ACTA ARITHMETICA
178.3 (2017)

Gauss sums, Stickelberger's theorem and the Gras conjecture for ray class groups

by

Timothy All (Terre Haute, IN)

1. Introduction. Let k denote a real abelian number field with Galois group G. Let $\mathfrak{o}_k = \mathfrak{o}$ denote the ring of integers of k, and let $E = \mathfrak{o}^\times$. Fix $d \in \mathbb{N}$ and let E_d denote the group of units of $\mathfrak{o}$ that are congruent to 1 modulo d. Let $\overline{d}$ denote the product of distinct prime divisors of d, and for every $n \in \mathbb{N}$ let ζ_n stand for a primitive nth root of unity. We assume the ζ_n have been chosen so that for every $t \mid n$ we have $\zeta_n^t = \zeta_{n/t}$. For every $n \in \mathbb{N}$, let $k^n = \mathbb{Q}(\zeta_n) \cap k$, and for $n > 1$ satisfying $n \nmid \overline{d}$, let

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

where $\mu(t)$ denotes the Möbius function.

Let $D(d)$ denote the G-module generated by the $\delta_{n,d}$ for all $n \nmid \overline{d}$ in $k^\times$. We let

$$C(d) = E \cap D(d), \qquad C_d = E_d \cap D(d).$$

We call the modules $D(d)$, $C(d)$, and C_d the *d-cyclotomic numbers*, *units*, and *units congruent to 1 modulo d*, respectively. We write D for $D(1)$ and C for $C(1)$. Note that $C(1) = C_1$. These modules were originally introduced by Sinnott [S] (for $d = 1$) and by Schmidt [Sch] (for $d > 1$). Note that C is not quite the full Sinnott group of cyclotomic units but rather its subgroup of totally positive units.

For an ideal $\mathfrak{a} \subseteq \mathfrak{o}$, let $\mathfrak{C}(\mathfrak{a})$ denote the ray class group of k of modulus $\mathfrak{a}$, and let $H(\mathfrak{a})$ denote the corresponding ray class field of k so that $\mathrm{Gal}(H(\mathfrak{a})/k) \simeq \mathfrak{C}(\mathfrak{a})$ via the Artin map. Let $H_\mathfrak{a} = H(\mathfrak{a}) \cap \mathbb{Q}^{\mathrm{ab}}$, the maximal subextension of $H(\mathfrak{a})/k$ abelian over $\mathbb{Q}$, and let $\mathfrak{C}_\mathfrak{a} \leq \mathfrak{C}(\mathfrak{a})$ be such that

2010 *Mathematics Subject Classification*: Primary 11R80.
Key words and phrases: ray class group, Stickelberger, circular units, Gauss sum, real abelian number field.
Received 28 May 2016; revised 30 January 2017.
Published online 26 April 2017.

DOI: 10.4064/aa8537-2-2017

$\mathfrak{C}_{\mathfrak{a}} \simeq \mathrm{Gal}(H(\mathfrak{a})/H_{\mathfrak{a}})$. In the case when $p \nmid [k:\mathbb{Q}]$, note that

$$\mathrm{Syl}_p(\mathfrak{C}_{\mathfrak{a}}) = (1-e_1)\,\mathrm{Syl}_p(\mathfrak{C}(\mathfrak{a}))$$

where $e_1 \in \mathbb{Z}_p[G]$ is the idempotent associate to the trivial character.

There is a fascinating interplay between unit structures and ideal structures in algebraic number theory. For example, the following theorem was proven by Sinnott [S, Theorem 4.1] for $d = 1$, and by Schmidt [Sch, Satz 3] for $d > 1$ using similar methods.

THEOREM 1.1. *If $p \nmid 2|G|$, then $|\mathrm{Syl}_p(E_d/C_d)| = |\mathrm{Syl}_p(\mathfrak{C}_d)|$.*

One of the aims of this article is to prove a Galois-equivariant version of the theorem above. To be precise, let $[\chi]$ be the $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{|G|})/\mathbb{Q}_p)$-orbit of a non-trivial character χ of G and define $\rho = \sum_{\psi\in[\chi]} \psi$. Let ϵ_ρ be the $\mathbb{Z}_p$-valued idempotent

$$\epsilon_\rho = \frac{1}{|G|}\sum_{\sigma\in G} \rho(\sigma)\sigma^{-1} \in \mathbb{Z}_p[G].$$

For a $\mathbb{Z}_p[G]$-module M, we let M_ρ denote the submodule $\epsilon_\rho M$.

Let $e(p)$ denote the ramification index of p in k. One of our main results is the following

THEOREM 1.2. *If $p \nmid 2|G|$ and $e(p) < p-1$, then*

$$|\mathrm{Syl}_p(E_d/C_d)_\rho| = |\mathrm{Syl}_p(\mathfrak{C}_d)_\rho|.$$

This is a ray class version of the Gras Conjecture [Gra], the statement of the claim when $d = 1$. Greenberg [Gre] observed that the Gras Conjecture followed from the Main Conjecture of Iwasawa theory which was later on proven by Mazur and Wiles [MW].

In the case when p possibly divides the order of G, we prove a result akin to Rubin's [R, Theorem 1.3], which itself was a generalization of a theorem of Thaine [Th, Theorem 3]. Our method of proof follows along those same lines. In particular, we define a subgroup $\mathcal{S}(\mathfrak{a})$ of E which we call the $\mathfrak{a}$-*special units*. These are akin to Rubin's special units [R], and we show that the d-cyclotomic units of Schmidt are a special instance of d-special units. We then show

THEOREM 1.3. *Let $\alpha : E \to \mathcal{O}[G]$ be any G-module map where $\mathcal{O}$ is the valuation ring of any finite extension of $\mathbb{Q}_p$, and let $\varsigma_{\mathfrak{a}} \in \mathcal{S}(\mathfrak{a})$. Then $\alpha(\varsigma_{\mathfrak{a}})$ annihilates $\mathfrak{C}_{\mathfrak{a}} \otimes_{\mathbb{Z}} \mathcal{O}$.*

As stated, our method of proof originates in the work of Thaine and Rubin. Thaine noticed that cyclotomic units could be used to generate elements α that act like real analogues of Gauss sums much like roots of unity are used to generate classical Gauss sums. To generate α, Thaine relied on an invocation of Hilbert's Theorem 90. A key feature here is that we give α

explicitly. This affords finer control over the ideal relations revealed by the factorization of α, thus paving the way towards annihilation results concerning ray classes. In particular we prove the following ray class version of a conjecture of D. Solomon [Sol, Conjecture 4.1] which acts as a sort of Stickelberger Theorem for ray class groups.

THEOREM 1.4. *Let $\mathcal{O}$ denote the valuation ring of a p-adic completion of k, and let $\varpi \in \mathcal{O}$ be a local parameter. For every $\varsigma_{\mathfrak{a}} \in \mathcal{S}(\mathfrak{a})$ the element*

$$\frac{|e(p)|_p^{-1}}{\varpi^{|e(p)|_p^{-1}}} \sum_{\sigma \in G} \log_p(\varsigma_{\mathfrak{a}}^{\sigma})\sigma^{-1} \in \mathcal{O}[G]$$

annihilates $\mathfrak{C}_{\mathfrak{a}} \otimes_{\mathbb{Z}} \mathcal{O}$.

2. Preliminaries. In this section, we collect some results concerning the structure of relevant G-modules contained in k. Until further notice, we consider p to be an odd prime not dividing $[k : \mathbb{Q}]$. Let

$$\begin{aligned} K &= \text{a local field containing the character values of } G, \\ \mathcal{O} &= \text{the valuation integers of } K, \\ \mathbb{F} &= \text{the residue field of } \mathcal{O}, \\ \mathbb{F}_p &= \text{the finite field with } p \text{ elements.} \end{aligned}$$

We normalize the p-adic absolute value in the usual way: $|p|_p = p^{-1}$. For any finite set X, we use $|X|$ to denote the number of elements in X. For $H \subseteq G$, we write $s(H)$ to denote the sum

$$s(H) = \sum_{\sigma \in H} \sigma \in \mathbb{Z}[G].$$

We write $\widehat{G}$ for $\mathrm{Hom}_{\mathbb{Z}}(G, \mathcal{O}^{\times})$. For every $\chi \in \widehat{G}$, we let

$$e_{\chi} = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in \mathcal{O}[G],$$

the idempotent associate to χ. We may naturally view $e_{\chi} \in \mathbb{F}[G]$.

Throughout, we use $\otimes$ as an abbreviation for $\otimes_{\mathbb{Z}}$. For a $\mathbb{Z}[G]$-module M and commutative ring R, we make $M \otimes R$ into an $R[G]$-module in the obvious way. The following proposition generalizes [A2, Theorem 3.3]. It will be useful later on for demonstrating that certain G-modules are cyclic.

PROPOSITION 2.1. *Let M be a free $\mathbb{Z}$-submodule of either $(k, +)$ or $(k^{\times}, \cdot)$ of finite rank such that $\sigma(M) = M$ for all $\sigma \in G$. For $H \leq G$, let M^H denote the collection of all elements of M fixed by H. For every $H \leq G$, suppose that the inclusion $M^H \subseteq M$ induces*

$$M^H \otimes \mathbb{F}_p \hookrightarrow M \otimes \mathbb{F}_p.$$

If there exists $m \in M$ such that $[M : \langle m\rangle_{\mathbb{Z}[G]}] < \infty$, then $M \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}_p[G]$-module.

Proof. Suppose $k/\mathbb{Q}$ is cyclic with σ generating G. Let $r = \operatorname{rank}_{\mathbb{Z}} M$ and let $\varrho : G \to \mathrm{GL}(r, \mathbb{Z})$ be the representation induced by the action of G on a fixed $\mathbb{Z}$-basis, say $\{m_1, \dots, m_r\}$, for M. Let $m_{\varrho(\sigma)}$ and $h_{\varrho(\sigma)}$ be the minimal and characteristic polynomials for $\varrho(\sigma)$, respectively. Suppose $m \in M$ is such that the index $[M : \langle m\rangle_{\mathbb{Z}[G]}]$ is finite. From this it follows that $r = \operatorname{rank}_{\mathbb{Z}}\langle m\rangle_{\mathbb{Z}[G]}$ and

$$h_{\varrho(\sigma)}(x) = m_{\varrho(\sigma)}(x) \mid x^{|G|} - 1.$$

Now, let $\overline{\varrho} : G \to \mathrm{GL}(r, \mathbb{F}_p)$ be the representation induced by the action of G on the $\mathbb{F}_p$-basis $\{m_1 \bmod pM, \dots, m_r \bmod pM\}$. Note that

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

Since $p \nmid |G|$, it follows that $h_{\overline{\varrho}(\sigma)}$ factors into a product of distinct irreducibles modulo p. So $M/pM \simeq M \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}_p[G]$-module.

Now suppose k is merely abelian over $\mathbb{Q}$, and let $\chi \in \widehat{G}$. Then χ naturally determines a character of $G' = G/\ker\chi$, the Galois group of the cyclic extension $k'/\mathbb{Q}$ where $k' = k^{\ker\chi}$. We write M' for $M^{\ker\chi}$, and let e'_χ denote the idempotent associate to $\chi \in \mathrm{Hom}_{\mathbb{Z}}(G', \mathcal{O}^\times)$, i.e.,

$$e'_\chi = \frac{1}{|G'|}\sum_{\sigma\in G'} \chi(\sigma)\sigma^{-1}.$$

Note that $e_\chi = |\ker\chi|^{-1} \operatorname{cores}^k_{k'} e'_\chi$ where $\operatorname{cores}^k_{k'}$ denotes corestriction from k' to k. We may naturally view e_χ and e'_χ as being $\mathbb{F}$-valued, in particular, we may view $\widehat{G}$ as a $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$-module. Let $[\chi] = \{\chi^\tau : \tau \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)\}$, and let $e_{[\chi]}, e'_{[\chi]} \in \mathbb{F}_p[G]$ be defined by

$$e_{[\chi]} = \sum_{\psi\in[\chi]} e_\psi \quad \text{and} \quad e'_{[\chi]} = \sum_{\psi\in[\chi]} e'_\psi.$$

It follows that $e_{[\chi]} = |\ker\chi|^{-1} \operatorname{cores}^k_{k'} e'_{[\chi]}$.

By assumption, $M' \subseteq M$ induces $M' \otimes \mathbb{F}_p \hookrightarrow M \otimes \mathbb{F}_p$. So we may view $M' \otimes \mathbb{F}_p \subseteq M \otimes \mathbb{F}_p$. For $m \in M$, we have

$$e_{[\chi]}(m \otimes 1) = \operatorname{cores}^k_{k'} e'_{[\chi]}(m \otimes (|\ker\chi|^{-1})) = e'_{[\chi]}(m^{s(\ker\chi)} \otimes (|\ker\chi|^{-1})).$$

Since $p \nmid n$, the map $M \otimes \mathbb{F}_p \to M' \otimes \mathbb{F}_p$ defined by $x \mapsto x^{s(\ker\chi)}$ is surjective. It follows that

$$e_{[\chi]}(M \otimes \mathbb{F}_p) = e'_{[\chi]}(M' \otimes \mathbb{F}_p) \subseteq M \otimes \mathbb{F}_p. \tag{2.1}$$

Now, viewing M' as a G'-module, we note that $k'/\mathbb{Q}$ is cyclic and M' satisfies all the hypotheses of the proposition: M' is a free $\mathbb{Z}$-module of finite rank that is preserved under the action of G', and for all $H' \subseteq G'$ the inclusion

$(M')^{H'} \subseteq M'$ induces $(M')^{H'} \otimes \mathbb{F}_p \hookrightarrow M' \otimes \mathbb{F}_p$ (otherwise there exists $H \leq G$ such that $M^H \otimes \mathbb{F}_p \hookrightarrow M \otimes \mathbb{F}_p$, contrary to assumption). So $M' \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}_p[G']$-module, whence $M' \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}_p[G]$-module.

Let $\mathfrak{m}' \in M' \otimes \mathbb{F}_p$ be such that $\mathfrak{m}'$ generates $M' \otimes \mathbb{F}_p$ as an $\mathbb{F}_p[G]$-module, and let $\mathfrak{m}_{[\chi]} = e_{[\chi]}\mathfrak{m}' \in M \otimes \mathbb{F}_p$. Using (2.1), we get

$$e_{[\chi]}(M \otimes \mathbb{F}_p) = e'_{[\chi]}(M' \otimes \mathbb{F}_p) = \langle \mathfrak{m}_{[\chi]} \rangle_{\mathbb{F}_p[G]}.$$

Let $\mathfrak{m} \in M \otimes \mathbb{F}$ be defined by $\mathfrak{m} = \sum \mathfrak{m}_{[\chi]}$ where the sum is taken over X, a complete system of representatives of $\widehat{G}/\operatorname{Gal}(\mathbb{F}/\mathbb{F}_p)$. Since $e_{[\chi]}\mathfrak{m} = \mathfrak{m}_{[\chi]}$, we have

$$M \otimes \mathbb{F}_p = \bigoplus_{\chi \in X} e_{[\chi]}(M \otimes \mathbb{F}_p) = \bigoplus_{\chi \in X} \langle \mathfrak{m}_{[\chi]} \rangle_{\mathbb{F}_p[G]} = \langle \mathfrak{m} \rangle_{\mathbb{F}_p[G]}.$$

This completes the proof of Proposition 2.1. ∎

LEMMA 2.2. *Let M be a $\mathbb{Z}[G]$-module. The following are equivalent:*

(i) *$M \otimes \mathbb{Z}_p$ is a cyclic $\mathbb{Z}_p[G]$-module.*
(ii) *$M \otimes \mathbb{F}_p$ is a cyclic $\mathbb{F}_p[G]$-module.*

Proof. For $\mathfrak{m} \in M \otimes \mathbb{Z}_p$, we have the exact sequence

$$\langle \mathfrak{m} \rangle_{\mathbb{Z}_p[G]} \otimes \mathbb{F}_p \to (M \otimes \mathbb{Z}_p) \otimes \mathbb{F}_p \simeq M \otimes \mathbb{F}_p \to \big((M \otimes \mathbb{Z}_p)/\langle \mathfrak{m} \rangle_{\mathbb{Z}_p[G]}\big) \otimes \mathbb{F}_p \to 0.$$

If $\langle \mathfrak{m} \rangle_{\mathbb{Z}_p[G]} = M \otimes \mathbb{Z}_p$, then the third term in this exact sequence is zero. Thus the first map must be onto, hence $\overline{\mathfrak{m}}$, the image of $\mathfrak{m}$ through the first map, generates $M \otimes \mathbb{F}_p$. So (i) implies (ii).

Conversely, suppose that $\overline{\mathfrak{m}} \in M \otimes \mathbb{F}_p$ satisfies $\langle \overline{\mathfrak{m}} \rangle_{\mathbb{F}_p[G]} = M \otimes \mathbb{F}_p$. Let $\mathfrak{m} \in M \otimes \mathbb{Z}_p$ reduce to $\overline{\mathfrak{m}}$ in $M \otimes \mathbb{F}_p$. Then the first map in the exact sequence above is onto, hence the third term in that sequence is zero. It follows that $\langle \mathfrak{m} \rangle_{\mathbb{Z}_p[G]} = M \otimes \mathbb{Z}_p$. So (ii) implies (i). ∎

COROLLARY 2.3. *The modules $E \otimes \mathbb{Z}_p$ and $\mathfrak{o} \otimes \mathbb{Z}_p$ are cyclic $\mathbb{Z}_p[G]$-modules. In fact*

$$E \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p[G]/s(G) \quad \textit{and} \quad \mathfrak{o} \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p[G].$$

Proof. Let $H \leq G$. Then E^H is the set of units of k^H and $\mathfrak{o}^H$ is the ring of integers of k^H. Since k is real and Galois, it follows that

$$E^H \otimes \mathbb{F}_p \hookrightarrow E \otimes \mathbb{F}_p.$$

Similarly,

$$\mathfrak{o}^H \otimes \mathbb{F}_p = \mathfrak{o}^H/(p) \hookrightarrow \mathfrak{o}/(p) = \mathfrak{o} \otimes \mathbb{F}_p.$$

The cyclicality of $E \otimes \mathbb{Z}_p$ and $\mathfrak{o} \otimes \mathbb{Z}_p$ now follows Proposition 2.1 and Lemma 2.2. The particular isomorphisms given in the claim are now straightforward to prove. ∎

For a prime ℓ, we adopt the following notation to be used throughout:

$$\begin{aligned}\sigma_\ell &= \text{a Frobenius automorphism in } G \text{ for } \ell,\\ I_\ell &= \text{the inertia subgroup in } G \text{ of } \ell,\\ e_\ell &= s(I_\ell)/|I_\ell|.\end{aligned}$$

We may consider $e_\ell \in \mathbb{Z}_p[G]$ since $p \nmid [k:\mathbb{Q}]$.

COROLLARY 2.4. *Suppose $\ell \neq p$ is a rational prime and $\mathfrak{L}$ the product of primes of $\mathfrak{o}$ over ℓ. Then for a positive integer e,*

$$(\mathfrak{o}/\mathfrak{L}^e)^\times \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p[G]/(\ell - \sigma_\ell e_\ell).$$

If $e(p)$ is less than $p-1$, then

$$(\mathfrak{o}/(p^e))^\times \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p[G]/(p^{e-1}(p - \sigma_p e_p)).$$

Proof. Suppose $\ell \neq p$. Then

$$(\mathfrak{o}/\mathfrak{L}^e)^\times \otimes \mathbb{Z}_p \simeq (\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}_p \simeq \prod_{\mathfrak{l}|\ell} (\mathfrak{o}/\mathfrak{l})^\times \otimes \mathbb{Z}_p$$

where the product is over all prime ideals $\mathfrak{l}$ of $\mathfrak{o}$ dividing ℓ. Fix such an ideal $\mathfrak{l}$ and let $u \in \mathfrak{o}^\times$ be such that $u \bmod \mathfrak{l}$ is a generator for the group $(\mathfrak{o}/\mathfrak{l})^\times$ and $u \equiv 1 \bmod \mathfrak{l}^\sigma$ for all $\sigma \in G$, $\sigma \neq 1$. We have

$$(\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}_p = \langle \mathfrak{u} \rangle_{\mathbb{Z}_p[G]} \quad \text{where} \quad \mathfrak{u} = u \otimes 1 \in (\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}_p.$$

Consider the surjective map

$$\varphi : \mathbb{Z}_p[G] \to (\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}_p, \qquad \theta \mapsto \mathfrak{u}^\theta.$$

Clearly, $(\ell - \sigma_\ell e_\ell) \subseteq \ker \varphi$. The claim will now follow from the fact that the quotient ring $\mathbb{Z}_p[G]$ modulo the ideal $(\ell - \sigma_\ell e_\ell)$ has the correct order.

To compute this order, we note that χ induces a homomorphism $\mathbb{Z}_p[G] \to \mathcal{O}$ in a natural way so that

$$|\mathbb{Z}_p[G]/(\ell - \sigma_\ell e_\ell)| = \prod_\chi |\chi(\ell - \sigma_\ell e_\ell)|_p^{-1}.$$

Note that

$$\chi(\ell - \sigma_\ell e_\ell) = \begin{cases} \ell, & I_\ell \not\subset \ker \chi,\\ (\ell - \chi(\sigma_\ell)), & I_\ell \subset \ker \chi.\end{cases}$$

So

$$|\mathbb{Z}_p[G]/(\ell - \sigma_\ell e_\ell)| = \prod_{\chi \in \widehat{G'}} |\ell - \chi(\sigma_\ell)|_p^{-1}$$

where $G' = G/I_\ell$. Let $G'_\ell = G_\ell/I_\ell$ where G_ℓ is the decomposition group for ℓ. Since the order of $\sigma_\ell \in G'_\ell$ is $f = [\mathfrak{o}/\mathfrak{l} : \mathbb{Z}/(\ell)]$, it follows that

$$\prod_{\chi \in \widehat{G'}} (\ell - \chi(\sigma_\ell)) = \prod_{a=0}^{f-1} (\ell - \zeta_f^a)^r = (\ell^f - 1)^r, \qquad r = [G : G_\ell].$$

Hence

$$|\mathbb{Z}_p[G]/(\ell - \sigma_\ell e_\ell)| = |\ell^f - 1|_p^{-r} = |(\mathfrak{o}/\mathfrak{L})^\times \otimes \mathbb{Z}_p| = |(\mathfrak{o}/\mathfrak{L}^e)^\times \otimes \mathbb{Z}_p|.$$

This proves the claim in the $\ell \neq p$ case.

Now, suppose $\ell = p$ and $e(p) < p-1$. For each prime $\mathfrak{p}$ of $\mathfrak{o}$ dividing p, let $U_\mathfrak{p}^{(j)} = \{x \in \mathfrak{o} : x \equiv 1 \bmod \mathfrak{p}^j\}$. Then

$$(\mathfrak{o}/(p^e))^\times \otimes \mathbb{Z}_p \simeq \prod_{\mathfrak{p}|p} (\mathfrak{o}/\mathfrak{p}^{e\cdot e(p)})^\times \otimes \mathbb{Z}_p \simeq \prod_{\mathfrak{p}|p} U_\mathfrak{p}^{(1)}/U_\mathfrak{p}^{(e\cdot e(p))}. \tag{2.2}$$

For all $x \in \mathfrak{o}$ satisfying $|x|_p < p^{-1/(p-1)}$, we know that $\log_p(1+x)$ and $\exp_p(x)$ are defined by their power series, moreover, $\exp_p(\log_p(1+x)) = 1+x$. Since $e(p) < p-1$, we have $|1+x|_p < p^{-1/(p-1)}$ for all $1+x \in U_\mathfrak{p}^{(1)}$. Thus the following map is a $\mathbb{Z}_p[G_p]$-isomorphism:

$$U_\mathfrak{p}^{(1)}/U_\mathfrak{p}^{(e\cdot e(p))} \to \mathfrak{p}/\mathfrak{p}^{e\cdot e(p)}, \qquad 1+x \mapsto \log_p(1+x) \bmod \mathfrak{p}^{e\cdot e(p)}.$$

From (2.2), we now have

$$(\mathfrak{o}/(p^e))^\times \otimes \mathbb{Z}_p \simeq \prod_{\mathfrak{p}|p} \mathfrak{p}/\mathfrak{p}^{e\cdot e(p)} \simeq \mathfrak{P}/(p^e)$$

as $\mathbb{Z}_p[G]$-modules where $\mathfrak{P}$ is the product of primes of $\mathfrak{o}$ over p. It follows from Prosposition 2.1 that $\mathfrak{P} \otimes \mathbb{Z}_p$ is a cyclic module, so the above isomorphism tells us that $(\mathfrak{o}/(p^e))^\times \otimes \mathbb{Z}_p$ is cyclic. It remains to show that $\mathfrak{P}/(p^e)$ is isomorphic to $\mathbb{Z}_p[G]/(p^e - p^{e-1}\sigma_p e_p)$ as a $\mathbb{Z}_p[G]$-module.

Since $\mathfrak{o}/(p^e)$ is cyclic, there is an onto homomorphism $\psi : \mathbb{Z}_p[G] \to \mathfrak{o}/(p^e)$. Note that

$$(p, 1-e_p) = p\mathbb{Z}_p[G] + (1-e_p)\mathbb{Z}_p[G] \xrightarrow{\psi} \mathfrak{P}/(p^e).$$

Moreover, since $e_\chi(1-e_p) = 0$ for all χ that are trivial on I_p (otherwise $e_\chi(1-e_p) = e_\chi$), we have

$$|\mathbb{Z}_p[G]/(p, 1-e_p)| = \prod_{\ker\chi \supseteq I_p} p = p^{[G:I_p]} = |\mathfrak{o}/\mathfrak{P}|,$$

so $\psi((p, 1-e_p)) = \mathfrak{P}/(p^e)$. From the preceding paragraph, we know that $\mathfrak{P}/(p^e)$ is also cyclic, so there exists an onto homomorphism $\psi' : \mathbb{Z}_p[G] \to \mathfrak{P}/(p^e)$. Since $(p^e - p^{e-1}\sigma_p e_p) \cdot (p, 1-e_p) \subseteq (p^e)$, it follows that $(p^e - p^{e-1}\sigma_p e_p) \subseteq \ker\psi'$.

$$\begin{array}{ccccc}
\mathbb{Z}_p[G] & \xrightarrow{\psi} & \mathfrak{o} & & \\
\big| & & \big| & & \\
(p, 1-e_p) & \longrightarrow & \mathfrak{P} & \xleftarrow{\psi'} & \mathbb{Z}_p[G] \\
\big| & & \big| & & \big| \\
(p^e) & \longrightarrow & (p^e) & \longleftarrow & \ker \psi' \\
 & & & & \big| \\
 & & & & (p^e - p^{e-1}e_p)
\end{array}$$

Since $e_\chi e_p = 0$ for all χ that are non-trivial on I_p (otherwise $e_\chi e_p = e_\chi$), we see that $|\mathbb{Z}_p[G]/(p^e - p^{e-1}\sigma_p e_p)|$ equals

$$\prod_{\ker\chi \supseteq I_p} p^{e-1} \prod_{\ker\chi \not\supseteq I_p} p^e = p^{|G|e-[G:I_p]} = |\mathfrak{P}/(p^e)|.$$

So $\ker\psi' = (p^e - p^{e-1}\sigma_p e_p)$, and the claim follows. ∎

Remark 2.5. If one takes $M = E$ (or $M = \mathfrak{o}$) in Lemma 2.2, then (i) and (ii) are also equivalent to the statement that there exists $\epsilon \in E$ (or $\alpha \in \mathfrak{o}$) such that $[E : \langle\epsilon\rangle_{\mathbb{Z}[G]}]$ (or $[\mathfrak{o} : \langle\alpha\rangle_{\mathbb{Z}[G]}]$) is finite and coprime to p. In particular, there exists $\epsilon \in E$ such that $\epsilon \otimes 1$ generates $E \otimes \mathbb{Z}_p$ as a $\mathbb{Z}_p[G]$-module.

The results of Corollaries 2.4 and 2.3 also hold under extension of scalars. For example, we have

$$E \otimes \mathcal{O} \simeq \mathcal{O}[G]/s(G), \qquad (\mathfrak{o}/\mathfrak{L}^e)^\times \otimes \mathcal{O} \simeq \mathcal{O}[G]/(\ell - \sigma_\ell e_\ell).$$

3. The ray class Gras Conjecture. In this section, we aim to prove Theorem 1.2. Theorem 1.1 was proven by way of the mapping $l : k^\times \to \mathbb{R}[G]$ defined by

$$l(x) = -\frac{1}{2}\sum_{\sigma\in G} \log(|x^\sigma|)\sigma^{-1}.$$

Since $E_d/C_d \simeq l(E_d)/l(C_d)$, the index $[E_d : C_d]$ may be studied by decomposing the index $[l(E_d) : l(C_d)]$ into various parts. Our method will be similar, but we work p-adically.

3.1. Notation & preliminaries. Fix a positive integer d and let m be the conductor of k. Let Ω_p (resp. Ω) denote the algebraic closure of $\mathbb{Q}_p$ (resp. $\mathbb{Q}$), and fix an embedding $\Omega \hookrightarrow \Omega_p$ so that we may view $\Omega \subseteq \Omega_p$. Let k_p denote the topological closure of k, and let

- K denote the field k_p adjoined with all character values of G,
- $\mathcal{O}$ denote the valuation integers of K.

Throughout this section we assume that

- $n > 1$ and $n \nmid \overline{d}$ unless stated otherwise,
- p is an odd prime not dividing $[k : \mathbb{Q}]$,
- $e(p)$ is the ramification index of p in k (or in K), and is less than $p-1$,
- $f(p)$ is the residue of p in K.

A *lattice* L in a K-vector space V is a free $\mathcal{O}$-module whose $\mathcal{O}$-rank equals the K-dim of KL and which satisfies $V = KL$. If L and M are lattices in V for which there exists an automorphism ϕ of V where $\phi(L) = M$, then we define the generalized index $(L : M)$ by

$$(L : M) = p^{f(p)\,\mathrm{ord}_{\varpi}\,\det\phi} = |\det\phi|_p^{-e(p)f(p)}$$

where (ϖ) is the prime ideal of $\mathcal{O}$. This index is independent of the choice of ϕ, and if $M \subseteq L$ with $[L : M] < \infty$, then $(L : M) = [L : M]$.

If M is a lattice contained in $K[G]$ and $\alpha \in K[G]$, we let αM denote the lattice

$$\alpha M = \{\alpha m : m \in M\}.$$

In particular, we write M_χ for $e_\chi M$. If M is additionally a G-module, we have the natural decomposition

$$M = \bigoplus M_\chi,$$

the direct sum taken over all χ such that $M_\chi \neq 0$. A character $\chi \in \widehat{G}$ naturally induces a ring homomorphism $K[G] \to K$. The index $(M : \alpha M)$ exists if and only if $\chi(\alpha) \neq 0$ whenever $M_\chi \neq 0$. If this is the case, then

$$(M : \alpha M) = \prod |\chi(\alpha)|_p^{-e(p)f(p)},$$

the product taken over all χ such that $M_\chi \neq 0$.

For $\alpha \in \mathcal{O}[G]$, note that $\chi(\alpha)e_\chi = e_\chi\alpha$. In this case, we define $\alpha^{-1} \in K[G]$ to be the element defined by

$$\alpha^{-1} := \sum \chi(\alpha)^{-1}e_\chi$$

where the sum is taken over all characters χ satisfying $\chi(\alpha) \neq 0$. This gives

$$\alpha \cdot \alpha^{-1} = \sum e_\chi,$$

the sum over all χ such that $\chi(\alpha) \neq 0$.

Since we are assuming $e(p) < p - 1$, we get $\log_p(k^\times) \subseteq \mathcal{O}$ where $\log_p$ is the Iwasawa logarithm. Let $\vartheta : k^\times \to \mathcal{O}[G]$ be the G-module map defined by

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

This map takes the place of the map l defined at the forefront of this section. If $x \in \ker \vartheta$, then $x = \zeta p^r$ where ζ is a root of unity and r is a rational number. Since k is real and Galois, it follows that $\ker \vartheta$ consists of ± 1 and either all powers of p or all powers of $\sqrt{p}$. We fix the following notation to be used throughout:

$$\mathscr{E}_d = \text{the ideal of } \mathcal{O}[G] \text{ generated by } \vartheta(E_d),$$
$$\mathscr{C}_d = \text{the ideal of } \mathcal{O}[G] \text{ generated by } \vartheta(C_d).$$

We omit the subscript when $d = 1$. Since $\mathcal{O}$ is a flat $\mathbb{Z}$-module, we have

$$(E_d \otimes \mathcal{O})/(C_d \otimes \mathcal{O}) \simeq (E_d/C_d) \otimes \mathcal{O}.$$

Consider the natural map $E_d \otimes \mathcal{O} \to \mathscr{E}_d$ defined by $\epsilon \otimes \alpha \mapsto \vartheta(\epsilon)\alpha$ extended by linearity. Since $\ker \vartheta$ consists of $\pm 1 \cdot$ (rational powers of p) and k satisfies Leopoldt's Conjecture with p an odd prime, it follows that

$$E_d \otimes \mathcal{O} \simeq \mathscr{E}_d.$$

In fact, we have

$$(E_d/C_d) \otimes \mathcal{O} \simeq \mathscr{E}_d/\mathscr{C}_d.$$

As in the previous section, if $H \subseteq G$, then we write $s(H)$ to denote the sum in $\mathbb{Z}[G]$ of those automorphisms in H. We write

$$\sum_{\sigma \in G/H}{}'$$

for the restricted sum over a system of unique representatives in G of G/H. We also keep the notation σ_ℓ, e_ℓ and I_ℓ from the previous section.

We will often make use of the following proposition.

PROPOSITION 3.1. *The group ring $\mathcal{O}[G]$ is a principal ring.*

Proof. Note that $\mathcal{O}/(\varpi^n)$ is a local Artinian principal ring. Since G is assumed to have no p-part, it follows that $(\mathcal{O}/(\varpi^n))[G] \simeq \mathcal{O}[G]/(\varpi^n \mathcal{O}[G])$ is a principal ring [D, Theorem 4]. So for an ideal I of $\mathcal{O}[G]$, for every $n \in \mathbb{N}$, there exists $\alpha_n \in \mathcal{O}[G]$ such that

$$(I + \varpi^n \mathcal{O}[G])/\varpi^n \mathcal{O}[G] = ((\alpha_n) + \varpi^n \mathcal{O}[G])/\varpi^n \mathcal{O}[G].$$

Since $\mathcal{O}[G]$ is compact (in the product topology), we see that $\alpha_n \to \alpha \in \mathcal{O}[G]$, i.e., there exists $\alpha \in \mathcal{O}[G]$ such that $\alpha \equiv \alpha_n \bmod \varpi^n \mathcal{O}[G]$ for all $n \in \mathbb{N}$. We now show that $I = (\alpha)$. For each $\gamma \in I$ and $n \in \mathbb{N}$, there exist $\beta, \beta_n \in \mathcal{O}[G]$ such that $\alpha\beta_n \equiv \gamma \bmod \varpi^n \mathcal{O}[G]$ and $\beta_n \to \beta$. Then $\gamma = \alpha\beta$, hence I is principal generated by α. ∎

3.2. The modules $\mathscr{E}$ and $\mathscr{C}$. For a non-trivial character $\chi \in \widehat{G}$ of conductor f_χ, let $L'_p(0,\chi)$ denote the special value

$$L'_p(0,\chi) = \sum_{a=1}^{f_\chi} \log_p(1-\zeta_{f_\chi}^a)\overline{\chi}(a) \in \mathcal{O}.$$

Also let

$$\omega' = \sum_{\chi\neq 1} L'_p(0,\chi)e_\chi \in \mathcal{O}[G].$$

Our goal will be to dissect the χ-components of $\mathscr{E}_d/\mathscr{C}_d$. The following useful proposition is a p-adic formulation of a result of Sinnott.

PROPOSITION 3.2. *Let $n > 1$, and write k^n for $\mathbb{Q}(\zeta_n)\cap k$, G_n for $\mathrm{Gal}(k/k^n)$, and $\delta_n^{(t)}$ for $N_{k^n}^{\mathbb{Q}(\zeta_n)}(1-\zeta_n^t)$. Then*

$$(1-e_1)\vartheta(\delta_n^{(t)}) = \omega'[\mathbb{Q}(\zeta_n) : k^n\mathbb{Q}(\zeta_{n/t})]s(G_{n/t})\prod_{\ell\mid n}(1-\sigma_\ell^{-1}e_\ell). \tag{3.1}$$

Proof. Let L and R denote the left and right hand sides of (3.1). It suffices to show that $\psi(R) = \psi(L)$ for every $\psi \in \widehat{G}$.

Since

$$\vartheta(\delta_n^{(t)}) = [\mathbb{Q}(\zeta_n) : k^n\mathbb{Q}(\zeta_{n/t})]s(G_{n/t}) \sum_{\sigma\in G/G_{n/t}}{}' \log_p((\delta_{n/t}^{(1)})^\sigma)\sigma^{-1},$$

it follows that $\psi(R) = \psi(L) = 0$ if ψ is either the trivial character or is a non-trivial character on $G_{n/t}$.

Now, suppose $\psi \neq 1$ and ψ is trivial on $G_{n/t}$. Note that

$$\psi(R) = L'_p(0,\psi)[\mathbb{Q}(\zeta_n) : k^n\mathbb{Q}(\zeta_{n/t})]\cdot|G_{n/t}|\prod_{\ell\mid n/t}(1-\overline{\psi}(\ell))$$

and

$$\psi(\vartheta(\delta_n^{(t)})) = [\mathbb{Q}(\zeta_n) : k^n\mathbb{Q}(\zeta_{n/t})]\cdot|G_{n/t}| \sum_{\sigma\in G/G_{n/t}}{}' \log_p((\delta_{n/t}^{(1)})^\sigma)\overline{\psi}(\sigma),$$

so

$$\psi(L) = [\mathbb{Q}(\zeta_n) : k^n\mathbb{Q}(\zeta_{n/t})]\cdot|G_{n/t}| \sum_{\substack{a=1\\(a,n/t)=1}}^{n/t} \log_p(1-\zeta_{n/t}^a)\overline{\psi}(a).$$

Write f_ψ for the conductor of ψ. Since $G_{n/t} \leq \ker\psi$, it follows that $f_\psi \mid n/t$.

We set $f_\psi g = n/t$ and interpret $\log_p(0)\cdot 0$ to be equal to 0 to obtain

$$\begin{aligned}\sum_{\substack{a=1\\(a,n/t)=1}}^{f_\psi g} \log_p(1-\zeta_{n/t}^a)\overline{\psi}(a) &= \sum_{a=1}^{f_\psi g} \log_p(1-\zeta_{n/t}^a)\overline{\psi}(a)\prod_{\ell\mid n/t}(1-\overline{\psi}(\ell))\\ &= \sum_{a=1}^{f_\psi} \log_p(1-\zeta_{f_\psi}^a)\overline{\psi}(a)\prod_{\ell\mid n/t}(1-\overline{\psi}(\ell))\\ &= L_p'(0,\psi)\prod_{\ell\mid n/t}(1-\overline{\psi}(\ell)).\end{aligned}$$

So $\psi(L)=\psi(R)$. ∎

Using Corollary 2.3, we may fix an $\epsilon\in E$ such that $\vartheta(\epsilon)=\varepsilon$ generates $\mathscr{E}$ as an ideal in $\mathcal{O}[G]$. We define a special element $\omega\in\mathscr{C}$ by

$$\omega=\sum_{\chi\neq 1} e_\chi\vartheta(\delta_\chi),\qquad \delta_\chi = N_{k^{f_\chi}}^{\mathbb{Q}(\zeta_{f_\chi})}(1-\zeta_{f_\chi})$$

where f_χ is the conductor of χ. This element generates $\mathscr{C}$:

COROLLARY 3.3. *The ideal $\mathscr{C}\subseteq\mathcal{O}[G]$ is generated by ω; in fact,*

$$\mathscr{C}=\omega\varepsilon^{-1}\mathscr{E}.$$

In particular, if $\chi\neq 1$, then

$$[\mathscr{E}_\chi:\mathscr{C}_\chi]=|\chi(\varepsilon)^{-1}L_p'(0,\chi)|_p^{-e(p)f(p)}.$$

Proof. Let $\mathscr{D}$ denote the $\mathcal{O}[G]$-ideal generated by $\vartheta(D)$. Note that $\mathscr{C}$ is the kernel in $\mathscr{D}$ of multiplication by $s(G)$, i.e.,

$$(1-e_1)\mathscr{D}=\mathscr{C}.$$

Since $\omega=(1-e_1)\omega$, we apply Proposition 3.2 to obtain

$$\chi(\omega)=|G_{f_\chi}|L_p'(0,\chi).$$

Since $|G_{f_\chi}|$ is a p-adic unit, it follows that

$$\chi(\varepsilon)^{-1}L_p'(0,\chi)e_\chi\in(\varepsilon^{-1}\mathscr{C})_\chi.$$

Since

$$\mathscr{E}/\mathscr{C}\simeq\varepsilon^{-1}\mathscr{E}/\varepsilon^{-1}\mathscr{C}=(1-e_1)\mathcal{O}[G]/\varepsilon^{-1}\mathscr{C},$$

we have

$$[\mathscr{E}_\chi:\mathscr{C}_\chi]\le|\chi(\varepsilon)^{-1}L_p'(0,\chi)|_p^{-e(p)f(p)}. \tag{3.2}$$

Moreover, Theorem 1.1 gives

$$|\mathfrak{C}\otimes\mathcal{O}|=[\mathscr{E}:\mathscr{C}]\le\prod_{\chi\neq 1}|\chi(\varepsilon)^{-1}L_p'(0,\chi)|_p^{-e(p)f(p)}.$$

Now, note that

$$\prod_{\chi\neq 1}\chi(\varepsilon)=\det(\alpha\mapsto\varepsilon\alpha)=\mathrm{Reg}_p'$$

where Reg_p' differs from Reg_p, the Leopoldt regulator of k, by a unit of $\mathbb{Z}_p$. Substituting Reg_p' into the p-adic class number formula, we get

$$|\mathfrak{C}| =_p \frac{1}{\mathrm{Reg}_p}\prod_{\chi\neq 1}L_p'(0,\chi) =_p \prod_{\chi\neq 1}\chi(\varepsilon)^{-1}L_p'(0,\chi) \tag{3.3}$$

where $a =_p b$ means that a and b differ by a p-adic unit. So (3.3) and Theorem 1.1 give

$$[\mathscr{E}:\mathscr{C}]=\prod_{\chi\neq 1}[\mathscr{E}_\chi:\mathscr{C}_\chi]\le\prod_{\chi\neq 1}|\chi(\varepsilon)^{-1}L_p'(0,\chi)|_p^{-e(p)f(p)}=[\mathscr{E}:\mathscr{C}]. \tag{3.4}$$

Putting (3.2) and (3.4) together yields

$$[\mathscr{E}_\chi:\mathscr{C}_\chi]=|\chi(\varepsilon)^{-1}L_p'(0,\chi)|_p^{-e(p)f(p)}$$

for all $\chi\neq 1$. It follows that

$$\mathscr{C}=\omega\varepsilon^{-1}\mathscr{E}=\omega(1-e_1)\mathcal{O}[G]=\omega\mathcal{O}[G].$$

This completes the proof of Corollary 3.3. ∎

3.3. The modules $\mathscr{E}_d$ and $\mathscr{C}_d$. We will make use of the following auxiliary $\mathcal{O}[G]$-modules:

$$\mathscr{D}(d)=\text{the ideal of }\mathcal{O}[G]\text{ generated by }\vartheta(D(d)),$$
$$\mathscr{C}(d)=\text{the ideal of }\mathcal{O}[G]\text{ generated by }\vartheta(C(d)).$$

Again, we omit the parentheses when $d=1$. For any $t\mid n$, let $\alpha_n(t)\in\mathcal{O}[G]$ be defined by

$$\alpha_n(t):=[\mathbb{Q}(\zeta_n):k^n\mathbb{Q}(\zeta_{n/t})]s(G_{n/t})\prod_{\ell\mid n/t}(1-\sigma_\ell^{-1}e_\ell),$$

the product taken over primes ℓ dividing n/t. Let $\mathscr{U}$ denote the $\mathcal{O}[G]$-ideal generated by these elements $\alpha_n(t)$ (for all $n\ge 1$ and all $t\mid n$). Then Proposition 3.2 reads

$$(1-e_1)\vartheta(\delta_n^{(t)})=\omega'\alpha_n(t).$$

More generally, since $\omega'\alpha_1(1)=\omega'\alpha_n(n)=0$, it follows that

$$\mathscr{C}=(1-e_1)\mathscr{D}=\omega'\mathscr{U}.$$

We need to know what the above formula looks like if we replace $\mathscr{C}$ with $\mathscr{C}(d)$. Towards that end, for an integer $t>1$, we define

$$\kappa_t=\prod_{\ell\mid t}(\ell-\sigma_\ell),$$

the product taken over all primes ℓ dividing t. We first make a few observations that whittle down the ideal $\mathscr{D}(d)$.

LEMMA 3.4. *Let* $\bar{d}_m = (\bar{d}, m)$. *Then*

$$\mathscr{D}(d) = \frac{d}{\bar{d}} \kappa_{\bar{d}/\bar{d}_m} \mathscr{D}(\bar{d}_m).$$

Proof. This follows from [Sch, Lemmas 3.2 and 3.5]. ∎

For $n \geq 1$, we let

$$\alpha_{n,\bar{d}_m} := \kappa_{\bar{d}_m/(\bar{d}_m,n)} \sum_{t|(\bar{d}_m,n)} \mu(t) \frac{(\bar{d}_m, n)}{t} \alpha_n(t).$$

Note that since $p \nmid [k : \mathbb{Q}]$, we find that $\alpha_{n,\bar{d}_m} \in \mathcal{O}[G]$ for all $n \geq 1$.

COROLLARY 3.5. *If* $n > 1$ *and* $n \nmid \bar{d}_m$, *then*

$$(1 - e_1)\vartheta(\delta_{n,\bar{d}_m}) = \omega' \alpha_{n,\bar{d}_m}.$$

Proof. For a prime divisor ℓ of $\bar{d}_m$ such that $\ell \nmid n$, we have

$$\delta_{n,\bar{d}_m} = N_{k^n}^{\mathbb{Q}(\zeta_n)} \prod_{t|\bar{d}_m/\ell} (1 - \zeta_n^t)^{(\mu(t)\bar{d}_m/(t\ell))\ell} (1 - \zeta_n^t)^{(\mu(t\ell)\bar{d}_m/(t\ell))\sigma_\ell} = \delta_{n,\bar{d}_m/\ell}^{\ell - \sigma_\ell}.$$

So

$$\vartheta(\delta_{n,\bar{d}_m}) = \kappa_{\bar{d}_m/(\bar{d}_m,n)} \vartheta(\delta_{n,(\bar{d}_m,n)}).$$

Since

$$\vartheta(\delta_{n,(\bar{d}_m,n)}) = \sum_{t|(\bar{d}_m,n)} \mu(t) \frac{(\bar{d}_m, n)}{t} \vartheta(\delta_n^{(t)}),$$

the corollary follows from Proposition 3.2. ∎

LEMMA 3.6. *If* $\delta_{n,\bar{d}_m} \in D(\bar{d}_m)$ *and* q *is a prime dividing* $(n, \bar{d}_m)$ *such that* $v_q(n) > v_q(m)$, *then* $\delta_{n,\bar{d}_m} = 1$.

Proof. Note that

$$\delta_{n,\bar{d}_m} = \prod_{t|\bar{d}_m/q} N_{k^n}^{\mathbb{Q}(\zeta_n)} \left(\frac{(1 - \zeta_n^t)^q}{1 - \zeta_n^{tq}} \right)^{\mu(t) \cdot \frac{\bar{d}_m/q}{t}}.$$

Since $v_q(n) > v_q(m)$, it follows that $k^n \subseteq \mathbb{Q}(\zeta_{n/q}) \subseteq \mathbb{Q}(\zeta_n)$. Now consider

$$N_{k^n}^{\mathbb{Q}(\zeta_n)} \frac{(1 - \zeta_n^t)^q}{1 - \zeta_n^{tq}} = N_{k^n}^{\mathbb{Q}(\zeta_{n/q})} N_{\mathbb{Q}(\zeta_{n/q})}^{\mathbb{Q}(\zeta_n)} \frac{(1 - \zeta_n^t)^q}{1 - \zeta_n^{tq}}.$$

Since $\zeta_n^t = \zeta_{n/t}$ and $q^2 \mid n$, we have

$$N_{\mathbb{Q}(\zeta_{n/q})}^{\mathbb{Q}(\zeta_n)} (1 - \zeta_{n/t}) = 1 - \zeta_{n/(tq)},$$

whence the assertion. ∎

PROPOSITION 3.7. *Let $\mathscr{U}(\bar{d}_m)$ be the $\mathcal{O}[G]$-ideal generated by the $\alpha_{n,\bar{d}_m}$ with $n \mid m$. Then*

$$\mathscr{C}(d) = (1 - e_1)\mathscr{D}(d) = \frac{d}{\bar{d}}\kappa_{\bar{d}/\bar{d}_m}\omega'\mathscr{U}(\bar{d}_m).$$

Proof. Let $\mathscr{U}'(\bar{d}_m)$ be the $\mathcal{O}[G]$-ideal generated by $\alpha_{n,\bar{d}_m}$ satisfying $n > 1$ and $n \nmid \bar{d}_m$. The proposition then follows from Corollary 3.5 if we replace $\mathscr{U}(\bar{d}_m)$ with $\mathscr{U}'(\bar{d}_m)$. So the proposition rests on showing that

$$\omega'\mathscr{U}(\bar{d}_m) = \omega'\mathscr{U}'(\bar{d}_m).$$

Toward that end, note that from Lemma 3.6 it follows that

$$\alpha_{n,\bar{d}_m} = \alpha_{(n,m),\bar{d}_m} \prod_{\ell \mid \bar{n}/(\bar{n},m)} (1 - \sigma_\ell^{-1}). \tag{3.5}$$

So $\mathscr{U}'(\bar{d}_m)$ is generated by those $\alpha_{n,\bar{d}_m}$ satisfying $n > 1$, $n \nmid \bar{d}_m$, and $n \mid m$. Hence $\omega'\mathscr{U}'(\bar{d}_m) \subseteq \omega'\mathscr{U}(\bar{d}_m)$.

Going the other way, note that $\alpha_{1,\bar{d}_m} = \kappa_{\bar{d}_m}\alpha_1(1)$. Since $\alpha_1(1) = s(G)$, it follows that $\omega'\alpha_{1,\bar{d}_m} = 0$. Now suppose $\alpha_{n,\bar{d}_m} \in \mathscr{U}(\bar{d}_m)$ where $n \mid \bar{d}_m$. Let q be a prime such that $q \nmid m$ and consider $\alpha_{nq,\bar{d}_m}$. From (3.5), we have

$$\alpha_{nq,\bar{d}_m} = \alpha_{n,\bar{d}_m}(1 - \sigma_q^{-1}).$$

Since any given element of G is the Frobenius of infinitely many primes, there exists a collection Q of primes such that $|Q| = |G|$ and

$$\sum_{q \in Q} \alpha_{nq,\bar{d}_m} = \alpha_{n,\bar{d}_m} \sum_{\tau \in G} (1 - \tau^{-1}) = \alpha_{n,\bar{d}_m}(|G| - s(G)).$$

Hence

$$\omega' \sum_{q \in Q} \alpha_{nq,\bar{d}_m} = \omega'\alpha_{n,\bar{d}_m}|G|.$$

Since $|G|$ is a p-adic unit, it follows that $\omega'\mathscr{U}(\bar{d}_m) \subseteq \omega'\mathscr{U}'(\bar{d}_m)$. ∎

It remains to determine a generator for $\mathscr{U}(\bar{d}_m)$. For $t \in \mathbb{N}$, let $\varkappa_t$ be the element of $\mathcal{O}[G]$ defined by

$$\varkappa_t = \prod_{\ell \mid t} (\ell - \sigma_\ell e_\ell),$$

the product taken over all primes ℓ dividing t.

PROPOSITION 3.8. *The ideal $\mathscr{U}(\bar{d}_m)$ of $\mathcal{O}[G]$ is generated by $\varkappa_{\bar{d}_m}$.*

Proof. Suppose $\chi = 1$. If $n \mid \bar{d}_m$, then

$$\chi(\alpha_{n,\bar{d}_m}) = \pm\varphi\left(\frac{\bar{d}_m}{(\bar{d}_m, n)}\right)[\mathbb{Q}(\zeta_n) : k^n] \cdot |G| = \pm\varphi(\bar{d}_m)[k : k^n].$$

Otherwise $\chi(\alpha_{n,\bar{d}_m}) = 0$. On the other hand, we have $\chi(\varkappa_{\bar{d}_m}) = \varphi(\bar{d}_m)$. Since $[k : k^n]$ is a p-adic unit, it follows that $e_1\mathscr{U}(\bar{d}_m) = e_1\varkappa_{\bar{d}_m}\mathcal{O}[G]$.

Now, let χ be a non-trivial character of G with conductor f. Suppose $n \mid m$ is such that χ is non-trivial on $G_{n/t}$ for all $t \mid (\bar{d}_m, n)$. Then

$$\chi(s(G_{n/t})) = 0,$$

so $\chi(\alpha_{n,\bar{d}_m}) = 0$. So in order to get a non-trivial contribution to the χ-part of $\mathscr{U}(\bar{d}_m)$, we consider those $\alpha_{fN,\bar{d}_m}$ satisfying $N \geq 1$ and $fN \mid m$.

We have

(3.6)
$$\chi(\alpha_{fN,\bar{d}_m}) = \prod_{\ell \mid \bar{d}_m/(\bar{d}_m, fN)} (\ell - \chi(\sigma_\ell)) \Bigg[\sum_{t \mid (\bar{d}_m, fN)} \mu(t) \frac{(\bar{d}_m, fN)}{t} \chi(\alpha_{fN}(t)) \Bigg],$$

where

$$\chi(\alpha_{fN}(t)) = \begin{cases} 0, & f \nmid fN/t, \\ [\mathbb{Q}(\zeta_{fN}) : k^{fN}\mathbb{Q}(\zeta_{fN/t})] \cdot |G_{fN/t}| \prod_{\ell \mid Nf/t} (1 - \chi(\sigma_\ell^{-1} e_\ell)), & f \mid fN/t. \end{cases}$$

As far as $\chi(\alpha_{fN,\bar{d}_m})$ is concerned, we might as well only sum over all those $t \mid (\bar{d}_m, fN)$ satisfying $f \mid fN/t$. Such t's must divide N; moreover, it is easy to see that

$$[\mathbb{Q}(\zeta_{fN}) : k^{fN}\mathbb{Q}(\zeta_{fN/t})] \cdot |G_{fN/t}| = [\mathbb{Q}(\zeta_{fN}) : \mathbb{Q}(\zeta_{fN/t})] \cdot [k : k^{fN}].$$

Let $A_{fN,\bar{d}_m}$ denote the bracketed term in (3.6). So far we have

$$A_{fN,\bar{d}_m} = \sum_{t \mid (\bar{d}_m, N)} \mu(t) \frac{(\bar{d}_m, fN)}{t} \frac{\varphi(fN)}{\varphi(fN/t)} \cdot [k : k^{fN}] \prod_{\ell \mid fN/t} (1 - \chi(\sigma_\ell^{-1} e_\ell)).$$

Write $N = N_1 N_2^2$ where N_1 is a product of distinct primes. Write $(\bar{d}_m, N) = Q_1 Q_2$ where Q_1 is the product of those primes that divide N_1 and not N_2. Then $A_{fN,\bar{d}_m}$ equals

$$\sum_{t_1 \mid Q_1} \mu(t_1) \frac{(\bar{d}_m, fN)}{t_1} [k : k^{fN}] \times \Bigg[\sum_{t_2 \mid Q_2} \frac{\mu(t_2)}{t_2} \frac{\varphi(fN)}{\varphi(fN/(t_1 t_2))} \prod_{\ell \mid fN/(t_1 t_2)} (1 - \chi(\sigma_\ell^{-1} e_\ell)) \Bigg].$$

Notice that if $Q_2 \neq 1$, then the bracketed term above equals

$$\varphi(t_1) \prod_{\ell \mid fN/t_1} (1 - \chi(\sigma_\ell^{-1} e_\ell)) \sum_{t_2 \mid Q_2} \mu(t_2) = 0.$$

So we must have $N = N_1$, i.e., N is square-free, otherwise $\chi(\alpha_{fN,\bar{d}_m}) = 0$. If we now were to go back to the beginning of this paragraph and let Q_2

denote those primes that divide both N and f, then we could similarly deduce that $\chi(\alpha_{fN,\bar{d}_m}) = 0$ if $Q_2 \neq 1$, since the same bracketed term equals zero. Hence, N must not only be square-free but also coprime to f, otherwise $\chi(\alpha_{fN,\bar{d}_m}) = 0$.

Now, suppose N is square-free and coprime to f. Since $\chi(\sigma_\ell^{-1} e_\ell) = 0$ for all $\ell \mid f$, we now have

$$A_{fN,\bar{d}_m} = (\bar{d}_m, f)[k : k^{fN}]\Big[\sum_{t \mid (\bar{d}_m, N)} \mu(t)\frac{(\bar{d}_m, N)}{t}\varphi(t)\prod_{\ell \mid N/t}(1 - \chi(\sigma_\ell^{-1} e_\ell))\Big].$$

Let $B_{fN,\bar{d}_m}$ be the bracketed term above. Let q be a prime divisor of $(\bar{d}_m, N)$. Then

$$B_{fN,\bar{d}_m} = \sum_{t \mid (\bar{d}_m, N)/q} \mu(t)\frac{(\bar{d}_m, N)}{tq}\varphi(t) \times \prod_{\ell \mid N/(qt)} \big(1 - \chi(\sigma_\ell^{-1} e_\ell)\big) \cdot \big(q(1 - \chi(\sigma_q^{-1} e_q)) - \varphi(q)\big).$$

Repetition of the above on the remaining prime divisors of $(\bar{d}_m, N)$ yields

$$B_{fN,\bar{d}_m} = \prod_{\ell \mid N/(\bar{d}_m, N)} (1 - \chi(\sigma_\ell^{-1} e_\ell)) \prod_{q \mid (\bar{d}_m, N)} (1 - q\chi(\sigma_q^{-1} e_q)).$$

This quantity is largest (p-adically) when $N \mid \bar{d}_m$. Since N is assumed coprime to f, we have $\chi(e_q) = 1$ for all $q \mid N$, and for those $q \mid f$, we have $\chi(e_q) = 0$. It follows that

$$\begin{aligned} A_{fN,\bar{d}_m} &= \pm\chi(N)(\bar{d}_m, f)[k : k^{fN}] \prod_{q \mid N} (q - \chi(\sigma_q e_q)) \\ &= \pm\chi(N)[k : k^{fN}] \prod_{q \mid (\bar{d}_m, fN)} (q - \chi(\sigma_q e_q)), \end{aligned}$$

where

$$\chi(N) = \prod_{q \mid N} \chi(\sigma_q^{-1}).$$

Picking up where we left off with equation (3.6), we have shown that $\chi(\alpha_{fN,\bar{d}_m})$ is largest (p-adically) when N is square-free and coprime to f with $N \mid \bar{d}_m$, in which case

$$\chi(\alpha_{fN,\bar{d}_m}) = \pm\chi(N)[k : k^{fN}] \prod_{\ell \mid \bar{d}_m} (\ell - \chi(\sigma_\ell e_\ell)).$$

Since $\chi(\alpha_{fN,\bar{d}_m})$ differs from $\chi(\varkappa_{\bar{d}_m})$ by a p-adic unit (and since χ was arbitrary), it follows that $e_\chi \mathscr{U}(\bar{d}_m) = e_\chi \varkappa_{\bar{d}_m} \mathcal{O}[G]$.

We have shown that $e_\chi \mathscr{U}(\bar{d}_m) = e_\chi \varkappa_{\bar{d}_m} \mathcal{O}[G]$ for all characters χ of G. The proposition now follows. ∎

Since E_d is a finite index subgroup of E, it follows that $(\mathscr{E}/\mathscr{E}_d)_\chi$ is finite for every $\chi \neq 1$. Let ε'_d be a generator for the $\mathcal{O}[G]$-ideal $\mathscr{E}_d$. Since $\mathscr{E} = (\varepsilon) \supseteq (\varepsilon'_d) = \mathscr{E}_d$, there exists $\varepsilon_d \in \mathcal{O}[G]$ such that $\varepsilon \cdot \varepsilon_d = \varepsilon'_d$. So $\mathscr{E}_d = \varepsilon_d \mathscr{E}$, and what is more,

$$[\mathscr{E} : \mathscr{E}_d] = \prod_{\chi \neq 1} |\chi(\varepsilon_d)|_p^{-e(p)f(p)}.$$

Combining Propositions 3.8 and 3.7, we immediately obtain the following corollary.

COROLLARY 3.9. *The $\mathcal{O}[G]$-ideal $\mathscr{C}(d)$ is generated by $(d/\bar{d})\omega' \varkappa_{\bar{d}}$; in fact,*

$$\mathscr{C}(d) = \frac{d}{\bar{d}} \varkappa_{\bar{d}} \omega' \varepsilon^{-1} \varepsilon_d^{-1} \mathscr{E}_d.$$

3.4. Proof of Theorem 1.2. Let ρ be as in the statement of the theorem. Note that

$$|\mathrm{Syl}_p(E_d/C_d)_\rho| = |\mathrm{Syl}_p(\mathfrak{C}_d)_\rho| \quad \text{iff} \quad [\mathscr{E}_{d,\rho} : \mathscr{C}_{d,\rho}] = |(\mathfrak{C}_d \otimes \mathcal{O})_\rho|.$$

We aim to prove the latter equality. Define the linear transformation

$$\phi_\rho : \mathscr{E}_{d,\rho} K \to \mathscr{C}(d)_\rho K, \qquad x \mapsto \frac{d}{\bar{d}} \varkappa_{\bar{d}} \omega' \varepsilon^{-1} \varepsilon_d^{-1} x.$$

Note that Corollary 3.9 gives $\phi_\rho(\mathscr{E}_{d,\rho}) = \mathscr{C}(d)_\rho$. Since $C_d \subseteq C(d)$, it follows that

$$[\mathscr{E}_{d,\rho} : \mathscr{C}_{d,\rho}] \geq (\mathscr{E}_{d,\rho} : \mathscr{C}(d)_\rho) = |\det \phi_\rho|_p^{-e(p)f(p)}.$$

Now, we have

$$\det \phi_\rho = \prod \chi\left(\frac{d}{\bar{d}} \varkappa_{\bar{d}} \omega' \varepsilon^{-1} \varepsilon_d^{-1}\right),$$

where the product is over those χ such that $\chi(e_\rho) \neq 0$. Note that

$$\chi\left(\frac{d}{\bar{d}} \varkappa_{\bar{d}} \omega' \varepsilon^{-1} \varepsilon_d^{-1}\right) = \left[\frac{d}{\bar{d}} \prod_{\ell \mid \bar{d}} (\ell - \chi(\sigma_\ell e_\ell))\right] [L'_p(0,\chi)\chi(\varepsilon)^{-1}][\chi(\varepsilon_d)^{-1}].$$

Let $\mathscr{O}_d^\times = (\mathfrak{o}/d)^\times \otimes \mathcal{O}$. Extending scalars in Corollary 2.4, we get

$$\mathscr{O}_d^\times \simeq \prod_{\ell \mid d} \mathscr{O}_\ell^\times, \quad \text{where} \quad \mathscr{O}_\ell^\times \simeq \begin{cases} \mathcal{O}[G]/(\ell - \sigma_\ell e_\ell), & \ell \neq p, \\ \mathcal{O}[G]/(p^e - p^{e-1}\sigma_p e_p), & \ell = p. \end{cases}$$

It follows that $[\mathscr{O}_{d,\chi}^\times : 1] = |(d/\bar{d}) \prod_{\ell \mid \bar{d}} (\ell - \chi(\sigma_\ell e_\ell))|_p^{-e(p)f(p)}$, and from Corollary 3.3, we have $[\mathscr{E}_\chi : \mathscr{C}_\chi] = |L'_p(0,\chi)\chi(\varepsilon)^{-1}|_p^{-e(p)f(p)}$. Hence

$$[\mathscr{E}_{d,\rho} : \mathscr{C}_{d,\rho}] \geq (\mathscr{E}_{d,\rho} : \mathscr{C}(d)_\rho) = \frac{[\mathscr{O}_{d,\rho}^\times : 1][\mathscr{E}_\rho : \mathscr{C}_\rho]}{[\mathscr{E}_\rho : \mathscr{E}_{d,\rho}]}. \tag{3.7}$$

Now, recall the "unscrewing" of $\mathfrak{C}(\mathfrak{a}) = I(\mathfrak{a})/P_{\mathfrak{a}}$ where $\mathfrak{a}$ is an ideal of $\mathfrak{o}$:

$$\begin{array}{ccccccc}
\mathfrak{C} & \longleftarrow & I(\mathfrak{a}) & & & & \\
\Big| & & \Big| & & & & \\
1 & \longleftarrow & P(\mathfrak{a}) & \longrightarrow & k^{\times}(\mathfrak{a})E & & \\
 & & \Big| & & \Big| & & \\
 & & P_{\mathfrak{a}} & \longrightarrow & k_{\mathfrak{a}}^{\times}E & \longrightarrow & E \\
 & & & & \Big| & & \Big| \\
 & & & & k_{\mathfrak{a}}^{\times} & \longrightarrow & E_{\mathfrak{a}}
\end{array}$$

- $I(\mathfrak{a})$: fractional ideals coprime to d,
- $P(\mathfrak{a})$: principal fractional ideals coprime to p,
- $k^{\times}(\mathfrak{a})$: elements of $k^{\times}$ coprime to $\mathfrak{a}$,
- $k_{\mathfrak{a}}^{\times}$: elements of $k^{\times}$ congruent to 1 modulo $\mathfrak{a}$,
- $P_{\mathfrak{a}}$: principal fractional ideals generated by elements of $k_a^{\times}$.

Since (3.7) holds for all $\rho \neq 1$ with $[\mathscr{E}_d : \mathscr{C}_d] = |\mathfrak{C}_d \otimes \mathcal{O}|$ and $k^{\times}(d)E/k_d^{\times} \simeq (\mathfrak{o}/d)^{\times}$, taking the product over all such ρ we get

$$\begin{aligned}
|\mathfrak{C}_d \otimes \mathcal{O}| = [\mathscr{E}_d : \mathscr{C}_d] &\geq_p \frac{[(1-e_1)\mathscr{O}_d^{\times} : 1] \cdot [\mathscr{E} : \mathscr{C}]}{[\mathscr{E} : \mathscr{E}_d]} \\
&= \frac{[(1-e_1)\mathscr{O}_d^{\times} : 1] \cdot |\mathfrak{C} \otimes \mathcal{O}|}{[\mathscr{E} : \mathscr{E}_d]} = |\mathfrak{C}_d \otimes \mathcal{O}|.
\end{aligned}$$

In light of (3.7), it follows that

$$[\mathscr{E}_{d,\rho} : \mathscr{C}_{d,\rho}] = \frac{[\mathscr{O}_{d,\rho}^{\times} : 1] \cdot [\mathscr{E}_{\rho} : \mathscr{C}_{\rho}]}{[\mathscr{E}_{\rho} : \mathscr{E}_{d,\rho}]}.$$

But $[\mathscr{E}_{\rho} : \mathscr{C}_{\rho}] = |(\mathfrak{C} \otimes \mathcal{O})_{\rho}|$, hence

$$[\mathscr{E}_{d,\rho} : \mathscr{C}_{d,\rho}] = \frac{[\mathscr{O}_{d,\rho}^{\times} : 1] \cdot |(\mathfrak{C} \otimes \mathcal{O})_{\rho}|}{[\mathscr{E}_{\rho} : \mathscr{E}_{d,\rho}]} = |(\mathfrak{C}_d \otimes \mathcal{O})_{\rho}|.$$

This proves Theorem 1.2.

4. Gauss sums and Stickelberger's Theorem for ray class groups. We now relax the condition on p so that the results in this section are applicable to situations when $p \,|\, [k : \mathbb{Q}]$. The main goal is to prove Theorem 1.3, a ray class version of a theorem of Rubin [R, Theorem 1.3] (specialized to the case when the base field is $\mathbb{Q}$), which itself generalized a theorem of Thaine [Th, Theorem 3].

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

LEMMA 4.1. *Let ℓ be a rational prime completely split in k. For any $\epsilon \in \mathfrak{o}_{k(\zeta_\ell)}^\times$ such that $N_k^{k(\zeta_\ell)}(\epsilon) = 1$, the element*

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

is non-zero for some choice of ζ_ℓ; moreover, $\alpha^{1-\tau} = \epsilon$ where $\langle\tau\rangle = \mathrm{Gal}(k(\zeta_\ell)/k)$.

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

$$x \mapsto -\sum_{a=1}^{\ell-1} \frac{\zeta_\ell^{\tau^a}}{1 - x\zeta_\ell^{\tau^a}} \epsilon^{1+\tau+\cdots+\tau^{a-1}}.$$

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

$$\alpha(x) = \sum_{n=0}^{\infty} \big(-\zeta_\ell^{(n+1)\tau}\epsilon - \zeta_\ell^{(n+1)\tau^2}\epsilon^{1+\tau} - \cdots - \zeta_\ell^{(n+1)\tau^{\ell-1}}\epsilon^{1+\tau+\cdots+\tau^{\ell-2}}\big)x^n.$$

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, we get $\alpha \neq 0$ for some choice of ζ_ℓ. In fact, $\alpha \neq 0$ for at least two choices of ζ_ℓ, for otherwise $\alpha(x)$ has a pole at $x = 1$, a contradiction. This proves the first claim.

Now, notice that

$$\begin{aligned}\epsilon\alpha^\tau &= -\zeta_\ell^{\tau^2}\epsilon^{1+\tau} - \zeta_\ell^{\tau^3}\epsilon^{1+\tau+\tau^2} - \cdots - \zeta_\ell^{\tau^\ell}\epsilon^{1+\tau+\cdots+\tau^{\ell-1}} \\ &= -\zeta_\ell^{\tau^2}\epsilon^{1+\tau} - \zeta_\ell^{\tau^3}\epsilon^{1+\tau+\tau^2} - \cdots - \zeta_\ell^{\tau}\epsilon = \alpha,\end{aligned}$$

since $\tau^\ell = \tau$ and $1+\tau+\cdots+\tau^{\ell-1} = 1$. This proves the lemma (alternatively, see [A3]). ∎

Fix an ideal $\mathfrak{a} \subseteq \mathfrak{o}$. For odd primes ℓ that are completely split in k, let $k(\zeta_\ell)^\times(\mathfrak{a})$ denote the set of all elements of $k(\zeta_\ell)^\times$ that are coprime to $\mathfrak{a}$ and define

$$N_{\ell,\mathfrak{a}} : k(\zeta_\ell)^\times(\mathfrak{a}) \to (\mathfrak{o}/\mathfrak{a})^\times, \quad x \mapsto N_k^{k(\zeta_\ell)}(x) \bmod \mathfrak{a}.$$

Now set

$$E(\ell,\mathfrak{a}) := \{\epsilon \in E_{k(\zeta_\ell)} : N_k^{k(\zeta_\ell)}(\epsilon) = 1,\ N_{\ell,\mathfrak{a}}(\alpha(\ell,\epsilon)) \in \mathrm{im}(E/E_{\mathfrak{a}} \to (\mathfrak{o}/\mathfrak{a})^\times)\}.$$

The following is a generalization of [R, Theorem 5.1].

THEOREM 4.2. *Let $n \in \mathbb{N}$ and let ℓ be an odd prime split completely in k such that $\ell \equiv 1 \bmod n$ and (ℓ) is coprime to $\mathfrak{a}$. 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*

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

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 $\mathfrak{C}(\mathfrak{a})/n\mathfrak{C}(\mathfrak{a})$.

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

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

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

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

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 τ be a generator for $\mathrm{Gal}(k(\zeta_\ell)/k)$, and $\alpha = \alpha(\ell, \epsilon)$ be as in Lemma 4.1. Now, (α) is a non-zero ideal inert under the action imposed by $\mathrm{Gal}(k(\zeta_\ell)/k)$. It follows that there exists an ideal $\mathfrak{b} \subseteq \mathfrak{o}_k$ satisfying

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

where no conjugate of $\mathcal{L}$ is supported by $\mathfrak{b}$. Taking norms of both sides of the above we get

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

Since $N_{\ell,\mathfrak{a}}(\alpha) \in \mathrm{im}(E/E_\mathfrak{a} \to (\mathfrak{o}/\mathfrak{a})^\times)$, we see that $(N_k^{k(\zeta_\ell)}(\alpha)) \in P_\mathfrak{a}$. 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 $\mathfrak{C}(\mathfrak{a})/n\mathfrak{C}(\mathfrak{a})$.

It remains to relate the coefficients a_σ to θ. To this 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, 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

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

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

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

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

Remark 4.3. If in Lemma 4.1 we take $k = \mathbb{Q}(\zeta_m)$ and $\ell \equiv 1 \bmod m$ with $\epsilon = \zeta_m$, then α is the classical Gauss sum. In this case,

$$(\alpha^{\ell-1}) = \lambda^{\sum a_\sigma \sigma^{-1}},$$

where, similar to Theorem 4.2, we have $\zeta_m \equiv u^{a_\sigma \sigma^{-1}} \bmod \lambda^{\sigma^{-1}}$. The dependence of the coefficients a_σ on ℓ is easy to tease out of this congruence, and we are a hop, skip, and a jump away from the classical Stickelberger Theorem.

For the more general types of elements α in Lemma 4.1 and Theorem 4.2, the dependence of the a_σ on ℓ is more difficult to separate. Instead of reckoning with this obstacle, we step around it and show that any G-module map from E/E^{p^n} to $\mathbb{Z}/p^n\mathbb{Z}[G]$ can be effectively filtered through $(\mathfrak{o}_{k(\zeta_\ell)}/L)^\times \otimes \mathbb{Z}/p^n\mathbb{Z}$ for certain well-chosen primes ℓ. This idea was first employed by Rubin [R].

Theorem 4.2 inspires us to make the following definition.

Definition 4.4. For an ideal $\mathfrak{a} \subseteq \mathfrak{o}$, let $\mathcal{T}(\mathfrak{a})$ denote the set of numbers $\varsigma \in k^\times$ such that for all but finitely many primes ℓ split completely in k, there is an $\epsilon \in E(\ell, \mathfrak{a})$ such that for all $\sigma \in G$ we have

$$\epsilon \equiv \varsigma \bmod \mathcal{L}^\sigma$$

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

$$\mathcal{S}(\mathfrak{a}) := \mathcal{T}(\mathfrak{a}) \cap E.$$

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

The 1-special numbers are, in fact, Rubin's special numbers from [R]. It is fair to ask if $\mathfrak{a}$-special numbers even exist. For an appropriate choice of d, the following theorem will show that Schmidt's d-cyclotomic units are contained in the $\mathfrak{a}$-special units. So $\mathcal{S}(\mathfrak{a})$ is a subgroup of finite index of E.

Theorem 4.5. *If $\delta \in D(d)$, then $\pm\delta \in \mathcal{T}(d)$, i.e., $\pm D(d) \subseteq \mathcal{T}(d)$.*

Proof. It suffices to show that $\pm\delta_{n,d} \in \mathcal{T}(d)$ for all $n > 1$ and $n \nmid d$ since these numbers generate $D(d)$. 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

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

where σ_ℓ is the Frobenius automorphism for ℓ in k. Since ℓ splits completely in k, it follows that $\sigma_\ell = 1$, hence $N_{k^n}^{k_n(\zeta_\ell)}(\epsilon_{n,d}) = N_k^{k(\zeta_\ell)}(\epsilon_{n,d}) = 1$.

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

$$\epsilon_{n,d} = N_{k^n(\zeta_\ell)}^{\mathbb{Q}(\zeta_{n\ell})} \prod_{t \mid \overline{d}/q} \left[\frac{(\zeta_\ell^t - \zeta_n^t)^q}{\zeta_\ell^{tq} - \zeta_n^{tq}} \right]^{q^{j-1}\mu(t)d_q/t}.$$

For all $t \mid \overline{d}/q$ we see that ζ_ℓ^t and ζ_ℓ^{tq} are primitive ℓth roots of unity since $(\ell, nd) = 1$; moreover, ζ_n^t and ζ_n^{tq} are not equal to 1 since $n \nmid \overline{d}$. It follows that $\zeta_\ell^t - \zeta_n^t$ and $\zeta_\ell^{tq} - \zeta_n^{tq}$ are units in $\mathbb{Z}[\zeta_{n\ell}]$, hence $\epsilon_{n,d} \in \mathfrak{o}_{k(\zeta_\ell)}^\times$. We also have

$$\frac{(\zeta_\ell^t - \zeta_n^t)^q}{\zeta_\ell^{tq} - \zeta_n^{tq}} \equiv 1 \bmod q,$$

from which it follows that

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

whence $\epsilon_{n,d} \equiv 1 \bmod q^j$. Since q was an arbitrary divisor of d, it follows that $\epsilon_{n,d} \equiv 1 \bmod d$, hence $\pm\epsilon_{n,d} \equiv \pm 1 \bmod d$.

Now, let $N_b = 1 + \tau + \cdots + \tau^{b-1}$. Note that

$$\alpha(\ell, \pm\epsilon_{n,d}) = \mp \sum_{b=1}^{\ell-1} \zeta_\ell^{\tau^b} \epsilon_{n,d}^{N_b} \equiv \mp \sum_{b=1}^{\ell-1} \zeta_\ell^{\tau^b} \bmod d \equiv \mp 1 \bmod d.$$

So $N_k^{k(\zeta_\ell)}(\alpha(\ell, \pm\epsilon_{n,d})) \equiv 1 \bmod d$. This proves that $\pm\epsilon_{n,d} \in E(\ell, d)$, as claimed. ∎

Now, let

$$\begin{aligned} A_n(\mathfrak{a}) &= \mathfrak{C}(\mathfrak{a})/p^n\mathfrak{C}(\mathfrak{a}), \\ A(\mathfrak{a}) &= \mathrm{Syl}_p(\mathfrak{C}(\mathfrak{a})), \\ F_n(\mathfrak{a}) &= \text{the ray class field over } k \text{ associate to } A_n(\mathfrak{a}), \\ F(\mathfrak{a}) &= \text{the ray class field over } k \text{ associate to } A(\mathfrak{a}). \end{aligned}$$

Note that

$$\mathrm{Gal}(F_n(\mathfrak{a})/k) \simeq A_n(\mathfrak{a}) \quad \text{and} \quad \mathrm{Gal}(F(\mathfrak{a})/k) \simeq A(\mathfrak{a})$$

via the Artin map. Let $A'_n(\mathfrak{a}) \le A_n(\mathfrak{a})$ be such that we have $A'_n(\mathfrak{a}) \simeq \mathrm{Gal}(F_n(\mathfrak{a})/(F_n(\mathfrak{a}) \cap k(\zeta_{p^n})))$.

THEOREM 4.6. *Let $\alpha : E/E^{p^n} \to \mathbb{Z}/p^n\mathbb{Z}[G]$ be a G-module map. Then*

$$\alpha(\mathcal{S}(\mathfrak{a})E^{p^n}/E^{p^n}) \text{ annihilates } A'_n(\mathfrak{a}).$$

Proof. The argument here is essentially the same as in [R] (with base field $\mathbb{Q}$) but with some natural adjustments, so we give a somewhat abbre-

viated version of the proof. Let $\mathcal{G} = \mathrm{Gal}(k(\zeta_{p^n})/\mathbb{Q})$ and let

$$\Gamma = \mathrm{Gal}\big(k(\zeta_{p^n}, E^{1/p^n})/k(\zeta_{p^n}, (\ker\alpha)^{1/p^n})\big).$$

Let $\mathcal{G}$ act on Γ by conjugation, and let $\gamma_1, \dots, \gamma_j$ be a complete system of unique representatives of $\Gamma/\mathcal{G}$. We claim that $F_n(\mathfrak{a})$ and $k(\zeta_{p^n}, E^{1/p^n})$ are linearly disjoint over $F_n(\mathfrak{a}) \cap k(\zeta_{p^n})$. Indeed, Kummer theory gives us an isomorphism of $\mathrm{Gal}(k(\zeta_{p^n})/k)$-modules

$$\mathrm{Gal}\big(k(\zeta_{p^n})(F_n(\mathfrak{a}) \cap k(\zeta_{p^n}, E^{1/p^n}))/k(\zeta_{p^n})\big) \simeq \mathrm{Hom}_{\mathbb{Z}}(B, \mu_{p^n})$$

where $B \leq E/E^{p^n}$ is such that $k(\zeta_{p^n}, E^{1/p^n}) = k(B^{1/p^n})$ and μ_{p^n} is the group of p^nth roots of unity. The Galois group on the left is abelian, so it follows that $\mathrm{Gal}(k(\zeta_{p^n})/k)$ acts trivially on $\mathrm{Hom}_{\mathbb{Z}}(B, \mu_{p^n})$. Since k is real and p is an odd prime, $\mathrm{Hom}_{\mathbb{Z}}(B, \mu_{p^n})$ must be trivial, whence the claim.

Now, let $\mathfrak{c} \in A_n'(\mathfrak{a})$. We may choose $\beta_i \in \mathrm{Gal}(F_n(\mathfrak{a})k(\zeta_{p^n}, E^{1/p^n})/k)$ such that

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

By the Chebotarev Density Theorem, there exist infinitely many degree 1 non-conjugate j-tuples of primes $\lambda_1, \dots, \lambda_j \subseteq \mathfrak{o}_k$ such that $(\lambda_i, \mathfrak{a}) = 1$ and β_i is in the conjugacy class of Frobenius automorphisms for λ_i in $\mathrm{Gal}(F_n(\mathfrak{a})k(\zeta_{p^n}, E^{1/p^n})/k)$. It follows that $\lambda_i \in \mathfrak{c}$. We let ℓ_i be the rational prime below λ_i. Since $\beta_i|_{k(\zeta_{p^n})} = \mathrm{id}$, it follows that $\ell_i \equiv 1 \bmod p^n$.

Let ϕ be the natural map $E/E^{p^n} \to (\mathfrak{o}/\mathfrak{L})^\times \otimes (\mathbb{Z}/p^n\mathbb{Z})$ where $\mathfrak{L} = \prod_{i=1}^{j} \ell_i$. From the exact sequence of $\mathrm{Gal}(k(\zeta_{p^n})/k)$-modules

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

we obtain the exact sequence of $\mathrm{Gal}(k(\zeta_{p^n})/k)$-invariants

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

So $[k(\zeta_{p^n})^{\times p^n} \cap k : k^{\times p^n}] = 1$. Therefore

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

In short, since Γ is saturated with Frobenius automorphisms for the λ_i, it follows that $\epsilon \in \ker\alpha$ if and only if $\epsilon \in \ker\phi$. This allows us to consider the well-defined map

$$\alpha \circ \phi^{-1} : \mathrm{im}(\phi) \to (\mathbb{Z}/p^n\mathbb{Z})[G]$$

which we may lift to a map $f : (\mathfrak{o}/\mathfrak{L})^\times \otimes (\mathbb{Z}/p^n\mathbb{Z}) \to (\mathbb{Z}/p^n\mathbb{Z})[G]$, obtaining the following commutative diagram:

$$\begin{array}{ccc} E/E^{p^n} & \xrightarrow{\alpha} & (\mathbb{Z}/p^n\mathbb{Z})[G] \\ {\scriptstyle\phi}\downarrow & \nearrow_{f} & \\ (\mathfrak{o}/\mathfrak{L})^\times \otimes (\mathbb{Z}/p^n\mathbb{Z}) & & \end{array}$$

Now, let $\varsigma_\mathfrak{a} \in \mathcal{S}(\mathfrak{a})$. Without loss of generality, we may assume that for each i, there exists $\epsilon_i \in E(\ell_i, \mathfrak{a})$ such that

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

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

$$L_i := \prod_{\sigma \in G} \mathcal{L}_i^\sigma.$$

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

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

This association allows us to consider ϕ and f as functions defined, respectively, into and on

$$\prod (\mathfrak{o}_{k(\zeta_{\ell_i})}/L_i)^\times \otimes (\mathbb{Z}/p^n\mathbb{Z}).$$

Let $u_i \in \mathfrak{o}_{k(\zeta_{\ell_i})}$ be such that

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

where $\langle s_i \rangle = (\mathbb{Z}/\ell_i\mathbb{Z})^\times$, as in Theorem 4.2. Note that

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

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

$$\mathfrak{s}_\mathfrak{a} = \mathfrak{u}_i^{\theta_i}, \quad \text{where} \quad \left\{ \begin{matrix} \mathfrak{s}_\mathfrak{a} = (\varsigma_\mathfrak{a} \bmod L_i) \otimes 1 \\ \mathfrak{u}_i = (u_i \bmod L_i) \otimes 1 \end{matrix} \right\} \in (\mathfrak{o}_{k(\zeta_{\ell_i})}/L_i)^\times \otimes (\mathbb{Z}/p^n\mathbb{Z}).$$

Since $\varsigma_\mathfrak{a} \bmod L_i \equiv \epsilon_i \bmod L_i$, it follows that θ_i is an annihilator of the cokernel of the map

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

So θ_i annihilates the class of $[\lambda_i] = \mathfrak{c}$ in $\mathfrak{C}(\mathfrak{a})/p^n\mathfrak{C}(\mathfrak{a})$ by Theorem 4.2. Let $\overline{\varsigma_\mathfrak{a}} = \varsigma_\mathfrak{a} \bmod E^{p^n}$. Then

$$\alpha(\overline{\varsigma_\mathfrak{a}}) = f(\mathfrak{s}_\mathfrak{a}) = \sum_{i=1}^{j} \theta_i f(\mathfrak{u}_i),$$

and we get

$$\mathfrak{c}^{\alpha(\overline{\varsigma_{\mathfrak{a}}})} = \prod_{i=1}^{j} (\mathfrak{c}^{\theta_i})^{f(\mathfrak{u}_i)} = \prod_{i=1}^{j} 1^{f(\mathfrak{u}_i)} = 1.$$

This completes the proof of the theorem. ∎

Proof of Theorem 1.3. Let $\omega_1, \ldots, \omega_t$ be a $\mathbb{Z}_p$-basis for $\mathcal{O}$. For $i = 1, \ldots, t$ define $\alpha_i : E \to \mathbb{Z}_p[G]$ by

$$\alpha(\epsilon) = \sum_{i=1}^{t} \alpha_i(\epsilon)\omega_i.$$

Each α_i is a G-module map, and since $\mathrm{Syl}_p(\mathfrak{C}_{\mathfrak{a}}) \leq A'_n(\mathfrak{a})$, the assertion now follows from Theorem 4.6. ∎

Proof of Theorem 1.4. Let ϑ be the G-module map defined in the previous section. For every $\alpha \in \mathrm{Hom}_G(E, \mathcal{O}[G])$, there exists $\beta \in K[G]$ such that $\alpha = \beta\vartheta$ by [A1, Theorem 5.1]. So for every $\beta \in K[G]$ such that $\beta\vartheta(E) \subseteq \mathcal{O}[G]$, $\beta\vartheta(\mathcal{S}(\mathfrak{a}))$ annihilates $\mathfrak{C}_{\mathfrak{a}} \otimes \mathcal{O}$. If the ramification index of p in k is $e(p) = p^j b$ where $(p, b) = 1$, then we could take

$$\beta = \varpi^{je(p)-p^j} = \frac{|e(p)|_p^{-1}}{\varpi^{|e(p)|_p^{-1}}}$$

(see [A1, Lemma 2.3]). In particular, we get the explicit annihilation result: for every $\varsigma_{\mathfrak{a}} \in \mathcal{S}(\mathfrak{a})$ (perhaps a d-cyclotomic unit for an appropriate d), the element

$$\frac{|e(p)|_p^{-1}}{\varpi^{|e(p)|_p^{-1}}} \sum_{\sigma \in G} \log_p(\varsigma_{\mathfrak{a}}^{\sigma})\sigma^{-1} \in \mathcal{O}[G]$$

annihilates $\mathfrak{C}_{\mathfrak{a}} \otimes \mathcal{O}$. ∎

Remark 4.7. The above theorem confirms a suspicion of D. Solomon regarding a stronger annihilation result lying beyond his [Sol, Conjecture 4.1] (see [Sol, Remark 4.1]). In particular, let U denote the maximal abelian pro-p-extension of k. The elements of Theorem 1.4 are explicit annihilators of explicit quotients of $\mathrm{Gal}(U/k) \otimes \mathcal{O}$.

Remark 4.8. The group $\mathrm{Syl}_p(E/\mathcal{S}(\mathfrak{a}))$ is mysterious. In the case when $p \nmid |G|$, the order of $\mathrm{Syl}_p(E/\mathcal{S}(d))_\rho$ seems to be less than or equal to that of $\mathrm{Syl}_p(E_d/C_d)_\rho$. One wonders whether $\mathrm{Syl}_p(E/\mathcal{S}(\mathfrak{a}))$ is encoding information more akin to the *exponent* of $\mathrm{Syl}_p(\mathfrak{C}_{\mathfrak{a}})$.

References

[A1] T. All, *On p-adic annihilators of real ideal classes*, J. Number Theory 133 (2013), 2324–2338.

[A2] T. All, *On the p-adic completion of the units of a real abelian number field*, J. Number Theory 136 (2014), 1–21.

[A3] T. All, *On Stickelberger elements for* $\mathbb{Q}(\zeta_{p^{n+1}})^+$ *and p-adic L-functions*, J. Number Theory 160 (2016), 287–306.

[D] T. Dorsey, *Morphic and principal-ideal group rings*, J. Algebra 318 (2007), 393–411.

[Gra] G. Gras, *Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés*, Ann. Inst. Fourier (Grenoble) 27 (1977), no. 1, 1–66.

[Gre] R. Greenberg, *On p-adic L-functions and cyclotomic fields. II*, Nagoya Math. J. 67 (1977), 139–158.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. 76 (1984), 179–330.

[R] K. Rubin, *Global units and ideal class groups*, Invent. Math. 89 (1987), 511–526.

[Sch] C.-G. Schmidt, *Stickelbergerideale und Kreiseinheiten zu Klassenkörpern abelscher Zahlkörper*, J. Reine Angew. Math. 353 (1984), 14–54.

[S] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.

[Sol] D. Solomon, *On a construction of p-units in abelian fields*, Invent. Math. 109 (1992), 329–350.

[Th] F. Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. (2) 128 (1988), 1–18.

Timothy All
Department of Mathematics
Rose-Hulman Institute of Technology
5500 Wabash Ave
Terre Haute, IN 47803, U.S.A.
E-mail: timothy.all@rose-hulman.edu