Journal of Number Theory 213 (2020) 187–220

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Annihilators of the ideal class group of an imaginary cyclic field

Pavel Francírek

Faculty of Science, Masaryk university, 611 37 Brno, Czech Republic

A R T I C L E   I N F O

Article history:
Received 14 November 2019
Received in revised form 19 December 2019
Accepted 24 December 2019
Available online 20 January 2020
Communicated by L. Smajlovic

MSC:
11R20
11R29

Keywords:
Annihilators
Class group
Stickelberger ideal
Cyclic fields

A B S T R A C T

For certain infinite family of imaginary cyclic fields we can obtain annihilators of the ideal class group by factoring nontrivial roots of modified Gauss sums. In this paper we investigate whether and when these annihilators live outside the Stickelberger ideal.

0. Introduction

In [5] Greither and Kučera managed to obtain new annihilators of the ideal class group of certain real cyclic fields (i.e., cyclic extensions of $\mathbb{Q}$). They modified Rubin-Thaine machinery to accept so-called semispecial units. In order to get some units which are semispecial, they enlarged the Sinnott's group of circular units by adding nontrivial roots

E-mail address: pfrancirek@seznam.cz.

https://doi.org/10.1016/j.jnt.2019.12.003

of circular units. The idea of taking roots can also be applied to Gauss sums. For certain imaginary cyclic fields this approach leads to new annihilators of the ideal class group.

Let ℓ be a fixed odd prime number. Let K be a cyclic number field of ℓ-power degree $d = \ell^k = [K : \mathbb{Q}]$. Let $p_1, \ldots, p_t$ be the primes ramified in $K/\mathbb{Q}$. Let F be an imaginary cyclic number field whose degree $r = [F : \mathbb{Q}]$ is not divisible by ℓ. Hence the compositum $L = FK$ is cyclic, too. We suppose that ℓ does not ramify in $L/\mathbb{Q}$. Let f be the conductor of F and m be the conductor of K, so $\ell \nmid fm$. We assume that f and m are relatively prime, i.e., the product fm is the conductor of L. For every prime number q and every ideal $A \subseteq \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ we shall denote $A\mathbb{Z}_q[\mathrm{Gal}(L/\mathbb{Q})]$ by A_q.

We begin with a module generated by Gauss sums. Distribution relations satisfied by these sums allow us to work with some Sinnott module instead. It is more convenient, since in [3] Greither and Kučera described the image of its top generator in any linear form. This allows us to prove that a nontrivial root of a certain modified Gauss sum belongs to L. Factoring this nontrivial root gives rise to an element ξ^L of the integral group ring $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$. In the same fashion we shall construct an element $\xi^M \in \mathbb{Z}[\mathrm{Gal}(M/\mathbb{Q})]$ for every imaginary subfield $M \subseteq L$. The ideal of $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ generated by the corestrictions of all these elements will be denoted by $\mathcal{J}^{\mathcal{L}}$. In this paper we shall prove:

Theorem 9.5. *The ideal $\mathcal{J}^{\mathcal{L}}$ annihilates the ideal class group* $\mathrm{Cl}(L)$ *of L.*

In order to decide whether $\mathcal{J}^{\mathcal{L}}$ contains new annihilators or not, we compare $\mathcal{J}^{\mathcal{L}}$ to $\mathcal{I}^{\mathcal{L}}$ which is essentially the minus part of the Stickelberger ideal of the field L. Even though we are unable to determine the index $[\mathcal{J}^{\mathcal{L}} : \mathcal{I}^{\mathcal{L}}]$ in general, we can compute the index $[\mathcal{J}_q^{\mathcal{L}} : \mathcal{I}_q^{\mathcal{L}}]$ for almost all primes q (see Theorem 9.4). It can be shown that the index $[\mathcal{J}_\ell^{\mathcal{L}} : \mathcal{I}_\ell^{\mathcal{L}}]$ is greater than 1 if and only if there exist at least two primes ramified in $K/\mathbb{Q}$ which split completely in $F_0/\mathbb{Q}$ where F_0 is the smallest imaginary subfield of F.

The case of F being a quadratic imaginary field was already studied by Greither and Kučera in [2, section 6]. Using our approach one may obtain even stronger annihilation result in this concrete situation. A detailed comparison of these results is provided at the end of Section 9.

1. Cyclotomic polynomials

This section is devoted to a result on polynomials with integral coefficients which we shall need later on. Even though the following lemma is probably well-known and it might have been already published, the author could not find any source.

Lemma 1.1. *Let $F, G \in \mathbb{Z}[X]$ be polynomials which have no common root in $\mathbb{C}$ and suppose that F is monic. Then the index of the ideal (F, G) in $\mathbb{Z}[X]$ is equal to the absolute value of the resultant of F and G, i.e. we have*

$$\left|\mathbb{Z}[X]/\big(F, G\big)\right| = \left|\mathrm{Res}\big(F, G\big)\right| .$$

Proof. At first, let us suppose that G is also monic, so we can write

$$F(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

and

$$G(X) = X^s + b_1X^{s-1} + \cdots + b_{s-1}X + b_s,$$

where a_i and b_i are integers. If $F = 1$ or $G = 1$, then the lemma holds, so we can assume that both s and n are at least 1. Third isomorphism theorem gives us the following isomorphism of groups

$$\mathbb{Z}[X]/(F,G) \cong \mathbb{Z}[X]/(F\cdot G)\Big/(F,G)/(F\cdot G)\cdot$$

Let $\overline{X}$ be the class of $\mathbb{Z}[X]/(F\cdot G)$ containing X. Clearly $\mathbb{Z}[X]/(F\cdot G)$ is a free $\mathbb{Z}$-module of rank $n+s$ and the elements $1, \overline{X}, \ldots, \overline{X}^{n+s-1}$ form its $\mathbb{Z}$-basis. Since F and G have no common root in $\mathbb{C}$, every element of the ideal (F,G) can be uniquely expressed in the form

$$u\cdot F + v\cdot G + w\cdot F\cdot G$$

with $u, v, w \in \mathbb{Z}[X]$ satisfying $\deg u < \deg G$ and $\deg v < \deg F$. It follows that the following $s+n$ elements

$$F(\overline{X}), \overline{X}F(\overline{X}), \ldots, \overline{X}^{n-1}F(\overline{X}), G(\overline{X}), \overline{X}G(\overline{X}), \ldots, \overline{X}^{s-1}G(\overline{X})$$

form a $\mathbb{Z}$-basis for

$$(F,G)/(F\cdot G).$$

Therefore the index

$$[\mathbb{Z}[X]/(F\cdot G) \colon (F,G)/(F\cdot G)]$$

is finite and it is equal to the absolute value of the following determinant

$$\begin{vmatrix}
1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
a_1 & 1 & \cdots & 0 & b_1 & 1 & \cdots & 0 \\
a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\
\vdots & \vdots & \ddots & 1 & \vdots & \vdots & \ddots & 1 \\
a_n & a_{n-1} & \cdots & \vdots & b_s & b_{s-1} & \cdots & \vdots \\
0 & a_n & \ddots & \vdots & 0 & b_s & \ddots & \vdots \\
\vdots & \vdots & \ddots & a_{n-1} & \vdots & \vdots & \ddots & b_{s-1} \\
0 & 0 & \cdots & a_n & 0 & 0 & \cdots & b_s
\end{vmatrix},$$

which is the resultant $\operatorname{Res}(F,G)$. We shall suppose now that G is not monic. We take the following polynomial

$$H = X^{1+\deg G} \cdot F + G \in \mathbb{Z}[X].$$

Clearly H is monic and we have $(F,G) = (F,H)$. Therefore it only remains to show the equality of resultants $\operatorname{Res}(F,G) = \operatorname{Res}(F,H)$. Let $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$ be all the roots of F. Then we have

$$\operatorname{Res}(F,H) = \prod_{i=1}^{n} H(\alpha_i) = \prod_{i=1}^{n} \big(\alpha_i^{s+1} F(\alpha_i) + G(\alpha_i)\big) = \prod_{i=1}^{n} G(\alpha_i) = \operatorname{Res}(F,G)$$

and the lemma follows. □

The sth cyclotomic polynomial will be denoted by Φ_s.

Proposition 1.2. *Let $s, n, s < n$ be positive integers. Then we have*

$$|\mathbb{Z}[\zeta_n]/\big(\Phi_s(\zeta_n)\big)| = \begin{cases} p^{\varphi(s)} & \text{if } \frac{n}{s} = p^k \text{ for some prime } p, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. It follows immediately from [1, Theorem 4] using Lemma 1.1. □

Proposition 1.3. *Let $n, r_1, r_2, \dots, r_u$ be positive integers such that $r_i \mid n$ for all $i = 1, \dots, u$ and $r_i \nmid r_j$ for all i, j, $i \neq j$. For every $i = 1, 2, \dots, u$ we define*

$$f_i(X) = \frac{X^n - 1}{X^{r_i} - 1} = \prod_{\substack{j \mid n \\ j \nmid r_i}} \Phi_j(X).$$

For each $i = 1, \dots, u$ we put

$$g_i(X) = \gcd\big(f_1(X), f_2(X), \dots, f_i(X)\big).$$

Then for each $i = 1, \dots, u$ we have

$$\left| \mathbb{Z}[X] \Big/ \left(\tfrac{f_1}{g_i}, \tfrac{f_2}{g_i}, \dots, \tfrac{f_i}{g_i}\right) \right| = 1.$$

Proof. We prove this by induction on i: if $i = 1$ then $g_1 = f_1$. Assume that $i \geq 2$ and that the lemma has been proved for $i - 1$. The induction hypothesis gives the following equality of ideals in $\mathbb{Z}[X]$

$$\left(\frac{f_1}{g_{i-1}}, \frac{f_2}{g_{i-1}}, \dots, \frac{f_{i-1}}{g_{i-1}}\right) = (1),$$

hence

$$\left(\frac{f_1}{g_i}, \frac{f_2}{g_i}, \ldots, \frac{f_{i-1}}{g_i}\right) = \left(\frac{g_{i-1}}{g_i}\right).$$

It follows that

$$\left(\frac{f_1}{g_i}, \frac{f_2}{g_i}, \ldots, \frac{f_{i-1}}{g_i}, \frac{f_i}{g_i}\right) = \left(\frac{g_{i-1}}{g_i}, \frac{f_i}{g_i}\right).$$

It can be easily shown that

$$\frac{g_{i-1}(X)}{g_i(X)} = \prod_{\substack{j|n \\ j\nmid r_1,\ldots,j\nmid r_{i-1},j|r_i}} \Phi_j(X) \quad \text{and} \quad \frac{f_i(X)}{g_i(X)} = \prod_{\substack{j|n,j\nmid r_i \\ \exists\, a \in \{1,\ldots,i-1\}:\ j|r_a,}} \Phi_j(X).$$

Therefore we obtain using Lemma 1.1 that

$$\begin{aligned} \left| \mathbb{Z}[X] \Big/ \left(\tfrac{g_{i-1}}{g_i}, \tfrac{f_i}{g_i}\right) \right| &= \left|\mathrm{Res}\left(\frac{g_{i-1}}{g_i}, \frac{f_i}{g_i}\right)\right| = \prod_{j_1}\prod_{j_2} |\,\mathrm{Res}(\Phi_{j_1}, \Phi_{j_2})| \\ &= \prod_{j_1}\prod_{j_2} |\mathbb{Z}[X]/(\Phi_{j_1}, \Phi_{j_2})|, \end{aligned}$$

where neither of $\frac{j_1}{j_2}$ and $\frac{j_2}{j_1}$ is an integer. Proposition 1.2 gives

$$|\mathbb{Z}[X]/(\Phi_{j_1}, \Phi_{j_2})| = 1 \qquad \text{for all } j_1, j_2$$

and the result follows. □

Corollary 1.4. *Keep the same notation as above. For every $i = 1, 2, \ldots, u$ there exists $P_i \in \mathbb{Z}[X]$ such that*

$$\sum_{i=1}^{u} P_i f_i = g_u.$$

Proof. Lemma 1.3 implies that

$$\left| \mathbb{Z}[X] \Big/ \left(\tfrac{f_1}{g_u}, \tfrac{f_2}{g_u}, \ldots, \tfrac{f_u}{g_u}\right) \right| = 1,$$

which is equivalent to

$$\left(\frac{f_1}{g_u}, \frac{f_2}{g_u}, \ldots, \frac{f_u}{g_u}\right) = (1).$$

This means that for every $i = 1, 2, \ldots, u$ there exists $P_i \in \mathbb{Z}[X]$ such that

$$\sum_{i=1}^{u} P_i \frac{f_i}{g_u} = 1.$$

Multiplying both sides by g_u proves the corollary. $\square$

2. Distribution relations for Gauss sums

For any positive integer n let $\zeta_n = e^{2\pi i/n}$. Let us fix a prime number $p \equiv 1 \pmod{fm}$. Fix a prime $\mathfrak{P}$ of $\mathbb{Q}(\zeta_{fm})$ dividing p. Let $\omega\colon \mathbb{F}_p^\times \to \langle \zeta_{fm} \rangle$ be the fm-th power residue symbol determined by $\mathfrak{P}$, i.e. for any $a \in \mathbb{Z}[\zeta_{fm}]$ such that $\mathfrak{P} \nmid a$ we have

$$\omega(a \bmod \mathfrak{P}) \equiv a^{(p-1)/fm} \pmod{\mathfrak{P}}.$$

Let $\psi\colon \mathbb{F}_p \to \mathbb{Q}(\zeta_p)$ be the usual additive character of $\mathbb{F}_p$, i.e. $\psi(c) = \zeta_p^c$. For any multiplicative character $\chi\colon \mathbb{F}_p^\times \to \mathbb{C}^\times$ we define the Gauss sum

$$g(\chi, \psi) = -\sum_{c=1}^{p-1} \chi(c)\psi(c).$$

For any $n \mid fm$ let $\chi_n\colon \mathbb{F}_p^\times \to \langle \zeta_n \rangle$ be the multiplicative character of $\mathbb{F}_p^\times$ given by

$$\chi_n = \omega^{-\frac{fm}{n}}.$$

For any $a \in \mathbb{Z}$ we set

$$z(a,n) = \begin{cases} 1, & \text{if } n \mid a \\ g(\chi_n^a, \psi)^{n(1-\tau)}, & \text{otherwise,} \end{cases} \tag{1}$$

where τ is the complex conjugation. The following lemma describes basic properties of the numbers $z(a,n)$. For any $n \mid fm$ and any integer b relatively prime to n let $\sigma_{b,n} \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big)$ be the automorphism determined by $\zeta_n \mapsto \zeta_n^b$.

Lemma 2.1. *For any $n \mid fm$, any $a \in \mathbb{Z}$ and any $b \in \mathbb{Z}$ relatively prime to n we have*

1. $z(a,n) \in \mathbb{Q}(\zeta_n)$.
2. $z(a,n)^{\sigma_{b,n}} = z(ab,n)$.
3. $z(aq,n) = z(a,n/q)^q$ *for any prime $q \mid n$.*

Proof. The first two properties follow from [8, Lemma 6.4] and for any prime $q \mid n$ we have

$$z(aq,n) = g(\chi_n^{aq}, \psi)^{n(1-\tau)} = g(\chi_{n/q}^a, \psi)^{q(n/q)(1-\tau)} = z(a,n/q)^q. \quad \square$$

Let q be a prime number. Let q^a be the highest power of q dividing fm, so we can write $fm = q^a b$ with b relatively prime to q. By $\mathrm{Frob}(q)$ we shall denote the unique element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{fm})/\mathbb{Q})$ satisfying

$$\mathrm{res}_{\mathbb{Q}(\zeta_{fm})/\mathbb{Q}(\zeta_{q^a})}\mathrm{Frob}(q) = \mathrm{id} \qquad \text{and} \qquad \mathrm{res}_{\mathbb{Q}(\zeta_{fm})/\mathbb{Q}(\zeta_b)}\mathrm{Frob}(q) = \sigma_{q,b}.$$

If there is no danger of confusion all its restrictions will be also denoted by $\mathrm{Frob}(q)$.

We remark that our number $z(a,n)$ is equal to $z_a^{(n)} \cdot (-1)^{p-1/2}$ which is defined in [2, section 5].

Proposition 2.2. *Let $n \mid fm$. Let $s > 1$ be a power of a prime q dividing n. Then we have*

$$\mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/s})}\big(z(1,n)\big) = \begin{cases} z(1,n/s)^{s(1-\mathrm{Frob}(q)^{-1})} & \text{if } (s,n/s)=1, \\ z(1,n/s)^s & \text{otherwise.} \end{cases}$$

Proof. It follows from [2, Corollary 5.2] and [2, Corollary 5.3] using $z(a,n) = z_a^{(n)} \cdot (-1)^{\frac{p-1}{2}}$. $\square$

Let $I = \{1,\dots,t\}$ be the set of indices of primes ramified in $K/\mathbb{Q}$. For each $i \in I$ let K_i be the unique subfield of the p_i-th cyclotomic field $\mathbb{Q}(\zeta_{p_i})$ whose degree is equal to the ramification index of p_i in $K/\mathbb{Q}$. For every subset $T \subseteq I$ let $m_T = \prod_{i\in T} p_i$ and $L_T = FK_T$, where $K_T = \prod_{i\in T} K_i$, the compositum of fields K_i for $i \in T$. Then K_I is the genus field of K and L is a subfield of L_I. Let $G_T = \mathrm{Gal}(L_T/F)$. Each group G_T may be canonically identified (via restrictions) with the product of the groups $G_{\{i\}}$ with i running over T. Finally, let $J = \{1,\dots,t+1\}$ and $G_J = \mathrm{Gal}(L_I/\mathbb{Q})$. So G_T is also canonically (via restriction) identified with the subgroup $\mathrm{Gal}(L_I/L_{I-T})$ of G_J. For any $T \subseteq I$ we define

$$x_T = \mathrm{N}_{\mathbb{Q}(\zeta_{fm_T})/L_T}\big(z(1,fm_T)\big)^{\frac{2fm}{m_T}}. \tag{2}$$

Corollary 2.3. *The system of numbers $x_T \in L_T, T \subseteq I$, satisfies distribution relations, i.e. for any $T \subseteq I$ and any $i \in T$ we have*

$$\mathrm{N}_{L_T/L_{T-\{i\}}}(x_T) = x_{T-\{i\}}^{1-\mathrm{Frob}(p_i)^{-1}}.$$

Proof. For any $T \subseteq I$ and any $i \in T$ we have by Proposition 2.2

$$\begin{aligned}\mathrm{N}_{L_T/L_{T-\{i\}}}(x_T) &= \mathrm{N}_{\mathbb{Q}(\zeta_{fm_T})/L_{T-\{i\}}}\big(z(1,fm_T)\big)^{\frac{2fm}{m_T}} \\ &= \mathrm{N}_{\mathbb{Q}(\zeta_{fm_{T-\{i\}}})/L_{T-\{i\}}}\left(\mathrm{N}_{\mathbb{Q}(\zeta_{fm_T})/\mathbb{Q}(\zeta_{fm_{T-\{i\}}})}\big(z(1,fm_T)\big)^{\frac{2fm}{m_T}}\right) \\ &= \mathrm{N}_{\mathbb{Q}(\zeta_{fm_{T-\{i\}}})/L_{T-\{i\}}}\left(z(1,fm_{T-\{i\}})^{\frac{2fm\left(1-\mathrm{Frob}(p_i)^{-1}\right)}{m_{T-\{i\}}}}\right)\end{aligned}$$

$$= \mathrm{N}_{\mathbb{Q}(\zeta_{fm_{T-\{i\}}})/L_{T-\{i\}}}\big(z(1, fm_{T-\{i\}})\big)^{\frac{2fm\left(1-\mathrm{Frob}(p_i)^{-1}\right)}{m_{T-\{i\}}}}$$
$$= x_{T-\{i\}}^{1-\mathrm{Frob}(p_i)^{-1}}. \quad \square$$

3. Sinnott module

Recall that $J = \{1, 2, \ldots, t+1\}$ and $G_J = \mathrm{Gal}(L_I/\mathbb{Q})$. We also recall that the numbers x_T were defined by (2). Now for each $T \subseteq J$ we define

$$y_T = \begin{cases} x_{T\smallsetminus\{t+1\}}, & \text{if } t+1 \in T \\ 1, & \text{otherwise.} \end{cases}$$

Let U' be the Sinnott module defined in [3] for $v = t+1$, $T_i = G_{\{i\}}$ for $i \neq t+1$, $T_{t+1} = \mathrm{Gal}(L_I/K_I)$, $\lambda_i = \mathrm{Frob}(p_i)$ for $i \neq t+1$ and $\lambda_{t+1} = \mathrm{id}$. Since the complex conjugation τ lies in $\mathrm{Gal}(L_T/K_T)$ for each $T \subseteq I$ we have

$$\mathrm{N}_{L_T/K_T}(y_{T\cup\{t+1\}}) = \mathrm{N}_{L_T/K_T}(x_T) = 1. \tag{3}$$

Let D be the $\mathbb{Z}[G_J]$-submodule of $L_I^\times$ generated by $y_T, T \subseteq J$.

Lemma 3.1. *There is a surjective homomorphism of $\mathbb{Z}[G_J]$-modules*

$$\nu\colon U' \to D$$

determined by $\nu(\varrho'_{J-T}) = y_T$ for all $T \subseteq J$.

Proof. This follows from Corollary 2.3 and (3) using the presentation of U' given by [3, Corollary 1.6(i)]. $\square$

For any $i \in J$, the kernel of the natural map

$$\mathbb{Z}[G_J] \to \mathbb{Z}[G_J/\langle \lambda_i, T_i\rangle]$$

will be denoted by I_i. The ideal I_i is generated by $\lambda_i - 1$ and $g - 1$ for all $g \in T_i$. For any $H \subseteq G_J$ let $s(H) = \sum_{h\in H} h \in \mathbb{Z}[G_J]$.

Proposition 3.2. *Let H be a subgroup of G_J and $\varphi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}\big((U')^H, \mathbb{Z}[\Gamma]\big)$ where $\Gamma = G_J/H$.*

(i) *There is $\psi \in \mathrm{Hom}_{\mathbb{Z}[G_J]}(U', \mathbb{Z}[G_J])$ such that $\psi|_{(U')^H} = \mathrm{cor} \circ \varphi$.*
(ii) *We have*

$$\varphi\big(s(H)\rho'_\emptyset\big) \in \mathrm{res} \prod_{i=1}^{t+1} I_i,$$

where cor: $\mathbb{Z}[\Gamma] \to \mathbb{Z}[G_J]$ *and* res: $\mathbb{Z}[G_J] \to \mathbb{Z}[\Gamma]$ *means the corestriction and restriction maps, respectively.*

Proof. Part (i) can be proved in the same way as part (i) of [3, Corollary 1.7]. It follows immediately that

$$\operatorname{cor}\operatorname{res}\psi(\rho'_\emptyset) = s(H)\psi(\rho'_\emptyset) = \operatorname{cor}\varphi\big(s(H)\rho'_\emptyset\big).$$

This means that $\operatorname{res}\psi(\rho'_\emptyset) = \varphi\big(s(H)\rho'_\emptyset\big)$ because cor is injective. Using part (i) of [3, Theorem 1.1] we obtain that

$$\psi(\rho'_\emptyset) \in \prod_{i=1}^{t+1} I_i,$$

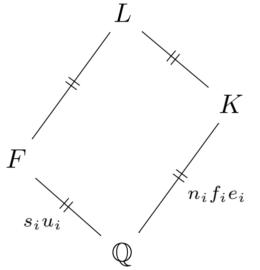
hence

$$\varphi\big(s(H)\rho'_\emptyset\big) = \operatorname{res}\psi(\rho'_\emptyset) \in \operatorname{res}\prod_{i=1}^{t+1} I_i$$

and the lemma is proved. □

4. Extracting roots

The aim of this section is to show that one may extract certain roots of modified Gauss sums. Recall that $r = [F : \mathbb{Q}]$ and $d = [K : \mathbb{Q}]$. For each $i \in I$ let n_i be the index of the decomposition group of p_i in $\mathrm{Gal}(K/\mathbb{Q})$. Let e_i be the ramification index of p_i in K. By f_i and s_i we shall denote the degree of inertia of p_i in K and F, respectively. The quotient r/s_i will be denoted by u_i. Hence n_i, u_i, and n_iu_i equals the number of prime ideals dividing p_i in K, F, and L, respectively. We have



Now we fix a generator γ of $\mathrm{Gal}(L/\mathbb{Q})$. We define

$$g_i(X) = \begin{cases} X^{n_iu_i} - 1, & \text{for } i \in I, \\ X - 1, & \text{for } i = t+1. \end{cases}$$

Lemma 4.1. *Let $H = \mathrm{Gal}(L_I/L) \subseteq G_J$. For each $i \in J$ we have*

$$\mathrm{res}\, I_i \subseteq \big(g_i(\gamma)\big)\mathbb{Z}[\langle\gamma\rangle],$$

where $\mathrm{res}\colon \mathbb{Z}[G_J] \to \mathbb{Z}[G_J/H]$ *is the restriction.*

Proof. Clearly we have $\mathrm{res}\, I_i \subseteq (\gamma - 1)\mathbb{Z}[\langle\gamma\rangle]$ for all $i \in J$. Now suppose $i \in I$. Since I_i is generated by $\mathrm{Frob}(p_i) - 1$ and $g - 1$ for all $g \in T_i$, it suffices to show that $\mathrm{res}\,\mathrm{Frob}(p_i)$ and $\mathrm{res}\, g$ lies in $\langle\gamma^{n_i u_i}\rangle$. For each $g \in T_i$ we have

$$g^{e_i} = \mathrm{id},$$

therefore

$$\mathrm{res}\, g \in \langle\gamma^{s_i u_i n_i f_i}\rangle.$$

Since s_i and $e_i f_i$ are coprime, the order of $\mathrm{res}\,\mathrm{Frob}(p_i) \in \mathrm{Gal}(L/\mathbb{Q})$ divides $s_i f_i e_i$, so

$$\mathrm{res}\,\mathrm{Frob}(p_i) \in \langle\gamma^{n_i u_i}\rangle.$$

Clearly both $\mathrm{res}\,\mathrm{Frob}(p_i)$ and all $\mathrm{res}\, g$ lie in $\langle\gamma^{n_i u_i}\rangle$ and the lemma follows. □

For each $i \in I$ let M_i be the decomposition field of p_i in L, so M_i is the maximal subfield of L where the prime p_i splits completely, and let $M_{t+1} = \mathbb{Q}$. Now define $h(X) \in \mathbb{Z}[X]$ as the least common multiple of polynomials g_i for $i \in J$. Observe that for every $j \in \mathbb{N}$ we have

$$\Phi_j(X) \mid h(X) \Rightarrow X^j - 1 \mid h(X). \tag{4}$$

We put

$$f(X) = \gcd(\tilde{g}_1, \tilde{g}_2, \ldots, \tilde{g}_{t+1}),$$

where

$$\tilde{g}_i(X) = \frac{X^{rd} - 1}{g_i(X)}.$$

Hence

$$f(X) \cdot h(X) = X^{rd} - 1.$$

Let

$$H(X) = \frac{\prod_{i=1}^{t+1} g_i(X)}{h(X)}. \tag{5}$$

Lemma 4.2. *The polynomials $H(X)$ and $f(X)$ are coprime.*

Proof. If $\Phi_j(X) \mid f(X)$ then $\Phi_j(X) \mid \tilde{g}_i(X)$ for each $i = 1, \dots, t+1$. It follows that $\Phi_j(X) \nmid g_i(X)$ for each $i = 1, \dots, t+1$. Hence $\Phi_j(X) \nmid H(X)$. □

Recall that D is the $\mathbb{Z}[G_J]$-module generated by y_T. Let $R = \mathbb{Z}[\langle\gamma\rangle]/\big(f(\gamma)\big) \cong \mathbb{Z}[X]/\big(f(X)\big)$. Then

$$\mathcal{M} = \{\alpha \in D \cap L; \alpha^{f(\gamma)} = 1\}$$

is an R-module.

Lemma 4.3. *The $\mathbb{Z}$-module $D \cap L$ has no $\mathbb{Z}$-torsion.*

Proof. Using (2), it follows from the definition of the numbers y_T that any element of D is a $2f$-th power in L_I. Therefore any $\alpha \in D \cap L$ satisfying $\alpha^c = 1$ for a positive integer c is the $2f$-th power of a root of unity in L_I. We assume $(f, m) = 1$, hence any root of unity in L_I is the product of a root of unity in F and a root of unity in K_I, and since K_I is real, such a root of unity belongs to F, and so its $2f$-th power equals 1. Thus $\alpha = 1$. □

It is easy to see that $\tilde{g}_i(\gamma)$ is the norm operator with respect to L/M_i for each $i \in J$. Let

$$\mathcal{M}_i = \{\alpha \in D \cap L; \mathrm{N}_{L/M_i}(\alpha) = 1\}.$$

Corollary 4.4. *We have $\mathcal{M} = \bigcap_{i=1}^{t+1} \mathcal{M}_i$.*

Proof. Clearly $\mathcal{M} \subseteq \bigcap_{i=1}^{t+1} \mathcal{M}_i$. Now we shall prove the other inclusion. Let $\alpha \in \bigcap_{i=1}^{t+1} \mathcal{M}_i$ be an arbitrary element. We have

$$\alpha^{\tilde{g}_i(\gamma)} = 1$$

for all $i = 1, \dots, t+1$. Using Bézout's identity in $\mathbb{Q}[X]$ we deduce that there exist polynomials $v_1, \dots, v_{t+1} \in \mathbb{Z}[X]$ and a positive integer n such that

$$v_1(X)\tilde{g}_1(X) + v_2(X)\tilde{g}_2(X) + \cdots + v_{t+1}(X)\tilde{g}_{t+1}(X) = nf(X).$$

It follows

$$\alpha^{nf(\gamma)} = \alpha^{v_1(\gamma)\tilde{g}_1(\gamma)+\cdots+v_{t+1}(\gamma)\tilde{g}_{t+1}(\gamma)} = \prod_{i=1}^{t+1} (\alpha^{\tilde{g}_i(\gamma)})^{v_i(\gamma)} = 1.$$

Since $D \cap L$ has no $\mathbb{Z}$-torsion by Lemma 4.3, we must have $\alpha^{f(\gamma)} = 1$, hence α belongs to $\mathcal{M}$. □

Lemma 4.5. *Let $z = \mathrm{N}_{L_I/L}(y_J) = \mathrm{N}_{L_I/L}(x_I)$. Then $z \in \mathcal{M}$.*

Proof. By Lemma 4.4 it is enough to show that $z \in \mathcal{M}_i$ for all $i \in J$. For $i = t+1$ we have $\tau \in \mathrm{Gal}(L_I/\mathbb{Q})$, hence

$$\mathrm{N}_{L/\mathbb{Q}}(z) = \mathrm{N}_{L_I/\mathbb{Q}}(x_I) = 1.$$

Since $L_{I-\{i\}}$ is the maximal subfield of L_I where p_i is unramified, M_i is a subfield of $L_{I-\{i\}}$ for each $i \in I$, and we have

$$\begin{aligned}\mathrm{N}_{L/M_i}(z) &= \mathrm{N}_{L_I/M_i}(x_I) = \mathrm{N}_{L_{I-\{i\}}/M_i}\big(\mathrm{N}_{L_I/L_{I-\{i\}}}(x_I)\big) \\ &= \mathrm{N}_{L_{I-\{i\}}/M_i}(x_{I-\{i\}})^{1-\mathrm{Frob}(p_i)^{-1}}\end{aligned}$$

by Corollary 2.3. Since $\mathrm{Frob}(p_i) \in \mathrm{Gal}(L/M_i)$, we have $\mathrm{N}_{L/M_i}(z) = 1$. □

Lemma 4.6. *The $\mathbb{Z}$-module $(D \cap L)/\mathcal{M}$ has no $\mathbb{Z}$-torsion.*

Proof. If any $\alpha \in D \cap L$ satisfies $\alpha^c \in \mathcal{M}$ for a positive integer c, then $\alpha^{cf(\gamma)} = (\alpha^{f(\gamma)})^c = 1$. By Lemma 4.3 the $\mathbb{Z}$-module $D \cap L$ has no $\mathbb{Z}$-torsion, hence $\alpha^{f(\gamma)} = 1$. □

Proposition 4.7. *Let $\delta = H(\gamma)$, where $H(X)$ was defined by (5). Then there is $\beta \in \mathcal{M}$ such that $z = \beta^\delta$.*

Proof. Since $H(X)$ and $f(X)$ are coprime by Lemma 4.2, it follows that $[\delta] \in R$ is a nonzerodivisor. By [4, Proposition 6.2(2)] it suffices to show that for any $\rho \in \mathrm{Hom}_R(\mathcal{M}, R)$ we have $\rho(z) \in [\delta]R$. Let $\lambda\colon R \to h(\gamma)\mathbb{Z}[\langle\gamma\rangle]$ be the isomorphism of $\mathbb{Z}[\langle\gamma\rangle]$-modules determined by $\lambda([x]) = h(\gamma)x$, where x is a representative of a class $[x] \in R$. Then

$$\lambda \circ \rho \in \mathrm{Hom}_{\mathbb{Z}[\langle\gamma\rangle]}(\mathcal{M}, \mathbb{Z}[\langle\gamma\rangle]).$$

Lemma 4.6 and [4, Proposition 6.2(1)] for $f(X) = X^{rd} - 1$ gives

$$\mathrm{Ext}^1_{\mathbb{Z}[\langle\gamma\rangle]}((D \cap L)/\mathcal{M}, \mathbb{Z}[\langle\gamma\rangle]) = 0,$$

and so there is $\phi \in \mathrm{Hom}_{\mathbb{Z}[\langle\gamma\rangle]}(D \cap L, \mathbb{Z}[\langle\gamma\rangle])$ such that $\phi|_{\mathcal{M}} = \lambda \circ \rho$. Let $H = \mathrm{Gal}(L_I/L) \subseteq G_J$. Then $G_J/H \cong \langle\gamma\rangle$, $D \cap L = D^H$ and the restriction of homomorphism ν of Lemma 3.1 gives the homomorphism $\bar{\nu}\colon (U')^H \to D^H$ satisfying $\bar{\nu}\big(s(H)\varrho'_\emptyset\big) = \mathrm{N}_{L_I/L}(y_J) = z$. Proposition 3.2 for $\varphi = \phi \circ \bar{\nu}$ together with Lemma 4.1 implies that

$$\lambda\big(\rho(z)\big) = \phi(z) = \varphi\big(s(H)\varrho'_\emptyset\big) \in \left(\prod_{i=1}^{t+1} g_i(\gamma)\right) \cdot \mathbb{Z}[\langle\gamma\rangle] = h(\gamma)\delta \cdot \mathbb{Z}[\langle\gamma\rangle].$$

This means $\rho(z) \in [\delta]R$ and the theorem follows. $\square$

5. Stickelberger ideal

For any $n \in \mathbb{N}$ and any $b \in \mathbb{Z}$ relatively prime to n let $\sigma_{b,n} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ be the automorphism determined by $\zeta_n \mapsto \zeta_n^b$. For any $n \in \mathbb{N}$ and any $a \in \mathbb{Z}$ we define

$$\theta_n(a) = \sum_{\substack{1 \le b \le n \\ (b,n)=1}} \left\langle -\frac{ab}{n} \right\rangle \sigma_{b,n}^{-1} \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})],$$

where $\langle x \rangle$ is the fractional part of the real number x, i.e., the unique real number x' satisfying $0 \le x' < 1$ and $x - x' \in \mathbb{Z}$. Let $\mathfrak{p}$ denote the prime ideal of L lying under $\mathfrak{P}$, where $\mathfrak{P}$ was introduced at the beginning of Section 2. The Stickelberger factorization of the principal ideal generated by the Gauss sum (see [8, page 99]) gives

$$g(\chi_{fm}, \psi)^{fm} \cdot \mathcal{O}_{\mathbb{Q}(\zeta_{fm})} = \mathfrak{P}^{fm\theta_{fm}(-1)}.$$

Recall that

$$x_I = \mathrm{N}_{\mathbb{Q}(\zeta_{fm})/L_I}\left(g(\chi_{fm}, \psi)^{fm(1-\tau)}\right)^{2f}.$$

It follows that

$$\mathrm{N}_{L_I/L}(x_I) \cdot \mathcal{O}_L = \mathfrak{p}^{\Theta_L}, \tag{6}$$

where

$$\Theta_L = 2f(1-\tau) \sum_{\substack{1 \le b < fm \\ (b,fm)=1}} b \cdot \mathrm{res}_{\mathbb{Q}(\zeta_{fm})/L} \sigma_{b,fm}^{-1} \in \mathbb{Z}[\langle \gamma \rangle]. \tag{7}$$

For any $n \in \mathbb{N}$ and any $a \in \mathbb{Z}$ we put

$$\theta'_n(a) = \mathrm{cor}_{L/L \cap \mathbb{Q}(\zeta_n)} \mathrm{res}_{\mathbb{Q}(\zeta_n)/L \cap \mathbb{Q}(\zeta_n)} \theta_n(a) \in \mathbb{Q}[\langle \gamma \rangle]. \tag{8}$$

Let $S' \subseteq \mathbb{Q}[\langle \gamma \rangle]$ be the abelian group generated by all the elements $\theta'_n(a)$ for all $n \ge 1$ and all $a \in \mathbb{Z}$. In fact, S' is a $\mathbb{Z}[\langle \gamma \rangle]$-module and it follows from [6, Remark following Lemma 15] that this module is generated by

$$\{\theta'_n(-1); n \mid fm\} \cup \{\tfrac{1}{2}N_1\}, \tag{9}$$

where $N_1 = \sum_{i=1}^{rd} \gamma^i$. The Sinnott's Stickelberger ideal S of L is defined by $S = S' \cap \mathbb{Z}[\langle \gamma \rangle]$ and this ideal annihilates $\mathrm{Cl}(L)$, the ideal class group of L, see [7, Theorem 3.1]. The equality $S' = S$ does not hold in general. Nevertheless, for each prime $q \nmid 2fm$ all the generators (9) belong to $\mathbb{Z}_q[\langle\gamma\rangle]$, hence we have $S_q = S'_q$, where $S_q = S\mathbb{Z}_q[\langle\gamma\rangle]$ and $S'_q = S'\mathbb{Z}_q[\langle\gamma\rangle]$.

Let $e^- = \frac{1}{2}(1-\tau) \in \mathbb{Q}[\langle\gamma\rangle]$. When $L\cap\mathbb{Q}(\zeta_n)$ is real, we have $\theta'_n(-1) = \frac{\varphi(n)}{2[L\cap\mathbb{Q}(\zeta_n)\colon\mathbb{Q}]}N_1$. Since $e^-N_1 = 0$, it follows that the module e^-S' is generated by

$$\{e^-\theta'_n(-1); n \mid fm, L\cap\mathbb{Q}(\zeta_n) \text{ is imaginary}\}.$$

We finish this section by determining the $\mathbb{Z}$-rank of e^-S' which we shall use later on. It follows from [7, Theorem 2.1] and [7, Proposition 2.1] that

$$\operatorname{rank}_{\mathbb{Z}} S' = \frac{1}{2}[L\colon\mathbb{Q}] + 1.$$

Then [7, Lemma 2.1] implies

$$\operatorname{rank}_{\mathbb{Z}} e^-S' = \frac{1}{2}[L\colon\mathbb{Q}].$$

6. Construction of a new annihilator

Recall that $\mathfrak{P}$ is an unramified prime of $\mathbb{Q}(\zeta_{fm})$ of absolute degree 1, $\mathfrak{p} = \mathfrak{P}\cap\mathcal{O}_L$ and p is the prime number below $\mathfrak{P}$. The principal ideal of $\mathcal{O}_{L_I}$ generated by any element of D is supported only on conjugates of $\mathfrak{P}\cap L_I$. Therefore for β from Proposition 4.7 there is $\xi \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\beta\cdot\mathcal{O}_L = \mathfrak{p}^{\xi}. \tag{10}$$

Hence

$$z\cdot\mathcal{O}_L = \mathfrak{p}^{\delta\xi}$$

and the comparison with (6) gives

$$\delta\xi = \Theta_L. \tag{11}$$

Since p splits completely in $L/\mathbb{Q}$, this ξ is unique and the equality $\beta^{f(\gamma)} = 1$ implies that

$$f(\gamma)\cdot\xi = 0.$$

It follows that there exists $\xi' \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\xi = h(\gamma)\cdot\xi'. \tag{12}$$

The polynomial $H(X)$ defined by (5) can be written uniquely in the form

$$H(X)=\prod_{j\mid rd}\Phi_j(X)^{a_j}$$

for suitable nonnegative integers a_j, so we have

$$\delta=\prod_{j\mid rd}\Phi_j(\gamma)^{a_j}. \tag{13}$$

For each divisor j of rd let

$$N_j=\sum_{i=1}^{rd/j}\gamma^{ij}\quad\text{and}\quad\Delta_j=\sum_{i=1}^{(rd/j)-1}i\gamma^{ij},$$

so $(1-\gamma^j)N_j=0$ and $(1-\gamma^j)\Delta_j=N_j-\frac{rd}{j}$.

Proposition 6.1. *The equalities (11) and (12) determine $\xi\in\mathbb{Z}[\langle\gamma\rangle]$ uniquely, in fact*

$$\xi=\Theta_L\cdot\prod_{j\mid rd}\Big(\frac{j}{rd}\Delta_j\prod_{\substack{i\mid j\\ i\neq j}}\Phi_i(\gamma)\Big)^{a_j}. \tag{14}$$

Proof. Equalities (11) and (13) imply

$$\Theta_L\cdot\prod_{j\mid rd}\Big(\Delta_j\prod_{\substack{i\mid j\\ i\neq j}}\Phi_i(\gamma)\Big)^{a_j}=\delta\xi\cdot\prod_{j\mid rd}\Big(\Delta_j\prod_{\substack{i\mid j\\ i\neq j}}\Phi_i(\gamma)\Big)^{a_j}=$$
$$=\xi\cdot\prod_{j\mid rd}\Big(\Delta_j(\gamma^j-1)\Big)^{a_j}=\xi\cdot\prod_{j\mid rd}\Big(\frac{rd}{j}-N_j\Big)^{a_j}.$$

If $a_j\neq 0$ then $\Phi_j(X)\mid h(X)$. By (4) we have $(X^j-1)\mid h(X)$, hence $(\gamma^j-1)\mid h(\gamma)$. It follows that

$$N_jh(\gamma)=0 \tag{15}$$

whenever $a_j\neq 0$, and so (12) gives

$$\Theta_L\cdot\prod_{j\mid rd}\Big(\Delta_j\prod_{\substack{i\mid j\\ i\neq j}}\Phi_i(\gamma)\Big)^{a_j}=\xi\cdot\prod_{j\mid rd}\Big(\frac{rd}{j}\Big)^{a_j}$$

and the proposition follows. □

Let M be an abelian field. By $\mathrm{Cl}(M)_q$ we shall denote the q-Sylow subgroup of the ideal class group $\mathrm{Cl}(M)$ of M. For every odd q and every $\mathbb{Z}_q[\mathrm{Gal}(M/\mathbb{Q})]$-module A we define $A^-=\frac{1-\tau}{2}A$ and $A^+=\frac{1+\tau}{2}A$.

Proposition 6.2. *Let q be an odd prime. The element $\xi \in \mathbb{Z}[\langle\gamma\rangle]$ given by (14) is an annihilator of* $\mathrm{Cl}(L)_q^-$.

Proof. The natural map $\mathrm{Cl}\big(\mathbb{Q}(\zeta_{fm})\big)_q^- \to \mathrm{Cl}(L)_q^-$ is surjective by [2, Lemma 1.6(a)], and so every element in $\mathrm{Cl}(L)_q^-$ is represented by some prime $\mathfrak{p}$ of L lying under an unramified prime $\mathfrak{P}$ of $\mathbb{Q}(\zeta_{fm})$ of absolute degree 1, by Čebotarev's Density Theorem applied to $\mathbb{Q}(\zeta_{fm})$. Proposition 6.1 implies that ξ does not depend on $\mathfrak{p}$ and (10) shows that ξ annihilates the element of $\mathrm{Cl}(L)_q^-$ represented by $\mathfrak{p}$. $\square$

Let $\mathcal{L}$ be the lattice of all imaginary subfields of L ordered by inclusion. For every $M \in \mathcal{L}$ we define

$$\varkappa_M = \mathrm{cor}_{L/M}\Theta_M \in \mathbb{Z}[\langle\gamma\rangle],$$

where Θ_M means Θ_L of (7) for M instead of L. We also define

$$\xi_M = \mathrm{cor}_{L/M}\xi^M \in \mathbb{Z}[\langle\gamma\rangle],$$

where ξ^M means ξ of Proposition 6.1 for the field M instead of L. Let $Z = \{M_1, M_2, \ldots, M_n\} \subseteq \mathcal{L}$ be a lower set, i.e. a set with the property that, if M is in Z, $M' \in \mathcal{L}$, and $M' \subseteq M$, then M' is in Z. We define the following ideals of $\mathbb{Z}[\langle\gamma\rangle]$:

$$\mathcal{I}^Z = (\varkappa_{M_1}, \varkappa_{M_2}, \ldots, \varkappa_{M_n}) \qquad \text{and} \qquad \mathcal{J}^Z = (\xi_{M_1}, \xi_{M_2}, \ldots, \xi_{M_n}).$$

Recall that for every ideal $A \subseteq \mathbb{Z}[\langle\gamma\rangle]$ the ideal $A\mathbb{Z}_q[\langle\gamma\rangle]$ is denoted by A_q.

Proposition 6.3. *The ideal $\mathcal{I}^{\mathcal{L}}$ has the following properties:*

1. $\mathcal{I}^{\mathcal{L}}$ *annihilates* $\mathrm{Cl}(L)$.
2. $\mathcal{I}_q^{\mathcal{L}} = S_q^-$ *for every odd prime number q not dividing fm.*
3. $\mathrm{rank}_{\mathbb{Z}}\mathcal{I}^{\mathcal{L}} = \frac{1}{2}[L\colon \mathbb{Q}]$.

Proof. Let $n \mid fm$ and suppose that $L \cap \mathbb{Q}(\zeta_n)$ is imaginary. Using (7) and (8) we obtain

$$\varkappa_{L\cap\mathbb{Q}(\zeta_n)} = 2f_n n(1-\tau)\theta'_n(-1), \tag{16}$$

where f_n is the conductor of $F \cap \mathbb{Q}(\zeta_n)$. Suppose $M \in \mathcal{L}$ is a field of conductor n. Then we have

$$\varkappa_M = f(\gamma)\varkappa_{L\cap\mathbb{Q}(\zeta_n)},$$

where

$$f(X) = \frac{X^{[L\cap\mathbb{Q}(\zeta_n)\colon \mathbb{Q}]} - 1}{X^{[M\colon \mathbb{Q}]} - 1} \in \mathbb{Z}[X].$$

It means that $\mathcal{I}^{\mathcal{L}}$ is generated as a $\mathbb{Z}[\langle\gamma\rangle]$-module by

$$\{\varkappa_{L\cap\mathbb{Q}(\zeta_n)}; n \mid fm, L\cap\mathbb{Q}(\zeta_n) \text{ is imaginary}\}.$$

Recall that $e^- S'$ is generated as a $\mathbb{Z}[\langle\gamma\rangle]$-module by

$$\{\tfrac{1}{2}(1-\tau)\theta'_n(-1); n \mid fm, L\cap\mathbb{Q}(\zeta_n) \text{ is imaginary}\}.$$

It follows $\mathcal{I}^{\mathcal{L}} \subseteq e^- S' \cap \mathbb{Z}[\langle\gamma\rangle] \subseteq S$ using [7, Lemma 2.1], hence $\mathcal{I}^{\mathcal{L}}$ annihilates $\mathrm{Cl}(L)$ using [7, Theorem 3.1]. The quotient group $e^- S'/\mathcal{I}^{\mathcal{L}}$ is clearly finitely generated and by (16) torsion, hence it is finite. Therefore $\mathrm{rank}_{\mathbb{Z}}\mathcal{I}^{\mathcal{L}} = \mathrm{rank}_{\mathbb{Z}} e^- S' = \frac{1}{2}[L\colon\mathbb{Q}]$. Since $S_q = S'_q$ and $|e^- S'/\mathcal{I}^{\mathcal{L}}|$ is a unit in $\mathbb{Z}_q$ for every prime number $q \nmid 2fm$, we obtain $\mathcal{I}^{\mathcal{L}}_q = (e^- S')_q = (S'_q)^- = S^-_q$. $\square$

7. Relations among generators

In this section we derive relations that are satisfied by the numbers $\varkappa_M$ and ξ_M. These relations will be needed for calculating the index $[\mathcal{J}^{\mathcal{L}} : \mathcal{I}^{\mathcal{L}}]$. Let $M \in \mathcal{L}$ be an imaginary subfield of L of degree $s = [M\colon\mathbb{Q}]$. The conductor of M is $f_M m_{I_M}$, where f_M is the conductor of $F \cap M$ and $I_M \subseteq I$ is defined by

$$I_M = \{i \in I; p_i \text{ is ramified in } M \cap K\},$$

because m_{I_M} is the conductor of $K \cap M$ and M is equal to the compositum of $F \cap M$ and $K \cap M$. Let

$$z_M = N_{\mathbb{Q}(\zeta_{f_M m_{I_M}})/E_M}\big(z(1, f_M m_{I_M})\big)^{2f_M},$$

where $E_M = (M \cap F)K_{I_M}$ and $z(1, f_M m_{I_M})$ is defined by (1). Note that $I_L = I$ and $x_I = z_L$. We define $\theta^M \in \mathbb{Z}[\mathrm{Gal}(E_M/\mathbb{Q})]$ by

$$z_M \cdot \mathcal{O}_{E_M} = (\mathfrak{P} \cap E_M)^{\theta^M}. \tag{17}$$

We have

$$\Theta_M = \mathrm{res}_{E_M/M}\theta^M.$$

Recall that

$$\varkappa_M = \mathrm{cor}_{L/M}\Theta_M \qquad \text{and} \qquad \xi_M = \mathrm{cor}_{L/M}\xi^M,$$

where ξ^M means ξ of Proposition 6.1 for the field M instead of L. For each $i \in I_M$ let g_i^M be the polynomial g_i for M instead of L, so we have

$$g_i^M(X) = X^{n_i \gcd(u_i,s)} - 1,$$

where $s = [M\colon \mathbb{Q}]$. Note that $\gcd(u_i, s)$ is the number of prime ideals dividing p_i in $M \cap F$. Let h_M be the least common multiple of polynomials $X-1$ and g_i^M for $i \in I_M$. We set

$$H_M(X) = \frac{(X-1) \cdot \prod_{i \in I_M} g_i^M(X)}{h_M(X)}.$$

The equality (12) applied for M gives us $\alpha \in \mathbb{Z}[\mathrm{Gal}(M/\mathbb{Q})]$ such that

$$\xi^M = h_M\big(\mathrm{res}_{L/M}(\gamma)\big)\alpha = \alpha \cdot \mathrm{res}_{L/M}\big(h_M(\gamma)\big).$$

It follows that

$$\xi_M = \mathrm{cor}_{L/M}(\xi^M) = \mathrm{cor}_{L/M}\Big(\alpha \cdot \mathrm{res}_{L/M}\big(h_M(\gamma)\big)\Big) = h_M(\gamma)\mathrm{cor}_{L/M}(\alpha), \tag{18}$$

hence $h_M(\gamma) \mid \xi_M$ in $\mathbb{Z}[\langle\gamma\rangle]$. Let δ^M be δ of Proposition 4.7 for the field M instead of L. We define

$$\delta_M = H_M(\gamma).$$

It follows that

$$\delta^M = H_M\big(\mathrm{res}_{L/M}(\gamma)\big) = \mathrm{res}_{L/M}\delta_M,$$

so by (11) we have

$$\varkappa_M = \mathrm{cor}_{L/M}\Theta_M = \mathrm{cor}_{L/M}\big(\delta^M \cdot \xi^M\big) = \mathrm{cor}_{L/M}\big(\mathrm{res}_{L/M}(\delta_M) \cdot \xi^M\big) = \delta_M \xi_M. \tag{19}$$

Let $M, M' \in \mathcal{L}$ be two imaginary fields and denote their absolute degrees by s and s', respectively. Suppose that $M' \subseteq M$. We set

$$\mathcal{N}^{M/M'}(X) = \frac{\prod_{j|s} \Phi_j(X)}{\prod_{j|s'} \Phi_j(X)} = \sum_{j=0}^{\frac{s}{s'}-1} X^{js'} \in \mathbb{Z}[X],$$

so $\mathrm{res}_{L/M}\mathcal{N}^{M/M'}(\gamma) = \mathcal{N}^{M/M'}(\mathrm{res}_{L/M}\gamma)$ is the norm operator from M to M'. The following proposition describes a relation between $\varkappa_M$ and $\varkappa_{M'}$. The set of all primes that are ramified in M is denoted by S_M.

Proposition 7.1. *Let $M, M' \in \mathcal{L}$ and suppose $M' \subseteq M$. Then we have*

$$\mathcal{N}^{M/M'}(\gamma)\varkappa_M = \frac{f_M^2 m_{I_M}}{f_{M'}^2 m_{I_{M'}}}\Bigg(\prod_{q \in S_M \smallsetminus S_{M'}} \big(1 - \mathrm{Frob}(q)^{-1}\big)\Bigg)\varkappa_{M'}.$$

Proof. It follows from (17) that

$$N_{E_M/E_{M'}}(z_M) \cdot \mathcal{O}_{E_{M'}} = (\mathfrak{P} \cap E_{M'})^{\mathrm{res}_{E_M/E_{M'}} \theta^M}. \tag{20}$$

However, the number $N_{E_M/E_{M'}}(z_M)$ can also be computed using the distribution relations for Gauss sums from Proposition 2.2

$$N_{E_M/E_{M'}}(z_M) = z_{M'}^{\frac{f_M^2 m_{I_M}}{f_{M'}^2 m_{I_{M'}}} \cdot \prod_{q \in S_M \smallsetminus S_{M'}} (1-\mathrm{Frob}(q)^{-1})}.$$

Hence we have

$$N_{E_M/E_{M'}}(z_M) \cdot \mathcal{O}_{E_{M'}} = (\mathfrak{P} \cap E_{M'})^{\theta^{M'} \cdot \frac{f_M^2 m_{I_M}}{f_{M'}^2 m_{I_{M'}}} \cdot \prod_{q \in S_M \smallsetminus S_{M'}} (1-\mathrm{Frob}(q)^{-1})}$$

and the comparison with (20) gives

$$\mathrm{res}_{E_M/E_{M'}} \theta^M = \theta^{M'} \cdot \frac{f_M^2 m_{I_M}}{f_{M'}^2 m_{I_{M'}}} \cdot \prod_{q \in S_M \smallsetminus S_{M'}} (1 - \mathrm{Frob}(q)^{-1}).$$

Applying $\mathrm{res}_{E_{M'}/M'}$ to both sides gives

$$\mathrm{res}_{E_M/M'} \theta^M = \frac{f_M^2 m_{I_M}}{f_{M'}^2 m_{I_{M'}}} \cdot \Theta_{M'} \cdot \prod_{q \in S_M \smallsetminus S_{M'}} (1 - \mathrm{Frob}(q)^{-1}).$$

Now we apply $\mathrm{cor}_{L/M'}$ and we obtain

$$\mathrm{cor}_{L/M'} \mathrm{res}_{E_M/M'} \theta^M = \frac{f_M^2 m_{I_M}}{f_{M'}^2 m_{I_{M'}}} \Bigg(\prod_{q \in S_M \smallsetminus S_{M'}} (1 - \mathrm{Frob}(q)^{-1}) \Bigg) \varkappa_{M'}.$$

The left-hand side can be further simplified

$$\begin{aligned} \mathrm{cor}_{L/M'} \mathrm{res}_{E_M/M'} \theta^M &= \mathrm{cor}_{L/M} \mathrm{cor}_{M/M'} \mathrm{res}_{M/M'} \mathrm{res}_{E_M/M} \theta^M \\ &= \mathrm{cor}_{L/M} \mathrm{cor}_{M/M'} \mathrm{res}_{M/M'} \Theta_M \\ &= \mathrm{cor}_{L/M} \big(\Theta_M \cdot \mathrm{res}_{L/M} \mathcal{N}^{M/M'}(\gamma) \big) = \mathcal{N}^{M/M'}(\gamma) \varkappa_M \end{aligned}$$

and the result follows. □

The polynomial $H_M(X)$ can be uniquely written in the form

$$H_M(X) = \prod_{j|s} \Phi_j(X)^{a_{M,j}},$$

where $a_{M,j}$ are nonnegative integers depending only on M and j. The following lemma shows how to compute the numbers $a_{M,j}$.

Lemma 7.2. *For every $M \in \mathcal{L}$ and $j \in \mathbb{N}$ we have*

$$a_{M,j} = \begin{cases} 0, & \text{for } j \nmid [M\colon \mathbb{Q}] \\ |I_M|, & \text{for } j = 1 \\ \max\{0, |\{i \in I_M; j \mid n_i u_i\}| - 1\}, & \text{otherwise.} \end{cases}$$

Proof. It follows from the definition of $a_{M,j}$. □

Proposition 7.3. *Let $M, M' \in \mathcal{L}$ and suppose $M' \subseteq M$ with $[M\colon M'] = \ell^n$ for some $n \in \mathbb{N}$. Then we have*

$$\mathcal{N}^{M/M'}(\gamma)\xi_M \in \xi_{M'}\mathbb{Z}[\langle\gamma\rangle].$$

Proof. Let us denote the degrees $[M\colon \mathbb{Q}]$ and $[M'\colon \mathbb{Q}]$ by s and s', respectively. We shall further denote $\frac{f_M^2 m_{I_M}}{f_{M'}^2 m_{I_{M'}}} \in \mathbb{N}$ by b. By Proposition 7.1 we have

$$\mathcal{N}^{M/M'}(\gamma)\varkappa_M = b\Bigg(\prod_{q \in S_M \smallsetminus S_{M'}} \big(1 - \mathrm{Frob}(q)^{-1}\big)\Bigg)\varkappa_{M'},$$

which together with the equality (19) gives

$$\mathcal{N}^{M/M'}(\gamma)\delta_M\xi_M = b\Bigg(\prod_{q \in S_M \smallsetminus S_{M'}} \big(1 - \mathrm{Frob}(q)^{-1}\big)\Bigg)\delta_{M'}\xi_{M'}.$$

By assumption, the degree $[M\colon M']$ is a power of ℓ. It follows that

$$S_M \smallsetminus S_{M'} = \{p_i; i \in I_M \smallsetminus I_{M'}\}.$$

Hence

$$\prod_{q \in S_M \smallsetminus S_{M'}} \big(1 - \mathrm{Frob}(q)^{-1}\big) = \prod_{i \in I_M \smallsetminus I_{M'}} \big(1 - \mathrm{Frob}(p_i)^{-1}\big).$$

It also follows that $\gcd(u_i, s) = \gcd(u_i, s')$ for every $i \in I$, so

$$g_i^M = g_i^{M'} \qquad \text{for every } i \in I_{M'}.$$

Since $\mathrm{Frob}(p_i)$ lies in $\langle\gamma^{n_i u_i}\rangle$ and $g_i^M = X^{n_i \gcd(u_i,s)} - 1$ divides $X^{n_i u_i} - 1$ for each $i \in I_M$, there exists $\omega \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$b \prod_{i \in I_M \smallsetminus I_{M'}} \big(1 - \mathrm{Frob}(p_i)^{-1}\big) = \Bigg(\prod_{i \in I_M \smallsetminus I_{M'}} g_i^M(\gamma)\Bigg)\omega.$$

The equality (18) applied for M and M' gives us $\alpha \in \mathbb{Z}[\mathrm{Gal}(M/\mathbb{Q})]$ and $\alpha' \in \mathbb{Z}[\mathrm{Gal}(M'/\mathbb{Q})]$ such that

$$\xi_M = h_M(\gamma)\mathrm{cor}_{L/M}(\alpha) \qquad \text{and} \qquad \xi_{M'} = h_{M'}(\gamma)\mathrm{cor}_{L/M'}(\alpha'). \tag{21}$$

Therefore we have

$$\mathcal{N}^{M/M'}(\gamma)\delta_M h_M(\gamma)\mathrm{cor}_{L/M}(\alpha) = \Bigg(\prod_{i\in I_M \smallsetminus I_{M'}} g_i^M(\gamma)\Bigg)\omega\delta_{M'}h_{M'}(\gamma)\mathrm{cor}_{L/M'}(\alpha').$$

Recall that $\delta_{M'} = H_{M'}(\gamma)$, where

$$H_{M'}(X) = \frac{(X-1)\prod_{i\in I_{M'}} g_i^{M'}(X)}{h_{M'}(X)}.$$

It follows that

$$\delta_{M'}h_{M'}(\gamma) = H_{M'}(\gamma)h_{M'}(\gamma) = (\gamma-1)\prod_{i\in I_{M'}} g_i^{M'}(\gamma) = (\gamma-1)\prod_{i\in I_{M'}} g_i^{M}(\gamma).$$

Putting all this together we obtain

$$\mathcal{N}^{M/M'}(\gamma)\delta_M h_M(\gamma)\mathrm{cor}_{L/M}(\alpha) = \delta_M h_M(\gamma)\omega\mathrm{cor}_{L/M'}(\alpha'). \tag{22}$$

Now we use the same trick as in Proposition 6.1. For every $j \mid s$ let

$$N_j^M = \sum_{i=1}^{s/j}\gamma^{ij} \qquad \text{and} \qquad \Delta_j^M = \sum_{i=1}^{(s/j)-1} i\gamma^{ij}.$$

We define $\Lambda_M \in \mathbb{Z}[\langle\gamma\rangle]$ by

$$\Lambda_M = \prod_{j\mid s}\Big(\Delta_j^M \prod_{\substack{i\mid j\\ i\neq j}}\Phi_i(\gamma)\Big)^{a_{M,j}} \in \mathbb{Z}[\langle\gamma\rangle].$$

Recall that $\delta_M = H_M(\gamma) = \prod\limits_{j\mid s}\Phi_j(\gamma)^{a_{M,j}}$. Since

$$(\gamma^j - 1)\Delta_j^M = \left(\frac{s}{j}-1\right)\gamma^s - \sum_{i=1}^{s/j-1}\big(i-(i-1)\big)\gamma^{ij} = \frac{s}{j}\gamma^s - \sum_{i=1}^{s/j}\gamma^{ij} = \frac{s}{j}\gamma^s - N_j^M,$$

it follows that

$$\Lambda_M\delta_M = \prod_{j\mid s}\Big(\Delta_j^M(\gamma^j-1)\Big)^{a_{M,j}} = \prod_{j\mid s}\Big(\frac{s}{j}\gamma^s - N_j^M\Big)^{a_{M,j}}.$$

The equation (15) applied for M instead of L gives us that

$$\operatorname{res}_{L/M}\big(N_j^M h_M(\gamma)\big) = 0,$$

so we have

$$\operatorname{res}_{L/M}\Bigg(\Lambda_M \delta_M h_M(\gamma)\Bigg) = \operatorname{res}_{L/M}\Bigg(h_M(\gamma)\prod_{j|s}\Big(\frac{s}{j}\Big)^{a_{M,j}}\Bigg).$$

Therefore

$$\mathcal{N}^{M/M'}(\gamma)\delta_M h_M(\gamma)\operatorname{cor}_{L/M}(\alpha)\Lambda_M = \mathcal{N}^{M/M'}(\gamma)h_M(\gamma)\operatorname{cor}_{L/M}(\alpha)\prod_{j|s}\Big(\frac{s}{j}\Big)^{a_{M,j}}$$

and also

$$\delta_M h_M(\gamma)\omega\operatorname{cor}_{L/M'}(\alpha')\Lambda_M = \omega h_M(\gamma)\operatorname{cor}_{L/M'}(\alpha')\prod_{j|s}\Big(\frac{s}{j}\Big)^{a_{M,j}}.$$

Multiplying both sides of the equation (22) by Λ_M we thus obtain

$$\mathcal{N}^{M/M'}(\gamma)\xi_M\prod_{j|s}\Big(\frac{s}{j}\Big)^{a_{M,j}} = h_M(\gamma)\omega\operatorname{cor}_{L/M'}(\alpha')\prod_{j|s}\Big(\frac{s}{j}\Big)^{a_{M,j}}.$$

The number $\prod_{j|s}\big(\frac{s}{j}\big)^{a_{M,j}} \in \mathbb{N}$ is a nonzerodivisor in $\mathbb{Z}[\langle\gamma\rangle]$ and $h_M(X)$ is divisible by $h_{M'}(X)$, so there exists an element $\varrho \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\mathcal{N}^{M/M'}(\gamma)\xi_M = h_M(\gamma)\omega\operatorname{cor}_{L/M'}(\alpha') = \varrho h_{M'}(\gamma)\omega\operatorname{cor}_{L/M'}(\alpha') = \varrho\omega\xi_{M'}$$

and the proposition is proved. □

Proposition 7.4. *Let $M, M' \in \mathcal{L}$ and suppose $M' \subseteq M$ with $\ell \nmid [M\colon M']$. Then we have*

$$\mathcal{N}^{M/M'}(\gamma)\xi_M \in \xi_{M'}\mathbb{Z}_q[\langle\gamma\rangle]$$

for every prime number $q \nmid [M\colon M']$.

Proof. We derive, as in the proof of Proposition 7.3, that there exist $\alpha \in \mathbb{Z}[\mathrm{Gal}(M/\mathbb{Q})]$, $\alpha' \in \mathbb{Z}[\mathrm{Gal}(M'/\mathbb{Q})]$ such that (21) and that

$$\mathcal{N}^{M/M'}(\gamma)\delta_M h_M(\gamma)\operatorname{cor}_{L/M}(\alpha) = \beta\delta_{M'}h_{M'}(\gamma)\operatorname{cor}_{L/M'}(\alpha'), \tag{23}$$

for suitable $\beta \in \mathbb{Z}[\langle\gamma\rangle]$. By assumption, the degree $[M\colon M']$ is not divisible by ℓ, hence $M \cap K = M' \cap K$. It follows that $I_M = I_{M\cap K} = I_{M'\cap K} = I_{M'}$, so we can write

$$\frac{H_M(X)h_M(X)}{H_{M'}(X)h_{M'}(X)} = \prod_{i \in I_M} \frac{g_i^M(X)}{g_i^{M'}(X)} \in \mathbb{Z}[X].$$

Now recall that

$$\mathcal{N}^{M/M'}(X) = \prod_{\substack{j|s \\ j\nmid s'}} \Phi_j(X),$$

where $s = [M : \mathbb{Q}]$ and $s' = [M' : \mathbb{Q}]$. Since $\frac{g_i^M}{g_i^{M'}} \Big| \mathcal{N}^{M/M'}$ for every $i \in I_M$, we conclude that there exists $v \in \mathbb{Z}[X]$ such that

$$\big(\mathcal{N}^{M/M'}(X)\big)^{|I_M|} H_{M'}(X)h_{M'}(X) = v(X)H_M(X)h_M(X).$$

Therefore we have

$$\big(\mathcal{N}^{M/M'}(\gamma)\big)^{|I_M|} \delta_{M'}h_{M'}(\gamma) = v(\gamma)\delta_M h_M(\gamma).$$

Multiplying both sides of the equality (23) by $\big(\mathcal{N}^{M/M'}(\gamma)\big)^{|I_M|}$ we obtain

$$\big(\mathcal{N}^{M/M'}(\gamma)\big)^{|I_M|+1} \delta_M h_M(\gamma)\mathrm{cor}_{L/M}(\alpha) = \beta v(\gamma)\delta_M h_M(\gamma)\mathrm{cor}_{L/M'}(\alpha').$$

By the same reasoning as we used at the end of the proof of Proposition 7.3, we have

$$\big(\mathcal{N}^{M/M'}(\gamma)\big)^{|I_M|+1} \xi_M = \beta'\xi_{M'}$$

for suitable $\beta' \in \mathbb{Z}[\langle\gamma\rangle]$. Since $\mathrm{res}_{L/M}\left(\mathcal{N}^{M/M'}(\gamma)\right)$ is the norm operator from M to M', it follows that

$$\mathrm{res}_{L/M}\left(\big(\mathcal{N}^{M/M'}(\gamma)\big)^{|I_M|+1}\right) = \left(\frac{s}{s'}\right)^{|I_M|} \mathrm{res}_{L/M}\left(\mathcal{N}^{M/M'}(\gamma)\right).$$

Consequently,

$$\big(\mathcal{N}^{M/M'}(\gamma)\big)^{|I_M|+1} \xi_M = \left(\frac{s}{s'}\right)^{|I_M|} \mathcal{N}^{M/M'}(\gamma)\xi_M.$$

The number $\frac{s}{s'}$ is not divisible by q. Therefore the number $\left(\frac{s}{s'}\right)^{|I_M|}$ is a unit in $\mathbb{Z}_q$, so we have

$$\mathcal{N}^{M/M'}(\gamma)\xi_M = \left(\frac{s'}{s}\right)^{|I_M|} \beta'\xi_{M'},$$

where $(s'/s)^{|I_M|}\beta' \in \mathbb{Z}_q[\langle\gamma\rangle]$. $\square$

In what follows, we shall suppose that $q = 2$ or q is an odd prime not dividing $r = [F : \mathbb{Q}]$.

Corollary 7.5. *Let $M, M' \in \mathcal{L}$ and suppose $M' \subseteq M$. Then we have*

$$\mathcal{N}^{M/M'}(\gamma)\xi_M \in \xi_{M'}\mathbb{Z}_q[\langle\gamma\rangle].$$

Proof. Let T denote the compositum of M' and $M \cap K$. This is the unique subfield of M containing M' such that $[M : T]$ is not divisible by ℓ and $[T : M']$ is a power of ℓ. Clearly we have

$$\mathcal{N}^{M/M'}(X) = \mathcal{N}^{M/T}(X) \cdot \mathcal{N}^{T/M'}(X)$$

and the result follows from Proposition 7.3 and Proposition 7.4. $\square$

Lemma 7.6. *Let $M \in \mathcal{L}$ be an arbitrary field of degree $s = [M : \mathbb{Q}]$. Then we have*

$$(\gamma^{\frac{s}{2}} + 1) \cdot \varkappa_M = (\gamma^{\frac{s}{2}} + 1) \cdot \xi_M = 0.$$

Proof. It follows from Proposition 6.1 that there exists $\alpha \in \mathbb{Q}[\mathrm{Gal}(M/\mathbb{Q})]$ such that

$$\xi_M = \mathrm{cor}_{L/M}(\Theta_M \cdot \alpha).$$

Hence we have

$$\begin{aligned}(\gamma^{\frac{s}{2}} + 1) \cdot \xi_M &= (\gamma^{\frac{s}{2}} + 1) \cdot \mathrm{cor}_{L/M}(\Theta_M \cdot \alpha)\\ &= \mathrm{cor}_{L/M}\big(\mathrm{res}_{L/M}(\gamma^{\frac{s}{2}} + 1) \cdot \Theta_M \cdot \alpha\big)\\ &= \mathrm{cor}_{L/M}\Big(\mathrm{res}_{E_M/M}\big((1+\tau) \cdot \theta^M\big) \cdot \alpha\Big) = 0\end{aligned}$$

and the result follows. $\square$

Let $M \in \mathcal{L}$ be a field of degree $s = [M : \mathbb{Q}]$. The set of all subfields of M that lie in $\mathcal{L}$, will be denoted by $Z(M)$. We define $\mathcal{F}_M \in \mathbb{Z}[X]$ to be the greatest common divisor of $X^{\frac{s}{2}} + 1$ and $\mathcal{N}^{M/M'}$ for all $M' \in Z(M) \setminus \{M\}$. Since $M/\mathbb{Q}$ is cyclic, it follows that for every $j \mid s$, $j \nmid \frac{s}{2}$, $j \neq s$ there exists $M' \in Z(M) \setminus \{M\}$ such that $\Phi_j \nmid \mathcal{N}^{M/M'}$. Therefore we have

$$\mathcal{F}_M(X) = \Phi_s(X). \tag{24}$$

Lemma 7.7. *For every $M \in \mathcal{L}$ we have*

$$\sum_{T \in Z(M)} \deg \mathcal{F}_T = \frac{1}{2}[M : \mathbb{Q}].$$

Proof. Since M is imaginary, the degree $[M\colon \mathbb{Q}]$ is even. Write $[M\colon \mathbb{Q}] = 2^a b$ with $a > 0$ and b odd. Then

$$\sum_{T\in Z(M)} \deg \mathcal{F}_T = \sum_{\substack{s|2^a b\\ 2^a|s}} \varphi(s) = \sum_{s|b} \varphi(2^a)\varphi(s) = \varphi(2^a)b = 2^{a-1}b = \frac{1}{2}[M\colon \mathbb{Q}],$$

as desired. □

Proposition 7.8. *Let $Z = \{M_1, M_2, \dots, M_n\} \subseteq \mathcal{L}$ be a non-empty lower set and let M_1 be a maximal element of Z. Suppose that $q = 2$ or q is an odd prime not dividing r. If $n \geq 2$, then we have*

$$\mathcal{F}_{M_1}(\gamma)\varkappa_{M_1} \in \mathcal{I}_q^{Z\smallsetminus\{M_1\}} \qquad \textit{and} \qquad \mathcal{F}_{M_1}(\gamma)\xi_{M_1} \in \mathcal{J}_q^{Z\smallsetminus\{M_1\}}.$$

If $n = 1$ then we have

$$\mathcal{F}_{M_1}(\gamma)\varkappa_{M_1} = \mathcal{F}_{M_1}(\gamma)\xi_{M_1} = 0.$$

Proof. Let us denote the degree $[M_i\colon \mathbb{Q}]$ by s_i. If $n = 1$, then $\mathcal{F}_{M_1}(X) = X^{\frac{s_1}{2}} + 1$ and the result follows from Lemma 7.6. Suppose that $n \geq 2$ and that $M_2, M_3, \dots, M_u$, $u \leq n$, are all the maximal elements of $Z(M_1) \smallsetminus \{M_1\}$. Clearly $\mathcal{F}_{M_1}(X)$ is the greatest common divisor of $X^{\frac{s_1}{2}} + 1$ and $\mathcal{N}^{M_1/M_i}$ for all $i = 2, \dots u$. Applying Corollary 1.4 for $n = s_1, r_1 = \frac{s_1}{2}$ and $r_i = s_i$ for each $i = 2, \dots, u$ we obtain that there exist polynomials $P_1, P_2, \dots, P_u \in \mathbb{Z}[X]$ such that

$$P_1(X)(X^{\frac{s_1}{2}} + 1) + \sum_{i=2}^{u} P_i(X)\mathcal{N}^{M_1/M_i}(X) = \mathcal{F}_{M_1}(X).$$

Proposition 7.1 and Lemma 7.6 imply

$$\mathcal{F}_{M_1}(\gamma)\varkappa_{M_1} = P_1(\gamma)(\gamma^{\frac{s_1}{2}} + 1)\varkappa_{M_1} + \sum_{i=2}^{u} P_i(\gamma)\mathcal{N}^{M_1/M_i}(\gamma)\varkappa_{M_1} \in \mathcal{I}_q^{Z\smallsetminus\{M_1\}}$$

and Corollary 7.5 together with Lemma 7.6 gives

$$\mathcal{F}_{M_1}(\gamma)\xi_{M_1} = P_1(\gamma)(\gamma^{\frac{s_1}{2}} + 1)\xi_{M_1} + \sum_{i=2}^{u} P_i(\gamma)\mathcal{N}^{M_1/M_i}(\gamma)\xi_{M_1} \in \mathcal{J}_q^{Z\smallsetminus\{M_1\}}$$

and the proposition is proved. □

8. Index of some finitely generated $R[X]$-modules

Let R be either $\mathbb{Z}$ or $\mathbb{Z}_q$, where q is a prime number. The algebraic closure of the field of fractions of R will be denoted by Ω. Let $\mathcal{L}$ be a finite partially ordered set which form a lattice. The least element of $\mathcal{L}$ will be denoted by 0. Recall that a lower set of a partially ordered set is a subset Z with the property that, if x is in Z, $y \in \mathcal{L}$, and $y \leq x$, then y is in Z. For each $i \in \mathcal{L}$ let $Z(i)$ be the lower set generated by i, i.e.

$$Z(i) = \{j \in \mathcal{L}; j \leq i\}.$$

Suppose that M is a finitely generated $R[X]$-module whose generators will be denoted by $\xi_i, i \in \mathcal{L}$. For each $i \in \mathcal{L}$ let $\varkappa_i$ be an element of M given by

$$\varkappa_i = H_i \cdot \xi_i$$

for some $H_i \in R[X]$. By N we shall denote the submodule of M generated by all the elements $\varkappa_i$. For each lower set $Z \subseteq \mathcal{L}$ we define the following submodules:
Let M_Z be the submodule of M generated by ξ_i for all $i \in Z$. Let N_Z be the submodule of N generated by $\varkappa_i$ for all $i \in Z$. For $Z = \emptyset$ we thus have $M_\emptyset = N_\emptyset = \{0\}$. We further assume that the elements ξ_i and $\varkappa_i$ satisfy the following relations:
For each $i \in \mathcal{L}$ there is a polynomial $F_i \in R[X]$ such that

$$F_i \cdot \varkappa_i \in N_{Z(i)\setminus\{i\}} \qquad \text{and} \qquad F_i \cdot \xi_i \in M_{Z(i)\setminus\{i\}}.$$

We shall prove the following proposition:

Proposition 8.1. *Suppose that all the polynomials F_i are monic. We shall further assume that for every lower set $\emptyset \neq Z \subseteq \mathcal{L}$ and every maximal element m of Z we have*

$$\operatorname{rank}_R M_Z = \operatorname{rank}_R M_{Z\setminus\{m\}} + \deg F_m,$$
$$\operatorname{rank}_R N_Z = \operatorname{rank}_R N_{Z\setminus\{m\}} + \deg F_m.$$

It follows that $\operatorname{rank}_R M = \operatorname{rank}_R N$ *and*

$$[M : N] = \prod_{i\in\mathcal{L}} \left|R[X]/\left(F_i, H_i\right)\right|.$$

Moreover, the polynomials F_i and H_i have no common root in Ω for each $i \in \mathcal{L}$.

Proof. Using induction with respect to the size of Z we shall prove that

$$\operatorname{rank}_R M_Z = \operatorname{rank}_R N_Z$$

and that

$$[M_Z\colon N_Z] = \prod_{i \in Z} \bigl| R[X]/\bigl(F_i, H_i\bigr) \bigr|.$$

Suppose $Z = \{0\}$. It is obvious that $\mathrm{rank}_R M_Z = \mathrm{rank}_R N_Z = \deg F_0$. The map $R[X]/(F_0) \to M_Z$ given by

$$[f] \mapsto f \cdot \xi_0,$$

where $[a]$ denotes the coset containing a, is a surjective homomorphism of $R[X]$-modules. Since they have the same R-rank and $R[X]/\bigl(F_0\bigr)$ is a free R-module, it is an isomorphism. The preimage of N_Z in this isomorphism is the ideal $([H_0])$. Therefore the quotient M_Z/N_Z is isomorphic to

$$R[X]/(F_0) \Big/ ([H_0]),$$

which is isomorphic to

$$R[X]/(F_0, H_0).$$

Now suppose that Z has at least two elements. Let m be a maximal element of Z. The lower set $Z \smallsetminus \{m\}$ will be denoted by Z'. Let T_Z be the $R[X]$-module generated by $M_{Z'}$ and $\varkappa_m$, so $N_Z \subseteq T_Z \subseteq M_Z$. We have

$$[M_Z\colon N_Z] = [M_Z\colon T_Z] \cdot [T_Z\colon N_Z].$$

From the induction hypothesis we derive that the modules M_Z, N_Z and T_Z have the same R-rank. Indeed, we have

$$\mathrm{rank}_R N_Z = \mathrm{rank}_R N_{Z \smallsetminus \{m\}} + \deg F_m = \mathrm{rank}_R M_{Z \smallsetminus \{m\}} + \deg F_m = \mathrm{rank}_R M_Z.$$

Moreover, the R-bases of T_Z and of N_Z can be obtained by adding $\{X^i \cdot \varkappa_m; 0 \le i < \deg F_m\}$ to R-bases of $M_{Z'}$ and of $N_{Z'}$, respectively. Hence, using the determinants of transition matrices we get

$$[T_Z\colon N_Z] = [M_{Z'}\colon N_{Z'}]. \tag{25}$$

The map $R[X]/(F_m) \to M_Z/M_{Z'}$ given by

$$[f] \mapsto f \cdot [\xi_m]$$

is a surjective homomorphism of $R[X]$-modules. Since they have the same R-rank and $R[X]/\bigl(F_m\bigr)$ is a free R-module, it is an isomorphism. The preimage of $T_Z/M_{Z'}$ in this isomorphism is the ideal $([H_m])$. Therefore we have

$$M_Z/T_Z \cong M_Z/M_{Z'} \Big/ T_Z/M_{Z'} \cong R[X]/(F_m) \Big/ ([H_m]),$$

which is isomorphic to

$$R[X]/(F_m, H_m).$$

The induction hypothesis together with (25) gives

$$\begin{aligned}[M_Z\colon N_Z] &= |R[X]/(F_m, H_m)| \cdot [M_{Z'}\colon N_{Z'}] = \\ &= |R[X]/(F_m, H_m)| \cdot \prod_{i \in Z'} |R[X]/(F_i, H_i)|.\end{aligned}$$

To conclude the proof it remains to show that the polynomials F_i and H_i have no common root for each $i \in Z$. Suppose that for some $i \in Z$ the polynomials F_i and H_i have a common root in Ω. Let us denote $P \in R[X]$ their monic greatest common divisor, so we can write

$$F_i = PF_i' \qquad \text{and} \qquad H_i = PH_i'$$

for suitable polynomials $F_i', H_i' \in R[X]$. It follows that the polynomial F_i' is monic. The lower set $Z(i) \smallsetminus \{i\}$ will be denoted by Z'. Let $T_{Z(i)}$ be the $R[X]$-module generated by $M_{Z'}$ and $\varkappa_i$. Now we have

$$F_i' \cdot \varkappa_i = F_i' \cdot (H_i \cdot \xi_i) = PF_i'H_i' \cdot \xi_i = H_i'F_i \cdot \xi_i \in M_{Z'}.$$

Hence

$$\mathrm{rank}_R T_{Z(i)} \leq \mathrm{rank}_R M_{Z'} + \deg F_i' < \mathrm{rank}_R M_{Z'} + \deg F_i = \mathrm{rank}_R M_{Z(i)},$$

which is not possible. □

9. Computing the index $[\mathcal{J}_q^{\mathcal{L}} \colon \mathcal{I}_q^{\mathcal{L}}]$

Since not all the relations derived in Section 7 hold in $\mathbb{Z}[\langle\gamma\rangle]$ (see Corollary 7.5), one cannot compute the index $[\mathcal{J}^{\mathcal{L}} \colon \mathcal{I}^{\mathcal{L}}]$ in general. Nevertheless, we can always determine the exact power of ℓ dividing this index. Moreover, it turns out that apart from ℓ only odd primes dividing the degree $[F\colon \mathbb{Q}]$ could possibly divide the index $[\mathcal{J}^{\mathcal{L}} \colon \mathcal{I}^{\mathcal{L}}]$.

Recall that $q = 2$ or q is an odd prime not dividing $[F\colon \mathbb{Q}]$.

Proposition 9.1. *For every lower set $Z \subseteq \mathcal{L}$ we have*

$$\mathrm{rank}_{\mathbb{Z}_q} \mathcal{J}_q^Z = \mathrm{rank}_{\mathbb{Z}_q} \mathcal{I}_q^Z = \sum_{M \in Z} \deg \mathcal{F}_M.$$

Proof. It follows from Proposition 7.8 that

$$\operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^Z \leq \sum_{M \in Z} \deg \mathcal{F}_M. \tag{26}$$

If there were a sharp inequality in (26) for some lower set $Z_0 \subseteq \mathcal{L}$, then there would be a sharp inequality for all lower sets that contain Z_0. In particular, there would be a sharp inequality for $\mathcal{L}$ since

$$\operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^{\mathcal{L}} \leq \operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^{Z_0} + \sum_{M \in \mathcal{L} \smallsetminus Z_0} \deg \mathcal{F}_M < \sum_{M \in \mathcal{L}} \deg \mathcal{F}_M.$$

Using Lemma 7.7, we would obtain

$$\operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^{\mathcal{L}} < \frac{1}{2}[L \colon \mathbb{Q}].$$

However, this is not the case since by Proposition 6.3 we have

$$\operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^{\mathcal{L}} = \operatorname{rank}_{\mathbb{Z}_q} (\mathcal{I}^{\mathcal{L}} \otimes_{\mathbb{Z}} \mathbb{Z}_q) = \operatorname{rank}_{\mathbb{Z}} \mathcal{I}^{\mathcal{L}} = \operatorname{rank}_{\mathbb{Z}} S^- = \frac{1}{2}[L \colon \mathbb{Q}].$$

It remains to show that $\operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^Z = \operatorname{rank}_{\mathbb{Z}_q} \mathcal{J}_q^Z$. Clearly $\operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^Z \leq \operatorname{rank}_{\mathbb{Z}_q} \mathcal{J}_q^Z$. It follows from Proposition 7.8 that

$$\operatorname{rank}_{\mathbb{Z}_q} \mathcal{J}_q^Z \leq \sum_{M \in Z} \deg \mathcal{F}_M,$$

hence

$$\operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^Z \leq \operatorname{rank}_{\mathbb{Z}_q} \mathcal{J}_q^Z \leq \sum_{M \in Z} \deg \mathcal{F}_M = \operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^Z$$

and the result follows. □

Proposition 9.2. *For any lower set $Z = \{M_1, M_2, \dots, M_n\} \subseteq \mathcal{L}$ we have*

$$[\mathcal{J}_q^Z : \mathcal{I}_q^Z] = \prod_{i=1}^{n} |\mathbb{Z}_q[X]/(\mathcal{F}_{M_i}(X), H_{M_i}(X))|.$$

Proof. To apply Proposition 8.1 we need to show that

$$\begin{aligned}
\operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^Z &= \operatorname{rank}_{\mathbb{Z}_q} \mathcal{I}_q^{Z \smallsetminus \{M\}} + \deg \mathcal{F}_M \\
\operatorname{rank}_{\mathbb{Z}_q} \mathcal{J}_q^Z &= \operatorname{rank}_{\mathbb{Z}_q} \mathcal{J}_q^{Z \smallsetminus \{M\}} + \deg \mathcal{F}_M
\end{aligned}$$

for every lower set $Z \subseteq \mathcal{L}$ and every maximal $M \in Z$. But this was established in the proof of Proposition 9.1. □

Recall that

$$a_{M,j} = \begin{cases} 0, & \text{for } j \nmid [M : \mathbb{Q}] \\ |I_M|, & \text{for } j = 1 \\ \max\{0, |\{i \in I_M; j \mid n_i u_i\}| - 1\}, & \text{otherwise.} \end{cases}$$

Proposition 9.3. *Let $M \in \mathcal{L}$ be an arbitrary field. Then we have*

$$|\mathbb{Z}[X]/(\mathcal{F}_M(X), H_M(X))| = \prod_{j=0}^{v-1} \ell^{\varphi(u\ell^j) a_{M,u\ell^j}},$$

where $u = [M \cap F : \mathbb{Q}]$ and $v = \mathrm{ord}_\ell([M \cap K : \mathbb{Q}])$.

Proof. The degree $[M : \mathbb{Q}]$ is $u\ell^v$. By (24) we have

$$\mathcal{F}_M(X) = \Phi_{u\ell^v}(X).$$

The polynomial H_M is by definition equal to

$$H_M(X) = \prod_{j \mid u\ell^v} \Phi_j(X)^{a_{M,j}}.$$

Therefore we have

$$\begin{aligned} |\mathbb{Z}[X]/(\mathcal{F}_M(X), H_M(X))| &= |\mathbb{Z}[X]/(\Phi_{u\ell^v}(X), \prod_{j \mid u\ell^v} \Phi_j(X)^{a_{M,j}})| \\ &= \prod_{j \mid u\ell^v} \left|\mathbb{Z}[\zeta_{u\ell^v}]/\big(\Phi_j(\zeta_{u\ell^v})\big)\right|^{a_{M,j}}. \end{aligned}$$

It follows from the definition of numbers $a_{M,j}$ that $a_{M,j} = 0$ whenever $\ell^v \mid j$. Hence, using Proposition 1.2 we obtain

$$\left|\mathbb{Z}[\zeta_{u\ell^v}]/\big(\Phi_j(\zeta_{u\ell^v})\big)\right|^{a_{M,j}} = \begin{cases} \ell^{\varphi(j) a_{M,j}} & \text{if } j = u\ell^i \text{ for } i = 1, 2, \ldots, v-1 \\ 1, & \text{otherwise} \end{cases}$$

and the result follows. □

Theorem 9.4. *Suppose that $q = 2$ or q is an odd prime not dividing r. The relative index $[\mathcal{J}_q^{\mathcal{L}} : \mathcal{I}_q^{\mathcal{L}}]$ is 1 whenever $q \neq \ell$. In case $q = \ell$ the index is given by the following formula*

$$[\mathcal{J}_\ell^{\mathcal{L}} : \mathcal{I}_\ell^{\mathcal{L}}] = \prod_{\substack{u \mid r \\ 2 \nmid \frac{r}{u}}} \prod_{i=1}^{k} \prod_{j=0}^{i-1} \ell^{\varphi(u\ell^j) b(u,i,j)},$$

where $k = \mathrm{ord}_\ell([K\colon \mathbb{Q}])$ *and* $b(u,i,j) = a_{M_u^{(i)}, u\ell^j}$ *with* $M_u^{(i)}$ *being the unique subfield of* L *of degree* $[M_u^{(i)}\colon \mathbb{Q}] = u\ell^i$*.*

Proof. This result follows from Proposition 9.2 using Proposition 9.3. □

Theorem 9.5. *The ideal* $\mathcal{J}^{\mathcal{L}}$ *annihilates the ideal class group* $\mathrm{Cl}(L)$ *of* L*.*

Proof. At first we suppose q is an odd prime. Proposition 6.2 implies that $\xi^M \in \mathbb{Z}[\mathrm{Gal}(M/\mathbb{Q})]$ annihilates $\mathrm{Cl}(M)_q^-$. It follows that $\xi_M = \mathrm{cor}_{L/M}\xi^M \in \mathbb{Z}[\langle\gamma\rangle]$ annihilates $\mathrm{Cl}(L)_q^-$. Since $\mathcal{J}^{\mathcal{L}}$ annihilates $\mathrm{Cl}(L)_q^+$, we conclude that it annihilates $\mathrm{Cl}(L)_q$ for every odd prime q. It remains to show that $\mathcal{J}^{\mathcal{L}}$ also annihilates $\mathrm{Cl}(L)_2$. It follows from Proposition 6.3 that $\mathcal{I}_2^{\mathcal{L}}$ annihilates $\mathrm{Cl}(L)_2$. Theorem 9.4 implies that $\mathcal{J}_2^{\mathcal{L}} = \mathcal{I}_2^{\mathcal{L}}$, so $\mathcal{J}^{\mathcal{L}}$ annihilates $\mathrm{Cl}(L)_2$. □

We now consider a special case. Suppose $[F\colon \mathbb{Q}] = 2$. For each $i = 0, 1, \dots k$ let $L^{(i)}$ be the unique subfield of L of degree $[L^{(i)}\colon \mathbb{Q}] = 2\ell^i$. The poset $\mathcal{L}$ is the following string

$$F = L^{(0)} \subsetneq L^{(1)} \subsetneq \cdots \subsetneq L^{(k)} = L.$$

We have

$$\mathcal{F}_{L^{(i)}}(X) = \Phi_{2\ell^i}(X).$$

Theorem 9.4 gives

$$[\mathcal{J}_\ell^{\mathcal{L}} : \mathcal{I}_\ell^{\mathcal{L}}] = \prod_{i=1}^{k}\prod_{c=0}^{i-1} \ell^{\varphi(2\ell^c)a_{L^{(i)},2\ell^c}} = \prod_{i=1}^{k}\left(\ell^{a_{L^{(i)},2}} \prod_{c=1}^{i-1} \ell^{\ell^{c-1}(\ell-1)a_{L^{(i)},2\ell^c}}\right),$$

where

$$a_{L^{(i)},2\ell^c} = \max\bigl\{|\{j \in I_{L^{(i)}}; 2\ell^c \mid n_j u_j\}| - 1, 0\bigr\}.$$

We can compare this to the result of Greither and Kučera. Their index in [2, Theorem 6.5] is equal to

$$\prod_{i=1}^{k} \ell^{a_{L^{(i)},2}},$$

which divides our index. Our index is strictly larger if and only if there exist two different indices $i, j \in I_L$ such that both p_i and p_j split completely in $L^{(1)}$.

10. Examples

To find an example of fields for which our index is strictly larger than the index from [2], we need to take $k \geq 2$, so the smallest possible degree of such a field over rationals is 18. Suppose $\ell = 3$, $d = 3^2$ and $r = 2$. We set $F = \mathbb{Q}(\sqrt{-83})$, thus $f = 83$. Let us take $p_1 = 19$, $p_2 = 7$ and $p_3 = 31$ and consider the following characters:

$$\begin{aligned} \chi_1 &: (\mathbb{Z}/19\mathbb{Z})^\times \to \mathbb{C}^\times & \chi_1(2) &= \zeta_9, \\ \chi_2 &: (\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{C}^\times & \chi_2(3) &= \zeta_3, \\ \chi_3 &: (\mathbb{Z}/31\mathbb{Z})^\times \to \mathbb{C}^\times & \chi_3(3) &= \zeta_3. \end{aligned}$$

Let K be the field belonging to $\chi_1\chi_2\chi_3$. Let L be the compositum of F and K, so the conductor of L is $n = 7 \cdot 19 \cdot 31 \cdot 83 = 342209$. We have $\mathrm{Gal}(L/\mathbb{Q}) = \langle\gamma\rangle$, where $\gamma = \mathrm{res}_{\mathbb{Q}(\zeta_n)/L}\sigma_{34}$.

$$\begin{tikzcd}
 & & L & \\
 & L^{(1)} \arrow[ur, dash, "3"] & & K \arrow[ul, dash, "2"'] \\
F \arrow[ur, dash, "3"] & & K^{(1)} \arrow[ul, dash, "2"'] \arrow[ur, dash, "3"'] & \\
 & \mathbb{Q} \arrow[ul, dash, "2"] \arrow[ur, dash, "3"'] & &
\end{tikzcd}$$

It can be shown that

$$\begin{aligned} \varkappa_F &= 2 \cdot 83^2 \cdot (3\gamma - 3) \cdot (\gamma^{16} + \gamma^{14} + \gamma^{12} + \gamma^{10} + \gamma^8 + \gamma^6 + \gamma^4 + \gamma^2 + 1), \\ \varkappa_{L^{(1)}} &= 2 \cdot 83^2 \cdot 19 \cdot (6\gamma^2 + 10\gamma + 10) \cdot (\gamma^{12} + \gamma^6 + 1) \cdot (\gamma^3 - 1), \\ \varkappa_L &= 2 \cdot 83 \cdot n \cdot (1 - \gamma^9) \cdot \tilde{\varkappa}_L \end{aligned}$$

where

$$\tilde{\varkappa}_L = 64\gamma^7 - 84\gamma^6 + 18\gamma^5 + 2\gamma^4 - 120\gamma^3 + 18\gamma^2 - 62\gamma - 36.$$

Since the primes 7 and 31 split completely in $L^{(1)}/\mathbb{Q}$ and the prime 19 is totally ramified in $K/\mathbb{Q}$ and inert in $F/\mathbb{Q}$ we have

$$a_{L^{(1)},1} = 1, \qquad a_{L,1} = 3, \qquad a_{L,6} = 1, \qquad a_{L,3} = 1, \qquad a_{L,2} = 1,$$

which are the only nonzero values. We can compute $\xi_F, \xi_{L^{(1)}}, \xi_L$:

$$\begin{aligned}
\xi_F &= \varkappa_F, \\
\xi_{L^{(1)}} &= \varkappa_{L^{(1)}} \cdot \left(\tfrac{1}{6}\Delta_1^{L^{(1)}}\right) = 38 \cdot 83^2 \cdot (13\gamma^2 + 7\gamma - 3) \cdot (1-\gamma^3) \cdot (1+\gamma^6+\gamma^{12}), \\
\xi_L &= \varkappa_L \cdot \left(\tfrac{1}{18}\Delta_1^L\right)^3 \cdot \left(\tfrac{1}{9}\Delta_2^L(\gamma-1)\right) \cdot \left(\tfrac{1}{6}\Delta_3^L(\gamma-1)\right) \cdot \left(\tfrac{1}{3}\Delta_6^L(\gamma^4+\gamma^3-\gamma-1)\right) \\
&= 4 \cdot 83 \cdot n \cdot (1-\gamma^9) \cdot \tilde{\xi}_L
\end{aligned}$$

where

$$\tilde{\xi}_L = 32\gamma^8 + 2\gamma^7 - 31\gamma^6 - 75\gamma^5 - 85\gamma^4 - 101\gamma^3 - 107\gamma^2 - 87\gamma - 70.$$

We used the system PARI to check that all these elements actually annihilate $\mathrm{Cl}(L)$. The index $[\mathcal{J}^{\mathcal{L}} : \mathcal{I}^{\mathcal{L}}]$ is given by

$$[\mathcal{J}^{\mathcal{L}} : \mathcal{I}^{\mathcal{L}}] = [\mathcal{J}^{\mathcal{L}}_\ell : \mathcal{I}^{\mathcal{L}}_\ell] = 3^{a_{L^{(1)},2}} \cdot 3^{a_{L,2}} \cdot 3^{2a_{L,6}} = 3^3,$$

while the index from [2] is in this case equal to $3^{a_{L^{(1)},2}} \cdot 3^{a_{L,2}} = 3$.

We conclude this section by exhibiting an example where F is imaginary but not quadratic. Suppose $\ell = d = 3$ and $r = 4$. We set $F = \mathbb{Q}(\zeta_5)$, thus $f = 5$. Let us take $p_1 = 19$, $p_2 = 31$ and $p_3 = 61$ and consider the following characters:

$$\begin{aligned}
&\chi_1 : (\mathbb{Z}/19\mathbb{Z})^\times \to \mathbb{C}^\times \qquad && \chi_1(2) = \zeta_3, \\
&\chi_2 : (\mathbb{Z}/31\mathbb{Z})^\times \to \mathbb{C}^\times && \chi_2(3) = \zeta_3, \\
&\chi_3 : (\mathbb{Z}/61\mathbb{Z})^\times \to \mathbb{C}^\times && \chi_3(2) = \zeta_3.
\end{aligned}$$

Let K be the field belonging to $\chi_1\chi_2\chi_3$. Let L be the compositum of F and K, so the conductor of L is $n = 5 \cdot 19 \cdot 31 \cdot 61 = 179645$. We have $\mathrm{Gal}(L/\mathbb{Q}) = \langle\gamma\rangle$, where $\gamma = \mathrm{res}_{\mathbb{Q}(\zeta_n)/L}\sigma_{33}$. It can be shown that

$$\begin{aligned}
\varkappa_F &= 10 \cdot (1-\gamma^6) \cdot (1 + 2\gamma + 4\gamma^2 + 3\gamma^3) \cdot (1 + \gamma^4 + \gamma^8) \\
&= 10 \cdot (\gamma + 3) \cdot (\gamma^{10} - \gamma^8 + \gamma^6 - \gamma^4 + \gamma^2 - 1), \\
\varkappa_L &= 10 \cdot n \cdot (64\gamma^5 - 32\gamma^4 + 26\gamma^3 - 70\gamma^2 - 38\gamma - 38) \cdot (1-\gamma^6).
\end{aligned}$$

We have $a_{F,j} = 0$ for all $j \in \mathbb{N}$, hence $\xi_F = \varkappa_F$. For the field L we obtain

$$a_{L,j} = \begin{cases} 3, & j = 1, \\ 2, & j = 2, \\ 1, & j = 4, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore we have

$$\begin{aligned}
\xi_F &= \varkappa_F, \\
\xi_L &= \varkappa_L \cdot \left(\tfrac{1}{12}\Delta_1^L\right)^3 \cdot \left(\tfrac{1}{6}\Delta_2^L(\gamma-1)\right)^2 \cdot \left(\tfrac{1}{3}\Delta_4^L(\gamma^2-1)\right) \\
&= 10 \cdot n \cdot (36\gamma^5 + 32\gamma^4 - 4\gamma^3 - 38\gamma^2 - 40\gamma - 70) \cdot (1-\gamma^6).
\end{aligned}$$

The fact that ξ_L annihilates $\mathrm{Cl}(L)$ was again checked by PARI. The index $[\mathcal{J}^{\mathcal{L}} : \mathcal{I}^{\mathcal{L}}]$ is equal to

$$[\mathcal{J}^{\mathcal{L}} : \mathcal{I}^{\mathcal{L}}] = [\mathcal{J}_\ell^{\mathcal{L}} : \mathcal{I}_\ell^{\mathcal{L}}] = 3^{\varphi(4)a_{L,4}} = 3^2.$$

Acknowledgment

I would like to thank Radan Kučera for fruitful discussions and many suggestions leading to an improvement of this paper. The author was supported under Project 18-11473S of the Czech Science Foundation.

References

[1] T.A. Apostol, Resultants of cyclotomic polynomials, Proc. Am. Math. Soc. 24 (3) (1970) 457–462, https://doi.org/10.2307/2037387.
[2] C. Greither, R. Kučera, Annihilators of minus class groups of imaginary Abelian fields, Ann. Inst. Fourier 57 (5) (2007) 1623–1653, https://doi.org/10.5802/aif.2309.
[3] C. Greither, R. Kučera, Linear forms on Sinnott's module, J. Number Theory 141 (5) (2014) 324–342, https://doi.org/10.1016/j.jnt.2014.02.003.
[4] C. Greither, R. Kučera, Eigenspaces of the ideal class group, Ann. Inst. Fourier 64 (5) (2014) 2165–2203, https://doi.org/10.5802/aif.2908.
[5] C. Greither, R. Kučera, Annihilators for the class group of a cyclic field of prime power degree III, Publ. Math. (Debr.) 86 (3–4) (2015) 401–421.
[6] R. Kučera, On the Stickelberger ideal and circular units of a compositum of quadratic fields, J. Number Theory 56 (1) (1996) 139–166, https://doi.org/10.1006/jnth.1996.0008.
[7] W. Sinnott, On the Stickelberger ideal and the circular units of an Abelian field, Invent. Math. 62 (2) (1980) 181–234, https://doi.org/10.1007/BF01389158.
[8] L.C. Washington, Introduction to cyclotomic fields, https://doi.org/10.1007/978-1-4612-1934-7, 1997.