Publ. Math. Debrecen
86/3-4 (2015), 401–421
DOI: 10.5486/PMD.2015.7029

Annihilators for the class group of a cyclic field of prime power degree III

By CORNELIUS GREITHER (Neubiberg) and RADAN KUČERA (Brno)

Abstract. The aim of this series of papers is to study cyclic extensions of $\mathbb{Q}$ of odd prime power degree. This paper, which is the third of this series, concentrates on the situation where some of the ramified primes are (partially) decomposed.

Introduction

As in the papers [1] and [2], we are interested in absolutely abelian cyclic fields K of odd prime power degree $l = p^k$. We systematically search for roots of circular units. This leads to an enlargement of Sinnott's group of circular units. The new group $\overline{\mathcal{C}}_K$, which we hope to be interesting on its own, is generated by a set of explicitly given generators (see Lemmas 3.3 and 5.1, where bases are described), and its index in the full group of units is given by Theorem 3.1. As a consequence we obtain nontrivial divisibility statements on h_K, often much stronger than what is afforded by genus theory, and annihilation statements for the class group of K. The difference with respect to [2] is that we allow the ramified primes to (partially) split as well. This allows for much stronger results.

The process of finding the roots of circular units (Section 1) is admittedly very similar to what was done in [2] and also in [3]. The same goes for the application of the slightly adapted Rubin–Thaine technique (semispecial units) in Section 2, which is crucial for getting annihilators of ideal classes. The authors faced a dilemma between two options. First option: refer to our earlier work for these

Mathematics Subject Classification: Primary: 11R20; Secondary: 11R27, 11R29.
Key words and phrases: annihilators, class group, circular (cyclotomic) units, cyclic fields.
The second author was supported under Project P201/11/0276 of the Czech Science Foundation.

proofs and leave the task of supplying the necessary modifications to the reader. Second option: take a couple of pages more to write out the proofs again in the precise setting that is required. We have chosen the second option; readers who are somewhat acquainted with these matters may go through these arguments very quickly.

There is a new aspect with respect to [1] and [2]. After obtaining a strong result on the divisibility of h_K by powers of p in Section 3, we describe in Section 4 an alternative approach to class number divisibility via the Ambiguous Class Number Formula. (Superfluous as it may be, we stress that the name of the latter result refers to ambiguous *ideal classes*, and of course not to ambiguous numbers or formulas.) The results in Section 3 that say "h_K is large" use circular units and the Analytic Class Number Formula; they do not allow to write down a single ideal class of order p, say. On the other hand, the ambiguous class number formula is much more concrete, even though this is not clear from its bare statement; going through its proof, one can somehow locate the nontrivial ideal classes. Ambiguous ideal classes tend to come from classes of ramified primes. It is remarkable in our opinion that both techniques (circular units, and the Ambiguous Class Number Formula) lead to exactly the same divisibility result in a lot of cases. Admittedly this does not happen in all cases; at the end of Section 4 we spend some time on the question just when the two approaches "match exactly", for whatever it is worth.

Our annihilation result in Section 5 is again different from the standard result which says, grossly simplified, that "every annihilator of the quotient of all units by the circular units is also an annihilator of the class group". In our situation, the circular unit group is replaced by something considerably larger, so the quotient has more annihilators. In compensation, we only get annihilation of a certain (very explicit) subgroup of the class group. But it is possible to translate this into a novel annihilation statement for the entire class group; see Theorem 5.3.

1. Extracting roots of Sinnott circular units in a cyclic field

Let us assume that the cyclic field K satisfies the assumptions of [2], p. 581. Explicitly, let us suppose that $K/\mathbb{Q}$ is a cyclic extension of degree $l = p^k$, where p is an odd prime, such that the conductor m of K is not a prime power. Let χ be a generator of the group of Dirichlet characters corresponding to K. Let us decompose $\chi = \chi_{p_1} \dots \chi_{p_s}$, where χ_{p_i} is a nontrivial Dirichlet character whose conductor f_i is a power of a prime p_i (the primes $p_1, \dots, p_s$ are different; if

$p_i \neq p$ then $f_i = p_i$). Let p^{k_i} be the order of χ_{p_i}. Hence $s > 1$ and $p_1, \dots, p_s$ are precisely the primes which ramify in K and p^{k_i} is the ramification index of p_i. Let $q_i = lp^{-k_i}$ and n_i be the indices of the inertia and decomposition groups of p_i in $\mathrm{Gal}(K/\mathbb{Q})$, respectively, so $n_i \mid q_i$. We can suppose that the primes $p_1, \dots, p_s$ are ordered in such a way that p_1 is totally ramified in $K/\mathbb{Q}$, so $n_1 = q_1 = 1$, and that $n_1 \leq n_2 \leq \cdots \leq n_s < l$.

Let ζ be a fixed l-th primitive root of unity and let σ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$ satisfying $\chi(\sigma) = \zeta$. Let K_j be the abelian field corresponding to χ_{p_j} and let σ_j be the generator of $\mathrm{Gal}(K_j/\mathbb{Q})$ determined by $\chi_{p_j}(\sigma_j) = \zeta^{q_j}$.

For any $J \subseteq I = \{1, \dots, s\}$ let $K_J = \prod_{i \in J} K_i$, let m_J be the conductor of K_J and, for $J \neq \emptyset$, let $\eta_J = \mathrm{N}_{\mathbb{Q}(\zeta_{m_J})/K_J}(1 - \zeta_{m_J})$ be the "Sinnott circular number of conductor level" of K_J; here $\zeta_{m_J} = e^{2\pi i/m_J}$. Since K_J is real, η_J is totally positive. Then $\overline{K} = K_I$ is the genus field of K and $\eta = \mathrm{N}_{\overline{K}/K}(\eta_I)$ is the "Sinnott circular unit of conductor level" of K.

Let $G = \mathrm{Gal}(\overline{K}/\mathbb{Q})$ and let $\mathcal{D}$ be the group of circular $\{p_1, \dots, p_s\}$-units of $\overline{K}$, i.e. $\mathcal{D}$ is the $\mathbb{Z}[G]$-module generated in $\overline{K}^\times$ by -1 and by η_J for all $J \subseteq I$, $J \neq \emptyset$. The following lemma describes $\mathcal{D}$ by means of the module $U = \langle \rho_J; J \subseteq I \rangle_{\mathbb{Z}[G]}$ defined in [4] with $v = s$, for T_i being the inertia group of p_i in G and λ_i being the Frobenius automorphism of p_i in G with trivial action on K_i (Frobenius is determined modulo T_i only). Hence $G = T_1 \times \cdots \times T_s$, and U is the $\mathbb{Z}[G]$-submodule of $\mathbb{Q}[G] \oplus \mathbb{Z}^s$ generated by

$$\rho_J = \begin{cases} s(T_J) \prod_{i \in I-J} (1 - p^{-k_i} \lambda_i^{-1} s(T_i)) & \text{if } |I - J| \neq 1, \\ s(T_J)(1 - p^{-k_j} s(T_j)) + e_j & \text{if } I - J = \{j\}, \end{cases} \tag{1.1}$$

where $e_1, \dots, e_s$ is the usual basis of $\mathbb{Z}^s$, considered as a $\mathbb{Z}[G]$-module with trivial action of G, and $s(H) = \sum_{h \in H} h$ for any $H \subseteq G$.

Lemma 1.1. *The $\mathbb{Z}[G]$-modules $\mathcal{D}/\{\pm 1\}$ and $U/(s(G)\mathbb{Z})$ are isomorphic. More precisely, $\Psi(\eta_J) = \rho_{I-J}$ for each $J \subseteq I$, $J \neq \emptyset$, and $\Psi(-1) = 0$ defines a homomorphism $\Psi : \mathcal{D} \to U$ of $\mathbb{Z}[G]$-modules satisfying $\ker \Psi = \{\pm 1\}$ and $U = \Psi(\mathcal{D}) \oplus (s(G)\mathbb{Z})$.*

Proof. The circular numbers satisfy the following well-known norm relations

$$\prod_{\tau \in T_i} \eta_J^\tau = \mathrm{N}_{K_J/K_{J-\{i\}}}(\eta_J) = \eta_{J-\{i\}}^{1-\lambda_i^{-1}} \quad \text{for each } J \subseteq I, \text{ and each } \{i\} \subsetneq J,$$

and

$$\prod_{\tau \in T_j} \eta_{\{j\}}^\tau = \mathrm{N}_{K_j/\mathbb{Q}}(\eta_{\{j\}}) = p_j \quad \text{for each } j \in I.$$

The presentation of U described in [4, Corollary 1.6(ii)] together with the fact that $\rho_I = s(G)$ does not appear in the relations [4, (1.9) and (1.10)] at all show that $U = \langle \rho_J; J \subsetneq I \rangle_{\mathbb{Z}[G]} \oplus (s(G)\mathbb{Z})$ and that

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

defines a homomorphism $\Phi : U \to \mathcal{D}$ of $\mathbb{Z}[G]$-modules whose image consists of all (totally) positive numbers in $\mathcal{D}$. Since the $\mathbb{Z}$-rank of U is $l+s$ and the $\mathbb{Z}$-rank of $\mathcal{D}$ is $l+s-1$, we obtain $\ker \Phi = \rho_I\mathbb{Z} = s(G)\mathbb{Z}$. This implies the existence of Ψ with the desired properties. □

Let $H = \mathrm{Gal}(\overline{K}/K) \subseteq G$. Notice that

$$\Psi(\eta) = \Psi(\mathrm{N}_{\overline{K}/K}(\eta_I)) = s(H)\Psi(\eta_I) = s(H)\rho_\emptyset.$$

Each circular number $\alpha \in \mathcal{D}$ is either totally positive or totally negative, so for each $\tau \in G$ we have $\alpha^{\tau-1} \neq -1$. Since $\alpha \in K$ if and only if $\alpha^{\tau-1} = 1$ for all $\tau \in H$, which is the case if and only if $(\tau-1)\Psi(\alpha) = 0$ for all $\tau \in H$, we have $\Psi(\mathcal{D} \cap K) = \Psi(\mathcal{D})^H$.

Let $n = n_s = \max\{n_1, \ldots, n_s\}$ and let $N_n = \sum_{i=1}^{l/n} \sigma^{in}$, so N_n is the norm operator from K to K', the subfield of K of absolute degree n. Let $R' = \mathbb{Z}[\langle\sigma\rangle]/(N_n)$ and let $\lambda' : R' \to (1-\sigma^n)\mathbb{Z}[\langle\sigma\rangle]$ be the isomorphism of $\mathbb{Z}[\langle\sigma\rangle]$-modules given by multiplication by $1-\sigma^n$, i.e. $\lambda'(x) = (1-\sigma^n)x$. Then

$$\mathcal{M} = \{x \in \Psi(\mathcal{D})^H; N_n x = 0\}$$

is an R'-module without $\mathbb{Z}$-torsion. If $\psi \in \mathrm{Hom}_{R'}(\mathcal{M}, R')$ then

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

Since $U^H/\mathcal{M}$ has no $\mathbb{Z}$-torsion, [3, Proposition 6.2] for $f(X) = X^l - 1$ gives $\mathrm{Ext}^1_{\mathbb{Z}[\langle\sigma\rangle]}(U^H/\mathcal{M}, \mathbb{Z}[\langle\sigma\rangle]) = 0$. Hence there is

$$\varphi \in \mathrm{Hom}_{\mathbb{Z}[\langle\sigma\rangle]}(U^H, \mathbb{Z}[\langle\sigma\rangle])$$

such that $\varphi|_{\mathcal{M}} = \lambda' \circ \psi$. Let $\upsilon \in \mathrm{Hom}_{\mathbb{Z}[\langle\sigma\rangle]}(U^H, \mathbb{Z}[\langle\sigma\rangle])$ be defined by $\upsilon(x) = (1-\sigma)\varphi(x)$, then $\upsilon(t_i e_i) = 0$ and [4, Corollary 1.7(ii)] gives

$$\upsilon(s(H)\rho_\emptyset) \in \prod_{i=1}^{s} (1-\sigma^{n_i})\mathbb{Z}[\langle\sigma\rangle],$$

because $(1-\sigma^{n_i})\mathbb{Z}[\langle\sigma\rangle]$ is the ideal of $\mathbb{Z}[\langle\sigma\rangle]$ generated by $1-\mathrm{res}_{\overline{K}/K}\,\lambda_i$ and by $1-\mathrm{res}_{\overline{K}/K}\,\tau$ for all $\tau\in T_i$. We have $\mathrm{N}_{K/K'}(\eta)=1$ as p_s splits completely in K' and $s>1$, hence $s(H)\rho_\emptyset\in\mathcal{M}$. The multiplication by $1-\sigma$ is injective on $(1-\sigma^n)\mathbb{Z}[\langle\sigma\rangle]$, which means

$$\lambda'\circ\psi(s(H)\rho_\emptyset)=\varphi(s(H)\rho_\emptyset)\in\prod_{i=2}^{s}(1-\sigma^{n_i})\mathbb{Z}[\langle\sigma\rangle],$$

hence

$$\psi(s(H)\rho_\emptyset)\in\prod_{i=2}^{s-1}(1-\sigma^{n_i})R'.$$

Since $y=\prod_{i=2}^{s-1}(1-\sigma^{n_i})$ is a non-zero-divisor in R', [3, Proposition 6.2] for $f(X)=\sum_{i=1}^{l/n}X^{(i-1)n}$ gives $\delta\in\mathcal{M}$ such that $y\delta=s(H)\rho_\emptyset=\Psi(\eta)$. Hence $\delta\in\Psi(\mathcal{D})^H=\Psi(\mathcal{D}\cap K)$ and $N_n\delta=0$. Therefore $\delta=\Psi(\alpha)$ for a suitable totally positive $\alpha\in\mathcal{D}\cap K$ and $\Psi(\alpha^y)=\Psi(\eta)$ and $\Psi(\mathrm{N}_{K/K'}(\alpha))=0$. As α is totally positive, we have $\mathrm{N}_{K/K'}(\alpha)=1$ and $\alpha^y=\eta$. Since $\alpha\in\mathcal{D}$ has absolute norm 1, it is a circular unit of $\overline{K}$. Notice that α is uniquely determined by the conditions $\alpha\in K$, $\mathrm{N}_{K/K'}(\alpha)=1$ and $\alpha^y=\eta$. Indeed, if there were two such α's, their quotient β would satisfy $\beta^y=1$, so $\beta\in K'$ and $1=\mathrm{N}_{K/K'}(\beta)=\beta^{l/n}$, hence $\beta=1$.

Theorem 1.2. *There is $\alpha\in\mathcal{D}\cap K$ such that the circular unit η is equal to α^y , where $y=\prod_{i=2}^{s-1}(1-\sigma^{n_i})$. Moreover α is a circular unit of $\overline{K}$ and there are $\gamma,\mu\in K^\times$ satisfying $\alpha=\gamma^{1-\sigma^{n_s}}=\mu^{1-\sigma}$ and $\mathrm{N}_{K/\mathbb{Q}}(\mu)\in\langle-1,p_1,\dots,p_s\rangle$.*

Proof. Hilbert's Theorem 90 for the cyclic extensions K/K' and $K/\mathbb{Q}$ implies that there are $\gamma,\mu\in K^\times$ such that $\alpha=\gamma^{1-\sigma^n}=\mu^{1-\sigma}$. Since $\mu^{1-\sigma}=\alpha$ is a unit, the ideal $\mu\mathcal{O}_K$ is ambiguous and so μ can be chosen to be supported only on ramified primes. □

Let ε be as in [2, Theorem 1.1]. Now we can prove the following stronger version of [2, Proposition 1.6].

Proposition 1.3. *Let v be the greatest common divisor of l and $\prod_{i=1}^{s}n_i$. Then the norm $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)$ is a v-th power in $\mathbb{Q}$.*

Proof. We have obtained

$$\varepsilon^{(\sigma-1)^{s-1}}=\eta=\alpha^y=\gamma^{y(1-\sigma^n)},\tag{1.2}$$

so $\vartheta=\varepsilon\cdot\gamma^{(-1)^s\prod_{i=2}^{s}\sum_{j=0}^{n_i-1}\sigma^j}\in\mathbb{Q}^\times$ because $\vartheta^{(\sigma-1)^{s-1}}=1$. Taking norms we obtain

$$\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)=\mathrm{N}_{K/\mathbb{Q}}(\vartheta\cdot\gamma^{(-1)^{s-1}\prod_{i=2}^{s}\sum_{j=0}^{n_i-1}\sigma^j})=\vartheta^l\cdot\mathrm{N}_{K/\mathbb{Q}}(\gamma^{(-1)^{s-1}})^{\prod_{i=1}^{s}n_i}.\quad\square$$

Remark 1.4. We can compute α explicitly as a p-power root of a specific circular unit. For each $j = 1, \dots, s$, let

$$N_{n_j} = \sum_{i=1}^{l/n_j} \sigma^{in_j} \quad \text{and} \quad \Delta_{n_j} = \sum_{i=1}^{(l/n_j)-1} i\sigma^{in_j},$$

so $(1-\sigma^{n_j})N_{n_j} = 0$ and $(1-\sigma^{n_j})\Delta_{n_j} = N_{n_j} - \frac{l}{n_j}$. Then (1.2) implies

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

because $\alpha^{N_n} = 1$, where $r = \prod_{i=2}^{s-1}\frac{l}{n_i}$ is a power of p, so

$$\alpha = \sqrt[r]{\eta^{(-1)^s\prod_{i=2}^{s-1}\Delta_{n_i}}}. \tag{1.3}$$

Similarly

$$\eta^{\prod_{i=2}^{s}\Delta_{n_i}} = \gamma^{\prod_{i=2}^{s}(N_{n_i}-\frac{l}{n_i})} = \gamma^{(-1)^s(N_n-\frac{l}{n})\prod_{i=2}^{s-1}\frac{l}{n_i}} = \gamma^{(-1)^s(N_n-\frac{l}{n})r}.$$

Therefore

$$\mathrm{N}_{K/K'}(\gamma)\cdot\gamma^{-l/n} = \sqrt[r]{\eta^{(-1)^s\prod_{i=2}^{s}\Delta_{n_i}}} = \alpha^{\Delta_n}.$$

It would be enough to compute $\mathrm{N}_{K/K'}(\gamma)$ to get a formula for γ but the authors have no idea how to obtain $\mathrm{N}_{K/K'}(\gamma)$ if $n > 1$ (the case $n = 1$ is described by [2, Theorem 1.1] since $K' = \mathbb{Q}$ and $\gamma\cdot\varepsilon^{(-1)^s} \in \mathbb{Q}$ in this case).

2. The root μ is semispecial

Let us recall the definition of semispecialness: let M be any p-power divisible by l^{s-1}. For any prime $q \equiv 1 \pmod M$ and any abelian field L let $L(q)$ be the compositum of L with the cyclic field $\mathbb{Q}(q)$ of absolute degree M and conductor q. Let

$$\mathcal{Q}_M = \{q \text{ prime};\ q \text{ totally split in } K,\ q \equiv 1 + M \pmod{M^2},$$
$$p_j \text{ is an } M\text{-th power modulo } q \text{ for each } j = 1, \dots, s\}.$$

A number ε in K is called *M-semispecial* if for all but finitely many $q \in \mathcal{Q}_M$, there exists $\varepsilon_q \in \mathcal{O}_{K(q)}^\times$ satisfying

- $\mathrm{N}_{K(q)/K}(\varepsilon_q) = 1$;
- If $\tilde{q}$ is the product of all primes of $K(q)$ dividing q, then ε and ε_q have the same image in $(\mathcal{O}_{K(q)}/\tilde{q})^\times/(M/l^{s-1})$.

Let us fix a p-power M divisible by l^{s-1} and any $q \in \mathcal{Q}_M$. To simplify notation, we denote $p_{s+1} = q$, $K_{s+1} = \mathbb{Q}(q)$ and $I' = \{1, \dots, s+1\}$. Again, for any $J \subseteq I'$ let $K_J = \prod_{i \in J} K_i$, let m_J be the conductor of K_J and, for $J \neq \emptyset$, let $\eta_J = \mathrm{N}_{\mathbb{Q}(\zeta_{m_J})/K_J}(1-\zeta_{m_J})$ be the "Sinnott circular number of conductor level" of K_J; here $\zeta_{m_J} = e^{2\pi i/m_J}$. This definition does not change the previous meaning of K_J and η_J if $J \subseteq I$. Then $\overline{K}(q) = K_{I'}$ is the genus field of $K(q)$.

Let $G_q = \mathrm{Gal}(\overline{K}(q)/\mathbb{Q})$ and let $\mathcal{D}_q$ be the group of circular $\{p_1, \dots, p_s, q\}$-units of $\overline{K}(q)$, i.e. $\mathcal{D}_q$ is the $\mathbb{Z}[G_q]$-module generated in $\overline{K}(q)^\times$ by -1 and by η_J for all $J \subseteq I'$, $J \neq \emptyset$. Let U_q be the module U defined in [4] with $v = s+1$, for T_i being the inertia group of p_i in G_q and λ_i being the Frobenius automorphism of p_i in G_q with trivial action on K_i.

We identify G with $\mathrm{Gal}(\overline{K}(q)/\mathbb{Q}(q))$, then the new groups T_i for $i \neq s+1$ are equal to the old ones and $H = \mathrm{Gal}(\overline{K}(q)/K(q))$. The assumption $q \in \mathcal{Q}_M$ implies that the new elements λ_i for $i \in I$ are also equal to the old ones and that $\lambda_{s+1} \in H$. But this is not the case for the generators of U and U_q, so we need to distinguish them. Recall the notation of [4], namely that $U \subseteq \mathbb{Q}[G] \oplus \mathbb{Z}^s$ has $\mathbb{Z}[G]$-generators ρ_J, $J \subseteq I$, described by (1.1), that the standard basis of $\mathbb{Z}^s$ is denoted by $e_1, \dots, e_s$, and that $\pi : \mathbb{Q}[G] \oplus \mathbb{Z}^s \to \mathbb{Q}[G]$ is the projection to the first coordinate, so $U' = \pi(U)$ is generated by $\rho'_J = \pi(\rho_J)$. Similarly we denote the $\mathbb{Z}[G_q]$-generators of $U_q \subseteq \mathbb{Q}[G_q] \oplus \mathbb{Z}^{s+1}$ by $\tilde{\rho}_J$, hence $U_q = \langle \tilde{\rho}_J; J \subseteq I' \rangle_{\mathbb{Z}[G_q]}$, and the standard basis of $\mathbb{Z}^{s+1}$ by $\tilde{e}_1, \dots, \tilde{e}_{s+1}$.

Lemma 2.1. *There are injective $\mathbb{Z}[G]$-homomorphisms $\chi : U \to U_q$ and $\chi' : U' \to U_q$ defined by*

$$\chi(\rho_J) = \tilde{\rho}_{J \cup \{s+1\}} \quad \text{and} \quad \chi'(\rho'_J) = \tilde{\rho}_J$$

for each $J \subseteq I$. As $\mathbb{Z}[G]$-modules, $U_q \cong U \oplus \mathbb{Z} \oplus (U')^{M-1}$.

Proof. The key role in this proof is played by the fact that λ_i for $i \in I$ are the same in U and in U_q. A presentation of both U and U' is described in [4, Corollary 1.6]. To show that χ' is well-defined, we need to check that the images of ρ'_J satisfy (1.8) of [4], which means that for each $J \subsetneq I$, $i \in I - J$ we have

$$s(T_i) \cdot \chi'(\rho'_J) = s(T_i) \cdot \tilde{\rho}_J = (1 - \lambda_i^{-1}) \cdot \tilde{\rho}_{J \cup \{i\}} = (1 - \lambda_i^{-1}) \cdot \chi'(\rho'_{J \cup \{i\}}).$$

Similarly one can show that the images of ρ_J satisfy [4, (1.10)] and so χ is well-defined.

For each $J \subsetneq I$ we have $s(T_{s+1}) \cdot \tilde{\rho}_J \in \langle \tilde{\rho}_{N \cup \{s+1\}}; N \subseteq I \rangle_{\mathbb{Z}[G]}$, while $s(T_{s+1}) \cdot \tilde{\rho}_I = M\tilde{e}_{s+1}$. Hence, as a $\mathbb{Z}[G]$-module, U_q is generated by $M\tilde{e}_{s+1}$, by $\tilde{\rho}_{J \cup \{s+1\}}$,

and by $\tau\tilde{\rho}_J$ for all $J \subseteq I$ and all $\tau \in T_{s+1}$, $\tau \neq 1$. Therefore the sum

$$\chi(U) + M\tilde{e}_{s+1}\mathbb{Z} + \sum_{\tau \in T_{s+1}-\{1\}} \tau\chi'(U') = U_q,$$

because it contains all the mentioned generators of U_q. As $\operatorname{rank}_{\mathbb{Z}} U = |G| + s$, $\operatorname{rank}_{\mathbb{Z}} U' = |G|$, $\operatorname{rank}_{\mathbb{Z}} U_q = |G_q| + s + 1 = M \cdot |G| + s + 1$, and $|T_{s+1}| = M$, the comparison of $\mathbb{Z}$-ranks gives that the sum is direct and that both χ and χ' are injective. □

We can apply Lemma 1.1 to our new situation to obtain the corresponding homomorphism $\Psi_q : \mathcal{D}_q \to U_q$ of $\mathbb{Z}[G_q]$-modules defined by $\Psi_q(\eta_J) = \tilde{\rho}_{I'-J}$ for each $J \subseteq I'$, $J \neq \emptyset$, and $\Psi_q(-1) = 0$, satisfying $\ker \Psi_q = \{\pm 1\}$ and $U_q = \Psi_q(\mathcal{D}_q) \oplus (s(G_q)\mathbb{Z})$. We have for $\hat{\eta} = \mathrm{N}_{\overline{K}(q)/K(q)}(\eta_{I'})$ that

$$\Psi_q(\hat{\eta}) = s(H)\Psi_q(\eta_{I'}) = s(H)\tilde{\rho}_{\emptyset}$$

and $\Psi_q(\mathcal{D}_q \cap K(q)) = \Psi_q(\mathcal{D}_q)^H$ since each element of $\mathcal{D}_q$ is either totally positive or totally negative.

We still have $n = n_s = \max\{n_1, \ldots, n_s\}$, $R' = \mathbb{Z}[\langle\sigma\rangle]/(N_n)$, where σ is now the generator of $\mathrm{Gal}(K(q)/\mathbb{Q}(q))$ whose restriction to K is the old σ, and the isomorphism of $\mathbb{Z}[\langle\sigma\rangle]$-modules $\lambda' : R' \to (1-\sigma^n)\mathbb{Z}[\langle\sigma\rangle]$. Then

$$\mathcal{M}_q = \{x \in \Psi_q(\mathcal{D}_q)^H;\ N_n x = 0\}$$

is again an R'-module without $\mathbb{Z}$-torsion such that $U_q^H/\mathcal{M}_q$ has no $\mathbb{Z}$-torsion and so [3, Proposition 6.2] gives $\mathrm{Ext}^1_{\mathbb{Z}[\langle\sigma\rangle]}(U_q^H/\mathcal{M}_q, \mathbb{Z}[\langle\sigma\rangle]) = 0$. Let us fix any $\psi \in \mathrm{Hom}_{R'}(\mathcal{M}_q, R')$, then there is $\varphi \in \mathrm{Hom}_{\mathbb{Z}[\langle\sigma\rangle]}(U_q^H, \mathbb{Z}[\langle\sigma\rangle])$ such that $\varphi|_{\mathcal{M}_q} = \lambda' \circ \psi$. The restriction of $\chi' \circ \pi : U \to U_q$ gives $\chi' \circ \pi : U^H \to U_q^H$ and

$$\varphi \circ \chi' \circ \pi \in \mathrm{Hom}_{\mathbb{Z}[\langle\sigma\rangle]}(U^H, \mathbb{Z}[\langle\sigma\rangle]).$$

As $\pi(t_j e_j) = 0$, we can use [4, Corollary 1.7(ii)] to obtain

$$\varphi(s(H)\tilde{\rho}_{\emptyset}) = \varphi \circ \chi' \circ \pi(s(H)\rho_{\emptyset}) \in \prod_{i=1}^{s} (1-\sigma^{n_i})\mathbb{Z}[\langle\sigma\rangle].$$

Since N_n is the norm operator with respect to $K(q)/K'(q)$, we have

$$N_n s(H)\tilde{\rho}_{\emptyset} = \Psi_q(\mathrm{N}_{K(q)/K'(q)}(\hat{\eta})) = 0,$$

because p_s splits completely in $K'(q)$. Hence $s(H)\tilde{\rho}_\emptyset \in \mathcal{M}_q$ and

$$\psi(s(H)\tilde{\rho}_\emptyset) \in \prod_{i=1}^{s-1}(1-\sigma^{n_i})R' = (1-\sigma)yR'.$$

Therefore [3, Proposition 6.2] gives $\delta \in \mathcal{M}_q$ such that $(1-\sigma)y\delta = s(H)\tilde{\rho}_\emptyset = \Psi_q(\hat{\eta})$. So $\delta = \Psi_q(\beta)$ for a suitable totally positive $\beta \in \mathcal{D}_q \cap K(q)$ and $\mathrm{N}_{K(q)/K'(q)}(\beta) = 1$ and $\beta^{(1-\sigma)y} = \hat{\eta}$. The argument already used in Remark 1.4 shows that

$$\beta^{1-\sigma} = \sqrt[r]{\hat{\eta}^{(-1)^s \prod_{i=2}^{s-1}\Delta_{n_i}}} \quad \text{and} \quad \beta = \sqrt[rl]{\hat{\eta}^{(-1)^{s-1}\prod_{i=1}^{s-1}\Delta_{n_i}}}, \tag{2.1}$$

where $r = \prod_{i=2}^{s-1}\frac{l}{n_i}$. Since $\mathrm{N}_{K(q)/K}(\hat{\eta}) = \mathrm{N}_{\overline{K}(q)/K}(\eta_{I'}) = 1$ as q splits completely in K, we have $\mathrm{N}_{K(q)/K}(\beta) = 1$.

Since both $\zeta_{m_{I'}}$ and $\zeta_{m_I}\cdot\zeta_q$ are primitive $m_{I'}$-th roots of unity, there is an automorphism ν of $m_{I'}$-th cyclotomic field satisfying $\zeta_{m_{I'}}^{\nu} = \zeta_{m_I}\cdot\zeta_q$. This means that

$$\hat{\eta}^{\nu} = \mathrm{N}_{\mathbb{Q}(\zeta_{m_{I'}})/K(q)}(1-\zeta_{m_{I'}})^{\nu} = \mathrm{N}_{\mathbb{Q}(\zeta_{m_{I'}})/K(q)}(1-\zeta_{m_I}\cdot\zeta_q)$$

and so

$$\hat{\eta}^{\nu} \equiv \mathrm{N}_{\mathbb{Q}(\zeta_{m_{I'}})/K(q)}(1-\zeta_{m_I}) = \mathrm{N}_{\mathbb{Q}(\zeta_{m_I})/K}(1-\zeta_{m_I})^{(q-1)/M} = \eta^{(q-1)/M} \pmod{\tilde{q}}.$$

Since $q = 1 + M \pmod{M^2}$, we have obtained that $\hat{\eta}^{\nu}$ and η have the same image in $(\mathcal{O}_{K(q)}/\tilde{q})^{\times}/M$. Therefore (2.1), (1.3), and $r \mid l^{s-2}$ give that $\beta^{(1-\sigma)\nu}$ and $\alpha = \mu^{1-\sigma}$ have the same image in $(\mathcal{O}_{K(q)}/\tilde{q})^{\times}/(M/l^{s-2})$. Therefore

$$\beta^{(1-\sigma)\Delta_1\nu} = \beta^{(N_1-l)\nu} = \beta^{-l\nu}$$

and

$$\mu^{(1-\sigma)\Delta_1} = \mu^{N_1-l} = N_{K/\mathbb{Q}}(\mu)\cdot\mu^{-l}$$

have the same image in $(\mathcal{O}_{K(q)}/\tilde{q})^{\times}/(M/l^{s-2})$. Theorem 1.2 gives that the rational integer $\mathrm{N}_{K/\mathbb{Q}}(\mu)$ is an M-th power modulo q, hence β^{ν} and μ have the same image in $(\mathcal{O}_{K(q)}/\tilde{q})^{\times}/(M/l^{s-1})$. We have proved the following

Theorem 2.2. *The number $\mu \in K^{\times}$ from Theorem 1.2 is M-semispecial for each p-power M such that $l^{s-1} \mid M$.*

3. An enlargement of Sinnott's group of circular units

We keep the notation of Section 1 and introduce some other. Let us give a name to each subfield of K as follows:

$$\mathbb{Q} = L_0 \subsetneq L_1 \subsetneq L_2 \subsetneq \cdots \subsetneq L_k = K, \tag{3.1}$$

then $[L_i : \mathbb{Q}] = p^i$. For each $i = 1, \dots, k$ let m_i be the conductor of L_i, $\zeta_{m_i} = e^{2\pi i/m_i}$,

$$\eta_i = \mathrm{N}_{\mathbb{Q}(\zeta_{m_i})/L_i}(1 - \zeta_{m_i})$$

be the "Sinnott circular number of conductor level" of L_i, and let

$$M_i = \big\{ j \in \{1, \dots, s\};\ q_j < p^i \big\}, \tag{3.2}$$

so $j \in M_i$ if and only if p_j ramifies in $L_i/\mathbb{Q}$. Finally, let $\mathcal{D}_i$ be the group of circular $\{p_j; j \in M_i\}$-units of L_i.

For each $j = 1, \dots, s$ let us fix an integer c_j such that $p \nmid c_j$ and that $\sigma^{-c_j n_j}$ coincides with the Frobenius of p_j on $L_{\log_p q_j}$, the largest subfield of K where p_j is unramified; we can take $c_j = 1$ if p_j is totally ramified in $K/\mathbb{Q}$. Hence $1 - \sigma^{c_j n_j}$ and $1 - \sigma^{n_j}$ are associated in $\mathbb{Z}[\langle\sigma\rangle]$, i.e. each of them divides the other. On one hand, if $|M_i| > 1$ then Theorem 1.2 implies that there are a unit $\alpha_i \in \mathcal{D}_i \cap L_i$ and a number $\gamma_i \in L_i^\times$ such that the circular unit $\eta_i = \alpha_i^{y_i}$ and $\alpha_i = \gamma_i^{z_i}$, where $z_i = 1 - \sigma^{c_{\max M_i} n_{\max M_i}}$ and $y_i = \prod_{j \in M_i,\ 1 < j < \max M_i} (1 - \sigma^{c_j n_j})$, so $y_i = 1$ if $|M_i| = 2$. On the other hand, if $|M_i| = 1$ then we put $\gamma_i = \eta_i$ and $\alpha_i = \eta_i^{1-\sigma}$.

Let $\mathcal{O}_{L_i}^\times$ and $\mathcal{C}_{L_i}$ be the full group of units of L_i and the Sinnott group of circular units of L_i, respectively. Moreover, we define $\overline{\mathcal{C}}_{L_i}$ to be the Galois submodule of $\mathcal{O}_{L_i}^\times$ generated by $-1, \alpha_1, \dots, \alpha_i$. The aim of this section is to prove the following

Theorem 3.1. *The Sinnott group $\mathcal{C}_K$ of circular units of K is a subgroup of $\overline{\mathcal{C}}_K$ of index $[\overline{\mathcal{C}}_K : \mathcal{C}_K] = p^\nu$, where*

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

Moreover

$$\big[\mathcal{O}_K^\times : \overline{\mathcal{C}}_K\big] = 2^{l-1} \cdot h_K \cdot \Big(\prod_{i=1}^{k} p^{n_{\max M_i}} \Big) \cdot \prod_{j=1}^{s} \Big(\frac{q_j}{l} \Big)^{n_j},$$

where h_K is the class number of K. Therefore

$$\varphi_K := \Big(\prod_{i=1}^{k} p^{-n_{\max M_i}}\Big) \cdot \prod_{j=1}^{s} \Big(\frac{l}{q_j}\Big)^{n_j} \tag{3.3}$$

is a divisor of h_K.

Before giving a proof, let us mention two examples. If there is at most one partially split prime among the ramified primes, i.e. if we suppose $n_1 = \cdots = n_{s-1} = 1$, then our group $\overline{\mathcal{C}}_K$ coincides with the group C of [2] and we have $[\mathcal{O}_K^\times : \overline{\mathcal{C}}_K] = 2^{l-1} \cdot h_K \cdot l^{1-s} \cdot \prod_{j=1}^{s} q_j$ in accordance with [2, Proposition 1.2]. If only p_1 is totally ramified and all the other ramified primes $p_2, \ldots, p_s$ split completely in L_{k-1} then $[\mathcal{O}_K^\times : \overline{\mathcal{C}}_K] = 2^{l-1} \cdot h_K \cdot p^{-1-(s-2)p^{k-1}}$.

We now state a lemma that is needed to prove the theorem of this section.

Lemma 3.2. *For each $v = 1, \ldots, k$ we have $[\overline{\mathcal{C}}_{L_v} : \mathcal{C}_{L_v}] = p^{\nu_v}$, where*

$$\nu_v = \sum_{i=1}^{v} \sum_{\substack{j \in M_i \\ 1 < j < \max M_i}} n_j.$$

Proof. We shall use induction with respect to v starting at $v = 0$ when we put $\overline{\mathcal{C}}_{\mathbb{Q}} = \mathcal{C}_{\mathbb{Q}} = \{\pm 1\}$ and the statement is obvious. Suppose that $1 \le v \le k$ and that the statement has been proved for $v-1$. We have $1 \in M_v$ as p_1 is supposed to ramify totally in $K/\mathbb{Q}$. If $|M_v| = 1$ then $\overline{\mathcal{C}}_{L_v} = \mathcal{C}_{L_v} = \langle \eta_v^{1-\sigma} \rangle_{\mathbb{Z}[\langle\sigma\rangle]}$. If $|M_v| = 2$ then again $\overline{\mathcal{C}}_{L_v} = \mathcal{C}_{L_v}$ since both these groups are generated by all conjugates of η_v and by $\overline{\mathcal{C}}_{L_{v-1}} = \mathcal{C}_{L_{v-1}}$. So we can suppose $|M_v| > 2$. It is well-known that $\mathrm{N}_{L_v/L_{v-1}}(\eta_v) \in \mathcal{C}_{L_{v-1}}$ but we need to show that $\mathrm{N}_{L_v/L_{v-1}}(\alpha_v) \in \overline{\mathcal{C}}_{L_{v-1}}$, too.

We have

$$\mathrm{N}_{L_v/L_{v-1}}(\eta_v) = \eta_{v-1}^{\prod_{j \in M_v - M_{v-1}} (1-\sigma^{c_j n_j})},$$

that is

$$\mathrm{N}_{L_v/L_{v-1}}(\gamma_v)^{y_v z_v} = \gamma_{v-1}^{y_v z_v}.$$

Since $(1-\sigma^{c_j n_j}) z_v \mid p^{k-1} z_v$ in $\mathbb{Z}[\langle\sigma\rangle]$ for each $j \in M_v$ and 1 is the only p-th root of unity in L_v, we have obtained

$$\mathrm{N}_{L_v/L_{v-1}}(\gamma_v)^{z_v} = \gamma_{v-1}^{z_v}, \tag{3.4}$$

and so

$$\mathrm{N}_{L_v/L_{v-1}}(\alpha_v) = \mathrm{N}_{L_v/L_{v-1}}(\gamma_v)^{z_v} = \gamma_{v-1}^{z_v} \in \langle \alpha_{v-1} \rangle_{\mathbb{Z}[\langle\sigma\rangle]}, \tag{3.5}$$

since $z_{v-1} \mid z_v$ in $\mathbb{Z}[\langle\sigma\rangle]$. Therefore to get a $\mathbb{Z}$-basis of $\overline{\mathcal{C}}_{L_v}$ it is enough to add $\{\alpha_v^{\sigma^i};\ 0 \le i < (p-1)p^{v-1}\}$ to a $\mathbb{Z}$-basis of $\overline{\mathcal{C}}_{L_{v-1}}$. Similarly $\mathbb{Z}$-bases of $\overline{\mathcal{C}}_{L_{v-1}} \mathcal{C}_{L_v}$

and of $\mathcal{C}_{L_v}$ can be obtained by adding $\{\eta_v^{\sigma^i};\ 0 \le i < (p-1)p^{v-1}\}$ to $\mathbb{Z}$-bases of $\overline{\mathcal{C}}_{L_{v-1}}$ and of $\mathcal{C}_{L_{v-1}}$, respectively. Hence, using the determinants of transition matrices,

$$\big[(\overline{\mathcal{C}}_{L_{v-1}}\mathcal{C}_{L_v}) : \mathcal{C}_{L_v}\big] = \big[\overline{\mathcal{C}}_{L_{v-1}} : \mathcal{C}_{L_{v-1}}\big]. \tag{3.6}$$

Let $f(X) = X^{(p-1)p^{v-1}} + \cdots + X^{p^{v-1}} + 1$ be the p^v-th cyclotomic polynomial. We have the following isomorphism of $\mathbb{Z}[\langle\sigma\rangle]$-modules

$$\mathbb{Z}[X]/(f(X)) \to \overline{\mathcal{C}}_{L_v}/\overline{\mathcal{C}}_{L_{v-1}}$$

sending the class of X to the class of α_v. Since $\mathbb{Z}[X]/(f(X)) \cong \mathbb{Z}[\zeta_{p^v}]$ and $\eta_v = \alpha_v^{y_v}$, we have

$$\begin{aligned}\big[\overline{\mathcal{C}}_{L_v} : (\overline{\mathcal{C}}_{L_{v-1}}\mathcal{C}_{L_v})\big] &= \big[\overline{\mathcal{C}}_{L_v}/\overline{\mathcal{C}}_{L_{v-1}} : (\overline{\mathcal{C}}_{L_{v-1}}\mathcal{C}_{L_v})/\overline{\mathcal{C}}_{L_{v-1}}\big] \\ &= \Big|\mathbb{Z}[\zeta_{p^v}]/\Big(\prod_{j\in M_v'}(1-\zeta_{p^v}^{c_j n_j})\Big)\Big| = \prod_{j\in M_v'} p^{n_j},\end{aligned}$$

where $M_v' = \{j \in M_v;\ 1 < j < \max M_v\}$. The lemma follows from (3.6) and the induction hypothesis. □

The statement concerning $\mathbb{Z}$-bases which we have used in the previous proof will be useful later on, so we state it here explicitly:

Lemma 3.3. *The set $\bigcup_{v=1}^{k}\{\alpha_v^{\sigma^i};\ 0 \le i < (p-1)p^{v-1}\}$ is a $\mathbb{Z}$-basis of $\overline{\mathcal{C}}_K$.*

Proof of Theorem 3.1. The index $[\overline{\mathcal{C}}_K : \mathcal{C}_K]$ is immediately given by Lemma 3.2 for $v = k$. We have

$$\sum_{i=1}^{k}\sum_{j\in M_i} n_j = \sum_{j=1}^{s}\sum_{\substack{i=1,\dots,k\\ p^i > q_j}} n_j = \sum_{j=1}^{s} n_j\big(k - \log_p q_j\big).$$

Therefore

$$n = \Big(\sum_{j=1}^{s} n_j\big(k-\log_p q_j\big)\Big) - \Big(\sum_{i=1}^{k} n_{\max M_i}\Big) - k + \big|\{i;\,|M_i| = 1\}\big|$$

and

$$\big[\overline{\mathcal{C}}_K : \mathcal{C}_K\big] = \Big(\prod_{j=1}^{s}\big(\tfrac{l}{q_j}\big)^{n_j}\Big)\cdot\Big(\prod_{i=1}^{k} p^{-n_{\max M_i}}\Big)\cdot p^{-k+|\{i;|M_i|=1\}|}.$$

Sinnott's index formula in [6, Theorems 4.1 and 5.3] gives in our case

$$\big[\mathcal{O}_K^{\times} : \mathcal{C}_K\big] = 2^{l-1}\cdot h_K \cdot p^{-k+|\{i;|M_i|=1\}|}.$$

The theorem follows by taking the quotient of the two index formulas. □

Let us show now that the divisibility of the class number h_K obtained in (3.3) is stronger than the divisibility by $[\overline{K} : K]$ given by genus theory.

Proposition 3.4. *The number*

$$\bar{\varphi}_K = \frac{1}{[\overline{K} : K]} \cdot \Big(\prod_{i=1}^{k} p^{-n_{\max M_i}}\Big) \cdot \prod_{j=1}^{s} \Big(\frac{l}{q_j}\Big)^{n_j}$$

is a positive integer. Moreover, $\bar{\varphi}_K = 1$ if and only if $n_1 = \cdots = n_{s-1} = 1$.

Proof. Recall that $q_j = lp^{-k_j}$ is the index of the inertia group of p_j in $\mathrm{Gal}(K/\mathbb{Q})$, so $\frac{l}{q_j} = p^{k_j}$ is the ramification index of p_j. Hence $[\overline{K} : K] = p^{-k} \prod_{j=1}^{s} p^{k_j}$ and (3.2) implies

$$k_j = |\{i; 1 \le i \le k,\ j \in M_i\}|.$$

Therefore

$$\bar{\varphi}_K = \prod_{j=1}^{s} \big(p^{k_j - |\{i; 1 \le i \le k,\ j = \max M_i\}|}\big)^{n_j - 1}.$$

Since

$$k_j - |\{i; 1 \le i \le k,\ j = \max M_i\}| = |\{i; 1 \le i \le k,\ j \in M_i,\ j < \max M_i\}|$$

we see that $\bar{\varphi}_K$ is an integer and that $\bar{\varphi}_K = 1$ if $n_1 = \cdots = n_{s-1} = 1$. Let us assume that $\bar{\varphi}_K = 1$ and $n_{s-1} > 1$. We have

$$n_j > 1 \implies \{i; 1 \le i \le k,\ j \in M_i\} = \{i; 1 \le i \le k,\ j = \max M_i\}$$

for each $j = 1, \ldots, s$. Let t be defined by $1 = n_1 = \cdots = n_t < n_{t+1}$, so $t < s - 1$. Then $t + 1 \in M_k$ gives $t + 1 = \max M_k = s$, contradiction. □

At the end of this section we shall give another interpretation of the product $\prod_{j=1}^{s} \big(\frac{l}{q_j}\big)^{n_j} = \prod_{j=1}^{s} p^{k_j n_j}$ appearing in (3.3). For a Galois extension L/F of number fields let $e(L/F)$ be the product of the ramification indices in L/F of all (non-zero) prime ideals of the ring $\mathcal{O}_F$ of integers of F.

Proposition 3.5. *Using the filtration* (3.1) *of subfields of K we get*

$$\prod_{j=1}^{s} \Big(\frac{l}{q_j}\Big)^{n_j} = \prod_{j=1}^{s} p^{k_j n_j} = \prod_{i=1}^{k} e(L_i/L_{i-1}).$$

Proof. Since the only ramifying primes in $K/\mathbb{Q}$ are the primes $p_1, \ldots, p_s$, it is enough to compute the contribution of primes above p_j to the product on the right-hand side for each $j = 1, \ldots, s$. The primes above p_j ramify in L_i/L_{i-1} if and only if $i > k - k_j$ and for each of these k_j values of i the number of primes of L_{i-1} above p_j equals n_j and their ramification degree in L_i/L_{i-1} is p. □

4. Another view on class number divisibility

In this section we give a different method of establishing divisibility statements on class numbers of the same type of fields as considered previously. In a certain class of cases we will get exactly the same divisibility, in the remaining cases we obtain somewhat less. The main tool is the Ambiguous Class Number Formula (AmCNF for short).

This formula contains as a crucial input the global ramification index $e(L/F)$ of a Galois extensions L/F, which was already defined at the end of the last section. Recall that an important part of the class number factor φ_K can also be expressed in terms of these ramification indices, see Proposition 3.5. Recall moreover that K is a cyclic abelian field of degree $l = p^k$, and the subfield of absolute degree p^i is denoted L_i (so $L_0 = \mathbb{Q}$ and $L_k = K$). The ramification degree of p_j in K is l/q_j. This defines q_j, and n_j (a divisor of q_j) is defined to be the index of the decomposition group of p_j in $\mathrm{Gal}(K/\mathbb{Q})$, in other words: the number of primes above p_j in K.

We now state the AmCNF for a cyclic Galois extension L/F with Galois group Γ (see [5, chapter 13, Lemma 4.1]). With E_F denoting the unit group $\mathcal{O}_F^\times$, it says

$$|\,\mathrm{cl}_L^\Gamma\,| = |\,\mathrm{cl}_F\,| \cdot \frac{e(L/F)}{[E_F : E_F \cap N_{L/F}L^\times] \cdot [L:F]}.$$

The term $[E_F : E_F \cap N_{L/F}F^\times]$ will be (a little inaccurately) called *norm index*; it is the most delicate ingredient, and we will just bound it from above, thus bounding the order of the Γ-invariant part of cl_L from below. If Γ is a p-group, then all factors except possibly $|\,\mathrm{cl}_L^\Gamma\,|$ and $|\,\mathrm{cl}_F\,|$ are p-powers, so it makes sense to replace them by the corresponding p-parts. Finally, the big fraction on the right hand side will be abbreviated to $\epsilon(L/F)$.

Now we return to $K/\mathbb{Q}$. Then an obvious inductive argument along the tower $\mathbb{Q} \subset L_1 \subset \ldots \subset L_{k-1} \subset K$ gives:

$$h_K = |\,\mathrm{cl}_K\,| \text{ is divisible by the } p\text{-power } \prod_{i=1}^{k} \epsilon(L_i/L_{i-1}). \tag{4.1}$$

(Should the exponent of that p-power be negative, this statement is simply to be regarded as void.) Note: we get this divisibility even for $|\,\mathrm{cl}_K^{\mathrm{Gal}(K/L_{k-1})}\,|$, but we do not get it for $\mathrm{cl}_K^{\mathrm{Gal}(K/\mathbb{Q})}$. So we prefer to stick to $|\,\mathrm{cl}_K\,|$, for simplicity.

We evaluate the product $\prod_{i=1}^{k} \epsilon(L_i/L_{i-1})$. By Proposition 3.5, the product of the e-terms is $\prod_{j=1}^{s} \left(\frac{l}{q_j}\right)^{n_j}$. The product of the terms $[L_i : L_{i-1}]$ in the denominator of each $\epsilon(L_i/L_{i-1})$ is simply p^k. Let us denote by ν_i the norm-index term $[E_{L_{i-1}} : E_{L_{i-1}} \cap N_{L_i/L_{i-1}}L_i^\times]$.

Lemma 4.1. (i) *We have the divisibility relation* $\nu_i \mid p^{p^{i-1}-1}$. *Note that the latter term is 1 for* $i = 1$.

(ii) *The product* $p^k \nu_2 \dots \nu_k$ *divides* $p^{(p^k-1)/(p-1)}$.

PROOF. (i) The index ν_i is the order of the abelian group $M = E_{L_{i-1}}/E_{L_{i-1}} \cap N_{L_i/L_{i-1}} L_i^{\times}$. This group is annihilated by p (the degree of L_i/L_{i-1}), and it requires at most $p^{i-1} - 1$ generators, since the rank of $E_{L_{i-1}}$ is precisely this number, by Dirichlet, and there are no p-th roots of unity in $E_{L_{i-1}}$. This also works for $i = 1$.

(ii) An easy consequence of (i) and the geometric summation formula. □

Hence (4.1) implies, by the preceding lemma and remarks, the following result.

Theorem 4.2. *The class number* h_K *is divisible by the number*

$$\varphi'_K := \prod_{j=1}^{s} \Big(\frac{l}{q_j}\Big)^{n_j} \Big/ p^{(p^k-1)/(p-1)}.$$

We now wish to compare this to the results of the previous section. Let $\mu_i = n_{\max M_i}$ (for the definition of the sets M_i, please refer back to (3.2)). It was shown in Theorem 3.1 that h_K is divisible by the number

$$\varphi_K = \prod_{j=1}^{s} \Big(\frac{l}{q_j}\Big)^{n_j} \Big/ \prod_{i=1}^{k} p^{\mu_i}.$$

It strikes the eye that the numerators in φ'_K and φ_K are the same, so the obvious task is to compare the denominators. If for instance $\mu_i = p^{i-1}$ for $i = 1, \dots, k$, then $\varphi_K = \varphi'_K$. And this can easily happen. Just assume that to each divisor $p^t > 1$ of l there exist at least one p_j having precisely this ramification index, and no inertia. Then j will be in M_{k-t+1}, and actually $n_j = p^{k-t}$ will equal μ_{k-t+1}, since no prime that starts ramifying in L_{k-j+1} can have decomposition index larger than p^{k-t}. That is, $\mu_i = p^{i-1}$ for all i.

On the other hand it is easy to find examples with $\varphi_K \neq \varphi'_K$. We discuss a somewhat more complicated example. Take $k = 3$ and $s = 4$; assume $M_1 = \{1\}$, $M_2 = \{1, 2, 3\}$ and $M_3 = \{1, 2, 3, 4\}$. We are forced to take $n_1 = 1$. We take $n_2 = n_3 = p$ (that is, we choose p_2 and p_3, the two primes that start to ramify in L_2/L_1, to be split in $L_1/\mathbb{Q}$), and we take $n_4 = p$ too. So p_4 is split in $L_1/\mathbb{Q}$, inert in L_2/L_1 and ramified in L_3/L_2.

The common numerator of φ_K and φ'_K comes out as $p^3 \cdot p^{2p} \cdot p^{2p} \cdot p^p = p^{5p+3}$. We compare the denominators, giving names to them. Let $d(K)$ and $d'(K)$ be the denominator of φ_K and φ'_K, respectively. Then

$$d'(K) = p^{(p^k-1)/(p-1)}, \quad d(K) = \prod_{i=1}^{k} p^{\mu_i}.$$

Hence $d'(K) = p^{1+p+p^2}$. For $d(K)$ we note that $\mu_1 = 1$ and $\mu_2 = \mu_3 = p$. So $d(K) = p^{1+2p}$, which is much smaller. That is, the divisibility result obtained in the last section is much stronger than the one obtained with AmCNF.

In fact there is a big improvement possible. In the example (and in many other cases as we will see) it is unwise to apply the AmCNF to *every* layer in the tower. Let us apply it to L_1/L_0 and to L_3/L_1. The only change is in the upper bounds for the norm index factors. For L_1/L_0 this is 1 (since $L_0 = \mathbb{Q}$ has unit rank zero). For L_3/L_1, the degree is now p^2 but the unit rank is just $p-1$, which gives an upper bound of p^{2p-2}. Previously we had 1 for L_1/L_0, p^{p-1} for L_2/L_1 and p^{p^2-1} for L_3/L_2. Let $d''(K)$ be the denominator that arises in the new procedure, that is, the product of the norm index bounds for L_1/L_0 and L_3/L_1 times the factor $p^k = p^3$ (which is also present in $d'(K)$). Then we get:

$$d'(K) = p^{1+p+p^2}; \quad d''(K) = p^{1+2p},$$

and the latter is much better; in fact it matches $d(K)$.

In the rest of this section we explain how to systematise this improvement of the AmCNF approach, and how close we get to the other approach. In a well-described and fairly large class of cases which contains the example just discussed, we will exactly match it.

Let us call the index $i \in \{1, \ldots, k-1\}$ a *jump* if $\mu_{i+1} > \mu_i$. Furthermore the indices 0 and k are declared to be jumps. In the preceding example, the jumps are 0, 1 and 3. If $i < i'$ are consecutive jumps, then for all $j \in M_{i'} - M_i$, the decomposition index of p_j is at most μ_{i+1}, the largest decomposition index of any prime in M_{i+1}, and hence p_j cannot split from L_i to $L_{i'}$. This implies that $e(L_{i'}/L_i) = \prod_{\iota=i+1}^{i'} e(L_\iota/L_{\iota-1})$: the global ramification index $e(-/-)$ is multiplicative between two jumps. This motivates the following procedure.

Let $0 = s_0 < s_1 < \ldots < s_\kappa = k$ be all the jumps (so $\kappa \leq k$). Apply the AmCNF to the extensions L_{s_1}/L_0, L_{s_2}/L_{s_1}, …, $K = L_{s_\kappa}/L_{s_{\kappa-1}}$. The product of the corresponding e-factors is, by the preceding paragraph, the same as the product $\prod_{i=1}^{k} e(L_i/L_{i-1})$, which was calculated already in Proposition 3.5. The degree factors $[L_{s_t} : L_{s_{t-1}}]$ also multiply up to give p^k as earlier. We are left

with the norm index factors $\nu^{(t)} := [E(L_{s_{t-1}}) : E(L_{s_{t-1}}) \cap N_{L_{s_t}/L_{s_{t-1}}} L_{s_t}^{\times}]$. Each of them is bounded above (by similar arguments as before) by p to the power $u_t := (s_t - s_{t-1})(p^{s_{t-1}} - 1)$. Define

$$d''(K) := p^k \prod_{t=1}^{\kappa} p^{u_t} = p^{\sum_{t=1}^{\kappa}(s_t - s_{t-1})p^{s_t - 1}}.$$

(This notation is consistent with the last example!) Then by the same arguments as before we obtain:

Theorem 4.3. *h_K is divisible by $\varphi''(K) = \prod_{j=1}^{s} (\frac{l}{q_j})^{n_j} / d''(K)$.*

For each $i = 1, \ldots, k$ let i' denote the biggest jump below i, plus one. In other words, i' is minimal with $\mu_{i'} = \mu_i$. We then can rewrite

$$d''(K) = \prod_{i=1}^{k} p^{p^{i'-1}}.$$

Clearly we have $p^{i'-1} \geq \mu_{i'} = \mu_i$. (The reason for $\geq$ is that primes with index in $M_{i'}$ have to ramify in $L_{i'}/L_{i'-1}$, so they are totally ramified from $L_{i'-1}$ onwards.) Now $d(K)$ equals $\prod_{i=1}^{k} p^{\mu_i}$. Therefore we have:

Proposition 4.4. (i) *$d(K) \mid d''(K)$ holds in general. This means that the divisibility statement in Theorem 4.3 is never stronger than the statement in Theorem 3.1.*

(ii) *The equality $d(K) = d''(K)$ holds if and only if*

$$p^i = \mu_{i+1} \text{ for all jumps } i < k. \tag{4.2}$$

(Note the notation shift in the last formula: $i' - 1$ has become i.)

It is helpful to recall our example. There the jumps were $i = 0, 1, 3$, and we had $\mu_1 = 1$, $\mu_2 = p$. So the equivalent conditions in part (ii) of the proposition hold.

It is tricky to understand the precise meaning of the equations (4.2). We give an equivalent characterisation with a sketch of a geometric proof.

Proposition 4.5. *The equations* (4.2) *are equivalent to the statement*

$$\begin{aligned} &\text{For every } j = 1, \ldots, s \text{ there exists } j' \in \{1, \ldots, s\} \text{ such} \\ &\qquad \text{that } n_j \leq n_{j'} \leq q_j \text{ and } p_{j'} \text{ has no inertia (that is, } n_{j'} = q_{j'}). \end{aligned} \tag{4.3}$$

Before the proof, we again look at our example. There $n_1 = 1$; actually (4.3) is void for $j = 1$, since p_1 is always fully ramified and hence without inertia. Looking at $j = 2, 3, 4$, we always have $n_j = p$; so we can take $j' = 2$, since p_2 has no inertia. Hence (4.3) holds. It certainly also holds in the situation where $\mu_i = p^{i-1}$ for all i, because this yields inertia-less primes of any given ramification index > 1.

Now for the sketch of proof. Each prime p_j defines a point with integer coordinates $(\log_p n_j, \log_p q_j)$ in the first quadrant of the x-y-plane. (Coordinates can be zero, but not negative.) Since n_j divides q_j, all such points are on or above the diagonal $x = y$. One should think of each p_j as defining a counter in a board game; the counter is to be placed at the position with the coordinates given above. One just has to accept the fact that positions may be occupied by many counters at once (just pile them up).

Then the sets M_i consist exactly of the counters whose y-coordinate is less than i. In particular, the origin $(0, 0)$ is occupied by the totally ramified p_j. Thus μ_i indicates how far the rows having $y < i$ extend to the right. Then i is a jump iff the rightmost counter in row $y = i$ is a "corner", that is, there are no counters in the south-east quadrant whose origin is occupied by this counter. (More formally, a counter at position (h, i) is a *corner* if all positions $(h', i') \neq (h, i)$ with $h' \geq h$ and $i' \leq i$ are empty.) Condition (4.2) says: Every corner is on the diagonal. Condition (4.3) says: Starting from every counter which is not on the diagonal one can find another one which is on the diagonal, no higher than the given one, and no farther to the left. It is now "clear" from intuition that the two statements are equivalent. Any corner not on the diagonal clearly violates the second statement. On the other hand, any counter from which no other counter is visible in the south-east is a corner. As an illustration we depict the situation in our example, with four counters. Note the counters 2 and 3 in the same position:

$$\begin{array}{cccc} \cdot & \cdot & \cdot & \cdot \\ \cdot & \odot_4 & \cdot & \\ \cdot & \odot_{2,3} & & \\ \odot_1 & & & \end{array}$$

One can see that the two corners are both on the diagonal. To finish, let us look at another situation:

$$\begin{array}{cccc} \cdot & \cdot & \odot_5 & \cdot \\ \cdot & \odot_4 & \cdot & \\ \cdot & \odot_{2,3} & & \\ \odot_1 & & & \end{array}$$

Here the fifth counter makes up a corner not on the diagonal, and hence the equalities (4.2) cannot all hold.

5. Annihilating the class group of K

In this section we introduce one more assumption: let us assume that $K/\mathbb{Q}$ is tamely ramified, in other words, the prime p is unramified in $K/\mathbb{Q}$. This allows us to use [1, Theorem 12] since the proof of this theorem has not used the assumption of paper [1] that each prime ramifying in $K/\mathbb{Q}$ ramifies totally.

We shall use the notation and terminology introduced above: recall that $\mu_i = n_{\max M_i}$ and that $\alpha_i = \gamma_i^{z_i}$, where z_i and $1-\sigma^{\mu_i}$ are associated in $\mathbb{Z}[\langle\sigma\rangle]$. We put $\mu_0 = 0$ and recall that $i \in \{0, 1, \dots, k\}$ is a jump iff $i = k$ or $i < k$ and $\mu_{i+1} > \mu_i$.

Lemma 5.1. *Let $0 = s_0 < s_1 < \ldots < s_\kappa = k$ be all the jumps. Then the set $\bigcup_{t=1}^{\kappa} \{\alpha_{s_t}^{\sigma^i};\ 0 \le i < p^{s_t} - p^{s_{t-1}}\}$ is a $\mathbb{Z}$-basis of $\overline{\mathcal{C}}_K$.*

Proof. Let $0 < u < v \le k$ satisfy $\mu_u = \mu_v$. Then all $z_u, z_{u+1}, \dots, z_v$ are associated with $1-\sigma^{\mu_u}$ in $\mathbb{Z}[\langle\sigma\rangle]$. Since (3.4) implies

$$\mathrm{N}_{L_v/L_u}(\gamma_v)^{z_v} = \gamma_u^{z_v},$$

we have

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

Therefore $\alpha_{s_1}, \dots, \alpha_{s_\kappa}$ are Galois module generators of $\overline{\mathcal{C}}_K$. The lemma follows because the given set has visibly at most $p^k - 1$ elements and the norm $\mathrm{N}_{L_{s_t}/L_{s_{t-1}}}$ corresponds to $1 + \sigma^{p^{s_{t-1}}} + \sigma^{2p^{s_{t-1}}} + \cdots + \sigma^{p^{s_t} - p^{s_{t-1}}}$. □

We denote $E = \mathcal{O}_K^\times$. We can suppose that μ described by Theorem 1.2 satisfies $\mu \notin E$ since otherwise we take $\mu \cdot p_1$ instead of μ (this change does not affect the properties of μ described by Theorems 1.2 and 2.2). For brevity, let $\langle\mu\rangle = \langle\mu\rangle_{\mathbb{Z}[\langle\sigma\rangle]} \subset K^\times$ be the $\mathbb{Z}[\langle\sigma\rangle]$ submodule generated by μ.

Lemma 5.2. *Let r be the highest jump less than k, i.e., $\mu_r < \mu_{r+1} = n_s$. If $\rho \in \mathbb{Z}[\langle\sigma\rangle]$ satisfies $\mu^\rho \in \overline{\mathcal{C}}_{L_r}$ then*

$$(1 + \sigma + \sigma^2 + \cdots + \sigma^{p^r - 1})\rho = 0.$$

Proof. There are $t \in \mathbb{Z}$ and $\rho' \in \mathbb{Z}[\langle\sigma\rangle]$ such that $\rho = t + (1-\sigma)\rho'$. Since $\mu^{1-\sigma} = \alpha_k \in E$, we get $\mu^t \in E$ and so $t = 0$. Hence $\alpha_k^{\rho'} = \mu^\rho \in \overline{\mathcal{C}}_{L_r}$. There is a

unique $f \in \mathbb{Z}[x]$, $\deg f < p^k$, such that $\rho' = f(\sigma)$. Let $g \in \mathbb{Z}[x]$, $\deg g < p^k - p^r$, be the remainder upon division of f by $x^{p^k-p^r} + \cdots + x^{2p^r} + x^{p^r} + 1$. Then $\alpha_k^{g(\sigma)} \in \overline{\mathcal{C}}_{L_r}$ and Lemma 5.1 implies that $g = 0$. Therefore

$$\rho' = (1 + \sigma^{p^r} + \sigma^{2p^r} + \cdots + \sigma^{p^k-p^r})\rho''$$

for suitable $\rho'' \in \mathbb{Z}[\langle\sigma\rangle]$ and the lemma follows. □

Let us fix an annihilator $\varkappa \in \mathrm{Ann}_{\mathbb{Z}[\langle\sigma\rangle]}(E/\overline{\mathcal{C}}_K)$ and a large p-power M divisible by l^{s-1}. We construct a map $z_1 : \langle\mu\rangle E \to \mathbb{Z}[\langle\sigma\rangle]$ as follows: for any $u \in \langle\mu\rangle E$ we have $u^\varkappa \in \langle\mu\rangle\overline{\mathcal{C}}_K = \langle\mu\rangle\overline{\mathcal{C}}_{L_r}$ due to Lemma 5.1, hence $u^\varkappa = \mu^\rho \cdot v$ for suitable $\rho \in \mathbb{Z}[\langle\sigma\rangle]$ and $v \in \overline{\mathcal{C}}_{L_r}$. If we put

$$z_1(u) = (1 + \sigma + \sigma^2 + \cdots + \sigma^{p^r-1})\rho$$

then $z_1(u)$ is well-defined due to Lemma 5.2. It is obvious that z_1 is $\mathbb{Z}[\langle\sigma\rangle]$-linear and that

$$z_1(\mu) = (1 + \sigma + \sigma^2 + \cdots + \sigma^{p^r-1})\varkappa.$$

Let $z_0 : (\langle\mu\rangle E)/M \to \mathbb{Z}/M[\langle\sigma\rangle]$ be the reduction of z_1 modulo M. Let $\tilde{V} = (\langle\mu\rangle E)/M$ and V be the image of $\tilde{V}$ in $K^\times/M$ under the canonical mapping $j : \tilde{V} \to V$.

Then [1, Lemmas 14 and 15] stated for π can be used for μ in our situation and [1, Proposition 16] gives a $\mathbb{Z}[\langle\sigma\rangle]$-linear map $z : V \to \mathbb{Z}/M[\langle\sigma\rangle]$ such that $z \circ j = (1 - \sigma)z_0$ and $z(V \cap \mathbb{Q}) = 0$.

Hence z satisfies all assumptions of [1, Theorem 12] and so Theorem 2.2 gives that $z(\mu)$, which is the class of $(1 - \sigma^{p^r})\varkappa$ modulo M, is an annihilator of $(\mathrm{cl}_{K,p})/(M/l^{s-1})$, a quotient of the p-Sylow subgroup $\mathrm{cl}_{K,p}$ of the class group cl_K of K. Since M can be arbitrarily large, we have proved the following generalization of [2, Theorem 1.3]:

Theorem 5.3. *If p is unramified in $K/\mathbb{Q}$ then*

$$\mathrm{Ann}_{\mathbb{Z}[\langle\sigma\rangle]}(\mathcal{O}_K^\times/\overline{\mathcal{C}}_K) \subseteq \mathrm{Ann}_{\mathbb{Z}[\langle\sigma\rangle]}\big((1 - \sigma^{p^r})\,\mathrm{cl}_{K,p}\big),$$

where r is the highest jump less than k, i.e., $\mu_r < \mu_{r+1} = n_s$. Therefore

$$(1 - \sigma^{p^r})\,\mathrm{Ann}_{\mathbb{Z}[\langle\sigma\rangle]}(\mathcal{O}_K^\times/\overline{\mathcal{C}}_K) \subseteq \mathrm{Ann}_{\mathbb{Z}[\langle\sigma\rangle]}(\mathrm{cl}_{K,p}).$$

The jump r can also be described as follows: $p^r = \min\{q_i;\ 1 \le i \le s,\ n_i = n_s\}$.

References

[1] C. Greither and R. Kučera, Annihilators for the class group of a cyclic field of prime power degree, *Acta Arith.* **112** (2004), 177–198.

[2] C. Greither and R. Kučera, Annihilators for the class group of a cyclic field of prime power degree II, *Canad. J. Math.* **58** (2006), 580–599.

[3] C. Greither and R. Kučera, Eigenspaces of the ideal class group, *Ann. Inst. Fourier (Grenoble)* **64** (2014), 2165–2203, doi: 10.5802/aif.2908.

[4] C. Greither and R. Kučera, Linear forms on Sinnott's module, *J. Number Theory* **141** (2014), 324–342, doi: 10.1016/j.jnt.2014.02.003.

[5] S. Lang, Cyclotomic Fields I and II, Combined 2nd Edition, Graduate Texts in Mathematics 121, *Springer, New York*, 1990.

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

CORNELIUS GREITHER
INSTITUT FÜR THEORETISCHE INFORMATIK
MATHEMATIK UND OR
FAKULTÄT FÜR INFORMATIK
UNIVERSITÄT DER BUNDESWEHR MÜNCHEN
85577 NEUBIBERG
GERMANY

E-mail: cornelius.greither@unibw.de

RADAN KUČERA
FACULTY OF SCIENCE
MASARYK UNIVERSITY
KOTLÁŘSKÁ 2
611 37 BRNO
CZECH REPUBLIC

E-mail: kucera@math.muni.cz

(Received April 1, 2014; revised December 2, 2014)