Canad. J. Math. Vol. 71 (6), 2019 pp. 1395–1419
http://dx.doi.org/10.4153/CJM-2018-035-9

Annihilators of the Ideal Class Group of a Cyclic Extension of an Imaginary Quadratic Field

Hugo Chapdelaine and Radan Kučera

Abstract. The aim of this paper is to study the group of elliptic units of a cyclic extension L of an imaginary quadratic field K such that the degree $[L:K]$ is a power of an odd prime p. We construct an explicit root of the usual top generator of this group, and we use it to obtain an annihilation result of the p-Sylow subgroup of the ideal class group of L.

Introduction

This work was motivated by a series of papers [5, 6, 9] that studied annihilators of the p-Sylow subgroup of the ideal class group of a cyclic abelian field L over $\mathbb{Q}$, whose degree is a power of an odd prime p; these annihilators were obtained by means of circular units. The goal of this paper is to study annihilators of the p-Sylow subgroup of the ideal class group of a field L that is a cyclic extension over K, where K is an imaginary quadratic field whose class number $h = h_K$ is not divisible by p. In this new setting, the former role played by the circular units is now being played by the so-called *elliptic units*. Similarly to the previous series of papers, certain annihilators of the ideal class group of L are obtained by means of elliptic units above K. Recall that, in essence, an elliptic unit above K is a unit that lives in an abelian extension of K and is obtained by evaluating a certain modular unit (*i.e.*, a modular function whose divisor is supported at the cusps) at an element $\tau \in K \cap \mathfrak{h}$, where $\mathfrak{h}$ corresponds to the Poincaré upper half-plane. Depending on what applications one has in mind, different choices of modular units have been considered in the literature. For this paper, we use a slight modification of the group of elliptic units introduced by Oukhaba in [11]; the only difference is that we do not raise the generators of the group of elliptic units considered in [11] to the h-th power. The index of our group of elliptic units $\mathcal{C}_L$ in the group $\mathcal{O}_L^\times$ of all units of L is given in Lemma 3.4. Then, starting from the group $\mathcal{C}_L$, we proceed to extract certain roots (where the root exponents are group ring elements) of the generators of $\mathcal{C}_L$ that again lie in L. These roots of elliptic units allow us to define an *enlarged group of elliptic units* $\overline{\mathcal{C}}_L$, whose index in $\mathcal{O}_L^\times$ is given in Theorem 5.2. This enlarged group $\overline{\mathcal{C}}_L$ forms an important ingredient of the main result of this paper: any

Received by the editors November 11, 2017; revised July 24, 2018.
Published electronically December 7, 2018.
The second author was supported under Project 15-15785S of the Czech Science Foundation.
AMS subject classification: **11R20**, 11R27, 11R29.
Keywords: annihilator, class group, elliptic unit.

annihilator of the p-Sylow part of the quotient $\mathcal{O}_L^\times/\overline{\mathcal{C}}_L$ must annihilate a certain (very explicit) subgroup of the p-Sylow part of the ideal class group of L; see Theorem 7.5.

We would like to emphasize that many of the techniques used in this paper borrow heavily from the ones introduced in [5] and [9]. In order to keep the paper within a reasonable size, we faced the problem of choosing which proofs to present in full detail and which to only sketch (or omit). For each of the proofs, we have decided to distinguish whether the needed modifications are straightforward or not. Of course, such choices are subjective but we hope that our chosen style clarifies the overall presentation, and, at the same time, has the effect of highlighting the new ideas. For example, in the construction of nontrivial roots of elliptic units given in Sections 4 and 6, we decided to give all the details, whereas the necessary modifications of Theorem 7.4 in the style of Rubin are left to the reader.

Finally, it does not seem that there is any overlap between the main result of this paper and the current literature. For example, in [10], Ohshita studies the higher Fitting ideals of Iwasawa modules associated with a given $\mathbb{Z}_p$- or $\mathbb{Z}_p^2$-extension K_∞/K_0, where K_0 is an abelian extension of an imaginary quadratic number field K whose degree $[K_0:K]$ is not divisible by p. As usual, such an Iwasawa module is defined as the projective limit of the p-parts of the ideal class groups of finite subextensions of K_∞/K_0. In particular, our field L can never be a subfield of Ohshita's field K_∞, because L/K is unramified at all the primes above p and is of p-power degree. In [1], Bley constructs generalized roots of elliptic units (in Solomon's style, via Hilbert's Theorem 90) in the layers of a $\mathbb{Z}_p$-extension of an abelian extension N of an imaginary quadratic number field K. He then uses these roots to construct certain elements in the p-adic completion of the group of $\mathfrak{p}$-units of N, where $\mathfrak{p}$ is a prime of K above p. In [2], he uses these elements to prove the p-part of the Equivariant Tamagawa Number Conjecture (ETNC) in the aforementioned setting. Even though our field L could play the role of the field N of Bley, there is no connection, a priori, between his $\mathfrak{p}$-units and our units obtained as roots of elliptic units. Of course, thanks to Burns, we know that the validity of ETNC has a lot of consequences (see [3]), but even in the situation when the results of Bley could be used (in our setting this would impose the additional assumptions that p splits in $K/\mathbb{Q}$ and that there exists a prime $\mathfrak{p}$ of K above p which splits in L/K), it does not seem that the general machinery of Burns can be used to derive the main result of this paper.

1 Notation and Preliminaries

Let K be an imaginary quadratic number field, let $H = H_K$ be the Hilbert class field of K, let $h = h_K = [H:K]$ be the class number of K, and let L/K be a cyclic Galois extension of degree p^k where p is an odd prime and k is a positive integer. We let $\Gamma = \mathrm{Gal}(L/K) = \langle\sigma\rangle$ where σ is a fixed generator. We suppose that $p \nmid h$ and that there are exactly $s \geq 2$ ramified primes in L/K. It follows from the first assumption that $L \cap H = K$. Let $\wp_1, \dots, \wp_s$ be all the (pairwise distinct) prime ideals of K that ramify in L/K. For each $j \in I = \{1, \dots, s\}$ we choose a generator $\pi_j \in \mathcal{O}_K$ of the principal ideal $\wp_j^h$, and we let $q_j \in \mathbb{Z}$ be the only rational prime number in $\wp_j$. We suppose that p is unramified in $L/\mathbb{Q}$ and that each q_j is unramified in $K/\mathbb{Q}$. In particular, this implies that $p \nmid |\mu_L|$ and that $p \neq q_j$ for all $j \in I$. Here μ_F denotes the group of roots of unity of a field F.

For each $j \in I$ let us fix an arbitrarily chosen prime ideal $\mathfrak{P}_j$ of L above $\wp_j$. Let t_j be the ramification index of $\mathfrak{P}_j$ over $\wp_j$ and let n_j be the index of the decomposition group of $\mathfrak{P}_j$ in Γ. It follows that $t_j n_j \mid p^k$ and that $\{\mathfrak{P}_j^{\sigma^i}\}_{i=0}^{n_j-1}$ is the full set of distinct prime ideals of L above $\wp_j$. In particular, we have the decomposition

$$\wp_j \mathcal{O}_L = \prod_{i=0}^{n_j-1} \mathfrak{P}_j^{t_j \sigma^i}.$$

We consider the completion $\mathbb{Q}_{q_j} \subseteq K_{\wp_j} \subseteq L_{\mathfrak{P}_j}$ of $\mathbb{Q} \subseteq K \subseteq L$. Since the extension of local fields $L_{\mathfrak{P}_j}/K_{\wp_j}$ has a ramification index equal to t_j, it follows from local class field theory that the group $\mathcal{O}_{K_{\wp_j}}^\times$ of units of $\mathcal{O}_{K_{\wp_j}}$ has a closed subgroup of index t_j, namely the subgroup $\mathrm{N}_{L_{\mathfrak{P}_j}/K_{\wp_j}}(\mathcal{O}_{L_{\mathfrak{P}_j}}^\times)$. It is well known that $\mathcal{O}_{K_{\wp_j}}^\times$ is the direct product of the group of principal units $\mathcal{U}_j = \{\epsilon \in \mathcal{O}_{K_{\wp_j}}^\times ; \epsilon \equiv 1 \pmod{\wp_j}\}$ and of the subgroup of roots of unity of orders coprime to q_j, which is a finite cyclic group isomorphic to $(\mathcal{O}_{K_{\wp_j}}/\wp_j \mathcal{O}_{K_{\wp_j}})^\times \cong (\mathcal{O}_K/\wp_j)^\times$, whose order is $|\mathcal{O}_K/\wp_j| - 1 = \mathrm{N}_{K/\mathbb{Q}}(\wp_j) - 1$. Moreover, it is well known that if the index of a closed subgroup of $\mathcal{U}_j$ is finite, then this index is a power of q_j, and so it is coprime to t_j (a power of p). Therefore, we must have $\mathrm{N}_{K/\mathbb{Q}}(\wp_j) \equiv 1 \pmod{t_j}$.

Since $\wp_1, \ldots, \wp_s$ are all the prime ideals that ramify in L/K and there is no real embedding of K we see that the conductor of L/K is $\prod_{j \in I} \wp_j^{a_j}$ for some positive integers $a_j \geq 1$. Since tamely ramified extensions have square-free conductors (see, for example, [4, II.5.2.2(ii), p. 151]), we must have $a_j = 1$ for all $j \in I$.

2 The Distinguished Subfields F_j

For each non-zero ideal $\mathfrak{m} \subseteq \mathcal{O}_K$, let us denote by $K(\mathfrak{m})$ the *ray class field of K of modulus* $\mathfrak{m}$. For any subset $\varnothing \neq J \subseteq I = \{1, \ldots, s\}$, we also let $\mathfrak{m}_J = \prod_{j \in J} \wp_j$. In the previous section we showed that $L \subseteq K(\mathfrak{m}_I)$. In fact, more is true. A simple exercise in class field theory shows that the index $[K(\mathfrak{m}_I) : \prod_{j \in I} K(\wp_j)]$ divides a power of $|\mu_K|$, where the product is meant for the compositum of the fields $K(\wp_j)$'s. Since $p \nmid |\mu_K|$, it follows that $L \subseteq \prod_{j \in I} K(\wp_j)$.

We would now like to introduce, for each index $j \in I$, a distinguished subfield $F_j \subseteq K(\wp_j)$. The following elementary lemma will be used in the definition of F_j and also in Definition 6.1.

Lemma 2.1 *Let T be an abelian group (written additively and not necessarily finite) and let n be a positive integer. If $T/nT \cong \mathbb{Z}/n\mathbb{Z}$, then T admits a unique subgroup of index n, namely nT. Let (T, S, n) be a triple such that T is an abelian group, $S \leq T$ is a subgroup of finite index $[T:S]$, and n is a positive integer. Assume that $\gcd(n, [T:S]) = 1$. Then the natural map $\pi\colon S/nS \to T/nT$ is an isomorphism.*

Proof The elementary proof is left to the reader. ∎

From class field theory we have a canonical isomorphism $\mathrm{Gal}(K(\wp_j)/H) \cong (\mathcal{O}_K/\wp_j)^\times/\operatorname{im}\mu_K$, which is a cyclic group of order divisible by t_j. Since $p \nmid h$, we can apply Lemma 2.1 to the triple $(\mathrm{Gal}(K(\wp_j)/K), \mathrm{Gal}(K(\wp_j)/H), t_j)$ and define F_j as the unique subfield of $K(\wp_j)$ such that $[F_j : K] = t_j$. One can check that the extension F_j/K satisfies the following properties: $F_j \cap H = K$ and F_j/K is unramified outside of $\wp_j$ and totally ramified at $\wp_j$.

For any $\varnothing \neq J \subseteq I = \{1, \ldots, s\}$, it is convenient to introduce the shorthand notation $K_J = K(\mathfrak{m}_J)$ and $F_J = \prod_{j\in J} F_j \subseteq K_J$. Note that the conductor of F_J over K is $\mathfrak{m}_J$. It follows from the definition of F_I that $\mathrm{Gal}(F_I/F_{I-\{j\}})$ is the inertia subgroup of a prime of F_I above $\wp_j$ (note that $I - \{j\} \neq \varnothing$, since $|I| \geq 2$). In particular, for each $j \in J$, $|\mathrm{Gal}(F_I/F_{I-\{j\}})| = t_j$. The next lemma gives the main properties of the Galois extension F_I/K.

Proposition 2.2 *For each $j \in I$, we have $F_j K_{I-\{j\}} = LK_{I-\{j\}}$. The Galois group*

$$G = \mathrm{Gal}(F_I/K) = \prod_{j\in I} \mathrm{Gal}(F_I/F_{I-\{j\}}) \tag{2.1}$$

is the direct product of its inertia subgroups. Moreover, $L \subseteq F_I$.

Proof Recall that the conductor of L over K is $\mathfrak{m}_I$, and hence $L \subseteq K_I$. For any $j \in I$, the inertia group of a prime of K_I above $\wp_j$ is $\mathrm{Gal}(K_I/K_{I-\{j\}})$, and so the inertia group of a prime of L above $\wp_j$ is $\mathrm{Gal}(L/L \cap K_{I-\{j\}})$ (the restriction of $\mathrm{Gal}(K_I/K_{I-\{j\}})$ to L). Hence $\mathrm{Gal}(LK_{I-\{j\}}/K_{I-\{j\}}) \cong \mathrm{Gal}(L/L \cap K_{I-\{j\}})$ is of order t_j. An easy ramification argument shows that

$$F_j \cap K_{I-\{j\}} = K. \tag{2.2}$$

Indeed, $F_j \cap K_{I-\{j\}}$ is an unramified abelian extension of K, so that $F_j \cap K_{I-\{j\}} \subseteq H \cap F_j = K$, where the last equality follows from the fact that $p \nmid h$. Therefore, $\mathrm{Gal}(F_j K_{I-\{j\}}/K_{I-\{j\}}) \cong \mathrm{Gal}(F_j/K)$ is also of order t_j. We have thus proved that the two subgroups $\mathrm{Gal}(K_I/F_j K_{I-\{j\}})$ and $\mathrm{Gal}(K_I/LK_{I-\{j\}})$ have the same index inside $\mathrm{Gal}(K_I/K_{I-\{j\}})$. Since $K_I/K_{I-\{j\}}$ is totally tamely ramified at each prime of K_I above $\wp_j$, it follows that $\mathrm{Gal}(K_I/K_{I-\{j\}})$ is cyclic, which forces the group equality

$$\mathrm{Gal}(K_I/F_j K_{I-\{j\}}) = \mathrm{Gal}(K_I/LK_{I-\{j\}}) \subseteq \mathrm{Gal}(K_I/K_{I-\{j\}}). \tag{2.3}$$

In particular, it follows from (2.3) that $F_j K_{I-\{j\}} = LK_{I-\{j\}}$, which proves the first claim. Let us now show (2.1). An argument similar to the proof of (2.2) implies that $\bigcap_{j\in I} F_{I-\{j\}} = K$, and thus G is generated by $\bigcup_{j\in I} \mathrm{Gal}(F_I/F_{I-\{j\}})$. Also, since $F_{I-\{j\}} F_j = F_I$, we have $\mathrm{Gal}(F_I/F_{I-\{j\}}) \cap \mathrm{Gal}(F_I/F_j) = \{\mathrm{id}\}$, and therefore G is the direct product of the groups $\mathrm{Gal}(F_I/F_{I-\{j\}})$'s, which gives (2.1).

It remains to show that $L \subseteq F_I$. Set $M = \bigcap_{j\in I} F_j K_{I-\{j\}}$. Note that $L \subseteq M$ (by the first part of Proposition 2.2) and that $F_I H \subseteq M$.

We claim that $F_I H = M$; in particular, this will imply that $L \subseteq F_I H$. Let us prove it. The inertia group of each prime of M above $\wp_j$ is of order at most t_j since the ramification index of $\wp_j$ in $F_j K_{I-\{j\}}/K$ is equal to t_j. On the one hand, since the maximal unramified subextension of M/K is H/K, it follows that (i) $[M : H] \leq \prod_{j\in I} t_j$. On the other hand, since $\mathrm{Gal}(F_I/K)$ is a p-group and $p \nmid h = [H : K]$, we have $H \cap F_I = K$, so that $\mathrm{Gal}(F_I H/H) \cong \mathrm{Gal}(F_I/K)$, and thus from (2.1), we deduce that (ii)

$[F_I H : H] = [F_I : K] = \prod_{j \in I} t_j$. Combining (i) and (ii) with the inclusion $F_I H \subseteq M$, we obtain that $F_I H = M$.

The paragraph above just proved that $L \subseteq F_I H = M$. Since $p \nmid h = [F_I H : F_I]$ and $\mathrm{Gal}(F_I/K)$ is a p-group, it follows that $\mathrm{Gal}(F_I H/F_I)$ is the smallest subgroup of the abelian group $\mathrm{Gal}(F_I H/K)$ whose index is a power of p, which implies that $L \subseteq F_I$. This concludes the proof. ■

Corollary 2.3 (i) *For each index $j \in I$, the inertia subgroup of a prime of L above $\wp_j$ is $\mathrm{Gal}(L/L \cap F_{I-\{j\}}) = \langle \sigma^{p^k/t_j} \rangle$; moreover, $F_{I-\{j\}} L = F_I$ and $[L \cap F_{I-\{j\}} : K] = \frac{p^k}{t_j}$.*

(ii) *F_I/L is an unramified abelian extension.*

(iii) *There exists at least one index $j_0 \in I$ such that $t_{j_0} = p^k$ so that the abelian Galois group $G = \mathrm{Gal}(F_I/K)$ has exponent p^k.*

Proof Recall that $\mathrm{Gal}(F_I/F_{I-\{j\}})$ is the inertia subgroup of a prime of F_I above $\wp_j$. We have $L \subseteq F_I$ by Proposition 2.2, and so $\mathrm{Gal}(L/L \cap F_{I-\{j\}})$ is the inertia subgroup of a prime of L above $\wp_j$. Since both of these inertia subgroups have the same order t_j, and $\langle \sigma^{p^k/t_j} \rangle$ is the only subgroup of Γ of order t_j, we get (i) and we see that F_I/L is unramified at each prime of L above $\wp_j$. But F_I/L can be ramified only at primes above $\wp_1, \dots, \wp_s$, because the conductor of F_I over K is $\mathfrak{m}_I$, and (ii) follows. By (2.1), the exponent of G is the maximum of all t_j's, and so it divides p^k. But since Γ is a cyclic quotient of G of order p^k, we obtain (iii). ■

3 Introducing the Group of Elliptic Units

For the rest of the paper, we fix once and for all an embedding $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. In particular, the inclusion $K \subseteq \mathbb{C}$ singles out one of the two embeddings of K into $\mathbb{C}$. For any subset $\varnothing \neq J \subseteq I$, we let f_J be the least positive integer in $\mathfrak{m}_J$,

(3.1) $$w_J = \left| \left\{ \zeta \in \mu_K \,;\, \zeta \equiv 1 (\operatorname{mod} \mathfrak{m}_J) \right\} \right|,$$

so that w_J divides $w_K := |\mu_K|$, and we let

(3.2) $$\eta_J = \mathrm{N}_{K_J/F_J}(\varphi_{\mathfrak{m}_J})^{w_K f_I/(w_J f_J)} \in \mathcal{O}_{F_J}$$

where $\varphi_{\mathfrak{m}_J}$ is defined as in [11, Definition 2, p. 5]. We would like to point out that the definition of $\varphi_{\mathfrak{m}_J}$, as a complex number, uses implicitly the fact that K is included in $\mathbb{C}$.

For a finite abelian extension M/F and a prime ideal $\mathfrak{p}$ of F that is unramified in M/F, we use the Artin symbol $\left(\frac{M/F}{\mathfrak{p}}\right) \in \mathrm{Gal}(M/F)$ to denote the Frobenius automorphism of $\mathfrak{p}$ in the relative extension M/F.

For any $j \in I$, we let $\lambda_j \in G = \mathrm{Gal}(F_I/K)$ be the unique automorphism such that

$$\lambda_j\big|_{F_{I-\{j\}}} = \left(\frac{F_{I-\{j\}}/K}{\wp_j}\right) \quad \text{and} \quad \lambda_j\big|_{F_j} = 1.$$

The next lemma will be used in the proof of Theorem 4.2 as well as in Section 5.

Lemma 3.1 *For each $j \in I$, choose a prime $\mathfrak{P}_j$ of L above $\wp_j$. Then the inertia group of $\mathfrak{P}_j$ is $\langle \sigma^{p^k/t_j} \rangle = \mathrm{Gal}(L/L \cap F_{I-\{j\}})$ and the decomposition group of $\mathfrak{P}_j$ is $\langle \sigma^{n_j} \rangle = \langle \lambda_j|_L, \sigma^{p^k/t_j} \rangle$.*

Proof The first part was proved in Corollary 2.3(i). It thus follows that the maximal subextension of L/K which is unramified at $\wp_j$ is $L \cap F_{I-\{j\}}/K$. In particular, the Frobenius automorphism of $\wp_j$ in $L \cap F_{I-\{j\}}/K$ is equal to

$$\left(\frac{L \cap F_{I-\{j\}}/K}{\wp_j} \right) = \lambda_j\big|_{L \cap F_{I-\{j\}}}$$

and thus $\langle \lambda_j|_L, \sigma^{p^k/t_j} \rangle$ is equal to the decomposition group of $\mathfrak{P}_j$. Moreover, by definition of n_j, we have $[\Gamma : \langle \lambda_j|_L, \sigma^{p^k/t_j} \rangle] = n_j$. Finally, since $\langle \sigma^{n_j} \rangle$ is the only subgroup of Γ of index n_j, this forces $\langle \sigma^{n_j} \rangle = \langle \lambda_j|_L, \sigma^{p^k/t_j} \rangle$. ∎

The algebraic numbers η_J defined in (3.2) satisfy the following norm relations which can be derived from [11, Proposition 3, p. 5]: for each $J \subseteq I$ and each $j \in I$ such that $\{j\} \subsetneq J$,

$$\mathrm{N}_{F_J/F_{J-\{j\}}}(\eta_J) = \eta_{J-\{j\}}^{1-\lambda_j^{-1}}, \tag{3.3}$$

and for each $j \in I$,

$$\mathrm{N}_{F_j/K}(\eta_{\{j\}}) = \mathrm{N}_{H/K}\left(\frac{\Delta(\mathcal{O}_K)}{\Delta(\wp_j)} \right)^{f_I},$$

where Δ is the discriminant Delta function that appears in [11, Section 2.1]. It follows from [11, Proposition 1, p. 3] that $\mathrm{N}_{F_j/K}(\eta_{\{j\}})$ generates the ideal $\wp_j^{12hf_I} = (\pi_j \mathcal{O}_K)^{12f_I}$, hence

$$\mathrm{N}_{F_j/K}(\eta_{\{j\}}) = \xi_j \pi_j^{12f_I} \tag{3.4}$$

for some $\xi_j \in \mu_K$.

The next lemma gives an exact description of the roots of unity in F_I. In particular, it will allow us to replace μ_F by μ_K for any subfield $K \subseteq F \subseteq F_I$ in the sequel.

Lemma 3.2 *We have $\mu_{F_I} = \mu_K$.*

Proof We do a proof by contradiction. Let ζ be a root of unity in F_I that is not in K. In particular, we must have $2 | [\mathbb{Q}(\zeta) : \mathbb{Q}]$ and $[K(\zeta) : K] > 1$. Using the fact that p is odd, we see that $[K(\zeta) : \mathbb{Q}]$ is equal to twice a power of p, which implies that K is the only quadratic subfield of $K(\zeta)$. Since $\mathbb{Q}(\zeta) \subseteq K(\zeta)$ and $\mathbb{Q}(\zeta)$ contains at least one quadratic subfield, we also deduce that (i) K is the only quadratic subfield of $\mathbb{Q}(\zeta)$ and (ii) $K(\zeta) = \mathbb{Q}(\zeta)$. From (i), it follows that there is exactly one prime, say ℓ, which ramifies in $\mathbb{Q}(\zeta)/\mathbb{Q}$ and that its ramification is total. In particular, since $K \subseteq \mathbb{Q}(\zeta) \subseteq F_I$ and $[\mathbb{Q}(\zeta) : K] > 1$, the prime ℓ must also ramify in $[F_I : K]$. From Corollary 2.3(ii), we know that F_I/L is unramified, and therefore, ℓ must also ramify in L/K. We thus have shown the existence of a rational prime ℓ that ramifies in both $K/\mathbb{Q}$

and L/K; this contradicts our initial assumptions on the ramification of the extension $L/\mathbb{Q}$. ∎

Definition 3.3 We define the group of elliptic numbers P_{F_I} of F_I to be the $\mathbb{Z}[G]$-submodule of $F_I^\times$ generated by the group of roots of unity μ_{F_I} ($= \mu_K$ by Lemma 3.2) and by η_J for all $\varnothing \neq J \subseteq I$. The group of elliptic units $\mathcal{C}_{F_I}$ of F_I is defined as the intersection $\mathcal{C}_{F_I} = P_{F_I} \cap \mathcal{O}_{F_I}^\times$. The group of elliptic numbers P_L of L is defined as the $\mathbb{Z}[\Gamma]$-submodule of $L^\times$ generated by the group of roots of unity μ_L ($= \mu_K$) and by $\mathrm{N}_{F_J/F_J\cap L}(\eta_J)$ for all $\varnothing \neq J \subseteq I$. Finally, the group of elliptic units $\mathcal{C}_L$ of L is defined as the intersection $\mathcal{C}_L = P_L \cap \mathcal{O}_L^\times$.

Let M be a finite abelian extension of K. In [11, Definition 3, p. 7], Oukhaba introduced a group of units in $\mathcal{O}_M$, which we denote by C_M. The groups $\mathcal{C}_{F_I}$ and $\mathcal{C}_L$ that appear in Definition 3.3 differ slightly from the groups C_{F_I} and C_L, respectively. Using the key fact that $F_I \cap H = K$ one can check that $C_{F_I} = \langle \mu_K \cup \{\epsilon^h : \epsilon \in \mathcal{C}_{F_I}\}\rangle$. Similarly, since $L \cap H = K$, one can also check that $C_L = \langle \mu_K \cup \{\epsilon^h : \epsilon \in \mathcal{C}_L\}\rangle$. The two previous equalities will be used in the proof of the following lemma.

Lemma 3.4 (i) *The indices of $\mathcal{C}_{F_I}$ in $\mathcal{O}_{F_I}^\times$ and $\mathcal{C}_L$ in $\mathcal{O}_L^\times$ are finite and are given explicitly by*

$$[\mathcal{O}_{F_I}^\times : \mathcal{C}_{F_I}] = (12 w_K f_I)^{[F_I:K]-1} \cdot \frac{h_{F_I}}{h},$$
$$[\mathcal{O}_L^\times : \mathcal{C}_L] = (12 w_K f_I)^{[L:K]-1} \cdot \frac{h_L}{h \cdot [L:\widetilde{L}]},$$

where h_{F_I}, h_L, and h are the class numbers of F_I, L, and K, respectively, and $\widetilde{L}$ is a maximal subfield of L containing K such that $\widetilde{L}/K$ is ramified in at most one prime ideal of K. Note that such a field $\widetilde{L}$ is unique (and thus well defined), since $\Gamma = \mathrm{Gal}(L/K)$ is a cyclic group of a prime power order.

(ii) *For any $\beta \in P_{F_I}$, we have $\beta \in \mathcal{C}_{F_I}$ if and only if $\mathrm{N}_{F_I/K}(\beta) \in \mu_K$.*

Proof It follows from [11, Theorem 1] that Oukhaba's group of elliptic units is of finite index in the full group of units, and so, from the discussion before Lemma 3.4, we obtain that $[\mathcal{C}_{F_I} : C_{F_I}] = h^{[F_I:K]-1}$ and $[\mathcal{C}_L : C_L] = h^{[L:K]-1}$. For a finite abelian extension F/K, an index formula for $[\mathcal{O}_F^\times : C_F]$ is given in [11, Theorem 1]. It is formed by the product of four quotients, which we write here, using Oukhaba's notation:

$$[\mathcal{O}_F^\times : C_F] = \frac{(12 w_K f_I h)^{[F:K]-1}}{w_F/w_K} \cdot \frac{h_F}{h} \cdot \frac{\prod_{\mathfrak{p}}[F \cap K_{\mathfrak{p}^\infty} : F \cap H]}{[F : F \cap H]} \cdot \frac{(R_F : U_F)}{d(F)}. \tag{3.5}$$

The two formulae in (i) follow from Lemma 3.2 and an explicit computation of the third and the fourth quotient in (3.5) when $F = F_I$ and $F = L$. Let us start by computing the third quotient. The product is taken over all prime ideals $\mathfrak{p}$ of K, and $K_{\mathfrak{p}^\infty}$ means the union of the ray class fields of K of modulus $\mathfrak{p}^n$ for all positive integers n. Since $[F_I:K]$ and $[L:K]$ are powers of p and $p \nmid h$, we have $F_I \cap H = L \cap H = K$. Moreover, by definition of F_I, we have $F_I \cap K_{\mathfrak{p}^\infty} = F_{\{j\}}$ if $\mathfrak{p} = \wp_j$ and $F_I \cap K_{\mathfrak{p}^\infty} = F_I \cap K_{\mathfrak{p}^\infty} \cap H = K$ if $\mathfrak{p} \notin \{\wp_1, \dots, \wp_s\}$. Combining the previous two observations with

Proposition 2.2, we obtain that the third quotient is equal to 1 when $F = F_I$. In the case where $F = L$, the definition of $\widetilde{L}$ readily implies that $\prod_{\mathfrak{p}}[L \cap K_{\mathfrak{p}^\infty} : K] = [\widetilde{L} : K]$, so that the third quotient is equal to $1/[L : \widetilde{L}]$. Let us now handle the fourth quotient in (3.5). It follows from [14, Theorem 5.4] and Proposition 2.2 that $(R_F : U_F) = 1$ if $F = F_I$. Similarly, it follows from [14, Theorem 5.3] that $(R_F : U_F) = 1$ if $F = L$. Finally, $d(F_I) = d(L) = 1$ by [11, Remark 2].

Let us prove (ii). Let $\beta \in P_{F_I}$. By [11, Corollary 2, p. 5] we know that $\eta_J \in \mathcal{O}_{F_J}^\times$ if $|J| > 1$, and by (3.4) we know that $\eta_{\{j\}} \in \mathcal{O}_{F_j}$ is a generator of a power of the only prime of F_j above $\wp_j$, which ramifies totally in F_j/K. Hence for any $\tau \in \mathrm{Gal}(F_j/K)$, $\eta_{\{j\}}^{1-\tau} \in \mathcal{O}_{F_j}^\times$. Therefore, there is $\gamma \in \mathcal{C}_{F_I}$ and $c_1, \ldots, c_s \in \mathbb{Z}$ such that $\beta = \gamma \cdot \prod_{j=1}^{s} \eta_{\{j\}}^{c_j}$. Since $\wp_1, \ldots, \wp_s$ are different prime ideals, the elliptic numbers $\eta_{\{1\}}, \ldots, \eta_{\{s\}}$ are multiplicatively independent. Hence, $\beta \in \mathcal{C}_{F_I}$ if and only if $c_1 = \cdots = c_s = 0$. Using (3.4) we see that

$$\mathrm{N}_{F_I/K}(\beta) = \xi \cdot \prod_{j=1}^{s} \pi_j^{12 f_I [F_I : F_j] c_j}$$

for some $\xi \in \mu_K$ and the lemma follows due to the fact that $\pi_1, \ldots, \pi_s$ are multiplicatively independent. ■

Recall that $G = \mathrm{Gal}(F_I/K)$. In [7], a $\mathbb{Z}[G]$-module U was introduced that depended solely on the following set of parameters: $T_1, \ldots, T_\nu$ and $\lambda_1, \ldots, \lambda_\nu$. (Warning: here the module U has a different meaning than in the proof of Lemma 3.4, where we used the notation of [11, 14].) In our situation we put $\nu = s$, and we set $T_j = \mathrm{Gal}(F_I/F_{I-\{j\}})$ and $\lambda_j \in G$ to be the automorphism defined in the beginning of Section 3 for each $j = 1, \ldots, s$. For our purpose, it is enough to recall that U was defined explicitly as a certain $\mathbb{Z}[G]$-submodule of $\mathbb{Q}[G] \oplus \mathbb{Z}^s$, with the following set of $\mathbb{Z}[G]$-generators $U = \langle \rho_J; J \subseteq I \rangle_{\mathbb{Z}[G]}$. Here each $\mathbb{Z}$ summand in $\mathbb{Q}[G] \oplus \mathbb{Z}^s$ is endowed with the trivial G-action and each element of the standard basis of $\mathbb{Z}^s$ is denoted by e_j (for $j \in I$). Note that by construction U is a finitely generated $\mathbb{Z}$-module with no $\mathbb{Z}$-torsion, which implies that U is a free $\mathbb{Z}$-module of finite rank.

The next lemma describes the $\mathbb{Z}[G]$-module structure of P_{F_I} in terms of the $\mathbb{Z}[G]$-module U. For any subset $A \subseteq G$, we let $s(A) = \sum_{a \in A} a \in \mathbb{Z}[G]$.

Lemma 3.5 *The $\mathbb{Z}[G]$-modules P_{F_I}/μ_K and $U/(s(G)\mathbb{Z})$ are isomorphic. More precisely, if we set $\Psi(\eta_J) = \rho_{I-J}$ for each $J \subseteq I$, $J \neq \varnothing$, and $\Psi(\mu_K) = 0$, then it defines a $\mathbb{Z}[G]$-module homomorphism $\Psi \colon P_{F_I} \to U$, which satisfies $\ker \Psi = \mu_K$ and $U = \Psi(P_{F_I}) \oplus (s(G)\mathbb{Z})$.*

Proof It follows from the $\mathbb{Z}[G]$-module presentation of U given in [7, Corollary 1.6(ii)] and the observation that the generator $\rho_I = s(G)$ does not appear in the relation [7, (1.10)] that $U = \langle \rho_J; J \subsetneq I \rangle_{\mathbb{Z}[G]} \oplus (s(G)\mathbb{Z})$. Hence, there exists an embedding of $\mathbb{Z}[G]$-modules $\iota \colon U/(s(G)\mathbb{Z}) \to U$ such that $\operatorname{im} \iota = \langle \rho_J; J \subsetneq I \rangle_{\mathbb{Z}[G]}$. In order to define the map $\Psi \colon P_{F_I} \to U$, it is preferable to start by defining its "inverse". We define a map $\Phi \colon U \to P_{F_I}$ by setting

$$\Phi(\rho_J) = \eta_{I-J} \text{ for each } J \subsetneq I \text{ and } \Phi(\rho_I) = 1.$$

We claim that Φ is a well-defined $\mathbb{Z}[G]$-module homomorphism whose image together with μ_K generates P_{F_I}. Indeed, this follows directly from the $\mathbb{Z}[G]$-module presentation of U given in [7] and the norm relation (3.3). Since $s(G) \in \ker \Psi$ and $\langle \Phi(U), \mu_K \rangle = P_{F_I}$, it follows that Φ induces a surjective $\mathbb{Z}[G]$-module homomorphism $\widetilde{\Phi}\colon U/(s(G)\mathbb{Z}) \to P_{F_I}/\mu_K$. Note that U (so a fortiori $U/(s(G)\mathbb{Z})$, which is embedded in U via ι) and P_{F_I}/μ_K have no $\mathbb{Z}$-torsion. Therefore, in order to show that $\widetilde{\Phi}$ is a $\mathbb{Z}[G]$-module isomorphism, it is enough to prove that

$$\operatorname{rank}_{\mathbb{Z}}(U/(s(G)\mathbb{Z})) = \operatorname{rank}_{\mathbb{Z}}(P_{F_I}/\mu_K). \tag{3.6}$$

Let us prove (3.6). Since the prime ideals $\wp_1, \dots, \wp_s$ are distinct, the numbers $\pi_1, \dots, \pi_s$ are multiplicatively independent over $\mathbb{Z}$, and Lemma 3.4 implies that

$$\operatorname{rank}_{\mathbb{Z}}(P_{F_I}) = s + \operatorname{rank}_{\mathbb{Z}}(\mathcal{C}_{F_I}) = s + \operatorname{rank}_{\mathbb{Z}}(\mathcal{O}_{F_I}^{\times}) = s + \tfrac{1}{2}[F_I:\mathbb{Q}] - 1. \tag{3.7}$$

Moreover, it follows from [7, Remark 1.4] that $\operatorname{rank}_{\mathbb{Z}}(U) = |G| + s$, which, when combined with (3.7), proves (3.6). Finally, we define the map Ψ as the composition of the three maps

$$P_{F_I} \longrightarrow P_{F_I}/\mu_K \xrightarrow{\widetilde{\Phi}^{-1}} U/s(G)\mathbb{Z} \xrightarrow{\iota} U,$$

where the first map is the natural projection. This proves the existence of Ψ with the desired properties. ■

4 A Nontrivial Root of an Elliptic Unit

We call the element

$$\eta = \mathrm{N}_{F_I/L}(\eta_I) \tag{4.1}$$

the *top generator* of both the group of elliptic numbers P_L of L and of the group of elliptic units $\mathcal{C}_L$ of L. The aim of this section is to take a nontrivial root "$\sqrt[y]{\eta}$" of η (where the root exponent y is a group ring element in $\mathbb{Z}[\Gamma]$) such that $\sqrt[y]{\eta} \in L$. We define $B = \mathrm{Gal}(F_I/L) \subseteq \mathrm{Gal}(F_I/K) = G$, so that $\Gamma = \langle \sigma \rangle \cong G/B$.

Lemma 4.1 *An elliptic number $\beta \in P_{F_I}$ belongs to L if and only if $\Psi(\beta)$ is fixed by B,* i.e., *$\Psi(P_{F_I})^B = \Psi(P_{F_I} \cap L)$, where Ψ is the $\mathbb{Z}[G]$-module homomorphism introduced in Lemma 3.5.*

Proof Let $\beta \in P_{F_I}$. On one hand, if $\beta \in L$, then $\beta^{\tau-1} = 1$ for all $\tau \in B$, and so $(\tau - 1)\Psi(\beta) = 0$, which means $\Psi(\beta) \in \Psi(P_{F_I})^B$. On the other hand, if $\Psi(\beta) \in \Psi(P_{F_I})^B$, then, for any $\tau \in B$, we have $(\tau-1)\Psi(\beta) = 0$ and so $\beta^{\tau-1} = \xi \in \ker(\Psi) = \mu_K$. Note that $\tau^{p^k} = 1$ and $\xi^\tau = \xi$. Therefore, applying $1 + \tau + \cdots + \tau^{p^k-1}$ to the equality $\beta^{\tau-1} = \xi$ we find that $1 = \xi^{p^k}$. Finally, since $p \nmid |\mu_K|$, we must have $\xi = 1$, and therefore $\beta \in L$. ■

Recall from Section 1, that n_i was defined as the index of the decomposition group of the ideal $\mathfrak{P}_i \subseteq L$ in Γ. Without lost of generality, we can suppose that

$$n_1 \le n_2 \le \cdots \le n_s, \quad \text{and we set } n = n_s = \max\{n_i \,;\, i \in I\}. \tag{4.2}$$

Since $p|t_s$ we have $n|p^{k-1}$ and it follows from Corollary 2.3(iii) that we can suppose that $t_1 = p^k$ and so $n_1 = 1$. Let L' be the unique subfield of L containing K such that $[L':K] = n$. Note that $\langle\sigma^n\rangle = \mathrm{Gal}(L/L')$ and that $\wp_s$ splits completely in L'/K.

We can now state the main result of this section.

Theorem 4.2 *There is a unique $\alpha \in L$ such that $\mathrm{N}_{L/L'}(\alpha) = 1$ and such that the elliptic unit η defined by (4.1) satisfies $\eta = \alpha^y$, where $y = \prod_{i=2}^{s-1}(1-\sigma^{n_i})$ (if $s = 2$, the empty product is taken to mean 1). This α is an elliptic unit of F_I, so that $\alpha \in \mathcal{C}_{F_I} \cap L$. Moreover, there is $\gamma \in L^\times$ such that $\alpha = \gamma^{1-\sigma^n}$.*

Remark 4.3 Colloquially, we can say that Theorem 4.2 proves the existence of a y-th root of the top generator η of $\mathcal{C}_L$ which lies in $\mathcal{C}_{F_I} \cap L$, where the root exponent y is an element of the group ring $\mathbb{Z}[\Gamma]$. In general, even though y is not an integer, it is still possible to compute α explicitly as a p-power root of a specific elliptic unit constructed from the conjugates of η. Indeed, for each $j = 1,\dots,s$, define the group ring elements

$$N_{n_j} = \sum_{i=1}^{p^k/n_j} \sigma^{in_j} \qquad \text{and} \qquad \Delta_{n_j} = \sum_{i=1}^{(p^k/n_j)-1} i\sigma^{in_j}.$$

In particular, we have $(1-\sigma^{n_j})N_{n_j} = 0$ and $(1-\sigma^{n_j})\Delta_{n_j} = N_{n_j} - \frac{p^k}{n_j}$.

Note also that the relative norm operator $\mathrm{N}_{L/L'}$ corresponds to the group ring element N_n. From Theorem 4.2, we know that $\eta = \alpha^y$. Moreover, for all $j \in \{1,\dots,s\}$, we also have $\alpha^{N_{n_j}} = 1$, since $1 = \mathrm{N}_{L/L'}(\alpha) = \alpha^{N_n}$. Consequently, we find that

$$\eta^{\prod_{i=2}^{s-1}\Delta_{n_i}} = \alpha^{\prod_{i=2}^{s-1}(N_{n_i}-(p^k/n_i))} = \alpha^{(-1)^s\prod_{i=2}^{s-1}(p^k/n_i)} = \alpha^{(-1)^s r}, \tag{4.3}$$

where $r = \prod_{i=2}^{s-1}\frac{p^k}{n_i}$ is a power of p, and therefore

$$\alpha^r = \eta^{(-1)^s\prod_{i=2}^{s-1}\Delta_{n_i}}. \tag{4.4}$$

To prove Theorem 4.2, we use the following proposition.

Proposition 4.4 *Let f be a polynomial in $\mathbb{Z}[X]$, $f \notin \{0,\pm1\}$, and let $A = \mathbb{Z}[X]/f\mathbb{Z}[X]$. Let $\mathcal{M}$ be a finitely generated A-module without $\mathbb{Z}$-torsion. Then the following hold.*

(i) $\mathrm{Ext}^1_A(\mathcal{M}, A) = 0$.
(ii) *Let y be a nonzerodivisor in A, and let $x \in \mathcal{M}$. Then $x \in y\mathcal{M}$ if and only if for all $\varphi \in \mathrm{Hom}_A(\mathcal{M}, A)$ we have $\varphi(x) \in yA$.*

Proof This is [8, Proposition 6.2]. ∎

Proof of Theorem 4.2 If $s = 2$, then $y = 1$, and therefore the equality $\eta = \alpha^y$ trivially holds true with $\alpha = \eta$. If $s > 2$, we always have that y is a *zerodivisor* in $\mathbb{Z}[\Gamma]$, so that one cannot apply directly Proposition 4.4; hence we shall work in an appropriate quotient of $\mathbb{Z}[\Gamma]$ where the image of y is a nonzerodivisor. Let $N_n = \sum_{i=1}^{p^k/n}\sigma^{in}$, so that N_n can be understood as the norm operator from L to L'. Let $R = \mathbb{Z}[\Gamma]/N_n\mathbb{Z}[\Gamma]$ and let $\gamma\colon R \to (1-\sigma^n)\mathbb{Z}[\Gamma]$ be the isomorphism of $\mathbb{Z}[\Gamma]$-modules given by the multiplication by $1-\sigma^n$, *i.e.*, $\gamma(x + N_n\mathbb{Z}[\Gamma]) = (1-\sigma^n)x$. Let

$$\mathcal{M} = \left\{ x \in \Psi(P_{F_I})^B;\ N_n x = 0 \right\},$$

where Ψ is the map that appears in Lemma 3.5. It is an R-module, and since $\mathcal{M} \subseteq U$, it has no $\mathbb{Z}$-torsion. Using both (4.1) and the norm relation (3.3), we obtain

$$\Psi(\eta) = \Psi(\mathrm{N}_{F_I/L}(\eta_I)) = s(B)\Psi(\eta_I) = s(B)\rho_\varnothing, \tag{4.5}$$

where $s(B) = \sum_{\tau\in B} \tau \in \mathbb{Z}[G]$ and

$$\mathrm{N}_{L/L'}(\eta) = \mathrm{N}_{F_I/L'}(\eta_I) = \mathrm{N}_{F_{\{1,\dots,s-1\}}/L'}(\eta_{\{1,\dots,s-1\}})^{1-\lambda_s^{-1}} = 1, \tag{4.6}$$

where the last equality follows from the fact that the restriction of λ_s to L' is trivial since $\wp_s$ splits completely in L'/K. In particular, it follows from (4.5) and (4.6) that $\Psi(\eta) = s(B)\rho_\varnothing \in \mathcal{M}$.

Note that the natural $\mathbb{Z}[\Gamma]$-module structure on $\mathcal{M}$ is compatible with its R-module structure via the natural projection map $\mathbb{Z}[\Gamma] \to R$. In particular, since (from Lemma 3.5) $U^B = \Psi(P_{F_I})^B \oplus (s(G)\mathbb{Z})$, we can view $\mathcal{M}$ as a $\mathbb{Z}[\Gamma]$-submodule of U^B. We claim that $U^B/\mathcal{M}$ has no $\mathbb{Z}$-torsion. Indeed, suppose that $x \in U^B$ satisfies $cx \in \mathcal{M}$ for a positive integer c. Then $c(N_n x) = N_n(cx) = 0$. Since U has no $\mathbb{Z}$-torsion, this implies that $N_n x = 0$, and hence $x \in \mathcal{M}$.

With each R-linear map $\psi \in \mathrm{Hom}_R(\mathcal{M}, R)$ we can associate the $\mathbb{Z}[\Gamma]$-linear map $\gamma\circ\psi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(\mathcal{M}, \mathbb{Z}[\Gamma])$. Now we fix such a ψ. We aim at proving that $\psi(s(B)\rho_\varnothing) \in yR$ (see relation (4.9)). Note that it makes sense to apply ψ to $s(B)\rho_\varnothing$, since it was proved earlier that $s(B)\rho_\varnothing \in \mathcal{M}$.

Now, set $f = X^{p^k} - 1$ in Proposition 4.4, so that $A = \mathbb{Z}[X]/f\mathbb{Z}[X] \cong \mathbb{Z}[\Gamma]$. Since $U^B/\mathcal{M}$ has no $\mathbb{Z}$-torsion, it follows from Proposition 4.4(i) that $\mathrm{Ext}^1_{\mathbb{Z}[\Gamma]}(U^B/\mathcal{M}, \mathbb{Z}[\Gamma]) = 0$. In particular, the vanishing of this Ext^1 implies the existence of $\varphi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U^B, \mathbb{Z}[\Gamma])$ such that $\varphi|_{\mathcal{M}} = \gamma\circ\psi$. For each $x \in U^B$, we define $v(x) = (1-\sigma)\varphi(x)$, so that $v \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U^B, \mathbb{Z}[\Gamma])$. We now want to specialize the formula that appears in [7, Corollary 1.7(ii)] to the present situation in order to obtain the non-trivial relation

$$v(s(B)\rho_\varnothing) \in \prod_{i=1}^{s} (1-\sigma^{n_i})\mathbb{Z}[\Gamma]. \tag{4.7}$$

Relation (4.7) is a direct consequence of the formula in [7, Corollary 1.7(ii)] and the following two observations:

(i) For all $i \in I$, $v(t_i e_i) = 0$, where $t_i = |T_i|$ with $T_i = \mathrm{Gal}(F_I/F_{I-\{i\}})$. (Note that it makes sense to apply the map v to $t_i e_i$, since $t_i e_i \in U^B$.)

(ii) It follows from Lemma 3.1 that the element $1 - \lambda_i|_L$ lies in the principal ideal $(1-\sigma^{n_i})\mathbb{Z}[\Gamma]$. Similarly, for each $\tau \in T_i$ we have that $\tau|_L \in \langle \sigma^{p^k/t_i} \rangle$ by Corollary 2.3(i), and therefore $1 - \tau|_L \in (1-\sigma^{n_i})\mathbb{Z}[\Gamma]$.

Since the multiplication by $1-\sigma$ is injective on $(1-\sigma^n)\mathbb{Z}[\Gamma]$, it follows from (4.7) that

$$\gamma\circ\psi(s(B)\rho_\varnothing) = \varphi(s(B)\rho_\varnothing) \in \prod_{i=2}^{s} (1-\sigma^{n_i})\mathbb{Z}[\Gamma]. \tag{4.8}$$

Furthermore, it follows from (4.8) and the fact that γ is an R-module isomorphism that

$$\psi(s(B)\rho_{\varnothing}) \in \prod_{i=2}^{s-1}(1-\sigma^{n_i})R = yR, \tag{4.9}$$

where $y = \prod_{i=2}^{s-1}(1-\sigma^{n_i})$. We have thus proved that for each $\psi \in \mathrm{Hom}_R(\mathcal{M}, R)$ the relation (4.9) holds true.

Now set $f = \sum_{i=1}^{p^k/n} X^{(i-1)n}$. Since $n|p^{k-1}$, it follows that $f \notin \{0,1,-1\}$; we can thus apply Proposition 4.4 with f so that $A = \mathbb{Z}[X]/f\mathbb{Z}[X] \cong R$. Combining (4.9) with the observation that y is a nonzerodivisor in R (since the roots of $X^n - 1$ are distinct from the roots of f), it follows from Proposition 4.4(ii) that there exists an element $\delta \in \mathcal{M}$ such that $y\delta = s(B)\rho_{\varnothing} = \Psi(\eta)$. In particular, since $\delta \in \mathcal{M}$, we have $\delta \in \Psi(P_{F_I})^B$ and $N_n\delta = 0$.

By Lemma 4.1, there exists $\alpha' \in P_{F_I} \cap L$ (uniquely defined modulo μ_K) such that $\delta = \Psi(\alpha')$. We have $\Psi(\mathrm{N}_{L/L'}(\alpha')) = N_n\Psi(\alpha') = N_n\delta = 0$, and so $\mathrm{N}_{L/L'}(\alpha') = \xi \in \mu_K$ by Lemma 3.5. Since $p \nmid |\mu_K|$, there is $\xi' \in \mu_K$ such that $\mathrm{N}_{L/L'}(\xi') = \xi^{-1}$. Now if we set $\alpha = \alpha'\xi' \in P_{F_I} \cap L$ we obtain $\mathrm{N}_{L/L'}(\alpha) = 1$, while still keeping the condition $\delta = \Psi(\alpha)$. Hence, $\Psi(\alpha^y) = y\delta = \Psi(\eta)$ and $\xi'' = \alpha^{-y}\eta \in \ker(\Psi) = \mu_K$. We claim that $\xi'' = 1$ so that $\alpha^y = \eta$. Indeed, it follows from (4.6) that $1 = \mathrm{N}_{L/L'}(\alpha^{-y}\eta) = (\xi'')^{p^k/n}$ and consequently $\xi'' = 1$ (since $p \nmid |\mu_K|$). Moreover, since $\mathrm{N}_{L/K}(\alpha) = 1$, it follows from Lemma 3.4(ii) that α is an elliptic unit of F_I. Notice that α is uniquely determined by the three conditions (i) $\alpha \in L$, (ii) $\mathrm{N}_{L/L'}(\alpha) = 1$, and (iii) $\alpha^y = \eta$. Indeed, if there were two such α's, their quotient $\beta \in L$ would satisfy $\beta^y = 1$. Similarly to what we did in (4.3), we can apply the group ring element $\prod_{j=2}^{s-1}\Delta_{n_j}$ to the equality $\beta^y = 1$ to find that $1 = \beta^r$ (this uses (ii)) where r is some power of p. Since $p \nmid |\mu_L|$, this implies that $\beta = 1$.

Finally, applying Hilbert's Theorem 90 to the cyclic extension L/L' implies that there exists a $\gamma \in L^\times$, well defined up to a multiplication by numbers in $(L')^\times$, such that $\alpha = \gamma^{1-\sigma^n}$. This concludes the proof. ∎

5 Enlarging the Group $\mathcal{C}_L$ of Elliptic Units of L

We keep the same notation as in the previous sections, and we introduce some new one. Let us label each subfield of L containing K as follows:

$$K = L_0 \subsetneq L_1 \subsetneq L_2 \subsetneq \cdots \subsetneq L_k = L. \tag{5.1}$$

In particular, we must have $[L_i : K] = p^i$. For each $i = 1, \dots, k$ we define

$$M_i = \left\{ j \in \{1, \dots, s\} \,;\, t_j > p^{k-i} \right\}. \tag{5.2}$$

It follows from the definition of M_i that $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k = \{1, \dots, s\}$, and from the discussion below (4.2) that $1 \in M_1$. One can also check using Corollary 2.3(i) that $j \in M_i$ if and only if $\wp_j$ ramifies in L_i/K; in particular, the conductor of L_i/K is equal to $\mathfrak{m}_{M_i}$ and so $L_i \subseteq F_{M_i}$ by Proposition 2.2 applied to L_i/K instead of L/K. We define

$$\eta_i = \mathrm{N}_{F_{M_i}/L_i}(\eta_{M_i}) \quad \text{for } i \in \{1, \dots, k\}, \tag{5.3}$$

so that, for example, $\eta_k = \eta \in L = L_k$ is the top generator of $\mathcal{C}_L$, the group of elliptic units of L. Using the norm relation (3.3) one can check that $\mathcal{C}_L$ is the $\mathbb{Z}[\Gamma]$-module generated by μ_K and by $\eta_1, \ldots, \eta_k$.

Before defining the extended group of elliptic units (see Definition 5.1 below), we need to fix some more notation. We fix an index $j \in \{1, \ldots, s\}$, and we let L_i be the largest subfield of L that appears in the tower (5.1) where $\wp_j$ is unramified; the index i is determined by the condition $t_j = p^{k-i}$. Using Lemma 3.1, it makes sense to define c_j as the smallest positive integer such that $\sigma^{-c_j n_j}|_{L_i} = \lambda_j|_{L_i}$. Indeed, it follows from the group equality $\langle \sigma^{n_j} \rangle = \langle \lambda_j|_L, \sigma^{p^k/t_j} \rangle$ in Lemma 3.1 that

$$\langle \sigma^{n_j} \rangle / \langle \sigma^{p^k/t_j} \rangle = \langle \lambda_j, \sigma^{p^k/t_j} \rangle / \langle \sigma^{p^k/t_j} \rangle. \tag{5.4}$$

Note that the quotient group in (5.4) can also be interpreted as the restriction of $\langle \sigma^{n_j} \rangle$ to L_i. It follows from (5.4) that $\wp_j$ splits completely in L_i/K if and only if $\frac{p^k}{t_j} = n_j$; in particular, if $\wp_j$ splits completely in L_i/K, then $c_j = 1$, since σ^{n_j} lies already in the inertia group of $\mathfrak{P}_j$. If $\wp_j$ does not split completely in L_i/K, then it follows again from (5.4) that $n_j < p^k/t_j$ and thus $\langle (\sigma|_{L_i})^{n_j} \rangle = \langle (\lambda_j|_{L_i}) \rangle$. In particular, independently of the splitting behavior of $\wp_j$ in L_i, we always have that $p \nmid c_j$ and hence $1 - \sigma^{c_j n_j}$ and $1 - \sigma^{n_j}$ are associated in $\mathbb{Z}[\Gamma]$, *i.e.*, each of them divides the other.

Recall that we had chosen an ordering of the ramified primes $\wp_1, \ldots, \wp_s$ in the relative extension L/K in such a way that $1 = n_1 \le n_2 \le \cdots \le n_s$, and that this ordering was implicitly assumed in the statement of Theorem 4.2. For each index $i \in \{1, \ldots, k\}$ such that $|M_i| > 1$, Theorem 4.2, when applied to the extension L_i/K, implies the existence of an elliptic unit $\alpha_i \in \mathcal{C}_{F_I} \cap L_i$ and of a number $\gamma_i \in L_i^\times$ such that:

(i) the elliptic unit η_i defined in (5.3) satisfies $\eta_i = \alpha_i^{y_i}$,
(ii) $\alpha_i = \gamma_i^{z_i}$,

where $z_i = 1 - \sigma^{c_{\max M_i} n_{\max M_i}}$ and $y_i = \prod_{j \in M_i,\ 1<j<\max M_i} (1 - \sigma^{c_j n_j})$. In particular, if $|M_i| = 2$, we find that $y_i = 1$ and $\alpha_i = \eta_i$, since the product is empty. If $i \in \{1, \ldots, k\}$ is such that $|M_i| = 1$, then we set $\gamma_i = \eta_i$ and $\alpha_i = \eta_i^{1-\sigma}$.

Definition 5.1 We define the *extended group of elliptic units* $\overline{\mathcal{C}}_L$ to be the $\mathbb{Z}[\Gamma]$-submodule of $\mathcal{O}_L^\times$ generated by μ_K and by the units $\alpha_1, \ldots, \alpha_k$.

Repeating the arguments of [9] we can show the following theorem.

Theorem 5.2 *The group of elliptic units $\mathcal{C}_L$ of L is a subgroup of $\overline{\mathcal{C}}_L$ of index $[\overline{\mathcal{C}}_L : \mathcal{C}_L] = p^\nu$, where*

$$\nu = \sum_{j=1}^{k} \sum_{\substack{i \in M_j \\ 1<i<\max M_j}} n_i.$$

Moreover, if we let $\varphi_L = \left(\prod_{i=1}^{s} t_i^{n_i}\right) \cdot \prod_{j=1}^{k} p^{-n_{\max M_j}}$, which is a power of p, then

$$p^\nu = \varphi_L \cdot [L : \widetilde{L}]^{-1},$$

where $\widetilde{L}$ has the same meaning as in Lemma 3.4 and

$$[\mathcal{O}_L^\times : \overline{\mathcal{C}}_L] = (12w_K f_I)^{p^k-1} \cdot \frac{h_L}{h} \cdot \varphi_L^{-1}, \tag{5.5}$$

where h_L is the class number of L. In particular, if $p > 3$ then $p \nmid 12w_K f_I$, and thus it follows from (5.5) that $\varphi_L \mid h_L$.

Proof The proof goes along the same lines as in [9, Theorem 3.1]. The reason why the same algebraic manipulations are possible here (for elliptic units) and in [9] (for circular units) is given by the fact that in both cases we work with a module isomorphic to $U/(s(G)\mathbb{Z})$ (compare Lemma 3.5 with [9, Lemma 1.1]). ■

Remark 5.3 The divisibility statement $\varphi_L \mid h_L$ is stronger than what one can get from the mere fact that F_I/L is an unramified abelian extension, see Corollary 2.3(ii). Indeed, [9, Proposition 3.4] states that we always have $[F_I : L] \mid \varphi_L$ and that $\varphi_L = [F_I : L]$ if and only if $n_1 = \cdots = n_{s-1} = 1$.

6 Semispecial Numbers

We keep the same notation as in the previous sections. In particular, $\Gamma = \mathrm{Gal}(L/K) \cong \mathbb{Z}/p^k\mathbb{Z}$ and s is the exact number of prime ideals of K that ramify in L. For the rest of the paper, we fix m, a power of p, such that $p^{ks} \mid m$. For a prime ideal $\mathfrak{q}$ of K, recall that $K(\mathfrak{q})$ denotes the ray class field of K of modulus $\mathfrak{q}$. From Artin's Reciprocity Theorem we know that

$$\mathrm{Gal}\big(K(\mathfrak{q})/H\big) \cong (\mathcal{O}_K/\mathfrak{q})^\times / \mathrm{im}(\mu_K), \tag{6.1}$$

where H is the Hilbert class field of K. In particular, $\mathrm{Gal}(K(\mathfrak{q})/H)$ is a cyclic group. We are now ready to define a family of distinguished abelian extensions over K that have a cyclic Galois group of order m.

Definition 6.1 To each prime ideal $\mathfrak{q}$ of K such that $|\mathcal{O}_K/\mathfrak{q}| \equiv 1 \pmod{m}$ we define the field $K[\mathfrak{q}]$ to be the (unique) subfield of $K(\mathfrak{q})$ containing K such that $[K[\mathfrak{q}] : K] = m$. Moreover, given a finite field extension M/K we also define $M[\mathfrak{q}]$ to be the compositum of M with $K[\mathfrak{q}]$.

Note that since $|\mathcal{O}_K/\mathfrak{q}| \equiv 1 \pmod{m}$ and $p \nmid |\mu_K|$, the group $\mathrm{Gal}(K(\mathfrak{q})/H)$ is cyclic of order divisible by m. Therefore, since $p \nmid h$, the existence and the uniqueness of the field $K[\mathfrak{q}]$ follows directly from Lemma 2.1 applied to the triple $(\mathrm{Gal}(K(\mathfrak{q})/K), \mathrm{Gal}(K(\mathfrak{q})/H), m)$. It is clear that $\mathrm{Gal}(K[\mathfrak{q}]/K) \cong \mathbb{Z}/m\mathbb{Z}$ and one can also check that $K[\mathfrak{q}]/K$ is ramified only at $\mathfrak{q}$ and that this ramification is total and tame.

Definition 6.2 Let $\mathcal{Q}_m$ be the set of all prime ideals $\mathfrak{q}$ of K such that

(i) $\mathfrak{q}$ is of absolute degree 1, so that $q = |\mathcal{O}_K/\mathfrak{q}|$ is a prime number;
(ii) $q \equiv 1 + m \pmod{m^2}$;
(iii) $\mathfrak{q}$ splits completely in L;
(iv) for each $j = 1, \ldots, s$, the class of π_j is an m-th power in $(\mathcal{O}_K/\mathfrak{q})^\times$.

Let us make a few observations about the field $K[\mathfrak{q}]$ and also about the fourth condition of Definition 6.2. Note that Artin's Reciprocity Theorem gives slightly more information concerning the isomorphism (6.1): the class of $\alpha \in \mathcal{O}_K - \mathfrak{q}$ is mapped to the automorphism given by the Artin symbol $\left(\frac{K(\mathfrak{q})/K}{\alpha\mathcal{O}_K}\right)$. Since $H \cap K[\mathfrak{q}] = K$, we have $\mathrm{Gal}(H[\mathfrak{q}]/H) \cong \mathrm{Gal}(K[\mathfrak{q}]/K)$ where the isomorphism is given by restriction, and so factoring out the m-th powers in (6.1), we get the following sequence of isomorphisms:

$$(\mathcal{O}_K/\mathfrak{q})^\times/m \xrightarrow{\cong} \mathrm{Gal}(H[\mathfrak{q}]/H) \xrightarrow{\cong} \mathrm{Gal}(K[\mathfrak{q}]/K), \tag{6.2}$$

where the first map takes the class of $\alpha \in \mathcal{O}_K - \mathfrak{q}$ to $\left(\frac{H[\mathfrak{q}]/K}{\alpha\mathcal{O}_K}\right)$, and the second map takes $\left(\frac{H[\mathfrak{q}]/K}{\alpha\mathcal{O}_K}\right)$ to its restriction $\left(\frac{K[\mathfrak{q}]/K}{\alpha\mathcal{O}_K}\right)$. Hence combining the observations that $\pi_j\mathcal{O}_K = \wp_j^h$, $p \nmid h$, with the sequence of isomorphisms appearing in (6.2), we see that the fourth condition (iv) is equivalent to the statement that

$$\left(\frac{K[\mathfrak{q}]/K}{\wp_j}\right) = 1 \qquad \text{for each } j = 1, \dots, s. \tag{6.3}$$

Definition 6.3 A number $\varepsilon \in L^\times$ is called *m-semispecial* if for all but finitely many $\mathfrak{q} \in \mathcal{Q}_m$, there exists a unit $\varepsilon_\mathfrak{q} \in \mathcal{O}_{L[\mathfrak{q}]}^\times$ satisfying

- (i) $\mathrm{N}_{L[\mathfrak{q}]/L}(\varepsilon_\mathfrak{q}) = 1$;
- (ii) if $\widetilde{\mathfrak{q}}$ is the product of all primes of $L[\mathfrak{q}]$ above $\mathfrak{q}$, then ε and $\varepsilon_\mathfrak{q}$ have the same image in $(\mathcal{O}_{L[\mathfrak{q}]}/\widetilde{\mathfrak{q}})^\times/(m/p^{k(s-1)})$.

Let us make a few basic observations about the field $L[\mathfrak{q}]$ that appears in Definition 6.3. For each $\mathfrak{q} \in \mathcal{Q}_m$, we have that $\mathrm{Gal}(K[\mathfrak{q}]/K) \cong \mathbb{Z}/m\mathbb{Z}$, that $\mathfrak{q}$ is totally ramified in $K[\mathfrak{q}]/K$ and that it splits completely in L/K. In particular, we must have that $L[\mathfrak{q}]/L$ is totally ramified at each prime above $\mathfrak{q}$ and that $L \cap K[\mathfrak{q}] = K$. Since L and $K[\mathfrak{q}]$ are linearly disjoint over K, it follows that the two restriction maps $\mathrm{Gal}(L[\mathfrak{q}]/L) \to \mathrm{Gal}(K[\mathfrak{q}]/K)$ and $\mathrm{Gal}(L[\mathfrak{q}]/K[\mathfrak{q}]) \to \mathrm{Gal}(L/K)$ are isomorphisms.

Theorem 6.4 *The elliptic unit $\alpha \in \mathcal{C}_{F_I} \cap L$ described in Theorem 4.2 is m-semispecial.*

Proof Recall that the elliptic unit $\alpha \in \mathcal{C}_{F_I} \cap L$ was obtained in Theorem 4.2 as a y-th root of the top generator η of $\mathcal{C}_L$. In order to show that α is m-semispecial, we need to show that for almost all primes $\mathfrak{q} \in \mathcal{Q}_m$, there exists a unit $\varepsilon_\mathfrak{q} \in \mathcal{O}_{L[\mathfrak{q}]}^\times$ which satisfies conditions (i) and (ii) of Definition 6.3 for $\varepsilon = \alpha$. In order to show that such an $\varepsilon_\mathfrak{q}$ exists, we use an approach similar to the one used in the proof of Theorem 4.2. But this time, the role played by η in Theorem 4.2 will be played by $\widehat{\eta} = \mathrm{N}_{F_I[\mathfrak{q}]/L[\mathfrak{q}]}(\widetilde{\eta}_{I'})$ where $\widetilde{\eta}_{I'}$ (to be defined below) is the top generator of $P_{F_I[\mathfrak{q}]}$.

For the rest of the proof we fix a prime $\mathfrak{q} \in \mathcal{Q}_m$ unramified in $K/\mathbb{Q}$, which does not divide $q_1 \cdots q_s$. To simplify the notation, we let $\wp_{s+1} = \mathfrak{q}$, $F_{s+1} = K[\mathfrak{q}]$, and $I' = \{1, \dots, s+1\}$. Again, for any subset $J \subseteq I'$ with $J \neq \varnothing$, we set $F_J = \prod_{j\in J} F_j$, $\mathfrak{m}_J = \prod_{j \in J} \wp_j$ (the conductor of F_J), and

$$\widetilde{\eta}_J = \mathrm{N}_{K(\mathfrak{m}_J)/F_J}(\varphi_{\mathfrak{m}_J})^{w_K f_{I'}/(w_J f_J)}, \tag{6.4}$$

where f_J and w_J are defined as in (3.1) and $\varphi_{\mathfrak{m}_J}$ is defined as in [11, Definition 2, p. 5]. If $J \subseteq I$, this definition does not change the previous meaning of F_J while $\widetilde{\eta}_J = \eta_J^q$, where $q = |\mathcal{O}_K/\mathfrak{q}| = f_{I'}/f_I$. It follows also from the definitions that $F_I[\mathfrak{q}] = F_{I'}$ and $\mathfrak{m}_{I'} = \mathfrak{q}\mathfrak{m}_I$. By the same reasoning as in Lemma 3.2 we find that $\mu_{F_I[\mathfrak{q}]} = \mu_K$.

Let $G_\mathfrak{q} = \mathrm{Gal}(F_I[\mathfrak{q}]/K)$ and let $P_{F_I[\mathfrak{q}]}$ be the group of elliptic numbers of $F_I[\mathfrak{q}]$, *i.e.*, $P_{F_I[\mathfrak{q}]}$ is the $\mathbb{Z}[G_\mathfrak{q}]$-module generated in $F_I[\mathfrak{q}]^\times$ by μ_K and by $\widetilde{\eta}_J$ for all $J \subseteq I'$, $J \neq \varnothing$. Let $U_\mathfrak{q} \subseteq \mathbb{Q}[G_\mathfrak{q}] \oplus \mathbb{Z}^{s+1}$ be the $\mathbb{Z}[G_\mathfrak{q}]$-module defined in [7] with the following parameters: $v = s+1$, for each $j \in \{1,\dots,v\}$, $T_j = \mathrm{Gal}(F_{I'}/F_{I'-\{j\}})$ (the inertia group of $\wp_j$ in $G_\mathfrak{q}$), and $\lambda_j \in G_\mathfrak{q}$ is such that the restrictions

$$\lambda_j|_{F_j} = 1 \quad \text{and} \quad \lambda_j|_{F_{I'-\{j\}}} = \left(\frac{F_{I'-\{j\}}/K}{\wp_j}\right).$$

Now, in order to simplify the notation, we choose to make some natural identifications between certain objects: "the old ones" that have already appeared in the proof of Theorem 4.2 and "the new ones" that appear in this proof. Consider the sequence

$$\mathrm{Gal}\big(F_I[\mathfrak{q}]/K[\mathfrak{q}]\big) \subseteq G_\mathfrak{q} \longrightarrow G = \mathrm{Gal}(F_I/K), \tag{6.5}$$

where the arrow is given by the restriction map. We decide to identify $\mathrm{Gal}(F_I[\mathfrak{q}]/K[\mathfrak{q}])$ with G via the above diagram. In particular, the new groups T_i defined in the paragraph just above, for $i \neq s+1$, are identified to the old ones, and if we set $B = \mathrm{Gal}(F_I[\mathfrak{q}]/L[\mathfrak{q}])$, it is also identified with the old B. The assumption that $\mathfrak{q} \in \mathfrak{Q}_m$ also implies that the new elements λ_i, for $i \in I$, are identified to the old ones (by (6.3)) and that $\lambda_{s+1} \in B$ (since $\mathfrak{q}$ splits completely in L). However, the $\mathbb{Z}[G]$-generators of $U \subseteq \mathbb{Z}[G] \oplus \mathbb{Z}^s$ cannot be identified, in any meaningful way, to a subset of the $\mathbb{Z}[G_\mathfrak{q}]$-generators of $U_\mathfrak{q} \subseteq \mathbb{Z}[G_\mathfrak{q}] \oplus \mathbb{Z}^{s+1}$; so we need to distinguish between these two sets of generators. Recall, in the notation of [7], that $U = \langle \rho_J\ ;\ J \subseteq I\rangle_{\mathbb{Z}[G]}$, that the standard basis of $\mathbb{Z}^s$ is denoted by $e_1,\dots,e_s$, and that $\pi\colon \mathbb{Q}[G]\oplus\mathbb{Z}^s \to \mathbb{Q}[G]$ is the projection onto the first summand. We set $U' = \pi(U)$ so that U' is generated by $\rho'_J = \pi(\rho_J)$. We choose to denote the $\mathbb{Z}[G_\mathfrak{q}]$-generators of $U_\mathfrak{q}$ by $\widetilde{\rho}_J$ so that $U_\mathfrak{q} = \langle \widetilde{\rho}_J\ ;\ J \subseteq I'\rangle_{\mathbb{Z}[G_\mathfrak{q}]}$, and the standard basis of $\mathbb{Z}^{s+1}$ by $\widetilde{e}_1,\dots,\widetilde{e}_{s+1}$. The next lemma gives precise relationships between the modules U, U' and $U_\mathfrak{q}$; for its proof, see [9, Lemma 2.1]).

Lemma 6.5 *Recall that G is viewed as a subgroup of $G_\mathfrak{q}$ via (6.5). There are injective $\mathbb{Z}[G]$-homomorphisms $\chi\colon U \to U_\mathfrak{q}$ and $\chi'\colon U' \to U_\mathfrak{q}$ defined by*

$$\chi(\rho_J) = \widetilde{\rho}_{J\cup\{s+1\}} \qquad \textit{and} \qquad \chi'(\rho'_J) = \widetilde{\rho}_J,$$

for each $J \subseteq I$. Moreover, $U_\mathfrak{q} \cong U \oplus \mathbb{Z} \oplus (U')^{m-1}$ as $\mathbb{Z}[G]$-modules.

We can apply Lemma 3.5 to our present situation, which gives us a homomorphism $\Psi_\mathfrak{q}\colon P_{F_I[\mathfrak{q}]} \to U_\mathfrak{q}$ of $\mathbb{Z}[G_\mathfrak{q}]$-modules defined by $\Psi_\mathfrak{q}(\widetilde{\eta}_J) = \widetilde{\rho}_{I'-J}$ for each $J \subseteq I'$, $J \neq \varnothing$, and $\Psi_\mathfrak{q}(\mu_K) = 0$; where $\ker\Psi_\mathfrak{q} = \mu_K$ and $U_\mathfrak{q} = \Psi_\mathfrak{q}(P_{F_I[\mathfrak{q}]}) \oplus (s(G_\mathfrak{q})\mathbb{Z})$. Let us define

$$\widehat{\eta} = \mathrm{N}_{F_I[\mathfrak{q}]/L[\mathfrak{q}]}(\widetilde{\eta}_{I'}). \tag{6.6}$$

Then we have

$$\Psi_\mathfrak{q}(\widehat{\eta}) = s(B)\Psi_\mathfrak{q}(\widetilde{\eta}_{I'}) = s(B)\widetilde{\rho}_\varnothing, \tag{6.7}$$

and $\Psi_\mathfrak{q}(P_{F_I[\mathfrak{q}]} \cap L[\mathfrak{q}]) = \Psi_\mathfrak{q}(P_{F_I[\mathfrak{q}]})^B$, where the last equality can be proved along the same lines as Lemma 4.1. As in (4.2), we let $n = \max\{n_i\ ;\ i \in I\}$, and as in the proof of Theorem 4.2 we also let $N_n = \sum_{i=1}^{p^k/n} \sigma^{in}$, and $R = \mathbb{Z}[\Gamma]/N_n\mathbb{Z}[\Gamma]$, where now $\Gamma = \mathrm{Gal}(L[\mathfrak{q}]/K[\mathfrak{q}]) = \langle\sigma\rangle$ (here the new σ restricts to the old one). We also let $\gamma\colon R \to (1-\sigma^n)\mathbb{Z}[\Gamma]$ be the isomorphism of $\mathbb{Z}[\Gamma]$-modules induced by the multiplication by $1-\sigma^n$. Note that the group ring element $N_n \in \mathbb{Z}[\Gamma]$ corresponds to the norm operator of $L[\mathfrak{q}]/L'[\mathfrak{q}]$, where L' is the field defined just before Theorem 4.2.

One can also check that the set

$$\mathcal{M}_{\mathfrak{q}} = \left\{ x \in \Psi_{\mathfrak{q}}(P_{F_I[\mathfrak{q}]})^B \;;\; N_n x = 0 \right\}$$

is again an R-module (so also a $\mathbb{Z}[\Gamma]$-module) without $\mathbb{Z}$-torsion such that $U_{\mathfrak{q}}^B/\mathcal{M}_{\mathfrak{q}}$ has no $\mathbb{Z}$-torsion. In particular, we can apply Proposition 4.4 with the polynomial $f = X^{p^k} - 1$ to deduce that $\mathrm{Ext}^1_{\mathbb{Z}[\Gamma]}(U_{\mathfrak{q}}^B/\mathcal{M}_{\mathfrak{q}}, \mathbb{Z}[\Gamma]) = 0$. We also have the equalities

$$\widehat{\eta}^{N_n} = \mathrm{N}_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\widehat{\eta}) = \mathrm{N}_{F_I[\mathfrak{q}]/L'[\mathfrak{q}]}(\widetilde{\eta}_{I'}) = 1, \tag{6.8}$$

where $\widehat{\eta}$ is defined in (6.6) and $\widetilde{\eta}_{I'}$ in (6.4). Indeed, the first equality follows from the definition of N_n and the second one follows from (6.6). For the third equality, note that since $\wp_s$ splits completely in L' (by definition of L') and also in $K[\mathfrak{q}]$ (by (6.3)), then it must also split completely in $L'[\mathfrak{q}]$, and therefore, from the norm relation (3.3), the third equality follows. Combining (6.8) with (6.7), we obtain

$$s(B)\widetilde{\rho}_{\varnothing} \in \mathcal{M}_{\mathfrak{q}}. \tag{6.9}$$

To each R-linear functional $\psi \in \mathrm{Hom}_R(\mathcal{M}_{\mathfrak{q}}, R)$, we can associate the map $\gamma \circ \psi$ that can be viewed naturally as an element of $\mathrm{Hom}_{\mathbb{Z}[\Gamma]}(\mathcal{M}_{\mathfrak{q}}, \mathbb{Z}[\Gamma])$. Hence, because of the vanishing of the Ext^1, for any given $\psi \in \mathrm{Hom}_R(\mathcal{M}_{\mathfrak{q}}, R)$, there exists a $\varphi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_{\mathfrak{q}}^B, \mathbb{Z}[\Gamma])$ such that $\varphi|_{\mathcal{M}_{\mathfrak{q}}} = \gamma \circ \psi$.

The restriction of the projection $\pi\colon \mathbb{Q}[G] \oplus \mathbb{Z}^s \to \mathbb{Q}[G]$ to U gives a surjective map $\pi|_U\colon U \to U'$, which can be composed with the map χ' of Lemma 6.5, to give rise to the $\mathbb{Z}[G]$-linear map $\chi' \circ \pi|_U\colon U \to U_{\mathfrak{q}}$. Restricting further the previous map to U^B, we obtain the two maps $\chi' \circ \pi|_{U^B} \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U^B, U_{\mathfrak{q}}^B)$ and $\varphi \circ \chi' \circ \pi|_{U^B} \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U^B, \mathbb{Z}[\Gamma])$.

We have the relation

$$\begin{aligned} \varphi(s(B)\widetilde{\rho}_{\varnothing}) = \varphi \circ \chi' \circ \pi(s(B)\rho_{\varnothing}) &\in \prod_{i=1}^{s}(1-\sigma^{n_i})\mathbb{Z}[\Gamma] \\ &= (1-\sigma)y(1-\sigma^n)\mathbb{Z}[\Gamma], \end{aligned} \tag{6.10}$$

where $y = \prod_{i=2}^{s-1}(1-\sigma^{n_i})$ is defined as in the statement of Theorem 4.2. Indeed, the first equality follows from the facts that $\chi' \circ \pi(\rho_{\varnothing}) = \widetilde{\rho}_{\varnothing}$ and $\chi' \circ \pi$ is $\mathbb{Z}[G]$-linear. The membership relation follows from [7, Corollary 1.7(ii)] and the observation that $\pi(t_j e_j) = 0$ for all $j \in J$ in the same way as (4.7).

It follows from (6.9) that the evaluation $\psi(s(B)\widetilde{\rho}_{\varnothing})$ makes sense for any $\psi \in \mathrm{Hom}_R(\mathcal{M}_{\mathfrak{q}}, R)$; and it follows from (6.10) and the injectivity of γ that

$$\psi\big(s(B)\widetilde{\rho}_{\varnothing}\big) \in (1-\sigma)yR.$$

Since ψ was arbitrary, Proposition 4.4 implies that there exists $\delta \in \mathcal{M}_{\mathfrak{q}}$ such that

$$(1-\sigma)y \cdot \delta = s(B)\widetilde{\rho}_{\varnothing} = \Psi_{\mathfrak{q}}(\widehat{\eta}).$$

Since $\delta \in \mathcal{M}_{\mathfrak{q}}$, there exists a $\beta' \in P_{F_I[\mathfrak{q}]} \cap L[\mathfrak{q}]$ such that $\delta = \Psi_{\mathfrak{q}}(\beta')$ and $\Psi_{\mathfrak{q}}(\mathrm{N}_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta')) = 0$. In particular, we have that $\xi = \mathrm{N}_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta') \in \ker(\Psi_{\mathfrak{q}}) = \mu_K$. Since $\mathrm{N}_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\xi) = \xi^{p^k/n}$ and $p \nmid |\mu_K|$, there is $\xi' \in \mu_K$ such that $\mathrm{N}_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\xi') = \xi^{-1}$. We set $\beta = \beta'\xi'$, so that β satisfies the norm relation $\mathrm{N}_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta) = 1$ while still keeping the equality $\delta = \Psi_{\mathfrak{q}}(\beta)$. Since $\Psi_{\mathfrak{q}}(\beta^{(1-\sigma)y}) = (1-\sigma)y\delta = \Psi_{\mathfrak{q}}(\widehat{\eta})$, it follows that $\xi'' = \beta^{-(1-\sigma)y}\widehat{\eta} \in \ker(\Psi_{\mathfrak{q}}) = \mu_K$. We claim that $\xi'' = 1$. Indeed, from (6.8) we have $1 = \mathrm{N}_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\xi'') = (\xi'')^{p^k/n}$, and therefore $\xi'' = 1$. We thus have constructed an elliptic number $\beta \in P_{F_I[\mathfrak{q}]} \cap L[\mathfrak{q}]$ which satisfies the equality $\beta^{(1-\sigma)y} = \widehat{\eta}$.

Now, we would like to show that the elliptic number β constructed in the above paragraph is a unit that satisfies the additional condition $\mathrm{N}_{L[\mathfrak{q}]/L}(\beta) = 1$. By a similar computation as the one done in Remark 4.3, we find that

$$\beta^{r(1-\sigma)} = \widehat{\eta}^{(-1)^s \prod_{i=2}^{s-1} \Delta_{n_i}}, \quad \text{where} \quad r = \prod_{i=2}^{s-1} \frac{p^k}{n_i}. \tag{6.11}$$

In particular, applying Δ_1 on each side of the first equality in (6.11) and using the norm relation $\mathrm{N}_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta) = \beta^{N_n} = 1$, we find that

$$\beta^{rp^k} = \widehat{\eta}^{(-1)^{s+1} \prod_{i=1}^{s-1} \Delta_{n_i}}. \tag{6.12}$$

We have

$$\mathrm{N}_{L[\mathfrak{q}]/L}(\widehat{\eta}) = \mathrm{N}_{F_I[\mathfrak{q}]/L}(\widetilde{\eta}_{I'}) = \mathrm{N}_{F_I/L}(\widetilde{\eta}_I)^{1-\lambda_{s+1}^{-1}} = 1, \tag{6.13}$$

where the first equality follows from the definitions of $\widehat{\eta}$ and $\widetilde{\eta}_{I'}$, the second equality from the norm relations (3.3), and the last equality from the fact that $\mathfrak{q}$ splits completely in L/K. Combining (6.12) and (6.13) with the fact that $p \nmid |\mu_K|$, we deduce that $\mathrm{N}_{L[\mathfrak{q}]/L}(\beta) = 1$. From the previous equality we get that $\mathrm{N}_{F_I[\mathfrak{q}]/K}(\beta) = 1$, and therefore, applying Lemma 3.4(ii) we deduce that β is a unit.

In order to finish the proof that α is m-semispecial, we need to construct a unit $\varepsilon_{\mathfrak{q}} \in L[\mathfrak{q}]$ that satisfies conditions (i) and (ii) of Definition 6.3 for $\varepsilon = \alpha$. We set $\varepsilon_{\mathfrak{q}} = \beta^{1-\sigma}$. So far, from what has been proved on β, we know that $\varepsilon_{\mathfrak{q}}$ is a unit that satisfies the norm relation (i). By means of the next proposition (see Proposition 6.6) we will prove that $\varepsilon_{\mathfrak{q}}$ and α also satisfy the congruence relation (ii).

Let us recall some of the notation that was fixed at the beginning of Section 6. The integer m is a fixed power of p, such that $p^{ks}|m$, $\mathfrak{q}$ is a prime ideal of K that lies in the special set $\mathcal{Q}_m$. In particular, it follows from the definition of $\mathcal{Q}_m$ that $\mathfrak{q}$ splits completely in L/K, that the extension $L[\mathfrak{q}]/L$ is cyclic of degree m, and that it is totally ramified at each prime above $\mathfrak{q}$.

Proposition 6.6 *Let $\mathfrak{q} \in \mathcal{Q}_m$ be the prime that was fixed during the course of the proof of Theorem 6.4, and let $\widetilde{\mathfrak{q}}$ denote the product of all the primes of $L[\mathfrak{q}]$ above $\mathfrak{q}$. Then there exists a rational prime $\ell \equiv 1 \pmod m$ such that the following congruence holds:*

$$\widehat{\eta}^{\ell(1-\sigma)} \equiv \left(\eta^{\ell(1-\sigma)}\right)^{\frac{q-1}{m}} \pmod{\widetilde{\mathfrak{q}}}, \tag{6.14}$$

where $q = |\mathcal{O}_K/\mathfrak{q}|$, η is the top generator of the group $\mathcal{C}_L$ and $\widehat{\eta}$ is defined in (6.6).

The proof of Proposition 6.6 is given further below. Assuming Proposition 6.6, we can now finish the proof of Theorem 6.4 by proving the congruence relation (ii) in Definition 6.3. Using (6.11), (6.14), and (4.4) successively we find that

$$\begin{aligned}\beta^{r(1-\sigma)^2\ell} &= \widehat{\eta}^{(-1)^s\ell(1-\sigma)\prod_{i=2}^{s-1}\Delta_{n_i}} \equiv \eta^{(-1)^s\frac{q-1}{m}\ell(1-\sigma)\prod_{i=2}^{s-1}\Delta_{n_i}}\\ &= \alpha^{r\frac{q-1}{m}\ell(1-\sigma)} \pmod{\widetilde{\mathfrak{q}}},\end{aligned}$$

where r is the power of p defined in (6.11). Applying Δ_1 to each side of the previous equality and using the facts that $\alpha^{N_1} = 1$ (since $1 \le n$ and $\alpha^{N_n} = 1$), that $(1-\sigma)\Delta_1 = N_1 - p^k$, and that $(\sigma - 1)N_1 = 0$, we obtain

$$\beta^{p^k r(1-\sigma)\ell} \equiv \alpha^{p^k r\frac{q-1}{m}\ell} \pmod{\widetilde{\mathfrak{q}}}. \tag{6.15}$$

Because $\frac{q-1}{m} \equiv 1 \equiv \ell \pmod{m}$, it follows from (6.15) that $\beta^{p^k r(1-\sigma)}$ and $\alpha^{p^k r}$ have the same image in $(\mathcal{O}_{L[\mathfrak{q}]}/\widetilde{\mathfrak{q}})^\times/m$. Moreover, since $r \mid p^{k(s-2)}$ it also follows that $\beta^{1-\sigma}$ and α must have the same image in $(\mathcal{O}_{L[\mathfrak{q}]}/\widetilde{\mathfrak{q}})^\times/(m/p^{k(s-1)})$. We thus have shown that both $\varepsilon = \alpha$ and $\varepsilon_\mathfrak{q} = \beta^{1-\sigma}$ satisfy the congruence relation (ii). This completes the proof of Theorem 6.4. ■

Proof of Proposition 6.6 The proof will follow essentially from an idea of Rubin; see [13, Theorem 2.1]. Let $\pi \in \mathcal{O}_K$ be such that $\pi\mathcal{O}_K = \mathfrak{q}^h$. Let $K_m = K(\zeta_m)$ where ζ_m denotes a primitive m-th root of unity. Since $\mathcal{O}_K^\times = \mu_K$, $p \nmid |\mu_K|$ and K_m contains a primitive p-th root of unity, the field $M = K_m(\pi^{1/p})$ does not depend on the chosen generator π of $\mathfrak{q}^h$ and on the chosen p-th root of π. One can also check that M/K is a Galois extension. Furthermore, we claim that π cannot be a p-th power in K_m. Indeed, if it were the case then, since $p \nmid h$, this would imply that the ramification index of $\mathfrak{q}$ in K_m/K would be divisible by p; but this is impossible since K_m/K ramifies only at primes above p. Since π is not a p-th power in K_m, it follows that M/K_m is a cyclic extension of degree p.

In order to finish the proof of Proposition 6.6, we need the following technical lemma.

Lemma 6.7 *Let $\mathfrak{q}$ be as in Proposition 6.6 and recall that σ is the unique generator of* $\mathrm{Gal}(L[\mathfrak{q}]/K[\mathfrak{q}])$, *which restricts to the initial generator of* $\mathrm{Gal}(L/K)$ *(which was also denoted by σ). Then there exists a prime $\mathfrak{l}$ of K of absolute degree 1 satisfying the following three conditions:*

(i) *If we let $\ell = |\mathcal{O}_K/\mathfrak{l}|$, then $\ell \equiv 1 \pmod{m}$ and ℓ is unramified in $K/\mathbb{Q}$.*
(ii) *The prime $\mathfrak{l}$ is unramified in $L[\mathfrak{q}]$ and the Artin symbol $\left(\frac{L[\mathfrak{q}]/K}{\mathfrak{l}}\right) = \sigma^{-1}$.*
(iii) *The prime $\mathfrak{q}$ is inert in $K[\mathfrak{l}]/K$ (note that this is equivalent to say that $\mathfrak{q}$ is unramified in $K[\mathfrak{l}]$ and that $\left\langle \left(\frac{K[\mathfrak{l}]/K}{\mathfrak{q}}\right)\right\rangle = \mathrm{Gal}(K[\mathfrak{l}]/K)$).*

Recall here that the fields $K[\mathfrak{q}]$, $K[\mathfrak{l}]$, and $L[\mathfrak{q}]$ were introduced in Definition 6.1. Note that since $\mathfrak{q} \in \mathcal{Q}_m$ and σ acts as the identity on $K[\mathfrak{q}]$, it follows from the above condition (ii) that $\mathfrak{l}$ splits completely in $K[\mathfrak{q}]/K$ into m distinct primes that stay inert in $L[\mathfrak{q}]/K[\mathfrak{q}]$. Moreover, the fields $L[\mathfrak{q}]$ and $K[\mathfrak{l}]$ are linearly disjoint over K, since $\mathfrak{l}$ is unramified in $L[\mathfrak{q}]$ and $\mathfrak{l}$ is totally ramified in $K[\mathfrak{l}]$.

We find it more convenient to prove Lemma 6.7 first and then finish the proof of Proposition 6.6 afterwards.

Proof of Lemma 6.7 As the maximal abelian subextension of M/K is K_m/K and $L[\mathfrak{q}]/K$ is abelian, we have $L[\mathfrak{q}] \cap M = L[\mathfrak{q}] \cap K_m$. Since $L[\mathfrak{q}]/L$ is totally ramified at each prime above $\mathfrak{q}$ and $\mathfrak{q}$ is unramified in K_m/K, we have that $L[\mathfrak{q}] \cap K_m = L \cap K_m$. As p is unramified in $L/\mathbb{Q}$ and each prime above p is totally ramified in K_m/K, we also have that $L \cap K_m = K$, and therefore, $L[\mathfrak{q}] \cap M = K$. Now, since $L[\mathfrak{q}]$ and M were shown to be linearly disjoint over K, there exists a $\tau \in \mathrm{Gal}((L[\mathfrak{q}] \cdot M)/K)$ that restricts to $\sigma^{-1} \in \mathrm{Gal}(L[\mathfrak{q}]/K)$ and to a generator of $\mathrm{Gal}(M/K_m) \subseteq \mathrm{Gal}(M/K)$.

By the Čebotarev's Density Theorem, there are infinitely many primes of K of absolute degree 1 whose Artin symbol is the conjugacy class of τ. We can choose among them a prime $\mathfrak{l}$ not dividing $6q \cdot q_1 \ldots q_s$ (here $q = |\mathcal{O}_K/\mathfrak{q}|$) such that $\ell = |\mathcal{O}_K/\mathfrak{l}|$ is unramified in $K/\mathbb{Q}$. Since τ acts as the identity on K_m, it follows that ℓ splits completely in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. It is now clear that the first two conditions of the lemma are satisfied.

It remains to prove the third condition. Let $\mathfrak{L}$ be a prime of K_m above $\mathfrak{l}$. Since $\mathfrak{l}$ splits completely in K_m/K, it follows that $\mathcal{O}_{K_m}/\mathfrak{L} \cong \mathcal{O}_K/\mathfrak{l}$. Moreover, because $\langle \tau|_M \rangle = \mathrm{Gal}(M/K_m) \cong \mathbb{Z}/p\mathbb{Z}$, $\mathfrak{L}$ must be inert in M/K_m. From these observations, it follows that the element π cannot be a p-th power in $(\mathcal{O}_K/\mathfrak{l})^\times$.

Recall that from Artin's Reciprocity Theorem and the fact that $p \nmid |\mu_K|$, we have $(\mathcal{O}_K/\mathfrak{l})^\times/m \cong \mathrm{Gal}(K[\mathfrak{l}]/K)$ (see (6.2)). Since π was shown to be a non p-th power in $(\mathcal{O}_K/\mathfrak{l})^\times$, it follows that $\left(\frac{K[\mathfrak{l}]/K}{\pi\mathcal{O}_K}\right) = \left(\frac{K[\mathfrak{l}]/K}{\mathfrak{q}}\right)^h$ is not a p-th power in $\mathrm{Gal}(K[\mathfrak{l}]/K)$. Finally, since $\mathrm{Gal}(K[\mathfrak{l}]/K)$ is a cyclic group of order m (a power of p), it follows that $\left(\frac{K[\mathfrak{l}]/K}{\mathfrak{q}}\right)$ must generate $\mathrm{Gal}(K[\mathfrak{l}]/K)$, *i.e.*, $\mathfrak{q}$ is inert in $K[\mathfrak{l}]/K$. This concludes the proof of Lemma 6.7. ∎

We can now finish the proof of Proposition 6.6. Recall that $\mathfrak{q}$ is a fixed prime in $\mathcal{Q}_m$. Let $\mathfrak{l}$ be a prime that satisfies the three conditions in Lemma 6.7. As in the proof of Theorem 6.4, we let $\wp_{s+1} = \mathfrak{q}$, $F_{s+1} = K[\mathfrak{q}]$ and $I' = \{1, \ldots, s+1\}$. We introduce two auxiliary elliptic units:

$$\eta_{\mathfrak{l}} = \mathrm{N}_{K(\mathfrak{l}\mathfrak{m}_I)/L[\mathfrak{l}]}(\varphi_{\mathfrak{l}\mathfrak{m}_I})^{w_K},$$
$$\widehat{\eta}_{\mathfrak{l}} = \mathrm{N}_{K(\mathfrak{l}\mathfrak{m}_{I'})/L[\mathfrak{q}\mathfrak{l}]}(\varphi_{\mathfrak{l}\mathfrak{m}_{I'}})^{w_K},$$

where $L[\mathfrak{q}\mathfrak{l}]$ means the compositum of $L[\mathfrak{l}]$ and $L[\mathfrak{q}]$ (for the definition of $\varphi_{\mathfrak{l}\mathfrak{m}_I}$ and $\varphi_{\mathfrak{l}\mathfrak{m}_{I'}}$ see [11, Definition 2, p. 5]). Since $\mathfrak{l} \nmid 6$, we have for any $\zeta \in \mu_K - \{1\}$ that $\zeta \not\equiv 1 \pmod{\mathfrak{l}}$. Combining the previous observation with the norm relation (3.3), and the fact that $\left(\frac{L[\mathfrak{q}]/K}{\mathfrak{l}}\right) = \sigma^{-1}$, we can deduce that

$$\mathrm{N}_{L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{l}]}(\widehat{\eta}_{\mathfrak{l}}) = \eta_{\mathfrak{l}}^{q(1-\mathrm{Frob}(\mathfrak{q})^{-1})}, \tag{6.16}$$

$$\mathrm{N}_{L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{q}]}(\widehat{\eta}_{\mathfrak{l}}) = \widehat{\eta}^{\ell(1-\mathrm{Frob}(\mathfrak{l})^{-1})} = \widehat{\eta}^{\ell(1-\sigma)}, \tag{6.17}$$

$$\mathrm{N}_{L[\mathfrak{l}]/L}(\eta_{\mathfrak{l}}) = \eta^{\ell(1-\mathrm{Frob}(\mathfrak{l})^{-1})} = \eta^{\ell(1-\sigma)}, \tag{6.18}$$

where $q = |\mathcal{O}_K/\mathfrak{q}|$, $\ell = |\mathcal{O}_K/\mathfrak{l}|$, $\mathrm{Frob}(\mathfrak{q}) = \left(\frac{L[\mathfrak{l}]/K}{\mathfrak{q}}\right)$ and $\mathrm{Frob}(\mathfrak{l}) = \left(\frac{L[\mathfrak{q}]/K}{\mathfrak{l}}\right)$. In order to compare the different units $\widehat{\eta}_{\mathfrak{l}}, \eta_{\mathfrak{l}}, \widehat{\eta}$ and η, we will work in $\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$ modulo the product of all the primes of $L[\mathfrak{q}\mathfrak{l}]$ above $\mathfrak{q}$, which we denote by $\widehat{\mathfrak{q}}$. Since $\mathfrak{q} \in \mathcal{Q}_m$, $\mathfrak{q}$ splits completely in L/K, and by the third condition of Lemma 6.7, the primes of L above $\mathfrak{q}$ are inert in $L[\mathfrak{l}]/L$. Therefore, each prime of $L[\mathfrak{q}]$ above $\mathfrak{q}$ is inert in $L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{q}]$, and so $\widehat{\mathfrak{q}} = \widetilde{\mathfrak{q}}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$, where as before $\widetilde{\mathfrak{q}}$ corresponds to the product of all primes of $L[\mathfrak{q}]$ above $\mathfrak{q}$. We therefore have the following isomorphisms of rings:

$$\mathcal{O}_{L[\mathfrak{q}]}/\widetilde{\mathfrak{q}} \cong \mathcal{O}_L/\mathfrak{q}\mathcal{O}_L \cong (\mathbb{F}_q)^{p^k},$$

$$\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\widetilde{\mathfrak{q}}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]} \cong \mathcal{O}_{L[\mathfrak{l}]}/\mathfrak{q}\mathcal{O}_{L[\mathfrak{l}]} \cong (\mathbb{F}_{q^m})^{p^k}.$$

Since $L[\mathfrak{q}]$ and $L[\mathfrak{l}]$ are linearly disjoint over L, it makes sense to extend $\mathrm{Frob}(\mathfrak{q}) \in \mathrm{Gal}(L[\mathfrak{l}]/K)$ to $L[\mathfrak{q}\mathfrak{l}]$ in such a way that $\mathrm{Frob}(\mathfrak{q})$ is the identity on $L[\mathfrak{q}]$, and we still denote this extension by $\mathrm{Frob}(\mathfrak{q})$. In particular, $\mathrm{Frob}(\mathfrak{q})$ generates $\mathrm{Gal}(L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{q}])$.

It follows from the discussion above that $\mathrm{Frob}(\mathfrak{q})$ acts as raising to the q-th power on $\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\widetilde{\mathfrak{q}}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$, and that $\mathrm{Gal}(L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{l}])$ (the inertia group at $\mathfrak{q}$) acts trivially on $\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\widetilde{\mathfrak{q}}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$. From these two observations, it follows that the norms $\mathrm{N}_{L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{l}]}$ and $\mathrm{N}_{L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{q}]}$ act on the ring $\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\widetilde{\mathfrak{q}}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$ as raising to the m-th power and as raising to the $\left(\sum_{i=0}^{m-1} q^i\right)$-th power, respectively. Since $q \equiv 1 \pmod{m}$, there exists a positive integer r such that $\sum_{i=0}^{m-1} q^i = mr$.

Combining (6.17), (6.16), and (6.18), we find that

$$\widehat{\eta}^{\ell(1-\sigma)} \equiv \widehat{\eta}_{\mathfrak{l}}^{mr} \equiv \eta_{\mathfrak{l}}^{qr(1-\mathrm{Frob}(\mathfrak{q})^{-1})} \equiv \eta_{\mathfrak{l}}^{r(q-1)} \equiv \left(\eta_{\mathfrak{l}}^{mr}\right)^{\frac{q-1}{m}} \equiv \eta^{\ell(1-\sigma)\frac{q-1}{m}} \pmod{\widetilde{\mathfrak{q}}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}}. \tag{6.19}$$

Finally, since the natural map $\mathcal{O}_{L[\mathfrak{q}]}/\widetilde{\mathfrak{q}} \to \mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\widetilde{\mathfrak{q}}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$ is injective, it follows from (6.19) that $\widehat{\eta}^{\ell(1-\sigma)} \equiv \eta^{\ell(1-\sigma)\frac{q-1}{m}} \pmod{\widetilde{\mathfrak{q}}}$. This completes the proof of Proposition 6.6. ∎

7 Annihilating the Ideal Class Group

For this section we keep the same notation and assumptions as in the previous sections. In particular, $\mathrm{Gal}(L/K) = \Gamma = \langle\sigma\rangle \cong \mathbb{Z}/p^k\mathbb{Z}$ and the extended group of elliptic units $\overline{\mathcal{C}}_L$ is defined as the $\mathbb{Z}[\Gamma]$-submodule of $\mathcal{O}_L^\times$ generated by μ_K and by the units $\alpha_1, \dots, \alpha_k$; see Definition 5.1.

For each $j \in \{1, \dots, s\}$, recall that n_j (a power of p) was defined as the index of the decomposition group of $\mathfrak{P}_j$ (a prime of L above $\wp_j$) in Γ (see Section 1) and that $n_1 \le n_2 \le \cdots \le n_s$ (see (4.2)). For each $i \in \{1, \dots, k\}$, we define

$$\mu_i = n_{\max M_i}, \tag{7.1}$$

where $M_i \subseteq \{1, \dots, s\}$ is the set defined in (5.2). In particular, μ_i is always a power of p (possibly trivial). Since $M_i \subseteq M_{i+1}$, we always have that $\mu_i \le \mu_{i+1}$. Let us call an index $i \in \{1, \dots, k-1\}$ a *jump* if $\mu_i < \mu_{i+1}$. Furthermore, we declare the indices 0 and k to be jumps and we set $\mu_0 = 0$. Using the notion of jumps, one can write down a $\mathbb{Z}$-basis of $\overline{\mathcal{C}}_L/\mu_K$ using only conjugates of the generators $\alpha_1, \dots, \alpha_k$ whose indices correspond to jumps.

Lemma 7.1 *Let $0 = s_0 < s_1 < \cdots < s_\kappa = k$ be the ordered sequence of all the jumps. Note that $\kappa \ge 1$. Then the set $\bigcup_{t=1}^{\kappa}\{\alpha_{s_t}^{\sigma^i} ; 0 \le i < p^{s_t} - p^{s_{t-1}}\}$ gives a $\mathbb{Z}$-basis of $\overline{\mathcal{C}}_L/\mu_K$.*

Proof This is proved along similar lines to [9, Lemma 5.1]. Let us just point out the two main ideas. For each $1 < i \le k$ one can show that

$$\mathrm{N}_{L_i/L_{i-1}}(\alpha_i) \in \langle \alpha_{i-1} \rangle_{\mathbb{Z}[\Gamma]}, \tag{7.2}$$

and furthermore, for each $0 < u < v \le k$ such that $\mu_u = \mu_v$, one can prove the stronger result that

$$\langle \mathrm{N}_{L_v/L_u}(\alpha_v) \rangle_{\mathbb{Z}[\Gamma]} = \langle \alpha_u \rangle_{\mathbb{Z}[\Gamma]}.$$

This concludes the sketch of the proof. ∎

From the explicit $\mathbb{Z}$-basis for $\overline{\mathcal{C}}_L/\mu_K$, which appears in Lemma 7.1, we easily deduce the following lemma.

Lemma 7.2 *Let r be the highest jump less than k,* i.e., *$r = s_{\kappa-1}$ and $\mu_r < \mu_{r+1} = n_s$ where n_s is defined in (4.2). Let us assume that $\rho \in \mathbb{Z}[\Gamma]$ is such that $\alpha_k^\rho \in \overline{\mathcal{C}}_{L_r}$. Then*

$$(1 - \sigma^{p^r})\rho = 0. \tag{7.3}$$

Proof There is a unique polynomial $f \in \mathbb{Z}[x]$ with $\deg f < p^k$, such that $\rho = f(\sigma)$. Let $\phi = x^{p^k - p^r} + \cdots + x^{2p^r} + x^{p^r} + 1$. From the euclidean division of f by ϕ there exist polynomials $Q, g \in \mathbb{Z}[x]$ such that $f = \phi \cdot Q + g$ where $\deg g < p^k - p^r$. By assumption, we have $\alpha_k^\rho \in \overline{\mathcal{C}}_{L_r}$, and from (7.2) we know that $\alpha_k^{\phi(\sigma)} = \mathrm{N}_{L_k/L_r}(\alpha_k) \in \overline{\mathcal{C}}_{L_r}$; combining these two relations we obtain that

$$\alpha_k^{g(\sigma)} = \frac{\alpha_k^{f(\sigma)}}{\alpha_k^{\phi(\sigma)Q(\sigma)}} \in \overline{\mathcal{C}}_{L_r}.$$

Since $\{\alpha_k, \alpha_k^\sigma, \ldots, \alpha_k^{\sigma^{p^k - p^r - 1}}\}$ is a part of the $\mathbb{Z}$-basis given in Lemma 7.1, and the rest of this $\mathbb{Z}$-basis, namely $\bigcup_{t=1}^{\kappa-1}\{\alpha_{s_t}^{\sigma^i}\ ;\ 0 \le i < p^{s_t} - p^{s_{t-1}}\}$, is also a $\mathbb{Z}$-basis of $\overline{\mathcal{C}}_{L_r}/\mu_K$ (using again Lemma 7.1); we deduce that $g = 0$. In particular, $\rho = (1 + \sigma^{p^r} + \sigma^{2p^r} + \cdots + \sigma^{p^k - p^r})\rho'$ for some $\rho' \in \mathbb{Z}[\Gamma]$, and thus (7.3) follows. ∎

From Theorem 5.2, we know that $\mathcal{O}_L^\times/\overline{\mathcal{C}}_L$ is a finite $\mathbb{Z}[\Gamma]$-module. Let $(\mathcal{O}_L^\times/\overline{\mathcal{C}}_L)_p$ and $\mathrm{Cl}(L)_p$ denote the p-Sylow subgroups of the corresponding $\mathbb{Z}[\Gamma]$-modules. The aim of this section is to construct annihilators of $\mathrm{Cl}(L)_p$ by means of annihilators of $(\mathcal{O}_L^\times/\overline{\mathcal{C}}_L)_p$. To do this we appeal to the following key theorem which allows one to produce annihilators of $\mathrm{Cl}(L)_p$ from certain units of L. This theorem should be viewed as a modification of a similar result obtained first by Thaine (see [15, Proposition 6]) and then generalized by Rubin (see [12, Theorem 5.1]).

Theorem 7.3 *Let m be a power of p divisible by p^{ks}. Assume that $\varepsilon \in \mathcal{O}_L$ is m-semi-special, suppose that $V \subseteq L^\times/m$ is a finitely generated $\mathbb{Z}[\Gamma]$-submodule, and that the class containing ε belongs to V. Let $z\colon V \to \mathbb{Z}/m[\Gamma]$ be a $\mathbb{Z}[\Gamma]$-linear map such that $z(V \cap K^\times) = 0$, where $V \cap K^\times$ is taken to mean $V \cap (K^\times L^{\times m}/L^{\times m})$. Then $z(\varepsilon)$ annihilates $\mathrm{Cl}(L)_p/(m/p^{k(s-1)})$.*

Proof This can be proved along similar lines as [5, Theorem 12]. In order to guide the reader to make the necessary modifications needed for the proof, we chose to state Theorem 7.4 (the required version of [5, Theorem 17], which has its origin in [12, Theorem 5.5]). This concludes our rough sketch of the proof. ■

Theorem 7.4 *Fix a p-power m, suppose that $V \subseteq L^\times/m$ is a finitely generated $\mathbb{Z}_p[\Gamma]$-submodule. Without loss of generality we can assume that we have chosen a set of generators of V that belongs to $\mathcal{O}_L$. Let us suppose that we are given a $\mathbb{Z}_p[\Gamma]$-linear map $z\colon V \to \mathbb{Z}/m[\Gamma]$ that is such that $z(V \cap K^\times) = 0$. Then, for any $\mathfrak{c} \in \mathrm{Cl}(L)_p$, there exist infinitely many unramified primes $\mathfrak{Q}$ in L of absolute degree 1 satisfying the following conditions:*

Let $\mathfrak{q}$ be the prime ideal of K below $\mathfrak{Q}$ and let q be the rational prime number below $\mathfrak{q}$.

(i) $[\mathfrak{Q}] = \mathfrak{c}$, *where $[\mathfrak{Q}]$ is the projection of the ideal class of $\mathfrak{Q}$ into $\mathrm{Cl}(L)_p$;*
(ii) $q \equiv 1 + m \pmod{m^2}$;
(iii) *for each $j = 1, \dots, s$, the class of π_j is an m-th power in $(\mathcal{O}_K/\mathfrak{q})^\times$;*
(iv) *the support of any of the chosen generators of V does not contain any prime of L above $\mathfrak{q}$, and there is a $\mathbb{Z}_p[\Gamma]$-linear map $\varphi\colon (\mathcal{O}_L/\mathfrak{q})^\times/m \to \mathbb{Z}/m[\Gamma]$ such that the diagram*

$$\begin{array}{ccc} V & \xrightarrow{\ z\ } & \mathbb{Z}/m[\Gamma] \\ \big\downarrow{\scriptstyle\psi} & \nearrow{\scriptstyle\varphi} & \\ (\mathcal{O}_L/\mathfrak{q})^\times/m & & \end{array}$$

commutes, where ψ corresponds to the reduction map.

Proof This can be proved in the same way as [5, Theorem 17]. ■

We can finally present the main result of this paper.

Theorem 7.5 *Let r be the highest jump less than k,* i.e., *$\mu_r < \mu_{r+1} = n_s$. If $\varkappa \in \mathrm{Ann}_{\mathbb{Z}[\Gamma]}((\mathcal{O}_L^\times/\overline{\mathcal{C}}_L)_p)$, then $(1-\sigma^{p^r})\varkappa$ annihilates $\mathrm{Cl}(L)_p$. In other words, we have*

$$\mathrm{Ann}_{\mathbb{Z}[\Gamma]}((\mathcal{O}_L^\times/\overline{\mathcal{C}}_L)_p) \subseteq \mathrm{Ann}_{\mathbb{Z}[\Gamma]}((1-\sigma^{p^r})\mathrm{Cl}(L)_p).$$

The number r can be characterized as follows: $p^{k-r} = \max\{t_j\ ;\ j \in J\}$, where $J = \{j \in \{1, \dots, s\}\ ;\ n_j = n_s\}$.

Proof Fix a p-power m that is large enough so that $m \nmid p^{ks}h_L$ and let

$$\varkappa \in \mathrm{Ann}_{\mathbb{Z}[\Gamma]}((\mathcal{O}_L^\times/\overline{\mathcal{C}}_L)_p)$$

be a fixed annihilator. We first construct a $\mathbb{Z}[\Gamma]$-linear map $z'\colon \mathcal{O}_L^\times \to \mathbb{Z}[\Gamma]$, that will only depend on the annihilator $\varkappa$, and then consider the induced map $z\colon \mathcal{O}_L^\times/m \to \mathbb{Z}/m[\Gamma]$. Let f be the greatest divisor of the index $[\mathcal{O}_L^\times : \overline{\mathcal{C}}_L]$ that is not divisible by p. Then

$$f\varkappa \in \mathrm{Ann}_{\mathbb{Z}[\Gamma]}(\mathcal{O}_L^\times/\overline{\mathcal{C}}_L),$$

and thus, for any unit $\varepsilon \in \mathcal{O}_L^\times$, we have $\varepsilon^{f\varkappa} \in \overline{\mathcal{C}}_L$. From Lemma 7.1, there is $\rho \in \mathbb{Z}[\Gamma]$ and $\delta \in \overline{\mathcal{C}}_{L_r}$ such that $\varepsilon^{f\varkappa} = \delta\alpha_k^\rho$. We define $z'(\varepsilon) = (1-\sigma^{p^r})\rho$. Let us check that the the map z' is well defined. If $\varepsilon^{f\varkappa} = \delta'\alpha_k^{\rho'}$ for some $\rho' \in \mathbb{Z}[\Gamma]$ and $\delta' \in \overline{\mathcal{C}}_{L_r}$, then $\alpha_k^{\rho-\rho'} = \delta'\delta^{-1} \in \overline{\mathcal{C}}_{L_r}$; applying Lemma 7.2, we find that $(1-\sigma^{p^r})(\rho-\rho') = 0$, and so z' is well defined. It follows directly from the definition of z' that $z'(\alpha_k) = (1-\sigma^{p^r})f\varkappa$ and that $z'(\varepsilon) = 0$ if $\varepsilon \in \mathcal{O}_L^\times \cap K^\times = \mu_K$.

Let $V = \mathcal{O}_L^\times/m$. We want to apply Theorem 7.3 to the $\mathbb{Z}_p[\Gamma]$-linear map $z\colon V \to \mathbb{Z}/m[\Gamma]$ determined by the map z'. Now, from Theorem 6.4, we know that $\alpha_k \in \mathcal{O}_L^\times$ is m-semispecial, and therefore, from Theorem 7.3, we obtain that $z(\alpha_k) = (1-\sigma^{p^r})f\varkappa$ annihilates $\mathrm{Cl}(L)_p/(m/p^{k(s-1)})$. Finally, since $p \nmid f$ and $m \nmid p^{ks}h_L$, it follows that $\mathrm{Cl}(L)_p/(m/p^{k(s-1)}) = \mathrm{Cl}(L)_p$, and therefore $(1-\sigma^{p^r})\varkappa$ annihilates $\mathrm{Cl}(L)_p$.

It remains to prove the last equality in Theorem 7.5, which gives a characterization of the index r. Recall that for each index $i \in \{1,\dots,k\}$, $M_i = \{j \in \{1,\dots,s\}\ ;\ t_j > p^{k-i}\}$ by (5.2) and that $\mu_i = n_{\max M_i}$ by (7.1). It follows from the definitions of J and μ_i that

$$\mu_i < n_s \iff M_i \cap J = \varnothing. \tag{7.4}$$

In particular, if we set $i = r$ in (7.4) we find that $M_r \cap J = \varnothing$, and therefore, for each $j \in J$ we must have the inequality (a) $t_j \le p^{k-r}$. Let us show that the reverse inequality holds true for at least one index. Since $\mu_{r+1} = n_s$ it follows from (7.4) that $M_{r+1} \cap J \ne \varnothing$. Hence there must exist at least one index $j_0 \in M_{r+1} \cap J$, and by definition of M_{r+1}, we must have that (b) $t_{j_0} > p^{k-(r+1)}$. Finally, combining inequalities (a) and (b), we find that $t_{j_0} = p^{k-r}$ and thus $p^{k-r} = t_{j_0} = \max\{t_j\ ;\ j \in J\}$. ∎

References

[1] W. Bley, *Wild Euler systems of elliptic units and the equivariant Tamagawa number conjecture*. J. Reine Angew. Math. **577**(2004), 117–146. http://dx.doi.org/10.1515/crll.2004.2004.577.117

[2] ———, *Equivariant Tamagawa number conjecture for abelian extensions of a quadratic imaginary field*. Doc. Math. **11**(2006), 73–118.

[3] D. Burns, *Congruences between derivatives of abelian L-functions at s = 0*. Invent. Math. **169**(2007), 451–499. http://dx.doi.org/10.1007/s00222-007-0052-3

[4] G. Gras, *Class field theory. From theory to practice*. Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003.

[5] C. Greither and R. Kučera, *Annihilators for the class group of a cyclic field of prime power degree*. Acta Arith. **112**(2004), 177–198. http://dx.doi.org/10.4064/aa112-2-6

[6] ———, *Annihilators for the class group of a cyclic field of prime power degree II*. Canad. J. Math. **58**(2006), 580–599. http://dx.doi.org/10.4153/CJM-2006-024-2

[7] ———, *Linear forms on Sinnott's module*. J. Number Theory **141**(2014), 324–342, http://dx.doi.org/10.1016/j.jnt.2014.02.003

[8] ———, *Eigenspaces of the ideal class group*. Ann. Inst. Fourier (Grenoble) **64**(2014), 2165–2203. http://dx.doi.org/10.5802/aif.2908

[9] ———, *Annihilators for the class group of a cyclic field of prime power degree III*. Publ. Math. Debrecen **86**(2015), no. 3–4, 401–421.

[10] T. Ohshita, *On higher Fitting ideals of Iwasawa modules of ideal class groups over imaginary quadratic fields and Euler systems of elliptic units*. Kyoto J. Math. **53**(2013), 845–887. http://dx.doi.org/10.1215/21562261-2366118

[11] H. Oukhaba, *Index formulas for ramified elliptic units*. Compositio Math. **137**(2003), 1–22. http://dx.doi.org/10.1023/A:1023667807218

[12] K. Rubin, *Global units and ideal class groups*. Invent. Math. **89**(1987), 511–526. http://dx.doi.org/10.1007/BF01388983
[13] ———, *Stark units and Kolyvagin's "Euler systems"*. J. Reine Angew. Math. **425**(1992), 141–154. http://dx.doi.org/10.1515/crll.1992.425.141
[14] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*. Invent. Math. **62**(1980), 181–234. http://dx.doi.org/10.1007/BF01389158
[15] F. Thaine, *On the ideal class groups of real abelian number fields*. Ann. of Math. (2) **128**(1988), no. 1, 1–18. http://dx.doi.org/10.2307/1971460

Faculty of Science and Engineering, Laval University, Québec G1V 0A6, Canada
Email: hugo.chapdelaine@mat.ulaval.ca

Faculty of Science, Masaryk University, 611 37 Brno, Czech Republic
Email: kucera@math.muni.cz