.2 and Proposition 2.3]).*

The plan is to compute $[E : C(d)]$ by factoring it into various parts, e.g., we will show

$$[E : C(d)] := 2[l(E) : l(C(d))] = 2\big(l(E) : R_0\big) \cdot \big(R_0 : l(C(d))\big),$$

where R_0 denotes the trace zero subspace of $R := \mathbb{Z}[G]$ (note that this is a departure from the notation used in the previous chapter). With malice aforethought, the next few lemmas and propositions will help us compute the indices of the factors of $[E : C(d)]$.

For each character $\chi \in \widehat{G}$, let f_χ denote the conductor of χ, k_χ the field belonging to χ, and ρ_χ the induced ring homomorphism $\mathbb{C}[G] \to \mathbb{C}$ defined by

$$\sum_{\sigma\in G} a_\sigma \sigma \mapsto \sum_{\sigma\in G} a_\sigma \chi(\sigma).$$

Note that

$$\begin{aligned}\rho_\chi(s(\mathrm{Gal}(k/k_n))) \neq 0 &\Leftrightarrow \mathrm{Gal}(k/k_n) \subseteq \ker\chi = \mathrm{Gal}(k/k_\chi)\\ &\Leftrightarrow k_\chi \subseteq k_n \subseteq \mathbb{Q}(\zeta_n)\\ &\Leftrightarrow f_\chi \mid n.\end{aligned}$$

If $f_\chi \mid n$, then $\rho_\chi(s(\mathrm{Gal}(k/k_n))) = \#\mathrm{Gal}(k/k_n)$. Moreover, $\rho_\chi\big((p,k/\mathbb{Q})e_p\big) = \chi\big((p,k/\mathbb{Q})\big)$, and for all $t \geqslant 1$ we have

$$\rho_\chi(\gamma_t) = \prod_{p\mid t}\Big(p - \chi\big((p,k/\mathbb{Q})\big)\Big) \neq 0$$

since $p - \chi\big((p,k/\mathbb{Q})\big) \neq 0$ for any χ or p.

Proposition 3.9. *The $\mathbb{Z}$-module $U(d)$ is free and* $\mathrm{rank}_{\mathbb{Z}}\, U(d) = \#G$.

Proof. Sinnott [16, Proposition 2.3] has shown that $U(1)$ is finitely generated. In particular, $U(1)$ is generated by $\alpha_{f,f}$ where f varies over the divisors of the conductor of k. This shows that $U(d) \subseteq U(1)$, and therefore is also finitely generated. Hence, $U(d)$ is free of some finite rank less than or equal to $\#G$. To get equality it suffices to show that $\rho_\chi(U(d)) \neq 0$ for each $\chi \in \widehat{G}$.

If χ is the trivial character, then

$$\rho_\chi(v_{1,d}) = \frac{d}{\overline{d}} \cdot \rho_\chi(\gamma_{\overline{d}}) \cdot \rho_\chi(\alpha_{1,1}) = \frac{d}{\overline{d}} \cdot \rho_\chi(\gamma_{\overline{d}}) \cdot \#G \neq 0.$$

Suppose χ is non-trivial, and let ℓ be a prime such that $(\ell, f_\chi d) = 1$ and

$$\chi((\ell, k_\chi/\mathbb{Q})) \neq 1.$$

Then $v_{\ell f_\chi, d} \in U(d)$, and for every $t \mid (\overline{d}, \ell f_\chi)$, we have $f_\chi \nmid \ell f_\chi/t$ unless $t = 1$. So

$$\rho_\chi(v_{\ell f_\chi, d}) = \frac{d}{\overline{d}} \cdot \rho_\chi(\gamma_{\overline{d}/(\overline{d},\ell f_\chi)}) \cdot (\overline{d}, \ell f_\chi) \cdot \rho_\chi(\alpha_{\ell f_\chi, \ell f_\chi})$$

Since ℓ is coprime to f_χ, it follows that χ is trivial on T_ℓ. Hence

$$\rho_\chi(\alpha_{\ell f_\chi, \ell f_\chi}) = [\mathbb{Q}(\zeta_{\ell f_\chi}) : k_{\ell f_\chi}] \cdot \#G(k/k_{\ell f_\chi}) \cdot (1 - \overline{\chi}((\ell, k_\chi/\mathbb{Q})) \neq 0,$$

consequently $\rho_\chi(\upsilon_{\ell f_\chi, d}) \neq 0$. Hence, for each $\chi \in \widehat{G}$ we have $\rho_\chi(U(d)) \neq 0$. This proves the proposition. □

Lemma 3.10. *The set* $D(d)$ *is totally positive.*

Proof. Since k is real, k_n is real for every $n \in \mathbb{N}$. So $k_n \subseteq \mathbb{Q}(\zeta_n)^+$ for every $n \in \mathbb{N}$. Now, for any $n, t \in \mathbb{N}$ such that $n \nmid t$, we have

$$N_{k_n}^{\mathbb{Q}(\zeta_n)}(1 - \zeta_n^t) = N_{k_n}^{\mathbb{Q}(\zeta_n)^+}\big((1 - \zeta_n^t)(1 - \zeta_n^{-t})\big) > 0$$

Since $D(d)$ is generated by elements of the above type, the lemma follows. □

We write $\mathbb{Q}^{>0}$ to denote the multiplicative group of positive rational numbers.

Proposition 3.11. *Let*

$$Q(d) := \{a^{\phi(d)/[k_{\overline{d}}:\mathbb{Q}]} : a \in \mathbb{Q}^{>0}, (a, d) = 1, (a, k_{\overline{d}}/\mathbb{Q}) = \mathrm{id}\},$$

where $\phi(d) = \#\mathbb{Z}/d\mathbb{Z}^\times$. *Then* $Q(d) \subseteq D(d) \cap \mathbb{Q}$.

Proof. Let p be a prime such that $p \nmid d$. Then for any $t \mid \overline{d}$, $t < \overline{d}$ we have

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{\overline{d}})}^{\mathbb{Q}(\zeta_{\overline{dp}})}(1 - \zeta_{p\overline{d}}^t) &= N_{\mathbb{Q}(\zeta_{\overline{d}})}^{\mathbb{Q}(\zeta_{\overline{dp}})}(1 - \zeta_{\overline{d}}^{ty}\zeta_p^{tx}) \qquad \text{for} \quad x\overline{d} + yp = 1 \\ &= \frac{1 - \zeta_{\overline{d}}^{typ}}{1 - \zeta_{\overline{d}}^{ty}} \\ &= (1 - \zeta_{\overline{d}}^{ty})^{(p, \mathbb{Q}(\zeta_{\overline{d}})/\mathbb{Q}) - 1} \\ &= (1 - \zeta_{\overline{d}}^{t})^{1 - (p, \mathbb{Q}(\zeta_{\overline{d}})/\mathbb{Q})^{-1}}. \end{aligned}$$

On the other hand,

$$N_{k_{\overline{d}}}^{\mathbb{Q}(\zeta_{\overline{dp}})}(1 - \zeta_p) = N_{k_{\overline{d}}}^{\mathbb{Q}(\zeta_{\overline{d}})}(p) = p^{[\mathbb{Q}(\zeta_{\overline{d}}):k_{\overline{d}}]}.$$

Since $(d/\overline{d})[\mathbb{Q}(\zeta_{\overline{d}}) : k_{\overline{d}}] = \phi(d)/[k_{\overline{d}} : \mathbb{Q}]$, we have

$$N_{k_{\overline{d}}}^{k_{\overline{d}p}}(\delta_{\overline{d}p,d}) = \Bigg(\underbrace{N_{k_{\overline{d}}}^{\mathbb{Q}(\zeta_{\overline{d}p})} \prod_{\substack{t|\overline{d} \\ t<\overline{d}}} (1-\zeta_{\overline{d}p}^{t})^{\mu(t)d/t}}_{=\alpha \in k_{\overline{d}}} \Bigg)^{1-(p,k_{\overline{d}}/\mathbb{Q})^{-1}} \cdot p^{\pm\phi(d)/[k_{\overline{d}}:\mathbb{Q}]}$$
$$= \alpha^{1-(p,k/\mathbb{Q})^{-1}} \cdot p^{\pm\phi(d)/[k_{\overline{d}}:\mathbb{Q}]}.$$

Note that although p may be divisor of the conductor of k, we know that p is unramified in $k_{\overline{d}}$, so it matters not which Frobenius $(p, k/\mathbb{Q})$ we choose. Hence

$$p^{\pm\phi(d)/[k_{\overline{d}}:\mathbb{Q}]}\alpha \equiv \alpha^{(p,k/\mathbb{Q})^{-1}} \bmod D(d).$$

By repeated application, for all $(a, d) = 1$ we have

$$a^{\pm\phi(d)/[k_{\overline{d}}:\mathbb{Q}]}\alpha \equiv \alpha^{(a,k/\mathbb{Q})^{-1}} \bmod D(d).$$

If $(a, k/\mathbb{Q})|_{k_{\overline{d}}} = \mathrm{id}$, then $\alpha^{(a,k/\mathbb{Q})^{-1}} = \alpha$ whence

$$a^{\pm\phi(d)/[k_{\overline{d}}:\mathbb{Q}]} \in D(d).$$

□

What can we say about the index $[l(D(d) \cap \mathbb{Q}) : Q(d)]$? When $k = \mathbb{Q}(\zeta_m)^+$, it turns out that it's a power of 2. In preparation for this corollary, we make a few observations in the vein of Lemma 3.6 that are essentially in line with [15, Lemma 3.5].

Lemma 3.12. *For each $\delta_{n,d} \in D(d)$, there exists $n_0 \in \mathbb{N}$ and $\tau \in G$ such that*

$$\delta_{n,d} = \delta_{n_0,d_0}^{\pm(d/\overline{d})\cdot\tau\gamma_{\overline{d}/d_0}},$$

where $d_0 = (\overline{d}, m)$ and m is the conductor of k.

Proof. Let $n \in \mathbb{N}$ such that $n \nmid \overline{d}$, and write $n = p^j b$ where p is a prime divisor of $\overline{d}/d_0$ and b a positive integer such that $(p, b) = 1$. Then $k_n = k_b$ since $(p, m) = 1$, so

$$\begin{aligned}\delta_{p^j b, \overline{d}} &= N_{k_b}^{\mathbb{Q}(\zeta_{p^j b})} \prod_{t \mid (\overline{d}/p)} \left[\frac{(1-\zeta_n^t)^p}{1-\zeta_n^{tp}}\right]^{\mu(t)\overline{d}/(tp)} \\ &= N_{k_b}^{\mathbb{Q}(\zeta_{p^{j-1} b})} \prod_{t \mid (\overline{d}/p)} \left[\frac{N_{\mathbb{Q}(\zeta_{p^{j-1} b})}^{\mathbb{Q}(\zeta_{p^j b})}(1-\zeta_{p^j b}^t)^p}{(1-\zeta_{p^{j-1} b}^t)^p}\right]^{\mu(t)\overline{d}/(tp)}.\end{aligned}$$

If $j > 1$, then we can use an argument similar to the one given at the beginning of the proof of Proposition 3.11 to show that the numerator in the above product for any $t \mid (\overline{d}/p)$ is

$$N_{\mathbb{Q}(\zeta_{p^{j-1} b})}^{\mathbb{Q}(\zeta_{p^j b})}(1-\zeta_{p^j b}^t)^p = (1-\zeta_{p^{j-1} b}^t)^p,$$

hence $\delta_{p^j b, \overline{d}} = 1$ (since k is real and $D(d)$ is totally positive by Lemma 3.10). Similarly, if $j = 1$, then the numerator in the above product for any $t \mid (\overline{d}/p)$ is

$$N_{\mathbb{Q}(\zeta_b)}^{\mathbb{Q}(\zeta_{pb})}(1-\zeta_{pb}^t)^p = (1-\zeta_b^t)^{p - p(p, \mathbb{Q}(\zeta_b)/\mathbb{Q})^{-1}}.$$

In summary, we have

$$\delta_{p^j b, \overline{d}} = \begin{cases} 1 & \text{if } j > 1 \\ \delta_{b, \overline{d}/p}^{1-p(p,k/\mathbb{Q})^{-1}} & \text{if } j = 1 \\ \delta_{b, \overline{d}/p}^{p-(p,k/\mathbb{Q})} & \text{if } j = 0, \text{ (by Lemma 3.6).} \end{cases}$$

Repeated application of the above gives the lemma. □

Corollary 3.13. *If $k = \mathbb{Q}(\zeta_m)^+$, then for every $\delta \in D(d) \cap \mathbb{Q}$, we have $\delta^2 \in Q(d)$.*

Proof. We have $k_{\overline{d}} = k_{d_0} = \mathbb{Q}(\zeta_{d_0})^+$ where $d_0 = (\overline{d}, m)$, so

$$Q(d) = \{a^{2\phi(d)/\phi(d_0)} : a \in \mathbb{Q}^{>0}, (a, d) = 1, \ \ a \equiv \pm 1 \bmod d_0\}.$$

Let $\delta \in D(d) \cap \mathbb{Q}^\times$. By Lemma 3.12, let $\delta_0 \in D(d_0)$ such that $\delta = \delta_0^{(d/\overline{d})\cdot\gamma_{\overline{d}/d_0}}$. Note that $\gamma_{\overline{d}/d_0}$ is invertible in $\mathbb{Q}[G]$ (as is every γ_t). So there exists $N \in \mathbb{N}$ such that $\delta_0^N \in \mathbb{Q}$. Since k is real, it follows that $\delta_0^2 \in \mathbb{Q}$, and since the elements of $D(d)$ are totally positive, we get $\delta_0 \in \mathbb{Q}$. So

$$\begin{aligned}\delta &= \delta_0^{(d/\overline{d})\cdot\prod_{p|(\overline{d}/d_0)}(p-1)} \\ &= \delta_0^{\phi(d)/\phi(d_0)}.\end{aligned}$$

The corollary will follow once we show that $\delta_0 \equiv 1 \bmod d_0$.

Now, let p be a prime dividing d_0, $\mathfrak{P}$ a prime of $\mathbb{Q}(\zeta_n)$ over p, and $\delta_{n,d_0} \in D(d_0)$. As usual, we write

$$\delta_{n,d_0} = N_{k_n}^{\mathbb{Q}(\zeta_n)} \prod_{t|(d_0/p)} \left[\frac{(1-\zeta_n^t)^p}{1-\zeta_n^{tp}}\right]^{\mu(t)d_0/p}.$$

Suppose $n = tp^j$ for some $t \mid (d_0/p)$. Then $j > 1$ otherwise $n \mid d_0$. Note that $\zeta_n^t = \zeta_{p^j}$ and

$$\begin{aligned}\frac{(1-\zeta_{p^j})^p}{1-\zeta_{p^{j-1}}} &= \prod_{a=1}^{p} \frac{1-\zeta_{p^j}}{1-\zeta_{p^j}^{1+ap^{j-1}}} \\ &= \prod_{a=1}^{p} \left(\sum_{b=0}^{ap^{j-1}} \zeta_{p^j}^b\right)^{-1} \\ &\equiv \prod_{a=1}^{p} \left(1+ap^{j-1}\right)^{-1} \bmod 1-\zeta_{p^j} \\ &\equiv 1 \bmod 1-\zeta_{p^j}.\end{aligned}$$

Since $1-\zeta_{p^i} \mid \mathfrak{P}$, it follows that

$$\frac{(1-\zeta_n^t)^p}{1-\zeta_n^{tp}} \equiv 1 \bmod \mathfrak{P}.$$

If n/t is not equal to a p-th power, then the above congruence holds as well since $1-\zeta_n^t$ is a unit modulo $\mathfrak{P}$ and the p-th power map is an automorphism. Hence

$\delta_{n,d_0} \equiv 1 \bmod \mathfrak{p}$ where $\mathfrak{p} = \mathfrak{P} \cap k_n$. And so if $\delta_0 \in D(d_0) \cap \mathbb{Q}$, then $\delta_0 \equiv 1 \bmod p$. Since p was an arbitrary prime divisor of d_0, it follows that $\delta_0 \equiv 1 \bmod d_0$. This completes the proof of the corollary. □

The next proposition is essentially a combination of [16, Lemma 4.2 and Proposition 4.1] adjusted for our purposes. We let $T(d) = l(D(d))$ and any $\mathbb{Z}[G]$-module M, we denote by M_0 the kernel of multiplication by $s(G)$ in M, although, we write $T_0(d)$ (similarly, $U_0(d)$, etc) instead of the more cumbersome $T(d)_0$.

Proposition 3.14. *Let m denote the conductor of k. Then $l(C(d)) = T_0(d) = T(d) \cap (1 - e_1)T(d)$, moreover, $T_0(d)$ has finite index in $(1 - e_1)T(d)$, in fact,*

$$[(1 - e_1)T(d) : T_0(d)] = \left[\sum_{p \nmid d} \frac{\phi(d)}{[k_{p^{\nu_p(m)}\overline{d}} : \mathbb{Q}]} l(p)\mathbb{Z} : l(D(d) \cap \mathbb{Q}) \right].$$

The summation is over all primes $p \nmid d$. If $k = \mathbb{Q}(\zeta_m)^+$, then this index is equal to

$$\phi(d_0) \prod_{p \nmid d} \phi(p^{\nu_p(m)})$$

up to a power of 2.

Proof. We first show that the index on the right is, in fact, finite. Note that

$$\left[\sum_{p \nmid d} \frac{\phi(d)}{[k_{p^{\nu_p(m)}\overline{d}} : \mathbb{Q}]} l(p)\mathbb{Z} : \sum_{p \nmid d} \frac{\phi(d)}{[k_{\overline{d}} : \mathbb{Q}]} l(p)\mathbb{Z} \right] = \prod_{p \nmid d} \frac{[k_{p^{\nu_p(m)}\overline{d}} : \mathbb{Q}]}{[k_{\overline{d}} : \mathbb{Q}]}.$$

Now, by Proposition 3.11, we have

$$\begin{aligned} D(d) \cap \mathbb{Q}^\times \supseteq Q(d) &\supseteq \{a^{\phi(d)/[k_{\overline{d}}:\mathbb{Q}]} : a \in \mathbb{Q}^{>0}, (a, d) = 1, (a, \mathbb{Q}(\zeta_{\overline{d}})/\mathbb{Q}) = \mathrm{id}\} \\ &= \{a^{\phi(d)/[k_{\overline{d}}:\mathbb{Q}]} : a \in \mathbb{Q}^{>0}, (a, d) = 1, a \equiv 1 \bmod \overline{d}\} \\ &=: \mathcal{Q}(d). \end{aligned}$$

Since

$$\left[\sum_{p \nmid d} \frac{\phi(d)}{[k_{\overline{d}} : \mathbb{Q}]} l(p)\mathbb{Z} : l(\mathcal{Q}(d)) \right] = \phi(\overline{d}),$$

it follows that

$$\left[\sum_{p\nmid d}\frac{\phi(d)}{[k_{p^{\nu_p(m)}\overline{d}}:\mathbb{Q}]}l(p)\mathbb{Z}:l(D(d)\cap\mathbb{Q})\right]\quad\text{divides}\quad\phi(\overline{d})\prod_{p\nmid d}\frac{[k_{p^{\nu_p(m)}\overline{d}}:\mathbb{Q}]}{[k_{\overline{d}}:\mathbb{Q}]}.$$

If $k=\mathbb{Q}(\zeta_m)^+$, then $k_{\overline{d}}=\mathbb{Q}(\zeta_{d_0})^+$ where $d_0=(\overline{d},m)$. Moreover,

$$\frac{[k_{p^{\nu_p(m)}\overline{d}}:\mathbb{Q}]}{[k_{\overline{d}}:\mathbb{Q}]}=\frac{\phi(d_0)\phi(p^{\nu_p(m)})/2}{\phi(d_0)/2}=\phi(p^{\nu_p(m)}),$$

and

$$Q(d)=\{a^{\phi(d)/[k_{\overline{d}}:\mathbb{Q}]}:a\in\mathbb{Q}^{>0},(a,d)=1,a\equiv\pm1 \bmod d_0\}.$$

Since

$$\left[\sum_{p\nmid d}\frac{\phi(d)}{[k_{\overline{d}}:\mathbb{Q}]}l(p)\mathbb{Z}:l(Q(d))\right]=\phi(d_0)/2,$$

it follows that

$$\left[\sum_{p\nmid d}\frac{\phi(d)}{[k_{p^{\nu_p(m)}\overline{d}}:\mathbb{Q}]}l(p)\mathbb{Z}:l(D(d)\cap\mathbb{Q})\right]=\frac{\phi(d_0)}{2^{g+1}}\prod_{p\nmid d}\phi(p^{\nu_p(m)})$$

where $2^g=[D(d)\cap\mathbb{Q}:Q(d)]$ (recall Corollary 3.13).

Now, we show the first part of the proposition. The fact that $l(C(d))\subseteq T_0(d)$ is obvious. Going the other way, let $l(\delta)\in T_0(d)$. Then $0=s(G)l(\delta)=l(\delta^{s(G)})$, so $\delta^{s(G)}=1$. Since G acts trivially on $D(d)/C(d)$ (by virtue of the fact that $\delta^{\sigma-1}$ is a unit), it follows that $\delta^{\#G}\in C(d)$, hence $\delta\in C(d)$. So the first equality holds.

For the second equality, we obviously have $T(d)\cap(1-e_1)T(d)\subseteq T_0(d)$ since $s(G)(1-e_1)=0$. Going the other way is equally obvious since for every $l(\delta)\in T_0(d)$, we have $l(\delta)=(1-e_1)l(\delta)$. So the second equality holds.

Now, from the isomorphism theorems we get

$$(1-e_1)T(d)\Big/T(d)\cap(1-e_1)(T(d))\simeq(e_1T(d)+T(d))\Big/T,$$

and since $e_1T(d)\cap T(d)=T(d)^G$, we get

$$(1-e_1)T(d)\Big/T_0(d)\simeq e_1T(d)\Big/T(d)^G.$$

Now, since $e_1 T(d) = (\#G)^{-1} l\big(D(d)^{s(G)}\big)$ where $D(d)$ is generated by $\delta_{n,d}$ for $n \nmid \overline{d}$, we aim to compute $\delta_{n,d}^{s(G)}$ for which it suffices to compute $\delta_{n,(\overline{d},n)}^{s(G)}$ by Lemma 3.6. Note that for all $t \mid (\overline{d}, n)$ we have

$$N_{k_n}^{\mathbb{Q}(\zeta_n)}(1-\zeta_{n/t})^{s(G)} = N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(1-\zeta_{n/t})^{[k:k_n]},$$

so

$$\delta_{n,(\overline{d},n)}^{s(G)} = \prod_{t \mid (\overline{d},n)} N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(1-\zeta_{n/t})^{[k:k_n]\mu(t)(\overline{d},n)/t}.$$

Also note that $1-\zeta_{n/t}$ is a unit of $\mathbb{Z}[\zeta_n]$ if and only if n/t is divisible by two distinct primes. So if p and q are primes such that either

- $(p^2q^2, n) = p^2q^2$, or
- $(pq, n) = pq$ and $(pq, d) = 1$,

then $\delta_{n,(\overline{d},n)}^{s(G)} = 1$ since $(pq, n/t) = pq$ for all $t \mid (\overline{d}, n)$.

So we assume $n = p^e m$ where p is a prime such that $(p, m) = 1$ and $m \mid \overline{d}$. Suppose $p \mid d$. Then $e > 1$ else $n \mid \overline{d}$. In this case, n/t is a prime-power if and only if $t = pm$ or $t = m$. So

$$\begin{aligned}
\delta_{n,(\overline{d},n)}^{s(G)} &= N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(1-\zeta_{p^e})^{\pm[k:k_n]p} \cdot N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(1-\zeta_{p^{e-1}})^{\mp[k:k_n]} \\
&= \left(p^{[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_{p^e})]\cdot p - [\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_{p^{e-1}})]}\right)^{\pm[k:k_n]} \\
&= 1.
\end{aligned}$$

Suppose $p \nmid d$. Then $e \geqslant 1$ else $n \mid \overline{d}$. In this case, we have n/t is a prime-power if and only if $t = m$. Hence

$$\begin{aligned}
\delta_{n,(\overline{d},n)}^{s(G)} &= N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(1-\zeta_{p^e})^{\pm[k:k_n]} \\
&= p^{\pm[k:k_n]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_{p^e})]}.
\end{aligned}$$

So we have the following:

$$\begin{aligned}\delta_{n,d}^{s(G)} &= \delta_{n,(\overline{d},n)}^{s(G)\cdot(d/\overline{d})\cdot\gamma_{\overline{d}/(\overline{d},n)}} \\ &= \begin{cases} p^{\pm[k:k_n]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_{p^e})]\cdot(d/\overline{d})\cdot\prod_{q|(\overline{d}/(\overline{d},n))}(q-1)} & \text{if } n = p^e m,\ p\nmid d,\ m \mid \overline{d} \\ 1 & \text{else.} \end{cases}\end{aligned}$$

Since

$$[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_{p^e})]\cdot\prod_{q|\frac{\overline{d}}{(\overline{d},n)}}(q-1) = \phi(\overline{d})$$

and $(d/\overline{d})\cdot\phi(\overline{d}) = \phi(d)$, we have that $D(d)^{s(G)}$ is generated by $p^{[k:k_n]\cdot\phi(d)}$ where p runs through those primes not dividing d and n runs through those integers of the form $n = p^e m$ such that $m \mid \overline{d}$. Since $[k : k_n]$ is smallest when $n = p^e\overline{d}$ where $e = \nu_p(m)$, we have that

$$\begin{aligned}e_1 T(d) &= \frac{1}{\#G} l(D(d)^{s(G)}) \\ &= \sum_{p\nmid d}\left(\frac{\phi(d)}{[k_{p^{\nu_p(m)}\overline{d}}:\mathbb{Q}]}\cdot l(p)\right)\mathbb{Z}.\end{aligned}$$

Now, suppose $\delta \in D(d)$ such that $l(\delta) \in T(d)^G$. Then $\delta^{\sigma-1} = 1$ for all $\sigma \in G$ since k is real and Galois, so it follows that $\delta^2 \in \mathbb{Q}^{>0}$, thus $\delta \in \mathbb{Q}^{>0}$ since δ is totally real. Hence $T(d)^G = l(D(d)\cap\mathbb{Q}^\times)$, and we have

$$\begin{aligned}[(1-e_1)T(d) : T_0(d)] &= [e_1 T(d) : T(d)^G] \\ &= \left[\sum_{p\nmid d}\frac{\phi(d)}{[k_{p^{\nu_p(m)}\overline{d}}:\mathbb{Q}]} l(p)\mathbb{Z} : l(D(d)\cap\mathbb{Q})\right].\end{aligned}$$

□

We are now ready to prove Theorem 1.10. Let d_∞ be the cycle of k

$$d_\infty := d\prod_{v|\infty} v.$$

Let E_{d_∞} denote the units congruent to 1 modulo d_∞, (i.e. the totally positive units congruent to 1 modulo d). Recall that $U(d) \subseteq U(1)$, and that $U(1)$ corresponds to the set U, the $\mathbb{Z}[G]$-module generated by the elements $\alpha_{\frac{n}{t},n}$ for all $n \geqslant 1$ and all $t \mid n$ as defined in [16, Corollary to Proposition 2.2 and Proposition 2.3].

Theorem 3.15. *The index* $[E : C(d)]$ *is finite, in fact,*

$$[E : C(d)] = \#\mathrm{Cl}(d_\infty)\frac{[E : E_{d_\infty}]\big(R : U(d)\big)}{[k : \mathbb{Q}] \cdot \phi(d)^2}\left[\sum_{p\nmid d}\frac{\phi(d)}{[k_{p^{\nu_p(m)}\overline{d}} : \mathbb{Q}]}l(p)\mathbb{Z} : l(D(d)\cap\mathbb{Q})\right].$$

If $k = \mathbb{Q}(\zeta_m)^+$, *then*

$$[E : C(d)] = \#\mathrm{Cl}(d_\infty)\cdot\frac{[E : E_{d_\infty}][U : U(d)]}{2^{g+1}\phi(d)^2\prod_{p\mid d_0}p^{\nu_p(m)-1}}$$

where $2^g = [D(d)\cap\mathbb{Q} : Q(d)]$.

Proof. Note that $[E : C(d)] = 2[l(E) : l(C(d))]$ since the kernel of l is $\{\pm 1\}$, hence by Proposition 3.14

$$[E : C(d)] = 2\big(l(E) : R_0\big)\cdot\big(R_0 : U_0(d)\big)\cdot\big(U_0(d) : (1-e_1)T(d)\big)\cdot\big((1-e_1)T(d) : T_0(d)\big),$$

where $R = \mathbb{Z}[G]$. From Dirichlet's Unit Theorem, we have

$$2(l(E) : R_0) = \frac{2^{[k:\mathbb{Q}]}}{R(k)},$$

where $R(k)$ is the regulator of k.

For the second term, we use the formula [16, Lemma 1.2(a)] to get

$$(R : U(d)) = (s(G)R : s(G)U(d))\cdot(R_0 : U_0(d)).$$

Note that $s(G)R = s(G)\mathbb{Z}$, and since $s(G)\alpha_{n/t,n} = 0$ unless $t = n$ in which case $s(G)\alpha(1,n) = [k : \mathbb{Q}][\mathbb{Q}(\zeta_n) : k_n]s(G)$, we have

$$s(G)v_{n,d} = \frac{d}{\overline{d}}\cdot\phi(\overline{d}/(\overline{d},n))\cdot[k : \mathbb{Q}]\cdot[\mathbb{Q}(\zeta_n) : k_n]\cdot s(G).$$

It follows that $s(G)U(d) = \phi(d) \cdot [k : \mathbb{Q}] \cdot s(G)\mathbb{Z}$. Hence

$$(R_0 : U_0(d)) = \frac{\big(R : U(d)\big)}{[k : \mathbb{Q}] \cdot \phi(d)}.$$

For the third term, we use 3.7 and the fact that $\omega' v_{1,d} = 0$ to get

$$\big(U_0(d) : (1 - e_1)T(d)\big) = \big(U_0(d) : \omega' U_0(d)\big) = \det \omega' = \prod_{\chi \neq 1} L'(0, \overline{\chi}).$$

Now, we put everything together using Proposition 3.14, the analytic class number formula (see [6])

$$\# \mathrm{Cl} = \frac{1}{R(k)} \prod_{\chi \neq 0} L'(0, \overline{\chi}),$$

and the fact that (see [9, Chapter VI §1 Theorem 1])

$$\# \mathrm{Cl}(d_\infty) = \frac{(\# \mathrm{Cl}) 2^{[k:\mathbb{Q}]} \phi(d)}{[E : E_{d_\infty}]}.$$

The formula for $k = \mathbb{Q}(\zeta_m)^+$ follows from the second part of Proposition 3.14 and the fact that $(R : U) = 1$ in this case by [16, Theorem 5.4]. □

Remark 3.16. *We could relate* $[E : C(d)]$ *to* $\# \mathrm{Cl}$ *obviously. For example, if* $k = \mathbb{Q}(\zeta_m)^+$, *then*

$$[E : C(d)] = \# \mathrm{Cl} \cdot \frac{2^{[k:\mathbb{Q}]-g-1} \cdot [U : U(d)]}{\phi(d) \cdot \prod_{p \mid d_0} p^{\nu_p(m)-1}}.$$

Similarly, we could write

$$[E : C(d)] = \# \mathrm{Cl}(d) \cdot \frac{2^{[k:\mathbb{Q}]-g-1} \cdot [E : E_d] \cdot [U : U(d)]}{\phi(d)^2 \cdot \prod_{p \mid d_0} p^{\nu_p(m)-1}}.$$

In light of Remark 2.6 and Lemma 3.10, we chose the formulation seen in Theorem 3.15

CHAPTER 4

ON THE GALOIS MODULE STRUCTURE OF THE UNITS

4.1 Preliminaries

For a number field K, we write E_K to denote the units of the ring of integers of K. If $K = k$, we typically omit the subscript. We will make ample use of the following classical theorem.

Theorem 4.1 (Minkowski, [12]). *There exists a unit $\epsilon \in E$ such that $[E : \langle\epsilon\rangle_{\mathbb{Z}[G]}] < \infty$*

Any unit $\epsilon \in E$ such that $[E : \langle\epsilon\rangle_{\mathbb{Z}[G]}] < \infty$ will be called a *Minkowski unit*. Fix a fundamental system of units of E, say $\epsilon_1, \ldots, \epsilon_r > 0$ where $r = |G| - 1$. Let G act on $E/\pm 1$. This affords a faithful representation $\rho : G \to GL(r, \mathbb{Z})$.

Proposition 4.2. *Let $\sigma \in G$, and $m_{\rho(\sigma)}(x) \in \mathbb{Z}[x]$ the minimal polynomial for $\rho(\sigma)$. If σ has order n, then*

$$m_{\rho(\sigma)}(x) = \begin{cases} \dfrac{x^n - 1}{x - 1} & \text{if } \langle\sigma\rangle = G \\ x^n - 1 & \text{otherwise.} \end{cases}$$

Proof. Let $\epsilon \in E$ be a Minkowski unit. Write

$$m_{\rho(\sigma)}(x) = x^m + a_{m-1}x^{m-1} + \cdots a_1 x + a_0.$$

Suppose $G = \langle\sigma\rangle$. Then $m_{\rho(\sigma)}(x) \mid (x^n - 1)/(x - 1)$ since $(\sigma^n - 1)/(\sigma - 1) = N_{\mathbb{Q}}^k$. Suppose $m < n - 1$. Then

$$(\epsilon)^{a_0} \cdot (\epsilon^\sigma)^{a_1} \cdot \cdots \cdot (\epsilon^{\sigma^m}) = \pm 1$$

thus giving a dependence relation amongst $\epsilon, \epsilon^{\sigma}, \ldots, \epsilon^{\sigma^m}$. But, by Theorem 4.1, any $m < |G| - 1$ collection of conjugates of ϵ should be multiplicatively independent. This is absurd, so $m = n - 1$, hence $m_{\rho(\sigma)}(x) = (x^n - 1)/(x - 1)$.

Now, suppose $\langle\sigma\rangle \subsetneq G$. Then $m_{\rho(\sigma)}(x) \mid x^n - 1$. Suppose $m < n$. Then

$$(\epsilon)^{a_0} \cdot (\epsilon^{\sigma})^{a_1} \cdot \cdots \cdot (\epsilon^{\sigma^m}) = \pm 1$$

thus giving a dependence relation amongst $\epsilon, \epsilon^{\sigma}, \ldots, \epsilon^{\sigma^m}$. Any $m < |G| - 1$ collection of conjugates of ϵ should be multiplicatively independent. Since $m < n < |G| - 1$, this is impossible, so $m = n$, hence $m_{\rho(\sigma)}(x) = x^n - 1$. □

Likewise, the set $\epsilon_1 \otimes 1, \ldots, \epsilon_r \otimes 1$ forms a basis of the $\mathbb{F}_q$ vector space $E \otimes \mathbb{F}_q$ where $\mathbb{F}_q$ is a finite field of characteristic p with q elements. The action of G on $E \otimes \mathbb{F}_q$ with respect to this basis affords a representation $\overline{\rho} : G \to GL(r, \mathbb{F}_p) \subseteq GL(r, \mathbb{F}_q)$.

Lemma 4.3. *Let $\sigma \in G$, and let $h_{\rho(\sigma)}(x) \in \mathbb{Z}[x]$ and $h_{\overline{\rho}(\sigma)}(x) \in \mathbb{F}_p[x]$ be the characteristic polynomials of $\rho(\sigma)$ and $\overline{\rho}(\sigma)$ respectively. Then*

$$h_{\overline{\rho}(\sigma)}(x) \equiv h_{\rho(\sigma)}(x) \bmod p.$$

Proof. This follows immediately from the observation that $\overline{\rho}(\sigma) \equiv \rho(\sigma) \bmod p$, so

$$h_{\overline{\rho}}(\sigma)(x) = \det(xI - \overline{\rho}(\sigma)) \equiv \det(xI - \rho(\sigma)) \bmod p \equiv h_{\rho(\sigma)}(x) \bmod p.$$

□

Proposition 4.4. *Let O be the ring of integers of any finite extension of $\mathbb{Q}_p$. The following are equivalent:*

(i) There exists a Minkowski unit $\epsilon \in E$ such that $([E : \langle\epsilon\rangle_{\mathbb{Z}[G]}], p) = 1$.

(ii) $E \otimes \mathbb{F}_q$ is a cyclic $\mathbb{F}_q[G]$-module.

(iii) $E \otimes O$ *is a cyclic* $O[G]$*-module.*

Proof. Suppose (i) holds, and let $\epsilon \in E$ be a Minkowski unit such that $[E : \langle \epsilon \rangle_{\mathbb{Z}[G]}]$ is co-prime to p. The cyclicality of $E \otimes \mathbb{F}_p$ now follows from the exactness of

$$\langle \epsilon \rangle_{\mathbb{Z}[G]} \otimes \mathbb{F}_p \to E \otimes \mathbb{F}_p \to E \Big/ \langle \epsilon \rangle_{\mathbb{Z}[G]} \otimes \mathbb{F}_p \to 0 \tag{4.1}$$

and the fact that the third term of the sequence is zero. Note that there exists $u \in E \otimes \mathbb{F}_q$ such that $\langle u \rangle_{\mathbb{F}_q[G]} = E \otimes \mathbb{F}_q$ if and only if $\dim_{\mathbb{F}_q} \langle u^\sigma : \sigma \in G \rangle_{\mathbb{F}_q} = r$. Since

$$r = \dim_{\mathbb{F}_p} \langle \epsilon^\sigma \otimes 1 : \sigma \in G \rangle_{\mathbb{F}_p} = \dim_{\mathbb{F}_q} \langle \epsilon^\sigma \otimes 1 : \sigma \in G \rangle_{\mathbb{F}_q},$$

it follows that $E \otimes \mathbb{F}_q$ is cyclic, so (ii) holds.

Conversely, suppose $u \in E \otimes \mathbb{F}_q$ such that $\langle u \rangle_{\mathbb{F}_q[G]} = E \otimes \mathbb{F}_q$. Let $\sigma_1, \ldots, \sigma_r \in G \setminus \{\sigma_0\}$ such that

$$E \otimes \mathbb{F}_q = u^{\sigma_1}\mathbb{F}_q \oplus u^{\sigma_2}\mathbb{F}_q \oplus \cdots \oplus u^{\sigma_r}\mathbb{F}_q$$

as an $\mathbb{F}_q$-space. Let $s(G) \in \mathbb{F}_p[G]$ be the sum of the elements of G. Let $x_i \in \mathbb{F}_q$ such that $u = \sum \epsilon_i \otimes x_i$. Note that

$$u^{\sigma_0} + u^{\sigma_1} + \cdots + u^{\sigma_r} = \sum \epsilon_i^{s(G)} \otimes x_i = 0,$$

so

$$u^{\sigma_0} = -\sum_{i=1}^{r} u^{\sigma_i}.$$

It follows that $\mathrm{Ann}_{\mathbb{F}_q[G]}(u) = s(G)\mathbb{F}_q[G] = s(G)\mathbb{F}_q$, so $E \otimes \mathbb{F}_q \simeq \mathbb{F}_q[G]/\langle s(G) \rangle_{\mathbb{F}_q}$. On the other hand $E \otimes \mathbb{F}_q = (E \otimes \mathbb{F}_p) \otimes \mathbb{F}_q$, so as $\mathbb{F}_p[G]$-modules we have

$$\begin{aligned} \overbrace{(E \otimes \mathbb{F}_p) \oplus \cdots \oplus (E \otimes \mathbb{F}_p)}^{\times n} &\simeq (E \otimes \mathbb{F}_p) \otimes \mathbb{F}_q \\ &\simeq \mathbb{F}_p[G] \Big/ \langle s(G) \rangle_{\mathbb{F}_p} \otimes \mathbb{F}_q \\ &\simeq \underbrace{\mathbb{F}_p[G] \Big/ \langle s(G) \rangle_{\mathbb{F}_p} \oplus \cdots \oplus \mathbb{F}_p[G] \Big/ \langle s(G) \rangle_{\mathbb{F}_p}}_{\times n}, \end{aligned}$$

where $q = p^n$. The modules $E \otimes \mathbb{F}_p$ and $\mathbb{F}_p[G]/\langle s(G)\rangle_{\mathbb{F}_p}$ decompose uniquely (up to isomorphism) into a direct sum of indecomposable modules since they're finite (see [3, Theorem 14.5]). Considering the above, it follows that $E \otimes \mathbb{F}_p \simeq \mathbb{F}_p[G]/\langle s(G)\rangle_{\mathbb{F}_p}$, hence $E \otimes \mathbb{F}_p$ is cyclic. Let $\epsilon \in E$ such that $\langle \epsilon \otimes 1\rangle_{\mathbb{F}_p[G]} = E \otimes \mathbb{F}_p$. From the exactness of Equation (4.1) and the fact that the first map is now onto, we get that $([E : \langle \epsilon\rangle_{\mathbb{Z}[G]}], p) = 1$, so (i) holds.

Now, let $\mathfrak{K}$ denote the residue field of O. Much like Equation (4.1), for $u \in E \otimes O$ we have the exact sequence

$$\langle u\rangle_{O[G]} \otimes_O \mathfrak{K} \to (E \otimes O) \otimes_O \mathfrak{K} \to \left(E \otimes O \Big/ \langle u\rangle\right) \otimes_O \mathfrak{K} \to 0.$$

So we have

$$\begin{aligned} E \otimes O \text{ is cyclic} &\Leftrightarrow \left(E \otimes O \Big/ \langle u\rangle\right) \otimes_O \mathfrak{K} = 0 \\ &\Leftrightarrow \langle u\rangle_{O[G]} \otimes_O \mathfrak{K} \twoheadrightarrow (E \otimes O) \otimes_O \mathfrak{K} \\ &\Leftrightarrow (E \otimes O) \otimes_O \mathfrak{K} \simeq E \otimes \mathfrak{K} \text{ is cyclic,} \end{aligned}$$

for some $u \in E \otimes O$. This completes the proof of the proposition. □

4.2 On the G-module structure of $E \otimes \mathbb{F}_p$ when $p \nmid \#G$

In this section, we assume $p \nmid \#G$. We begin with the following special case.

Theorem 4.5. *If G is cyclic, then $E \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}_p[G]$-module.*

Proof. Let τ be a generator for G. By Proposition 4.2 it follows that the minimal polynomial for $\rho(\tau)$ is

$$m_{\rho(\tau)}(x) = x^r + x^{r-1} + \cdots + x + 1.$$

Since $\deg m_{\rho(\tau)} = r$, it must be that the characteristic polynomial for $\rho(\tau)$, say $h_{\rho(\tau)}(x)$, is equal to $m_{\rho(\tau)}(x)$. By Lemma 4.3 we have

$$\begin{aligned} h_{\overline{\rho}(\tau)}(x) &\equiv h_{\rho(\tau)}(x) && \bmod p \\ &\equiv \prod_{\substack{d \mid (r+1) \\ d>1}} \Phi_d(x) && \bmod p, \end{aligned}$$

where $\Phi_d(x) \in \mathbb{Z}[x]$ is the d-th cyclotomic polynomial. Since $p \nmid \#G = r+1$, it follows that for each $d \mid (r+1)$, we have $p \nmid d$. Hence $\Phi_d(x) \bmod p$ splits into a square free product of irreducibles. Moreover, $\Phi_d(x) \bmod p$ is coprime to $\Phi_{d'}(x) \bmod p$ for $d \neq d'$ since $\Phi_d(x)$ is coprime to $\Phi_{d'}(x)$ in $\mathbb{Z}[x]$. So $h_{\overline{\rho}(\tau)}(x)$ factors into a square free product of irreducibles. By the structure theorem for finitely generated modules over a principal ideal domain, it follows that $h_{\overline{\rho}(\tau)}(x)$ is the only invariant factor of the transformation $\overline{\rho}(\tau)$. Hence $E \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}_p[G]$-module. □

To address the general abelian case we need the following lemma.

Lemma 4.6. *Let $\mathbb{F}_q$ contain the $\#G$-th roots of unity. Then the following are equivalent.*

(i) There exists a Minkowski unit $\epsilon \in E$ such that $([E : \langle \epsilon \rangle_{\mathbb{Z}[G]}], p) = 1$.

(ii) For all $\chi \in \widehat{G}$ such that $\chi \neq 1$, we have $\dim_{\mathbb{F}_q} e_\chi(E \otimes \mathbb{F}_q) = 1$.

Proof. If (i) holds, then there exists $u \in E \otimes \mathbb{F}_q$ such that $E \otimes \mathbb{F}_q = \langle u \rangle_{\mathbb{F}_q[G]}$ by Proposition 4.4. Since the e_χ are orthogonal idempotents and $e_1(E \otimes \mathbb{F}_q) = 0$, it follows that

$$E \otimes \mathbb{F}_q = \bigoplus_{\chi \neq 1} e_\chi(E \otimes \mathbb{F}_q),$$

where

$$e_\chi(E \otimes \mathbb{F}_q) = \{e_\chi u^\theta : \theta \in \mathbb{F}_q[G]\} = \langle e_\chi u \rangle_{\mathbb{F}_q}.$$

So $\dim_{\mathbb{F}_q} e_\chi(E \otimes \mathbb{F}_q)$ is either 1 or 0 depending on whether or not $e_\chi u$ is non-zero or zero, respectively. Since

$$r = \dim_{\mathbb{F}_q} E \otimes \mathbb{F}_q = \sum_{\chi \neq 1} \dim_{\mathbb{F}_q} e_\chi(E \otimes \mathbb{F}_q),$$

where $\#\widehat{G} - 1 = r$, it follows that for every $\chi \neq 1$, we have $\dim_{\mathbb{F}_q} e_\chi(E \otimes \mathbb{F}_q) = 1$.

Conversely, suppose for all $\chi \in \widehat{G}$ such that $\chi \neq 1$, we have $\dim_{\mathbb{F}_q} e_\chi(E \otimes \mathbb{F}_q) = 1$. For every $\chi \neq 1$, let u_χ be any non-zero element of $e_\chi(E \otimes \mathbb{F}_q)$ so that $\langle u_\chi \rangle_{\mathbb{F}_q} = e_\chi(E \otimes \mathbb{F}_q)$. It follows that $\{u_\chi\}_{\chi \neq 1}$ forms a basis for $E \otimes \mathbb{F}_q$. Let

$$u = \sum_{\chi \neq 1} u_\chi \in E \otimes \mathbb{F}_q.$$

Since $e_\chi u = u_\chi$, it follows that $E \otimes \mathbb{F}_q$ is cyclic, hence (i) holds by Proposition 4.4.

□

We now show that $E \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}_p[G]$-module in general (when $p \nmid \#G$).

Proof of Theorem 1.11. Let $\mathbb{F}_q$ contain the $\#G$-th roots of unity, and let $\chi \in \widehat{G}$ such that $\chi \neq 1$. Let F be the fixed field of $\ker \chi$. Then χ is a non-trivial character of $H = G/\ker \chi$, the Galois group of the cyclic extension $F/\mathbb{Q}$. Since k is real and Galois while p is odd, we have

$$E_F \otimes \mathbb{F}_p \hookrightarrow E \otimes \mathbb{F}_p.$$

Note that

$$\begin{aligned} e_\chi &= \frac{1}{\#G} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \\ &= \frac{1}{\#G} \sum_{\tau \in H} \sum_{\sigma \in \ker \chi} \chi(\tau)\tau^{-1}\sigma^{-1}. \end{aligned}$$

So if we let χ^* denote the character χ as viewed in $\widehat{H}$, then

$$\begin{aligned} e_\chi|_{E_F \otimes \mathbb{F}_q} &= \frac{1}{\#G} \sum_{\tau \in H} (\#\ker \chi)\chi(\tau)\tau^{-1} \\ &= \frac{1}{\#H} \sum_{\tau \in H} \chi(\tau)\tau^{-1} \\ &= e_{\chi^*}, \end{aligned}$$

where $\langle \chi^* \rangle = \widehat{H}$. Since $F/\mathbb{Q}$ is cyclic, Theorem 4.5 and Lemma 4.6 give us that

$$\dim_{\mathbb{F}_q} e_\chi(E_F \otimes \mathbb{F}_q) = \dim_{\mathbb{F}_q} e_{\chi^*}(E_F \otimes \mathbb{F}_q) = 1.$$

Since $E_F \otimes \mathbb{F}_q \hookrightarrow E \otimes \mathbb{F}_q$, we get that

$$\dim_{\mathbb{F}_q} e_\chi(E \otimes \mathbb{F}_q) \geqslant \dim_{\mathbb{F}_q} e_\chi(E_F \otimes \mathbb{F}_q) = 1.$$

Since

$$r = \dim_{\mathbb{F}_q} E \otimes \mathbb{F}_q = \sum_{\chi \neq 1} \dim_{\mathbb{F}_q} e_\chi(E \otimes \mathbb{F}_q),$$

it follows that $\dim_{\mathbb{F}_q} e_\chi(E \otimes \mathbb{F}_q) = 1$. The theorem now follows from Lemma 4.6.

□

4.3 On the G-module structure of $E \otimes \mathbb{F}_p$ when $p \mid \#G$

In this section we assume $p \mid \#G$, and we write $\#G = p^e m$ where $(p, m) = 1$ and $e > 0$. For a number field K, we let P_K denote the collection of principal ideals of K. For a subfield F of k, let R_F denote the collection of principal ideals (b) of F such that $(b)\mathfrak{o}_k$ is the p-th power of a principal ideal of k.

Lemma 4.7. *Let $H \leqslant G$ and F the fixed field of H. Then*

$$(E/E^p)^H \simeq (Ek^{\times p} \cap F)/F^{\times p},$$

moreover,

$$\#(E/E^p)^H = p^{[F:\mathbb{Q}]-1} \cdot [R_F : P_F^p].$$

Proof. From the short exact sequence of H-modules

$$1 \to k^{\times p} \to Ek^{\times p} \to Ek^{\times p}/k^{\times p} \to 1,$$

we obtain the long exact sequence of H-invariants

$$1 \to k^{\times pH} \to (Ek^{\times pH}) \to \left(Ek^{\times p}/k^{\times p}\right)^H \to H^1(H, k^{\times p}) \to \cdots.$$

Hilbert's theorem 90 is the statement that $H^1(H, k^\times) = 1$. Since k is real, we have that $k^\times \to k^{\times p}$ is an isomorphism. Hence $H^1(H, k^{\times p}) = 1$, as well. Since k is Galois and contains no roots of unity while F is the fixed field of H, we have

$$(k^{\times p})^H = k^{\times p} \cap F = F^{\times p}.$$

Hence

$$(E/E^p)^H \simeq \left(Ek^{\times p}/k^{\times p}\right)^H \simeq (Ek^{\times p} \cap F)/F^{\times p},$$

which proves the first claim. For the second, notice that

$$\#\,(E/E^p)^H = \left[Ek^{\times p} \cap F : E_F F^{\times p}\right] \cdot \left[E_F F^{\times p} : F^{\times p}\right].$$

Since $E_F \cap F^{\times p} = E_F^p$, we have

$$E_F F^{\times p}/F^{\times p} \simeq E_F/E_F^p.$$

Since k is real, so is F. Hence, by Dirichlet's Unit Theorem, we have

$$[E_F : E_F^p] = p^{[F:\mathbb{Q}]-1}.$$

It remains to show that $[Ek^{\times p} \cap F : E_F F^{\times p}] = [R_F : P_F^p]$.

Now, from the natural map

$$\begin{aligned} Ek^{\times p} \cap F &\to R_F \\ b &\mapsto (b) \end{aligned}$$

we get that

$$Ek^{\times p} \cap F \Big/ E_F \simeq R_F,$$

from which we easily derive

$$Ek^{\times p} \cap F \Big/ E_F F^{\times p} \simeq R_F / P_F^p.$$

□

For the remainder of this section, we assume that G is cyclic and we let F denote the fixed field of $\mathrm{Syl}_p(G)$.

Theorem 4.8. *$E \otimes \mathbb{F}_p$ is a cyclic $\mathbb{Z}_p[G]$-module if and only if $[R_F : P_F^p] = p$.*

Proof. Let τ be a generator for G, and let $m_{\rho(\tau)}$ be the minimal polynomial for $\rho(\tau) \in \mathrm{GL}(r, \mathbb{Z})$. By Proposition 4.2 and Lemma 4.3, we have

$$\begin{aligned} m_{\rho(\tau)}(x) = \frac{x^{p^e m} - 1}{x - 1} &\equiv \left(\frac{x^m - 1}{x - 1} \right)^{p^e} \cdot (x-1)^{p^e - 1} \bmod p \\ &\equiv (x-1)^{p^e-1} \prod_{\substack{d \mid m \\ d \neq 1}} \Phi_d^{p^e}(x) \bmod p \\ &= h_{\overline{\rho}(\tau)}(x), \end{aligned}$$

where $h_{\overline{\rho}(\tau)}(x) \in \mathbb{F}_p[x]$ is the characteristic polynomial for $\overline{\rho}(\tau)$. For each $d \mid m$, we have $p \nmid d$, hence

$$\Phi_d(x) \equiv \prod_{j=1}^{r(d)} q_{d,j}(x) \bmod p,$$

where each $q_{d,j}(x) \in \mathbb{F}_p[x]$ is irreducible. If $d = 1$, then $r(d) = 1$ and $q_{1,1}(x) = x - 1$. From the structure theorem on finitely generated modules over principal ideal domains it follows that

$$E/E^p \simeq \bigoplus_{d \mid m} \bigoplus_{j=1}^{r(d)} \bigoplus_{i=1}^{t(d,j)} \mathbb{F}_p[x]/(q_{d,j}^{e_{d,j,i}}(x)), \tag{4.2}$$

where x acts like τ,

$$1 \leqslant e_{d,j,1} \leqslant \cdots \leqslant e_{d,j,t(d,j)},$$

and

$$\sum_{i=1}^{t(d,j)} e_{d,j,i} = \begin{cases} p^e - 1 & \text{if } d = 1 \\ p^e & \text{else.} \end{cases}$$

Now, note that $\mathrm{Syl}_p(G) = \langle \tau^m \rangle$, and

$$x^m - 1 \equiv \prod_{d|m} \prod_{j=1}^{r(d)} q_{d,j}(x) \bmod p.$$

Consider the map $\psi_{d,j,i} : \mathbb{F}_p[x]/\left(q_{d,j}^{e_{d,j,i}}(x)\right) \to \mathbb{F}_p[x]/\left(q_{d,j}^{e_{d,j,i}}(x)\right)$ defined by

$$g(x) \mapsto g(x) \cdot (x^m - 1).$$

If

$$g(x) \cdot (x^m - 1) \equiv 0 \bmod q_{d,j}^{e_{d,j,i}}(x),$$

then

$$g(x) \cdot q_{d,j}(x) \equiv 0 \bmod q_{d,j}^{e_{d,j,i}}(x)$$

since all other factors of $x^m - 1$ are co-prime to $q_{d,j}(x)$. Hence,

$$g(x) \equiv q_{d,j}^{e_{d,j,i}-1}(x) \cdot f(x) \bmod q_{d,j}^{e_{d,j,i}}(x),$$

where $f(x)$ can be any representative from $\mathbb{F}_p[x]/(q_{d,j}(x))$. It follows that

$$\# \ker \psi_{d,j,i} = p^{\deg q_{d,j}(x)}. \tag{4.3}$$

So, using Equation (4.2) and Equation (4.3), we have

$$\begin{aligned} \#(E/E^p)^{\mathrm{Syl}_p(G)} &= \#\{\epsilon \bmod E^p : \epsilon^{\tau^m} \bmod E^p \equiv \epsilon \bmod E^p\} \\ &= \# \ker (\tau^m - 1 : E/E^p \to E/E^p) \\ &= \prod_{d|m} \prod_{j=1}^{r(d)} \prod_{i=1}^{t(d,j)} \# \ker \psi_{d,j,i} \\ &= p^{\sum_{d|m} \sum_{j=1}^{r(d)} \deg q_{d,j}(x) \cdot t(d,j)}. \end{aligned}$$

Now, we have

$$\begin{aligned} E \otimes \mathbb{F}_p \text{ is a cyclic } \mathbb{F}_p[G]\text{-module} &\Leftrightarrow t(d,j) = 1 \text{ for all } j = 1,\dots,r(d), \text{ and } d \mid m \\ &\Leftrightarrow \#(E/E^p)^{\mathrm{Syl}_p(G)} = p^{\sum_{d\mid m}\sum_{j=1}^{r(d)} \deg q_{d,j}(x)} \\ &\Leftrightarrow \#(E/E^p)^{\mathrm{Syl}_p(G)} = p^m \\ &\Leftrightarrow p^{m-1}\cdot [R_F : P_F^p] = p^m \\ &\Leftrightarrow [R_F : P_F^p] = p, \end{aligned}$$

where the second to last equivalence follows from Lemma 4.7. The theorem now follows from Proposition 4.4. □

When is $[R_F : P_F^p] = p$? We relate this index to ideal classes in the following way. Let $\iota : Cl_F \to Cl_k$ be the natural map. Let I_k and I_F denote the group of fractional ideals of k and F, respectively. Let $D_k \subseteq I_k$ (resp. $D_F \subseteq I_F$) denote the subgroup of fractional ideals supported by those primes that are ramified over F (resp. those primes that ramify in k). Let $B_F \subseteq I_F$ denote the subgroup of fractional ideals supported by those primes that are unramified in k. Note that we naturally then have

$$I_F = D_F B_F \simeq D_F \times B_F.$$

Let $Dl_k \subseteq Cl_k$ (resp. $Dl_F \subseteq Cl_F$) denote the subgroup of ideal classes supported by D_k (resp. D_F). For any abelian group G, we let $G[p]$ denote the part of G annihilated by p.

We will explicitly give a homomorphism

$$\psi : R_F \Big/ P_F^p \to \left(\iota^{-1}(Dl_k)\Big/ Dl_F\right)[p]$$

with a bounded kernel (depending on the ramification in k/F) and in many cases onto. Suppose $(b) \in R_F$ and let $\mathfrak{d} \in D_F$, $\mathfrak{a} \in B_F$ such that

$$(b) = \mathfrak{d}\cdot\mathfrak{a}.$$

Since $\mathfrak{d} \in D_F$, there exists an ideal $\mathfrak{D} \in D_k$ such that $\mathfrak{D}^p = \mathfrak{d}\mathfrak{o}_k$. And since $(\mathfrak{b}) \in R_F$, there exists $(\beta) \in P_k$ such that $(\mathfrak{b})\mathfrak{o}_k = (\beta)^p$, so

$$(\mathfrak{b})\mathfrak{o}_k = \mathfrak{D}^p \cdot (\mathfrak{a}\mathfrak{o}_k) = (\beta)^p.$$

Since $\mathfrak{a} \in B_F$, it follows that $\mathfrak{a}$ is a p-th power in B_F, so $R_F \subseteq D_F B_F^p$. Let $\mathfrak{b} \in B_F$ such that $\mathfrak{a} = \mathfrak{b}^p$ so that

$$(\mathfrak{b})\mathfrak{o}_k = \mathfrak{D}^p(\mathfrak{b}\mathfrak{o}_k)^p = (\beta^p).$$

It follows that $\mathfrak{b}\mathfrak{o}_k = \mathfrak{D}^{-1}(\beta)$, that is, $[\mathfrak{b}] \in \iota^{-1}(Dl_k)$. On the other hand, $\mathfrak{b}^p = \mathfrak{d}^{-1}(\mathfrak{b})$, so

$$[\mathfrak{b}]^p \equiv 1 \bmod Dl_F.$$

Hence

$$[\mathfrak{b}] \bmod Dl_F \in \left(\iota^{-1}(Dl_k) \Big/ Dl_F\right)[p].$$

So we have a well defined homomorphism

$$\begin{aligned} R_F &\to \left(\iota^{-1}(Dl_k) \Big/ Dl_F\right)[p] \\ (\mathfrak{b}) &\mapsto [\mathfrak{b}] \bmod Dl_F, \end{aligned}$$

where $\mathfrak{b}$ is the p-th root of the projection of $(\mathfrak{b})$ into B_F. If $(\mathfrak{b}) \in P_F^p$, then $[\mathfrak{b}] \in Dl_F$, so we have the induced homomorphism

$$\begin{aligned} \psi : R_F \Big/ P_F^p &\to \left(\iota^{-1}(Dl_k) \Big/ Dl_F\right)[p] \\ (\mathfrak{b}) \bmod P_F^p &\mapsto [\mathfrak{b}] \bmod Dl_F \end{aligned} \tag{4.4}$$

The next two lemmas give us some information about the image and kernel of ψ.

Lemma 4.9. *If $p \nmid \# Dl_k$, then ψ is onto.*

Proof. Let $[\mathfrak{b}] \bmod Dl_F \in \left(\iota^{-1}(Dl_k) \Big/ Dl_F\right)[p]$, and let $\mathfrak{d} \in D_F$ such that

$$\mathfrak{b}^p = (\mathfrak{b})\mathfrak{d}$$

where $(b) \in P_F$. Also, let $\mathfrak{D} \in D_k$ such that $\mathfrak{b}\mathfrak{o}_k = (\beta)\mathfrak{D}$ where $(\beta) \in P_k$. Hence

$$(b\beta^{-p}) = (\mathfrak{d}^{-1}\mathfrak{o}_k)\mathfrak{D}^p.$$

Since $\mathfrak{d}^{-1} \in D_F$ we have that $\mathfrak{d}^{-1}\mathfrak{o}_k = \mathfrak{D}'^p$ for some $\mathfrak{D}' \in D_k$. So we have

$$(b\beta^{-p}) = (\mathfrak{D}'\mathfrak{D})^p.$$

Suppose $p \nmid \# Dl_k$. Then $\mathfrak{D}'\mathfrak{D}$ is principal, say $\mathfrak{D}'\mathfrak{D} = (\delta)$. So

$$(b) = (\delta\beta)^p,$$

hence $(b) \in R_F$ and $\psi((b) \bmod P_F^p) = [\mathfrak{b}] \bmod Dl_F$. So ψ is onto. □

Lemma 4.10. *The kernel of ψ is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^s$ where s is the number of primes ramifying in k/F.*

Proof. Suppose $(b) \bmod P_F^p \in \ker\psi$. Let $\mathfrak{d} \in D_F$ and $\mathfrak{b} \in B_F$ such that

$$(b) = \mathfrak{d}\mathfrak{b}^p.$$

Since $(b) \bmod P_F^p \in \ker\psi$, it follows that $[\mathfrak{b}] \in Dl_F$. Let $(c) \in P_F$ and $\mathfrak{d}' \in D_F$ such that $\mathfrak{b} = (c)\mathfrak{d}'$ so that

$$(bc^{-p}) = \mathfrak{d}\mathfrak{d}'^p \in D_F \cap P_F.$$

So we have

$$\begin{aligned}\ker\psi &\leqslant (D_F \cap P_F)P_F^p \Big/ P_F^p \\ &\simeq D_F \cap P_F \Big/ (D_F \cap P_F) \cap P_F^p \\ &= D_F \cap P_F \Big/ (D_F \cap P_F)^p\ .\end{aligned}$$

Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_s$ be the primes of F ramifying in k so that $D_F = \mathfrak{l}_1^{\mathbb{Z}} \cdots \mathfrak{l}_s^{\mathbb{Z}}$. Since each $[\mathfrak{l}_i]$ has finite order in Dl_F, it follows that $D_F \cap P_F$ is a finitely generated, rank s, torsion-free $\mathbb{Z}$-module. Hence

$$D_F \cap P_F \Big/ (D_F \cap P_F)^p \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^s,$$

and the lemma follows. □

This tells us that the index $[R_F : P_F^p]$ is influenced by the primes that ramify in k/F and the structure of the natural map $Cl_F \to Cl_k$. So in order to know more about the kernel and image of ψ, it's natural to start making assumptions about the quality of ramification from F to k.

The simplest situation is when there is a single prime ideal $\mathfrak{l}$ of F that ramifies in k/F. In this scenario, the ramification in k/F must come from a cyclotomic field with a conductor equal to a prime power. To be precise, let ℓ be the rational prime below $\mathfrak{l}$. Let F' be the fixed field of the non-p parts of G so that $k = FF'$ and $\mathbb{Q} = F \cap F'$. From the coprimality of $[F : \mathbb{Q}]$ and $[F' : \mathbb{Q}]$, it follows that ℓ is the only prime ramifying in $F'/\mathbb{Q}$. So $F' \subseteq \mathbb{Q}(\zeta_{\ell^n})$ for some n, and $\mathfrak{l}$ is totally ramified in k/F. Notice that this forces either $p = \ell$ or $\#\operatorname{Syl}_p(G) \mid \ell - 1$. In the former case, we have k/F is part of the $\mathbb{Z}_p$-extension of F. We tend to be able to say more in this situation than in any other, but for now we content ourselves with simply assuming that only one prime ramifies in k/F if anything for the sake of maintaining generality at no extra cost.

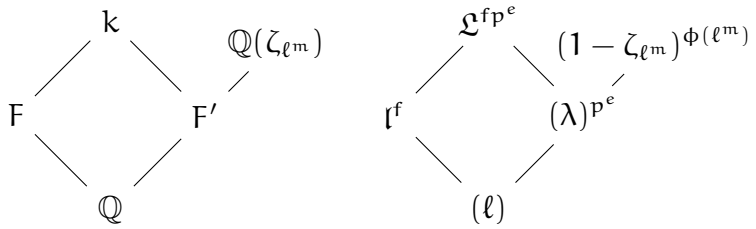
We also note that $\ker(Cl_F \to Cl_k)$ is a p-group. Indeed, let $[\mathfrak{a}] \in \ker(Cl_F \to Cl_k)$ and $(\alpha) \in P_k$ such that $\mathfrak{a}\mathfrak{o}_k = (\alpha)$. Taking norms we have $\mathfrak{a}^{\#\operatorname{Syl}_p(G)} = (N_F^k(\alpha))$, whence the claim. We now prove Theorem 1.12, in fact, we show a little more.

Theorem 4.11. *Suppose there is only one prime ideal $\mathfrak{l}$ of F ramifying in k/F. Then*

$$\operatorname{rank}_{\mathbb{F}_p} R_F \Big/ P_F^p = 1 + \operatorname{rank}_{\mathbb{F}_p} \ker(Cl_F \to Cl_k).$$

So $E \otimes \mathbb{F}_p$ is cyclic if and only if $Cl_F \to Cl_k$ is injective.

Proof. Let ℓ be the rational prime below $\mathfrak{l}$. We have the following field diagram on the left accompanied by the respective factorizations of ℓ on the right:



Note that Dl_k is generated by $[\mathfrak{L}]$ and

$$\mathfrak{L}^f = (\lambda)\mathfrak{o}_k,$$

so $\#\,\mathrm{Dl}_k \mid f$. Since $p \nmid f$, it follows that $p \nmid \#\,\mathrm{Dl}_k$. Hence, by Lemma 4.9, the map ψ is onto. Also, since raising to the p-th power is an automorphism of Dl_k, we have that Dl_k is generated by $[\iota(\mathfrak{l})] = [\mathfrak{L}]^{p^e}$, as well. It follows that $\iota^{-1}(\mathrm{Dl}_k) = (\ker\iota)\,\mathrm{Dl}_F$. This gives us the isomorphism

$$\begin{aligned}\left(\iota^{-1}(\mathrm{Dl}_k)\Big/\mathrm{Dl}_F\right)[p] &= \left((\ker\iota)\,\mathrm{Dl}_F\Big/\mathrm{Dl}_F\right)[p]\\ &\simeq \left(\ker\iota\Big/\mathrm{Dl}_F\cap\ker\iota\right)[p]\\ &\simeq (\ker\iota)[p],\end{aligned}$$

where the last isomorphism follows since $\ker\iota$ is a p-group and $p \nmid \#\,\mathrm{Dl}_F$ (since $p \nmid f$).

Now, let $(\mathfrak{l}) \in P_F$ such that $\mathfrak{l}^{\#\,\mathrm{Dl}_F} = (\mathfrak{l})$. Then $\#\,\mathrm{Dl}_F \mid f$ (since $\mathfrak{l}^f = (\ell)\mathfrak{o}_F$) so that

$$(\mathfrak{l})^{f/\#\,\mathrm{Dl}_F}\mathfrak{o}_k = \mathfrak{l}^f\mathfrak{o}_k = \mathfrak{L}^{fp^e} = (\lambda)^{p^e}\mathfrak{o}_k,$$

so $(\mathfrak{l})^{f/\#\,\mathrm{Dl}_F} \in R_F$. Let n be the least positive integer such that $(\mathfrak{l})^n \in R_F$. It follows that $n \mid f/\#\,\mathrm{Dl}_F$, so $p \nmid n$. Let $(L) \in R_F$ such that $(L) = (\mathfrak{l})^n$ and note that

$$(L) = (\mathfrak{l})^n = \mathfrak{l}^{\#\,\mathrm{Dl}_F\cdot n}.$$

Since $p \nmid \#\,\mathrm{Dl}_F \cdot n$, it follows that $(L) \not\equiv 1 \bmod P_F^p$. So (L) is a non-trivial element in $\ker\psi$. It follows that (L) generates $\ker\psi$ from Lemma 4.10.

Putting everything together we have

$$\begin{aligned}\operatorname{rank}_{\mathbb{F}_p} R_F \Big/ P_F^p &= \operatorname{rank}_{\mathbb{F}_p} \ker \psi + \operatorname{rank}_{\mathbb{F}_p} \operatorname{im} \psi \\ &= 1 + \operatorname{rank}_{\mathbb{F}_p} \ker \iota.\end{aligned}$$

This proves the first statement of the theorem while the second follows immediately from the first and Theorem 4.8. □

We now specialize to the setting alluded to before. Let F be a real cyclic extension of $\mathbb{Q}$ such that $p \nmid [F : \mathbb{Q}]$, and let

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_\infty$$

denote the $\mathbb{Z}_p$-extension of F. Let $R_{F,n}$ denote the collection of principal ideals of F that are p-th powers of principal ideals of F_n. Let $\iota_n : Cl_F \to Cl_{F_n}$ be the natural map, and

$$\psi_n : R_{F,n} \Big/ P_F^p \to \left(\iota_n^{-1}(Dl_{F_n}) \Big/ Dl_F \right)[p]$$

be the map defined in Equation (4.4). We need the following proposition.

Proposition 4.12 (Greenberg)**.** *Let $N \geqslant 0$. For all $\mathfrak{D} \in D_{F_N}$ such that $[\mathfrak{D}] \in \operatorname{Syl}_p(Cl_{F_N})$, there exists $N' \geqslant N$ such that for all $n \geqslant N'$, $\mathfrak{D}\mathfrak{o}_{F_n}$ is principal.*

Proof. See [5, Corollary to Proposition 1]. □

Theorem 4.13. *Suppose there exists s distinct primes of F lying over p. Then for all sufficiently large n, we have ψ_n is onto and $\operatorname{rank}_{\mathbb{F}_p} \ker \psi_n = s$ so that*

$$\operatorname{rank}_{\mathbb{F}_p} R_{F,n} \Big/ P_F^p = s + \operatorname{rank}_{\mathbb{F}_p} \left(\iota_n^{-1}(Dl_{F_n}) \Big/ Dl_F \right)[p].$$

Proof. Since Cl_F is finite, we may assume N is large enough so that for all $j \geqslant i \geqslant N$

$$\iota_i^{-1}(Dl_{F_i}) = \iota_j^{-1}(Dl_{F_j}) =: \widetilde{Dl}_F.$$

Let $[\mathfrak{b}] \in \left(\widetilde{\mathrm{Dl}}_F \Big/ \mathrm{Dl}_F\right)[p]$, and let $\mathfrak{D} \in D_{F_N}$, $(\beta) \in P_{F_N}$ such that

$$\mathfrak{b}\mathfrak{o}_{F_N} = \mathfrak{D}(\beta).$$

Also, let $\mathfrak{d} \in D_F$ and $(\mathfrak{b}) \in P_F$ such that $\mathfrak{b}^p = \mathfrak{d}(\mathfrak{b})$. Finally, let $\mathfrak{D}' \in D_{F_N}$ such that $\mathfrak{D}'^p = \mathfrak{d}^{-1}\mathfrak{o}_{F_N}$. Then

$$(\mathfrak{b}\beta^{-p}) = (\mathfrak{D}\mathfrak{D}')^p,$$

So $[\mathfrak{D}\mathfrak{D}'] \in \mathrm{Syl}_p(\mathrm{Cl}_{k_N})$, and we apply Proposition 4.12 to obtain an integer $N' = N'([\mathfrak{b}]) \geqslant N$ such that for all $n \geqslant N'$, $[\mathfrak{D}\mathfrak{D}'] \in \ker(\mathrm{Cl}_{F_N} \to \mathrm{Cl}_{F_n})$. Let $n \geqslant N'$ and let $\delta \in k_n^\times$ such that $\mathfrak{D}\mathfrak{D}'\mathfrak{o}_{F_n} = (\delta)$. It follows that $(\mathfrak{b}\beta^{-p}) = (\delta)^p$, so $(\mathfrak{b}) \in R_{F,n}$, moreover, $\psi_n((\mathfrak{b}) \bmod P_F^p) = [\mathfrak{b}] \bmod \mathrm{Dl}_F$. Now let

$$N_0 = \max\left\{N'([\mathfrak{b}]) : [\mathfrak{b}] \in \left(\widetilde{\mathrm{Dl}}_F \Big/ \mathrm{Dl}_F\right)[p]\right\}.$$

It follows that for all $n \geqslant N_0$, the map ψ_n is onto.

Now, suppose $(\mathfrak{b}) \in D_F \cap P_F$, and let

$$(\mathfrak{b}) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are the primes of F over p, i.e., the primes of F ramifying in F_N/F. Let $\mathfrak{D} \in D_{F_N}$ such that

$$(\mathfrak{b}) = \mathfrak{D}^p,$$

so $[\mathfrak{D}] \in \mathrm{Syl}_p(\mathrm{Cl}_{F_N})$. We apply Proposition 4.12 once more to obtain an integer

$$N'((e_1, e_2, \ldots, e_r)) = N' \geqslant N$$

such that for all $n \geqslant N'$, $[\mathfrak{D}] \in \ker(\mathrm{Cl}_{F_N} \to \mathrm{Cl}_{F_n})$. Let $n \geqslant N'$ and let $(\delta) \in P_{F_n}$ such that $\mathfrak{D}\mathfrak{o}_{F_n} = (\delta)$. It follows that $(\mathfrak{b}) = (\delta)^p$, so $(\mathfrak{b}) \in R_{F,n}$, moreover, $(\mathfrak{b}) \bmod P_F^p \in \ker \psi_n$ and

$$(\mathfrak{b}) \bmod P_F^p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} \bmod (D_F \cap P_F)^p.$$

Now let

$$N_1 = \max\{N'((e_1, \ldots, e_s)) : 0 \leqslant e_i < p\}.$$

It follows that for all $n \geqslant N_1$, we have

$$\ker \psi_n = D_F \cap P_F \Big/ (D_F \cap P_F)^p \ .$$

Hence, for all $n \geqslant \max\{N_0, N_1\}$ we have that ψ_n is onto and $\operatorname{rank}_{\mathbb{F}_p} \ker \psi_n = s$. This completes the proof of the theorem. □

Combining the previous two theorems gives us the following corollary.

Corollary 4.14. *For all sufficiently large n, the following are equivalent.*

(i) $E_{F_n} \otimes \mathbb{F}_p$ *is a cyclic* $\mathbb{F}_p[\mathrm{Gal}(F_n/\mathbb{Q})]$*-module.*

(ii) Precisely one prime of F *ramifies in* F_∞ *and the map* $\mathrm{Cl}_F \to \mathrm{Cl}_{F_n}$ *is injective.*

Theorem 4.11 is particularly interesting in lieu of the following theorem also due to Greenberg.

Theorem 4.15 (Greenberg)**.** *Suppose only one prime of* F *ramifies in* F_∞*. Then the following are equivalent.*

(i) $\#\,\mathrm{Syl}_p(\mathrm{Cl}_{F_n})$ *is bounded as* $n \to \infty$*.*

(ii) $\mathrm{Syl}_p(\mathrm{Cl}_F) = \ker(\mathrm{Cl}_F \to \mathrm{Cl}_{F_n})$ *for sufficiently large* n*.*

Proof. See [5, Theorem 1]. □

Greenberg conjectured that the above always holds, that is, that $\#\,\mathrm{Syl}_p(\mathrm{Cl}_{F_n})$ is indeed bounded as $n \to \infty$. A lot of work has gone into verifying this conjecture in various special cases (mainly when the base field is a real quadratic). In the special case when precisely one prime of F ramifies in F_∞ we get the following relationship between Greenberg's conjecture, the cyclicality of $E_{F_n} \otimes \mathbb{F}_p$, and the p divisibility of $\#\,\mathrm{Cl}_{F_n}$.

Corollary 4.16. *Suppose only one prime of* F *ramifies in* F_∞*. Then the following are equivalent:*

(i) For all $n \geqslant 0$, $p \nmid \#\mathrm{Cl}_{F_n}$.

(ii) $E_{F_n} \otimes \mathbb{F}_p$ *is cyclic and* $\#\mathrm{Syl}_p(\mathrm{Cl}_{F_n})$ *is bounded as* $n \to \infty$.

Proof. The fact that the first statement implies the second follows from Corollary 4.14. If the second statement holds, then Theorem 4.11 and Theorem 4.15 give us that

$$\mathrm{Syl}_p(\mathrm{Cl}_F) = \ker(\mathrm{Cl}_F \to \mathrm{Cl}_{F_n}) = 1,$$

for n sufficiently large, hence $p \nmid \#\mathrm{Cl}_F$. Since there are no unramified intermediate extensions of the p-extension F_n/F, it follows that $p \nmid \#\mathrm{Cl}_{F_n}$ for all n (see for example [20, Theorem 10.4(a)]). □

And now for something completely different. If τ is a generator for G, then the number of invariant factors of τ acting on $E \otimes \mathbb{F}_p$ is restricted by $[k : \mathbb{Q}]$ in the following way.

Proposition 4.17. *In the notation of Theorem 4.8, we have*

$$t(1,1) \leqslant e \qquad \textit{and} \qquad t(d,j) \leqslant e+1 \quad \textit{for} \quad d > 1.$$

Proof. Let τ be a generator for G, and fix a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_m]$ over p. We view $\rho(\tau) \in \mathrm{GL}(r, \mathbb{Z}[\zeta_m])$, and $\overline{\rho}(\tau) \in \mathrm{GL}(r, \mathbb{Z}[\zeta_m]/\mathfrak{p})$. From the proof of Theorem 4.2, we have

$$\begin{aligned} h_{\overline{\rho}(\tau)}(x) &\equiv \frac{x^{p^e m} - 1}{x - 1} \bmod \mathfrak{p} \\ &\equiv (x-1)^{p^e - 1} \prod_{a=1}^{m-1} (x - \zeta_m^a)^{p^e} \bmod \mathfrak{p}. \end{aligned}$$

Let $\overline{Q} \in \mathrm{GL}(r, \mathbb{Z}[\zeta_m]/\mathfrak{p})$ such that $(\overline{Q})^{-1}\overline{\rho}(\tau)\overline{Q}$ is in Jordan Canonical Form, and let $Q \in \mathrm{GL}(r, \mathbb{Z}[\zeta_m])$ be a lift of $\overline{Q}$. Note that $\det Q \notin \mathfrak{p}$ and $(\det Q)Q^{-1}$ has entries in $\mathbb{Z}[\zeta_m]$. Let $x \in \mathbb{Z}[\zeta_m]$ such that

$$x \cdot \det Q \equiv 1 \bmod \mathfrak{p},$$

so that

$$x \cdot (\det Q)Q^{-1}\rho(\tau)Q \equiv (\overline{Q})^{-1}\overline{\rho}(\tau)\overline{Q} \bmod \mathfrak{p}.$$

Let $J \in \mathrm{GL}(r, \mathbb{Z}[\zeta_m])$ be the naive lift of $(\overline{Q})^{-1}\overline{\rho}(\tau)\overline{Q}$ such that J is in Jordan Canonical Form. It follows that

$$x \cdot (\det Q)Q^{-1}\rho(\tau)Q = J + P',$$

where P' is an $r \times r$ matrix with entries in $\mathfrak{p}$. Hence

$$Q^{-1}\rho(\tau)Q = J + \underbrace{J\left(\frac{1}{x \cdot \det Q} - 1\right) + P'}_{=P},$$

where P is an $r \times r$ matrix with entries in $\mathbb{Q}(\zeta_m)$ having $\mathfrak{p}$-adic valuation greater than zero.

Now, fix $0 \leqslant a \leqslant m-1$, and suppose, in the notation of Theorem 4.8, we have ζ_m^a is a root of $q_{d,j}(x)$. Then the elementary divisors of $(x - \zeta_m^a)$ are

$$(x - \zeta_m^a)^{e_{d,j,1}}, (x - \zeta_m^a)^{e_{d,j,2}}, \ldots, (x - \zeta_m^a)^{e_{d,j,t(d,j)}}.$$

It follows that there are precisely $t(d,j)$ rows of $(p + \zeta_m^a)I - (J + P)$ composed entirely of entries with $\mathfrak{p}$-adic valuation greater than zero. It follows that

$$\nu_{\mathfrak{p}}(h_{\rho(\tau)}(p + \zeta_m^a)) = \nu_{\mathfrak{p}}\big(\det\big((p + \zeta_m^a)I - (J + P)\big)\big) \geqslant t(d,j).$$

On the other hand, we have

$$\begin{aligned}\nu_{\mathfrak{p}}(h_{\rho(\tau)}(p + \zeta_m^a)) &= \nu_{\mathfrak{p}}\left(\frac{(p + \zeta_m^a)^{p^e m} - 1}{p + \zeta_m^a - 1}\right) \\ &= \nu_{\mathfrak{p}}\left((p + \zeta_m^a)^{p^e m} - 1\right) - \nu_{\mathfrak{p}}(p + \zeta_m^a - 1).\end{aligned}$$

Note that $(\zeta_m^a + p)^m = 1 + pu$ where $\nu_\mathfrak{p}(u) = 0$, so

$$(\zeta_m^a + p)^{p^e m} - 1 = \sum_{j=1}^{p^e} \binom{p^e}{j} (pu)^j.$$

We also have $\nu_\mathfrak{p}(p) = 1$, so

$$\nu_\mathfrak{p}\left(\binom{p^e}{j}(pu)^j\right) = e - \nu_\mathfrak{p}(j) + j$$

is increasing $\mathfrak{p}$-adically. Hence

$$\begin{aligned}
\nu_\mathfrak{p}(h_{\rho(\tau)}(p + \zeta_m^a)) &= \nu_\mathfrak{p}\left(\sum_{j=1}^{p^e} \binom{p^e}{j}(pu)^j\right) - \nu_\mathfrak{p}(p + \zeta_m^a - 1) \\
&= \nu_\mathfrak{p}\left(\binom{p^e}{1} pu\right) - \nu_\mathfrak{p}(p + \zeta_m^a - 1) \\
&= e + 1 - \nu_\mathfrak{p}(p + \zeta_m^a - 1).
\end{aligned}$$

Putting it all together we get

$$t(d, j) \leqslant \nu_\mathfrak{p}(h_{\rho(\tau)}(p + \zeta_m^a)) = e + 1 - \nu_\mathfrak{p}(p + \zeta_m^a - 1).$$

Since

$$\nu_\mathfrak{p}(p + \zeta_m^a - 1) = \begin{cases} 1 & \text{if } a = 0 \\ 0 & \text{else,} \end{cases}$$

the theorem follows. □

So we immediately obtain

Proof of Theorem 1.13. Suppose $\#G = p$ and let τ be a generator for G. In the notation of Theorem 4.8, the invariant factors for $\overline{\rho}(\tau)$ are

$$(x-1)^{e_{1,1,1}}, (x-1)^{e_{1,1,2}}, \ldots, (x-1)^{e_{1,1,t(1,1)}}.$$

By Proposition 4.17, we have $t(1,1) = 1$. Hence $E \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}[G]$-module. □

Since it has nothing to do with anything, we end this section with a curious digression whose significance we don't fully understand.

Proposition 4.18. *There exists an embedding*

$$(D_F \cap P_F)/(D_F \cap P_F)^p \Big/ \ker\psi \hookrightarrow \mathrm{Dl}_k[p]$$

where we view $\ker\psi$ *as a subgroup of* $D_F \cap P_F \Big/ (D_F \cap P_F)^p$ *by Lemma 4.10.*

Proof. Let $(b) \in D_F \cap P_F$. Then $(b)\mathfrak{o}_k = \mathfrak{D}^p$ for some $\mathfrak{D} \in D_k$. So the following map is well-defined:

$$\begin{aligned} \Psi : D_F \cap P_F \Big/ (D_F \cap P_F)^p &\to \mathrm{Dl}_k[p] \\ (b) \bmod (D_F \cap P_F)^p &\mapsto [\mathfrak{D}] = [((b)\mathfrak{o}_k)^{1/p}]. \end{aligned}$$

If $(b) \bmod (D_F \cap P_F)^p \in \ker\Psi$, then $\mathfrak{D} = (\delta)$ for some $(\delta) \in P_k$. So $(b)\mathfrak{o}_k = (\delta)^p$, hence $(b) \in R_F$. Also, since $(b) \in D_F$, it follows that $(b) \bmod P_F^p \in \ker\psi$, so $\ker\Psi \subseteq \ker\psi$.

Conversely, if $(b) \bmod P_F^p \in \ker\psi$, then there exists $(c) \in P_F$ such that $(bc^p) \in D_F \cap P_F$, there exists $\mathfrak{D} \in D_k$ such that $(bc^p) = \mathfrak{D}^p$, and there exists $(\beta) \in P_k$ such that $(b)\mathfrak{o}_k = (\beta)^p$. It follows that $\mathfrak{D}^p = (c\beta)^p$, so $\mathfrak{D} = (c\beta)$. Hence $\ker\psi \subseteq \ker\Psi$, and the proposition follows. □

From Proposition 4.18, it follows that if the group

$$(D_F \cap P_F)/(D_F \cap P_F)^p \Big/ \ker\psi$$

is non-trivial, then $p \mid \#\,\mathrm{Dl}_k \mid \#\,\mathrm{Cl}$. This observation leads to the following corollary.

Corollary 4.19. *Let* s *denote the number of rational primes ramifying in* k *whose ramification indices are divisible by* p. *If* $s > e$, *then* $\mathrm{rank}_{\mathbb{F}_p} \mathrm{Cl}_k \geqslant s - e$.

Proof. Let F' denote the fixed field of the non-p parts of $\mathrm{Gal}(k/\mathbb{Q})$ so that $F'/\mathbb{Q}$ is a p-extension. Note that $\mathrm{Syl}_p(\mathrm{Cl}_{F'}) \hookrightarrow \mathrm{Cl}_k$ since $\ker(\mathrm{Cl}_{F'} \to \mathrm{Cl}_k)$ has exponent prime to p. So it suffices to prove the corollary under the assumption that $[k : \mathbb{Q}] = p^e$. In this case we have $F = \mathbb{Q}$, $\mathrm{Cl}_F = 1$, and so by Equation (4.4), Lemma 4.7, and Lemma 4.10 we get

$$\left(E/E^p\right)^G \simeq R_{\mathbb{Q}}\Big/P_{\mathbb{Q}}^p = \ker\psi \subseteq D_{\mathbb{Q}} \cap P_{\mathbb{Q}}\Big/(D_{\mathbb{Q}} \cap P_{\mathbb{Q}})^p$$

On the other hand, by Proposition 4.17 we have

$$\mathrm{rank}_{\mathbb{F}_p}\left(E/E^p\right)^G \leqslant e,$$

whereas

$$\mathrm{rank}_{\mathbb{F}_p} D_{\mathbb{Q}} \cap P_{\mathbb{Q}}\Big/(D_{\mathbb{Q}} \cap P_{\mathbb{Q}})^p = s$$

where s is the number of rational primes ramifying in $k/\mathbb{Q}$. So if $s > e$, we get that

$$\mathrm{rank}_{\mathbb{F}_p} (D_F \cap P_F)/(D_F \cap P_F)^p\Big/\ker\psi \geqslant s - e.$$

Hence, by Proposition 4.18, we get that $\mathrm{rank}_{\mathbb{F}_p} \mathrm{Cl}_k \geqslant s - e$. □

This result is surprising, if anything, because no class field theory was required to prove it.

CHAPTER 5

APPLICATIONS

5.1 Stickelberger Theorems for Real Fields

As in Chapter 2, let E_S denote the S-units of k, let $\mathcal{K}$ denote the topological closure of k in $\mathbb{Q}_p^{alg}$, let $\mathcal{O}$ denote the ring of integers of $\mathcal{K}$, and let ϖ denote a uniformizer of $\mathcal{O}$. We write E for E_S if S consists only of the Archimedean places.

Define the map $\vartheta : k^\times \to \mathcal{K}[G]$ by

$$x \mapsto \sum_{\sigma \in G} \log_p(x^\sigma)\sigma^{-1},$$

where $\log_p$ is the Iwasawa logarithm [13, §V.4.5].

Lemma 5.1. *The map ϑ is a G-module map.*

Proof. The additivity of ϑ is obvious. For any $\tau \in G$, note that

$$\begin{aligned} \vartheta(x^\tau) &= \sum_{\sigma \in G} \log_p(x^{\tau\sigma})\sigma^{-1} && \text{let } \rho = \tau\sigma \\ &= \sum_{\rho \in G} \log_p(x^\rho)\rho^{-1}\tau \\ &= \tau\vartheta(x). \end{aligned}$$

So ϑ is a G-module map. □

In general, ϑ is not integrally valued. This brings us to the following definition.

Definition 5.2. *A group ring element $\beta \in \mathcal{K}[G]$ is called an S-integralizer if $\beta\vartheta(E_S) \subseteq \mathcal{O}[G]$. If S consists only of the Archimedean places, we simply say that β is an integralizer.*

Remark 5.3. *Note that an S-integralizer need not be integral itself! This is a curious and essential difference between this setting and the classical Stickelberger theory.*

The next lemma ensures that S-integralizers exist by establishing an explicit one for every S.

Lemma 5.4. *Let the ramification index of $\mathfrak{p}$ in k be $e = p^n b$ where $(p, b) = 1$. Then $\vartheta(k^\times) \subseteq (\varpi)^{p^n - ne} \cdot \mathcal{O}[G]$.*

Proof. Let $y \in \mathcal{O}^\times$, and let m be sufficiently large so that

$$y^{p^m - 1} \equiv 1 \mod \varpi.$$

Write $y^{p^m-1} - 1 = \varpi^t u$ where $u \in \mathcal{O}^\times$. Then

$$\log_p(y) = \frac{\log_p(y^{p^m-1})}{p^m - 1} = \frac{1}{p^m - 1} \sum_{j=1}^{\infty} u^j (-1)^{j-1} \frac{\varpi^{tj}}{j}.$$

For $j = p^a c$ where $(p, c) = 1$, we have $j = \varpi^{ea} v$ for some $v \in \mathcal{O}^\times$. So

$$\frac{\varpi^{tj}}{j} \in \varpi^{tp^a c - ae} \mathcal{O} \subseteq \varpi^{p^a - ae} \mathcal{O}.$$

It's straightforward to show that the quantity $p^a - ae$ is smallest when $a = n$ because $b \leqslant \dfrac{p-1}{2}$. It follows that $\log_p(y) \in \varpi^{p^n - ne}\mathcal{O}$. □

Remark 5.5. *The above lemma shows that, for example, $\varpi^{ne - p^n}$ integralizes $\vartheta|_{E_S}$ for any given S. If $\mathfrak{p}$ is tamely ramified in k, this reduces to ϖ^{-1}. If $\mathfrak{p}$ is unramified, this reduces to p^{-1} as in Solomon [17, Conjecture 4.1].*

In lieu of Corollary 2.14, we also make the following definition.

Definition 5.6. *If k satisfies either (i) or (ii) of Corollary 2.14, then we say that k is $\mathfrak{p}$-simple. If, in addition, $\mathfrak{p} \nmid \mathfrak{a}$, then we say that k is $\mathfrak{p}$-simple for $\mathfrak{a}$.*

Combining the results of the previous chapters, we obtain one of the main goals of this dissertation: a proof of Theorem 1.14 and the explicit derivation of annihilators of the ray class groups of a real abelian number field (in lieu of Lemma 5.4). This gives the first full proof of (a much strengthened version of) a conjecture of D. Solomon [17, Conjecture 4.1], and is the real analog of the classical theorem of Stickelberger and its generalizations obtained by Sinnott and Schmidt.

Theorem 5.7. *Let β be an S-integralizer. If k is $\mathfrak{p}$-simple with respect to $\mathfrak{a}$, then*

$$\beta\vartheta(C_S(\mathfrak{a})) \quad \textit{annihilates} \quad \mathrm{Cl}(\mathfrak{a}) \otimes \mathcal{O}.$$

Otherwise

$$R_0 \cdot \beta\vartheta(C_S(\mathfrak{a})) \quad \textit{annihilates} \quad \mathrm{Cl}(\mathfrak{a}) \otimes \mathcal{O}.$$

Proof. This follows immediately from Corollary 2.14, Lemma 5.1, and Theorem 3.3. □

For an integralizer $\beta = \sum b_\sigma \sigma^{-1} \in \mathcal{K}[G]$, we set

$$\begin{aligned} R_0 &= \left\{ \sum a_\sigma \sigma^{-1} \in \mathcal{O}[G] : \sum a_\sigma = 0 \right\} \\ S_{0,\beta}(\mathfrak{a}) &= \text{the } \mathcal{O}[G] \text{ ideal generated by } \beta\vartheta(C(\mathfrak{a})) \\ T_{0,\beta} &= \text{the } \mathcal{O}[G] \text{ ideal generated by } \beta\vartheta(E). \end{aligned}$$

Additionally, let

$$L_\beta(x) = \sum_{\tau \in G} b_{\tau^{-1}} \log_p(x^\tau)$$

so that

$$\beta\vartheta(x) = \sum_{\sigma \in G} L_\beta(x^\sigma)\sigma^{-1}.$$

We also consider β as a linear transformation $\mathcal{K}[G] \to \mathcal{K}[G]$ defined by $\gamma \mapsto \beta\gamma$. Let $R_p(k)$ denote the Leopoldt regulator of k (see [10]) and $q = \#\mathcal{O}/(\varpi)$.

Theorem 5.8. *If* $[R_0 : S_{0,\beta}]$ *is finite, then*

$$[R_0 : S_{0,\beta}(\mathfrak{a})] = q^{\operatorname{ord}_\varpi [E:C(\mathfrak{a})] + \operatorname{ord}_\varpi R_p(k) + \operatorname{ord}_\varpi \det \beta|_{R_0}}.$$

Proof. Suppose the above index is finite, and note that $[R_0 : S_{0,\beta}(\mathfrak{a})]$ is finite if and only if $\det \beta|_{R_0} \neq 0$. Now, we observe $\ker \log_p \Big|_E = \{\pm 1\}$, so

$$1 \to \pm 1 \to E \xrightarrow{\beta\vartheta} \mathcal{O}[G]$$

is exact. Since $\mathcal{O}$ is a flat $\mathbb{Z}$-module, we get that the map $E \otimes \mathcal{O} \to \mathcal{O}[G]$ defined by $\epsilon \otimes x \mapsto \beta\vartheta(\epsilon)x$ is an injective homomorphism because $p \neq 2$. Moreover, for all $\sum a_\sigma \sigma \in \mathcal{O}[G]$ we have that

$$\sum (\epsilon^\sigma \otimes a_\sigma) \mapsto \sum \beta\vartheta(\epsilon^\sigma) a_\sigma = \beta\vartheta(\epsilon) \sum a_\sigma \sigma.$$

So $T_{0,\beta} \simeq E \otimes \mathcal{O}$, and similarly, $S_{0,\beta}(\mathfrak{a}) \simeq C(\mathfrak{a}) \otimes \mathcal{O}$ as $\mathcal{O}[G]$ modules. Hence

$$[T_{0,\beta} : S_{0,\beta}(\mathfrak{a})] = [E \otimes \mathcal{O} : C(\mathfrak{a}) \otimes \mathcal{O}] = \#\left((E/C(\mathfrak{a})) \otimes \mathcal{O}\right) = q^{\operatorname{ord}_\varpi [E:C(\mathfrak{a})]}.$$

It remains to compute $[R_0 : T_{0,\beta}]$. Let $\epsilon_1, \ldots, \epsilon_r$ be a system of fundamental units for E, and let $\sigma_1, \ldots, \sigma_r$ be the non-identity elements of G. Then $T_{0,\beta}$ is the $\mathcal{O}$-span of the $\beta\vartheta(\epsilon_i)$ while R_0 is the $\mathcal{O}$-span of the $\sigma_i^{-1} - 1$. Let $a_{ij} \in \mathcal{O}$ such that

$$\beta\vartheta(\epsilon_j) = \sum_{i=1}^{r} a_{ij}(\sigma_i^{-1} - 1),$$

for each $j = 1, \ldots, r$. If $[R_0 : T_{0,\beta}]$ is finite where $e_1, \ldots, e_r$ and $f_1, \ldots, f_r$ are bases of the $\mathcal{O}$-modules R_0 and $T_{0,\beta}$, respectively, with

$$f_j = \sum_{i=1}^{r} a_{ij} e_i,$$

then

$$[R_0 : T_{0,\beta}] = q^{\operatorname{ord}_\varpi \det(a_{ij})}.$$

Now, note that

$$\begin{aligned}\beta\vartheta(\epsilon_j) &= L_\beta(\epsilon_j) + \sum_{i=1}^{r} L_\beta(\epsilon_j^{\sigma_i})\sigma_i^{-1} \\ &= L_\beta(N_{\mathbb{Q}}^k(\epsilon_j)) + \sum_{i=1}^{r} L_\beta(\epsilon_j^{\sigma_i})(\sigma_i^{-1} - 1) \\ &= \sum_{i=1}^{r} L_\beta(\epsilon_j^{\sigma_i})(\sigma_i^{-1} - 1),\end{aligned}$$

since $N_{\mathbb{Q}}^k(\epsilon) = \pm 1 \in \ker \log_p\Big|_E$. Similarly, we have

$$\begin{aligned}L_\beta(\epsilon_j^{\sigma_i}) &= \sum_{\tau\in G} b_{\tau^{-1}} \log_p \epsilon_j^{\sigma_i\tau} \\ &= \sum_{\tau\in G} b_{\tau^{-1}\sigma_i} \log_p \epsilon_j^{\tau} \\ &= \sum_{k=1}^{r} (b_{\sigma_i\sigma_k^{-1}} - b_{\sigma_i}) \log_p \epsilon_j^{\sigma_k}.\end{aligned}$$

So

$$(a_{ij}) = (L_\beta(\epsilon_j^{\sigma_i})) = (b_{\sigma_i\sigma_j^{-1}} - b_{\sigma_i})(\log_p \epsilon_j^{\sigma_i}).$$

We also compute

$$\beta(\sigma_j^{-1} - 1) = \sum_{i=1}^{r} (b_{\sigma_i\sigma_j^{-1}} - b_{\sigma_i})(\sigma_i^{-1} - 1),$$

hence

$$\det(a_{ij}) = (\det \beta|_{R_0}) R_p(k).$$

This completes the proof of the theorem. □

Considering Corollary 2.14, we are even more interested in the following ideal

$$S_0(\mathfrak{a}) := \langle \alpha(C(\mathfrak{a})) : \alpha \in \mathrm{Hom}_G(E, \mathcal{O}[G]) \rangle_{\mathcal{O}[G]}.$$

As it happens, every element of $\mathrm{Hom}_G(E, \mathcal{O}[G])$ is of the type $\beta\vartheta$.

Theorem 5.9. *For every $\alpha \in \mathrm{Hom}_G(E, \mathcal{O}[G])$, there exists $\beta \in \mathcal{K}[G]$ such that $\alpha = \beta\vartheta|_E$. Consequently,*

$$T_0 = \sum T_{0,\beta} \quad \textit{and} \quad S_0(\mathfrak{a}) = \sum S_{0,\beta}(\mathfrak{a}),$$

where $T_0 = \langle \alpha(E) : \alpha \in \mathrm{Hom}_G(E, \mathcal{O}[G])\rangle_{\mathcal{O}[G]}$ and each sum varies over all integralizers.

Proof. Let $\epsilon \in E$ such that $[E : \langle\epsilon\rangle_{\mathbb{Z}[G]}] = m$ is finite. Let Q_0 denote the collection of trace-zero elements of $\mathcal{K}[G]$, and let $\Theta : Q_0 \to Q_0$ be the linear map defined by multiplication by $\vartheta(\epsilon)$. Then

$$\det\Theta = \prod_{\substack{\chi \in \widehat{G} \\ \chi \neq 1}} \sum_{\sigma \in G} \chi(\sigma) \log_p \epsilon^\sigma.$$

Since $\{\log_p \epsilon^\sigma\}_{\sigma \neq \mathrm{id}}$ are linearly independent over $\mathbb{Q}$, a theorem of Brumer [2] gives us that they are linearly independent over $\mathbb{Q}^{\mathrm{alg}}$. Note that

$$\sum_{\sigma \in G} \chi(\sigma) \log_p(\epsilon^\sigma) = \sum_{\sigma \neq 1} (\chi(\sigma) - 1) \log_p(\epsilon^\sigma),$$

hence $\det\Theta \neq 0$.

Now, let $\alpha \in \mathrm{Hom}_G(E, \mathcal{O}[G])$. Since Θ is onto, there exists $\beta \in Q_0$ such that

$$\Theta(\beta) = \beta\vartheta(\epsilon) = \alpha(\epsilon).$$

For any $\eta \in E$, we have that

$$\alpha(\eta) = \frac{\alpha(\eta^m)}{m},$$

where $\eta^m = \epsilon^\psi$ for some $\psi \in \mathbb{Z}[G]$. So

$$\alpha(\eta) = \frac{\psi\beta\vartheta(\epsilon)}{m} = \beta\vartheta(\eta).$$

Hence $\alpha = \beta\vartheta|_E$, as claimed. □

Remark 5.10. *In this way, we see that $S_0(\mathfrak{a})$ is analogous to the classical Stickelberger ideal, and the elements $\vartheta(\delta)$ for $\delta \in C(\mathfrak{a})$ are analogous to the classical Stickelberger elements.*

By comparison with Theorem 5.8, one might hope that the index $[R_0 : S_0(\mathfrak{a})]$ is free of the conspicuous contributions from the Leopoldt regulator and integralizer β. This is often the case, and the key step is understanding how T_0 relates to R_0.

Theorem 5.11. *If* $E \otimes \mathbb{F}_p$ *is a cyclic* $\mathbb{F}_p[G]$*-module, then* $T_0 = R_0$*. If we additionally assume that* $\mathrm{Syl}_p(G)$ *is cyclic, then*

$$R_0/S_0(\mathfrak{a}) \simeq (E/C(\mathfrak{a})) \otimes \mathcal{O}.$$

In particular, if $\mathfrak{a} = 1$ *and* $p \nmid \#G$*, then*

$$\#(R_0/S_0) = \#(\mathrm{Cl} \otimes \mathcal{O}).$$

Proof. Let $\epsilon \in E$ such that $[E : \langle \epsilon \rangle_{\mathbb{Z}[G]}] = m$ where $(p, m) = 1$. For any $\kappa \in R_0$, let $\alpha_\kappa : E \to \mathcal{O}[G]$ be defined by $\alpha_\kappa : \epsilon \mapsto \kappa$ extended to the rest of $\eta \in E$ by

$$\alpha_\kappa(\eta) = \frac{\alpha_\kappa(\eta^m)}{m}.$$

Note that α_κ is well-defined since $m \in \mathcal{O}^\times$, hence $T_0 = R_0$.

Now, suppose $\mathrm{Syl}_p(G)$ is cyclic. Then R_0 is cyclic (see [4]). Suppose κ is a generator for R_0 and let $\beta \in \mathcal{K}[G]$ such that $\alpha_\kappa = \beta\vartheta|_E$, by Theorem 5.9. It follows that $\ker \alpha_\kappa = \pm 1$, $T_{0,\beta} = R_0$, and $S_{0,\beta}(\mathfrak{a}) = S_0(\mathfrak{a})$ so that

$$\begin{aligned} R_0/S_0(\mathfrak{a}) &= T_{0,\beta}/S_{0,\beta}(\mathfrak{a}) \\ &\simeq \left(E \otimes \mathcal{O} \Big/ C(\mathfrak{a}) \otimes \mathcal{O} \right) \\ &\simeq (E/C(\mathfrak{a})) \otimes \mathcal{O}. \end{aligned}$$

The last statement of the theorem now follows from Theorem 3.15. □

5.2 On the Annihilators of $E/C(\mathfrak{a})$

In this section, we wish to know how $S_0(\mathfrak{a})$ compares with $\mathrm{Ann}_{\mathcal{O}[G]}(E/C(\mathfrak{a})) \otimes \mathcal{O}$. When $E \otimes \mathbb{F}_p$ is cyclic, these ideals are essentially equal.

Theorem 5.12. *If* $E \otimes \mathbb{F}_p$ *is cyclic, then*

$$S_0(\mathfrak{a}) = R_0 \cdot \mathrm{Ann}_{\mathcal{O}[G]}(E/C(\mathfrak{a})) \otimes \mathcal{O}.$$

Proof. Let $\epsilon \in E$ such that $[E : \langle\epsilon\rangle_{\mathbb{Z}[G]}] = m$ where $(p, m) = 1$. For any $\kappa \in R_0$, let $\alpha_\kappa : E \to \mathcal{O}[G]$ be defined as in the proof of Theorem 5.11. Let $\beta \in \mathcal{K}[G]$ such that $\alpha_\kappa = \beta\vartheta|_E$ (using Theorem 5.9). Let $E' = \ker \alpha_\kappa$, $C'(\mathfrak{a}) = E' \cap C(\mathfrak{a})$, and note that by the flatness of $\mathcal{O}$ as a $\mathbb{Z}$-module, we have

$$\begin{aligned} E \Big/ E'C(\mathfrak{a}) \otimes \mathcal{O} &\simeq (E/E') \otimes \mathcal{O} \Big/ (C(\mathfrak{a})/C'(\mathfrak{a})) \otimes \mathcal{O} \\ &\simeq T_{0,\beta}/S_{0,\beta}(\mathfrak{a}). \end{aligned}$$

It follows that if $\gamma \in \mathrm{Ann}_{\mathcal{O}[G]}(E/C(\mathfrak{a})) \otimes \mathcal{O}$, then $\gamma\alpha_\kappa(\epsilon) = \gamma\kappa \in S_{0,\beta}(\mathfrak{a})$. The theorem now follows by Theorem 5.9 . □

Combining Theorems 5.7 and 5.12 we immediately obtain the following corollary.

Corollary 5.13. *If* $E \otimes \mathbb{F}_p$ *is cyclic then*

$$\mathrm{Cl}(\mathfrak{a}) \otimes \mathcal{O} \quad \textit{is annihilated by} \quad \begin{cases} R_0 \cdot \mathrm{Ann}_{\mathcal{O}[G]}(E/C(\mathfrak{a})) \otimes \mathcal{O} & \textit{if } k \textit{ is } p\textit{-simple for } \mathfrak{a} \\ R_0^2 \cdot \mathrm{Ann}_{\mathcal{O}[G]}(E/C(\mathfrak{a})) \otimes \mathcal{O} & \textit{else.} \end{cases}$$

The above corollary is a generalization of Thaine's [19, Theorem 6], in fact, if $\mathfrak{a} = 1$ and $p \nmid \#G$, then it is precisely [19, Theorem 6].

Remark 5.14. *Recall the definition of* $\mathcal{C}(\mathfrak{a})$ *from Chapter 2. Let*

$$\begin{aligned} \mathcal{S}_{0,\beta}(\mathfrak{a}) &:= \langle \beta\vartheta(\mathcal{C}(\mathfrak{a}))\rangle_{\mathcal{O}[G]} \\ \mathcal{S}_0(\mathfrak{a}) &:= \langle \alpha(\mathcal{C}(\mathfrak{a})) : \alpha \in \mathrm{Hom}_G(E, \mathcal{O}[G])\rangle_{\mathcal{O}[G]}. \end{aligned}$$

By Theorem 5.9, we have $\mathcal{S}_0(\mathfrak{a}) = \sum \mathcal{S}_{0,\beta}$ *where the sum runs over all integralizers* β*. Note that Theorem 5.7, Theorem 5.8, the first part of Theorem 5.11, Theorem 5.12, and*

Corollary 5.13 all hold with $\mathcal{C}(\mathfrak{a})$, $\mathcal{S}_{0,\beta}(\mathfrak{a})$, *and* $\mathcal{S}_0(\mathfrak{a})$ *in place of* $C(\mathfrak{a})$, $S_{0,\beta}(\mathfrak{a})$, *and* $S_0(\mathfrak{a})$, *respectively. However, it isn't clear whether there exist* $\mathfrak{a}$*-special units other than the* $\mathfrak{a}$*-cyclotomic units. For fun, take* $k = \mathbb{Q}(\sqrt{p})$ *where* p *is a prime congruent to* 1 *modulo* 4. *Then the cyclotomic units of* k *are cyclic generated by*

$$\delta = \prod_{a=1}^{p} (1 - \zeta_p^a)^{-\chi(a)},$$

where $\chi : \mathbb{Z}/p\mathbb{Z}^\times \to \{\pm 1\}$ *is the quadratic character. It is known that* $\#Cl$ *is odd, and from Corollary 2.14, we have that* $(1-\tau)[E : \mathcal{C}]$ *annihilates* $\#\,Cl$ *where* τ *is the non-identity element of* G. *Since* τ *acts by inversion on the ideal class group of* k, *it follows that* $2[E : \mathcal{C}]$ *annihilates* $\#\,Cl$. *Since* $\#\,Cl$ *is odd, it follows that the exponent of* Cl *divides* $[E : \mathcal{C}]$. *On the other hand, from Chapter 3, we know that* $[E : C] = 2 \cdot \#\,Cl$. *If* Cl *is cyclic, then the exponent of* $\#\,Cl$ *equals the exponent, hence*

$$\#\,Cl \mid [E : \mathcal{C}] \mid [E : C] = 2 \cdot \#\,Cl\,.$$

Hence $[\mathcal{C} : C]$ *is equal to* 1 *or* 2. *On the other hand, suppose* $p = 62501$. *It is known that* $Cl \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *in this case, so if* $[\mathcal{C} : C]$ *was non-trivial, i.e., not equal to* 1 *or* 2, *then the* 3*-part of* $[E : \mathcal{C}]$ *is equal to the exponent of* $\mathrm{Syl}_3(Cl)$. *For this reason, it would be very interesting to know whether special units other than the cyclotomic units exist, and if so, do they make a habit of giving information about the exponent of* Cl.

BIBLIOGRAPHY

[1] Jean-Robert Belliard and Thống Nguyễn-Quang-Dỗ. On modified circular units and annihilation of real classes. *Nagoya Math. J.*, 177:77–115, 2005.

[2] Armand Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[3] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[4] Daniel R. Farkas and Robert L. Snider. When is the augmentation ideal principal? *Arch. Math. (Basel)*, 33(4):348–350, 1979/80.

[5] Ralph Greenberg. On the Iwasawa invariants of totally real number fields. *Amer. J. Math.*, 98(1):263–284, 1976.

[6] Helmut Hasse. *Über die Klassenzahl abelscher Zahlkörper*. Akademie-Verlag, Berlin, 1952.

[7] Kenkichi Iwasawa. A class number formula for cyclotomic fields. *Ann. of Math. (2)*, 76:171–179, 1962.

[8] E.E. Kummer. Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers. *Collected Papers I*, Berlin-Heidelberg-New York: Springer-Verlag, 1975.

[9] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[10] Heinrich-Wolfgang Leopoldt. Zur Arithmetik in abelschen Zahlkörpern. *J. Reine Angew. Math.*, 209:54–71, 1962.

[11] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[12] Hermann Minkowski. *Geometrie der Zahlen*. Bibliotheca Mathematica Teubneriana, Band 40. Johnson Reprint Corp., New York, 1968.

[13] Alain M. Robert. *A course in* p*-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[14] Karl Rubin. Global units and ideal class groups. *Invent. Math.*, 89(3):511–526, 1987.

[15] C.-G. Schmidt. Stickelbergerideale und Kreiseinheiten zu Klassenkörpern abelscher Zahlkörper. *J. Reine Angew. Math.*, 353:14–54, 1984.

[16] W. Sinnott. On the Stickelberger ideal and the circular units of an abelian field. *Invent. Math.*, 62(2):181–234, 1980/81.

[17] David Solomon. On a construction of p-units in abelian fields. *Invent. Math.*, 109(2):329–350, 1992.

[18] L. Stickelberger. Ueber eine Verallgemeinerung der Kreistheilung. *Math. Ann.*, 37(3):321–367, 1890.

[19] Francisco Thaine. On the ideal class groups of real abelian number fields. *Ann. of Math. (2)*, 128(1):1–18, 1988.

[20] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.