ACTA ARITHMETICA
143.3 (2010)

On annihilators of the class group of an imaginary compositum of quadratic fields

by

Radan Kučera (Brno)

1. Introduction. Let k be an imaginary compositum of quadratic fields and suppose -1 is not a square in the genus field K of k in the narrow sense. This paper resumes the study of the Stickelberger ideal of k that started in [1], in a similar way as [2] does for circular units of a real compositum of quadratic fields. The aim of the paper is to prove a divisibility relation for the relative class number h^- of k and, in the case that 2 does not ramify in $k/\mathbb{Q}$, to construct new explicit annihilators of the class group of k not belonging to the Stickelberger ideal. These new annihilators are obtained as quotients of elements of the Stickelberger ideal, the usual source of annihilators, by suitable powers of 2.

The main result of this paper can be summarized as follows:

Theorem 1.1. *Let k be an imaginary compositum of quadratic fields such that 2 does not ramify in $k/\mathbb{Q}$. Let X' be the set of all odd Dirichlet characters corresponding to k. Let $\mathcal{S}_k$ be the Stickelberger ideal of k defined by Sinnott in* [4] *and let $\mathcal{T}_k \subseteq \mathbb{Z}[\mathrm{Gal}(k/\mathbb{Q})]$ be the subgroup defined below by means of explicit generators. Then $\mathcal{S}_k + 2\mathcal{T}_k$ annihilates the ideal class group Cl_k of k, and*

$$[(\mathcal{S}_k + 2\mathcal{T}_k) : \mathcal{S}_k] = \prod_{\substack{\chi\in X' \\ K_\chi \neq k\cap K_\chi}} \frac{[K_\chi : (k\cap K_\chi)]}{2},$$

where K_χ is the genus field of the quadratic field corresponding to χ.

Hence this approach gives explicit new annihilators of Cl_k if and only if there is an odd Dirichlet character χ corresponding to k such that the degree $[K_\chi : (k\cap K_\chi)] \geq 4$.

2010 *Mathematics Subject Classification*: Primary 11R20; Secondary 11R29.
Key words and phrases: Stickelberger ideal, imaginary compositum of quadratic fields, annihilators of the class group.

DOI: 10.4064/aa143-3-5 © Instytut Matematyczny PAN, 2010

2. Definitions and basic results. Recall that k is a compositum of quadratic fields such that -1 is not a square in the genus field K of k in the narrow sense. This condition can be written equivalently as follows: either 2 does not ramify in k and $k=\mathbb{Q}(\sqrt{d_1},\dots,\sqrt{d_s})$, where $d_1,\dots,d_s$ with $s\ge 1$ are square-free integers all congruent to 1 modulo 4, or 2 ramifies in k and there is a unique $x\in\{2,-2\}$ such that $k=\mathbb{Q}(\sqrt{d_1},\dots,\sqrt{d_s})$, where $d_1,\dots,d_s$ with $s\ge 1$ are square-free integers such that $d_i\equiv 1 \pmod 4$ or $d_i\equiv x \pmod 8$ for each $i\in\{1,\dots,s\}$. In the former case, let

$$J=\{p\in\mathbb{Z};\ p\equiv 1 \pmod 4,\ |p| \text{ is a prime ramifying in } k\},$$

and, in the latter case, let

$$J=\{x\}\cup\{p\in\mathbb{Z};\ p\equiv 1 \pmod 4,\ |p| \text{ is a prime ramifying in } k\}.$$

We assume that k is imaginary, i.e. at least one of d_i's is negative. For any $p\in J$, let

$$n_{\{p\}}=\begin{cases}|p| & \text{if } p \text{ is odd},\\ 8 & \text{if } p \text{ is even}.\end{cases}$$

For any $S\subseteq J$ let (by convention, an empty product is 1)

$$n_S=\prod_{p\in S} n_{\{p\}},\quad \zeta_S=e^{2\pi i/n_S},\quad \mathbb{Q}^S=\mathbb{Q}(\zeta_S),\quad K_S=\mathbb{Q}(\sqrt{p};\ p\in S),$$

and $k_S=k\cap K_S$. It is easy to see that $K_J=K$ and that n_J is the conductor of k. For any $p\in J$ let σ_p be the non-trivial automorphism in $\mathrm{Gal}(K_J/K_{J\setminus\{p\}})$. Then $G=\mathrm{Gal}(K_J/\mathbb{Q})$ can be considered as a (multiplicative) vector space over $\mathbb{F}_2$ with $\mathbb{F}_2$-basis $\{\sigma_p;\ p\in J\}$.

For any positive integer n let

$$\theta_n=\sum_{\substack{0<t\le n\\ (t,n)=1}}\frac{t}{n}\,\tau_t^{-1}$$

be the usual Stickelberger element in the rational group ring over the Galois group of the nth cyclotomic field; here τ_t means the automorphism sending each root of unity to its tth power. For any $S\subseteq J$ we define

$$\begin{aligned}\alpha_S&=\mathrm{cor}_{K_J/K_S}\,\mathrm{res}_{\mathbb{Q}^S/K_S}\,\theta_{n_S}\in\mathbb{Q}[G],\\ \beta_S&=\mathrm{cor}_{k/k_S}\,\mathrm{res}_{\mathbb{Q}^S/k_S}\,\theta_{n_S}\in\mathbb{Q}[G_k],\end{aligned}$$

where $G_k=\mathrm{Gal}(k/\mathbb{Q})$. Here res and cor mean the usual restriction and corestriction maps between group rings (see [4]). Let $N_K=\sum_{\sigma\in G}\sigma\in\mathbb{Z}[G]$ and $N_k=\sum_{\sigma\in G_k}\sigma\in\mathbb{Z}[G_k]$. Finally, let $\mathcal{S}'_K$ be the G-module generated in $\mathbb{Q}[G]$ by $\{\frac12 N_K\}\cup\{\alpha_T;\ T\subseteq J\}$ and similarly let $\mathcal{S}'_k$ be the G_k-module generated in $\mathbb{Q}[G_k]$ by $\{\frac12 N_k\}\cup\{\beta_T;\ T\subseteq J\}$. We have proved in [1, p. 159, Remark] that $\mathcal{S}'_K$ and $\mathcal{S}'_k$ are precisely the modules S' for K and k used by

Sinnott (see [4, p. 189]) to define the Stickelberger ideal, so $\mathcal{S}_K = \mathcal{S}'_K \cap \mathbb{Z}[G]$ and $\mathcal{S}_k = \mathcal{S}'_k \cap \mathbb{Z}[G_k]$ are the Stickelberger ideals of K and k, respectively.

LEMMA 2.1. *For any $S \subseteq J$ and any $\sigma \in G$ we have*

$$(1+\sigma)\cdot\alpha_S = a\cdot N_K + 2\sum_{T\subseteq S} a_T\cdot\alpha_T \quad \textit{for suitable } a, a_T \in \mathbb{Z}.$$

Proof. This is a direct consequence of [1, Lemma 18], because

$$(1+\sigma)\alpha_S = 2\alpha_S - (1-\sigma)\alpha_S. \ \blacksquare$$

PROPOSITION 2.2. *For any $S \subseteq J$ we have $[K_S : k_S]^{-1}\cdot \operatorname{cor}_{K/k}\beta_S \in \mathcal{S}'_K$.*

Proof. It is easy to see that $\mathrm{Gal}(K/k)$ is a subspace of the (multiplicative) vector space $\mathrm{Gal}(K/\mathbb{Q})$ over $\mathbb{F}_2$. Let $\rho_1,\dots,\rho_r$ be a basis of $\mathrm{Gal}(K/k)$. Then $\operatorname{cor}_{K/k} 1 = \sum_{\sigma\in\mathrm{Gal}(K/k)}\sigma = (1+\rho_1)\cdots(1+\rho_r)$. Using [1, Lemma 17] we obtain

$$[K : kK_S]\operatorname{cor}_{K/k}\beta_S = \operatorname{cor}_{K/k}\operatorname{res}_{K/k}\alpha_S = (1+\rho_1)\cdots(1+\rho_r)\cdot\alpha_S.$$

It is now easy to show by induction on r using Lemma 2.1 that

$$[K : kK_S]\operatorname{cor}_{K/k}\beta_S = 2^{r-1}a\cdot N_K + 2^r\sum_{T\subseteq S} a_T\cdot\alpha_T$$

for suitable $a, a_T \in \mathbb{Z}$. The proposition follows from $[K : k] = 2^r$ and $[kK_S : k] = [K_S : k_S]$. ∎

Let τ denote the complex conjugation (both in G and G_k, but there is no danger of confusion). Following Sinnott, we define

$$A_K = \{\delta \in \mathbb{Z}[G];\ (1+\tau)\delta \in N_K\mathbb{Z}\},$$
$$A_k = \{\delta \in \mathbb{Z}[G_k];\ (1+\tau)\delta \in N_k\mathbb{Z}\}.$$

We have $\mathcal{S}_k \subseteq A_k$ and $\mathcal{S}_K \subseteq A_K$ (see [4, Lemma 2.1]). Moreover, we shall need

$$A'_K = \begin{cases} A_K + \frac{1}{2}N_K\mathbb{Z} & \text{if } -3 \notin J,\\ A_K + \frac{1}{2}N_K\mathbb{Z} + \alpha_{\{-3\}}\mathbb{Z} & \text{if } -3 \in J,\end{cases}$$

and

$$A'_k = \begin{cases} A_k + \frac{1}{2}N_k\mathbb{Z} & \text{if } -3 \notin J,\\ A_k + \frac{1}{2}N_k\mathbb{Z} + \beta_{\{-3\}}\mathbb{Z} & \text{if } -3 \in J.\end{cases}$$

LEMMA 2.3. *The indices $[A'_K : A_K]$ and $[A'_k : A_k]$ are equal to the numbers of roots of unity in K and k, respectively.*

Proof. First assume that $-3 \notin J$. Then ±1 are the only roots of unity in both K and k and the lemma follows. Now, let $-3 \in J$. Then K has exactly six roots of unity and $\alpha_{\{-3\}} = \operatorname{cor}_{K/\mathbb{Q}(\sqrt{-3})}(\frac{1}{3} + \frac{2}{3}\sigma_{-3})$. On one hand, if $\sqrt{-3} \notin k$ then $\beta_{\{-3\}} = N_k$. On the other hand, if $\sqrt{-3} \in k$ then $\beta_{\{-3\}} = \operatorname{cor}_{k/\mathbb{Q}(\sqrt{-3})}(\frac{1}{3} + \frac{2}{3}\sigma_{-3})$. The lemma follows in both cases. ∎

PROPOSITION 2.4. *For any $S \subseteq J$ we have $\gamma_S = [K_S : k_S]^{-1} \cdot \beta_S \in A'_k$.*

Proof. One can see immediately from the definitions that $\mathcal{S}_K + \frac{1}{2}N_K\mathbb{Z} \subseteq \mathcal{S}'_K$ and that in the case $-3 \in J$ we have $\mathcal{S}_K + \frac{1}{2}N_K\mathbb{Z} + \alpha_{\{-3\}}\mathbb{Z} \subseteq \mathcal{S}'_K$. Sinnott proved in [4, Proposition 2.1] that $[\mathcal{S}'_K : \mathcal{S}_K]$ is equal to the number of roots of unity in K, and a similar discussion to the proof of Lemma 2.3 gives

$$\mathcal{S}'_K = \begin{cases} \mathcal{S}_K + \frac{1}{2}N_K\mathbb{Z} & \text{if } -3 \notin J, \\ \mathcal{S}_K + \frac{1}{2}N_K\mathbb{Z} + \alpha_{\{-3\}}\mathbb{Z} & \text{if } -3 \in J. \end{cases}$$

This implies that $\mathcal{S}'_K \subseteq A'_K$. We can prove similarly $\mathcal{S}'_k \subseteq A'_k$. We have $\beta_S \in \mathcal{S}'_k \subseteq A'_k$, i.e. $[K_S : k_S] \cdot \gamma_S \in A'_k$. To avoid distinguishing two cases, in the case $-3 \notin J$ we put $\alpha_{\{-3\}} = 0$. Proposition 2.2 gives that there are $c, d \in \mathbb{Z}$ such that

$$[K_S : k_S]^{-1} \cdot \operatorname{cor}_{K/k} \beta_S + \frac{c}{2} \cdot N_K + d \cdot \alpha_{\{-3\}} \in A_K.$$

In both cases we have $3\alpha_{\{-3\}} \in A_K$ and so

$$3[K_S : k_S]^{-1} \cdot \operatorname{cor}_{K/k} \beta_S + \frac{3c}{2} \cdot N_K \in A_K.$$

Hence

$$\operatorname{cor}_{K/k}\left(3\gamma_S + \frac{3c}{2} \cdot N_k\right) \in A_K,$$

which means $3\gamma_S + (3c/2) \cdot N_k \in A_k$ and so $3\gamma_S \in A'_k$. The proposition follows as $[K_S : k_S]$ and 3 are relatively prime. ∎

LEMMA 2.5. *For any $S \subseteq J$ and any $\sigma \in G_k$ we have*

$$(1 - \sigma) \cdot \gamma_S = a \cdot N_k + 2 \sum_{T \subsetneq S} a_T \cdot \gamma_T \quad \textit{for suitable } a, a_T \in \mathbb{Z}.$$

Proof. In [1, proof of Lemma 19] we have derived the identity

$$(1 - \sigma) \cdot \beta_S = a[kK_S : k] \cdot N_k + 2 \sum_{T \subsetneq S} a_T [kK_S : kK_T] \cdot \beta_T$$

with $a, a_T \in \mathbb{Z}$. Dividing by $[kK_S : k] = [K_S : k_S]$ gives the lemma. ∎

LEMMA 2.6. *Let $p \in S \subseteq J$. Then*

$$(1 + \operatorname{res}_{K_J/k} \sigma_p)\gamma_S = (1 - \operatorname{Frob}(|p|, k))\gamma_{S\setminus\{p\}} + [\mathbb{Q}^S : K_S]N_k,$$

where $\operatorname{Frob}(|p|, k)$ *is any extension to k of the Frobenius automorphism of $|p|$ in $k_{J\setminus\{p\}}/\mathbb{Q}$.*

Proof. [1, Lemma 20] states

$$(1 + \operatorname{res}_{K_J/k} \sigma_p)\beta_S = (1 - \operatorname{Frob}(|p|, k))[kK_S : kK_{S\setminus\{p\}}]\beta_{S\setminus\{p\}} + [\mathbb{Q}^S : K_S][kK_S : k]N_k.$$

Since $[kK_S : kK_{S\setminus\{p\}}] = [kK_S : k][kK_{S\setminus\{p\}} : k]^{-1}$, the lemma follows. ∎

LEMMA 2.7. *For any non-empty $S \subseteq J$ we have*

$$(1+\tau)\gamma_S = [\mathbb{Q}^S : K_S]N_k.$$

Proof. The lemma follows from the identity $(1+\tau)\beta_S = [\mathbb{Q}^S : k_S]N_k$ given by [1, Lemma 21]. ∎

3. Divisibility of the relative class number h^- of k by a power of 2. Let

$$X = \{\xi \in \widehat{G};\ \xi(\tau) = 1,\ \xi(\sigma) = 1 \text{ for all } \sigma \in \mathrm{Gal}(K_J/k)\},$$
$$X' = \{\xi \in \widehat{G};\ \xi(\tau) = -1,\ \xi(\sigma) = 1 \text{ for all } \sigma \in \mathrm{Gal}(K_J/k)\},$$

where $\widehat{G}$ is the character group of G. Then X and X' can be viewed also as the sets of all even and of all odd Dirichlet characters corresponding to k, respectively. For any $\chi \in X \cup X'$ let

$$S_\chi = \{p \in J;\ \chi(\sigma_p) = -1\},$$

hence n_{S_χ} is the conductor of χ.

Let $\mathcal{T}'_k$ be the G_k-module generated in $\mathbb{Q}[G_k]$ by $\{\frac{1}{2}N_k\} \cup \{\gamma_S;\ S \subseteq J\}$. Proposition 2.4 states that $\mathcal{T}'_k \subseteq A'_k$.

THEOREM 3.1. *The set $B = \{\gamma_{S_\chi};\ \chi \in X'\} \cup \{\frac{1}{2}N_k\}$ is a $\mathbb{Z}$-basis of $\mathcal{T}'_k$ and*

$$[A'_k : \mathcal{T}'_k] = \frac{h^-}{Q} \cdot \left(\frac{2}{[K : K'] \cdot [K : k]}\right)^{[k:\mathbb{Q}]/4},$$

where K' is the genus field in the narrow sense of $k^+ = k \cap \mathbb{R}$, $h^- = h_k/h_{k^+}$ is the relative class number of k, and Q is the Hasse unit index of k, that is, $Q = [E : (E \cap \mathbb{R})W]$, where E and W are the group of units of k and the group of roots of unity in k, respectively.

Proof. We can prove that B is a system of generators of $\mathcal{T}'_k$ in the same way as [1, Lemma 22] was proved—it is enough to use Lemmas 2.5–2.7 instead of Lemmas 19–21 of [1]. In [1, Theorem 3] we have proved that the set

$$B' = \{\beta_{S_\chi};\ \chi \in X'\} \cup \{\tfrac{1}{2}N_k\}$$

is a basis of $\mathcal{S}'_k$. As $\mathcal{S}'_k \subseteq \mathcal{T}'_k$ and the sets B and B' have the same number of elements, we see that B is in fact a basis of $\mathcal{T}'_k$. The transition matrix from B' to B is the diagonal matrix whose diagonal consists of $[K_{S_\chi} : k_{S_\chi}]$, for all $\chi \in X'$, and 1. Thus

$$[\mathcal{T}'_k : \mathcal{S}'_k] = \prod_{\chi \in X'} [K_{S_\chi} : k_{S_\chi}].$$

Lemma 2.3 and [4, Proposition 2.1] give that both $[A'_k : A_k]$ and $[\mathcal{S}'_k : \mathcal{S}_k]$ are equal to the number of roots of unity in k and so $[A'_k : \mathcal{S}'_k] = [A_k : \mathcal{S}_k]$.

This equality and [1, Theorem 3] imply

$$[A'_k : \mathcal{S}'_k] = \frac{h^-}{Q} \cdot (\#X')^{-\frac{1}{2}(\#X')} \prod_{\chi\in X'} [k : k_{S_\chi}],$$

therefore

$$\begin{aligned}[A'_k : \mathcal{T}'_k] &= \frac{h^-}{Q} \cdot (\#X')^{-\frac{1}{2}(\#X')} \prod_{\chi\in X'} \frac{[k : k_{S_\chi}]}{[K_{S_\chi} : k_{S_\chi}]} \\ &= \frac{h^-}{Q} \cdot [k^+ : \mathbb{Q}]^{-[k^+:\mathbb{Q}]/2} \prod_{\chi\in X'} \frac{[k : \mathbb{Q}]}{[K_{S_\chi} : \mathbb{Q}]}.\end{aligned}$$

In [2, Lemma 8] we have proved

$$\prod_{\chi\in X} [K_{S_\chi} : \mathbb{Q}] = [K' : \mathbb{Q}]^{[k^+:\mathbb{Q}]/2}$$

and we can prove

$$\prod_{\chi\in X\cup X'} [K_{S_\chi} : \mathbb{Q}] = [K : \mathbb{Q}]^{[k:\mathbb{Q}]/2}$$

in the same way. Therefore

$$\prod_{\chi\in X'} [K_{S_\chi} : \mathbb{Q}] = [K : K']^{[k^+:\mathbb{Q}]/2} \cdot [K : \mathbb{Q}]^{[k^+:\mathbb{Q}]/2} \tag{3.1}$$

and the theorem follows. ∎

Corollary 3.2. *The relative class number h^- of k is divisible by the following power of* 2*:*

$$Q \cdot ([K : K'][K : k]/2)^{[k:\mathbb{Q}]/4} \mid h^-.$$

Proof. This follows from $\mathcal{T}'_k \subseteq A'_k$. ∎

Remark. Let us mention that the strength of Corollary 3.2 consists mainly in the algebraic interpretation of the divisibility result, because if $[k : \mathbb{Q}] \geq 8$ then one can get the stronger divisibility result (3.2) below using the analytical class number formula and genus theory as follows. For any $\chi \in X'$ let $B_{1,\chi}$ be the first generalized Bernoulli number and k_χ be the imaginary quadratic field corresponding to χ. Let h_χ and w_χ be the class number of k_χ and the number of roots of unity in k_χ, respectively. The analytical class number formula (for example, see [5, Theorem 4.17]) gives

$$h^- = Qw \prod_{\chi\in X'} (-\tfrac{1}{2}B_{1,\chi}) \quad \text{and} \quad h_\chi = w_\chi(-\tfrac{1}{2}B_{1,\chi}),$$

where $w = \#W \in \{2, 6\}$ is the number of roots of unity in k. It is easy to see that each w_χ equals 2 with at most one exception. This exceptional case

$w_\chi = 6$ appears if and only if $w = 6$, and in any case

$$h^- = 2Q \prod_{\chi \in X'} \frac{h_\chi}{2}.$$

The genus field of k_χ is K_{S_χ}, so genus theory gives

$$\tfrac{1}{2}[K_{S_\chi} : \mathbb{Q}] = [K_{S_\chi} : k_\chi] \mid h_\chi,$$

and using (3.1) we obtain

$$(3.2) \qquad 2Q \prod_{\chi \in X'} \frac{[K_{S_\chi} : \mathbb{Q}]}{4} = 2Q \cdot \left(\frac{[K : K'][K : \mathbb{Q}]}{16} \right)^{[k:\mathbb{Q}]/4} \Bigg| \, h^-.$$

4. The case of tame ramification. Let us assume that $k/\mathbb{Q}$ is not wildly ramified, i.e. 2 does not ramify in k, which means that the conductor $n = n_J$ of k is odd. Thus the parity of a character $\chi \in X \cup X'$ is determined by its conductor n_{S_χ}. Moreover n_S for all $S \subseteq J$ runs over all positive divisors of n without repetition. So we shall simplify our notation and if $d = n_S$ we shall write K_d, k_d, $\mathbb{Q}_d$, α_d, β_d, γ_d instead of K_S, k_S, $\mathbb{Q}^S$, α_S, β_S, γ_S etc.

We want to construct annihilators of the class group Cl_k of k outside of the Stickelberger ideal $\mathcal{S}_k$. Let $\mathcal{T}_k = \mathcal{T}_k' \cap \mathbb{Z}[G_k]$. The aim of this section is to show that elements of $\mathcal{T}_k$ annihilate the principal genus PG_k of k, i.e. the subgroup of Cl_k of all classes containing the prime ideals of k whose Frobenius on K/k is trivial. (Note that PG_k is also sometimes called the “non-genus part” of Cl_k.)

Lemma 4.1. *Each ideal class in the principal genus* PG_k *contains infinitely many prime ideals above primes* $p \equiv 1 \pmod{n}$.

Proof. As K is the maximal absolutely abelian subfield of the Hilbert class field H_k of k, and K is a subfield of the nth cyclotomic field $\mathbb{Q}_n$, we have $H_k \cap \mathbb{Q}_n = K$. Therefore for any class $C \in \mathrm{PG}_k$ there is an element in $\mathrm{Gal}(H_k\mathbb{Q}_n/k)$ whose restriction to $\mathbb{Q}_n$ is trivial and restriction to H_k is the Artin symbol of C. The lemma follows from the Chebotarev density theorem. ■

Let us fix a class $C \in \mathrm{PG}_k$ and a prime ideal $\mathcal{P} \in C$ above $p \equiv 1 \pmod{n}$. Of course, to show that elements of $\mathcal{T}_k$ annihilate C we shall use Stickelberger factorization of Gauss sums. Let $\chi\colon (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Q}_n^*$ be the nth power residue symbol modulo a prime ideal $\mathfrak{P}$ of $\mathbb{Q}_n$ above $\mathcal{P}$, i.e. for any $t \in \mathbb{Z}$ relatively prime to p we have $\chi(t) \equiv t^{(p-1)/n} \pmod{\mathfrak{P}}$. For any $a \in \mathbb{Z}$

with $n \nmid a$, we consider the Gauss sum

$$x_a = -\sum_{t=1}^{p-1} \chi(t)^{-a} \zeta_p^t,$$

where ζ_p is a fixed primitive pth root of unity. If $n \mid a \in \mathbb{Z}$ we put $x_a = 1$.

Lemma 4.2. *For any positive integer $r \mid n$ and any $a \in \mathbb{Z}$ we have*

$$\prod_{i=0}^{r-1} x_{a+in/r} = \chi(r)^{ar} \cdot p^{(r-1)/2} \cdot x_{ar}.$$

Proof. The Davenport–Hasse relation (for example, see [3, Theorem 10.2 of Chapter 2]) gives

$$\prod_{i=0}^{r-1} x_{a+in/r} = \chi(r)^{ar} \cdot x_{ar} \cdot \prod_{i=1}^{r-1} x_{in/r}.$$

Moreover if $n \nmid b$ then $x_b \cdot x_{-b} = \chi(-1)p$ (for example, see [3, GS 2 in §1 of Chapter 1]). But $\chi(-1) = 1$ as n is odd and the lemma follows. ∎

Well-known properties of Gauss sums show that $x_{n/d}^d$ is a non-zero element of the dth cyclotomic field $\mathbb{Q}_d$ for any positive $d \mid n$. We define $y_d = \mathrm{N}_{\mathbb{Q}_d/K_d}(x_{n/d}^d)$. Let $\mathfrak{p}$ be the prime ideal of K below $\mathfrak{P}$. Recall that $\mathcal{P}$ is the prime ideal of k below $\mathfrak{P}$.

Lemma 4.3. *We have*

$$(y_d) = \mathfrak{p}^{d\alpha_d} \qquad \textit{as ideals of } K$$

and

$$(\mathrm{N}_{K_d/k_d}(y_d)) = \mathcal{P}^{d\beta_d} \qquad \textit{as ideals of } k.$$

Proof. This has been proved by Sinnott (see [4, formulae (2.2), (3.2), (3.6), and (3.7)]), in the former case for Sinnott's k being our K, so Sinnott's $g_d'(-1, \mathfrak{p})$ and $\theta_d'(-1)$ correspond to our y_d and α_d, and in the latter case for Sinnott's k being our k, so Sinnott's $g_d'(-1, \mathcal{P})$ and $\theta_d'(-1)$ correspond to our $\mathrm{N}_{K_d/k_d}(y_d)$ and β_d. ∎

Lemma 4.4. *For any $d \mid n$ and any prime $q \mid d$ we have*

$$\mathrm{N}_{K_d/K_{d/q}}(y_d) = p^{d \cdot [\mathbb{Q}_d : K_d]} \cdot y_{d/q}^{q \cdot (1 - \mathrm{Frob}(q, K_{d/q}))}.$$

Proof. It is easy to see that

$$\mathrm{N}_{\mathbb{Q}_d/\mathbb{Q}_{d/q}}(x_{n/d}^d) = \prod_{\substack{b \equiv 1 \,(\mathrm{mod}\, n/q) \\ 1 \le b \le n,\, q \nmid b}} x_{bn/d}^d.$$

If an integer b satisfies $b \equiv 1 \pmod{n/q}$ and $q \mid b$ then $x_{bn/d}^{\mathrm{Frob}(q,\mathbb{Q}_{n/q})} = x_{qn/d}$. Hence

$$\mathrm{N}_{\mathbb{Q}_d/\mathbb{Q}_{d/q}}(x_{n/d}^d) = x_{qn/d}^{-d\cdot \mathrm{Frob}(q,\mathbb{Q}_{n/q})^{-1}} \cdot \prod_{i=0}^{q-1} x_{(n/d)+in/q}^d$$

and Lemma 4.2 gives

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}_d/\mathbb{Q}_{d/q}}(x_{n/d}^d) &= x_{qn/d}^{-d\cdot \mathrm{Frob}(q,\mathbb{Q}_{n/q})^{-1}} \cdot (\chi(q)^{qn/d} \cdot p^{(q-1)/2} \cdot x_{qn/d})^d \\ &= x_{qn/d}^{d\cdot (1-\mathrm{Frob}(q,\mathbb{Q}_{n/q})^{-1})} \cdot p^{d(q-1)/2}.\end{aligned}$$

Therefore

$$\mathrm{N}_{K_d/K_{d/q}}(y_d) = \mathrm{N}_{\mathbb{Q}_d/K_{d/q}}(x_{n/d}^d) = \mathrm{N}_{\mathbb{Q}_{d/q}/K_{d/q}}(x_{qn/d}^{d\cdot (1-\mathrm{Frob}(q,\mathbb{Q}_{n/q})^{-1})} \cdot p^{d(q-1)/2})$$

and the lemma follows. ∎

Let Y be the subgroup of the multiplicative group K^* generated by $-1, p$, and all conjugates of y_d for $d \mid n$. The following lemma shows that the action of the augmentation ideal of $\mathbb{Z}[G]$ on elements of Y gives the square of an element of Y multiplied by a power of p:

LEMMA 4.5. *For any $d \mid n$ and $\sigma \in G$ we have*

$$y_d^{1-\sigma} = p^a \cdot \prod_{t \mid d} y_t^{2a_t} \quad \textit{for suitable integers } a,\ a_t.$$

Proof. If $d = 1$ then $y_d = 1$ and the statement is trivial. Suppose that $d > 1$ and that the lemma has been proved for all divisors of n smaller than d. Let $R_\sigma \subseteq J$ be determined by $\sigma = \prod_{r \in R_\sigma} \sigma_r$. If $(n_{R_\sigma}, d) = 1$ then $y_d^{1-\sigma} = 1$. Suppose that $(n_{R_\sigma}, d) > 1$ and that the lemma has also been proved for this d and all $\rho \in G$ having $(n_{R_\rho}, d) < (n_{R_\sigma}, d)$. Fix any $q \in R_\sigma$, $q \mid d$. Then $\rho = \sigma_q \sigma$ satisfy $n_{R_\rho} = n_{R_\sigma}/|q|$. On one hand, if $n_{R_\rho} = 1$ then

$$y_d^{1-\sigma} = y_d^{1-\sigma_q} = y_d^2 \cdot (\mathrm{N}_{K_d/K_{d/|q|}}(y_d))^{-1}$$

and Lemma 4.4 together with the induction hypothesis gives what we need. On the other hand, if $n_{R_\rho} > 1$ then the lemma has already been proved for d with both ρ and σ_q. Hence

$$\begin{aligned} y_d^{1-\sigma} = y_d^{1-\sigma_q} \cdot (y_d^{1-\rho})^{\sigma_q} &= \Big(p^a \cdot \prod_{t \mid d} y_t^{2a_t}\Big) \cdot \Big(p^b \cdot \prod_{t \mid d} y_t^{2b_t}\Big)^{\sigma_q} \\ &= \Big(p^{a+b} \cdot \prod_{t \mid d} y_t^{2(a_t+b_t)}\Big) \cdot \prod_{t \mid d} (y_t^{1-\sigma_q})^{-2b_t}\end{aligned}$$

and the lemma follows from the induction hypothesis. ∎

THEOREM 4.6. *The set*

$$B = \{p\} \cup \{y_d;\ d \mid n,\ d > 0,\ d \equiv 3 \pmod 4\}$$

is a $\mathbb{Z}$-basis of Y, more precisely $B \cup \{-1\}$ is a system of generators of Y and B is multiplicatively independent over $\mathbb{Z}$.

Proof. Lemma 4.5 gives that Y is generated by $\{-1, p\} \cup \{y_d;\, d \mid n\}$. Let $d \mid n$, $d \equiv 1 \pmod 4$ and put $S = \{q \in J;\, q < 0,\, q \mid d\}$ and $\rho = \prod_{q \in S} \sigma_q$. Then the number of elements of S is even and ρ acts on y_d as the complex conjugation τ. Hence

$$y_d^\rho = y_d^\tau = \mathrm{N}_{\mathbb{Q}_d/K_d}(x_{-n/d}^d) = \mathrm{N}_{\mathbb{Q}_d/K_d}(p^d \cdot x_{n/d}^{-d}) = p^{d\cdot[\mathbb{Q}_d:K_d]} \cdot y_d^{-1}.$$

Therefore

$$\begin{aligned} y_d^2 &= p^{d\cdot[\mathbb{Q}_d:K_d]} \cdot y_d^{1-\rho} = p^{d\cdot[\mathbb{Q}_d:K_d]} \cdot \prod_{q \in S} (y_d^{1+\sigma_q})^{\prod_{t \in S,\, t<q}(-\sigma_t)} \\ &= p^{d\cdot[\mathbb{Q}_d:K_d]} \cdot \prod_{q \in S} \mathrm{N}_{K_d/K_{d/|q|}}(y_d)^{\prod_{t \in S,\, t<q}(-\sigma_t)}. \end{aligned}$$

Lemmas 4.4 and 4.5 give

$$y_d^2 = p^a \cdot \prod_{t \mid d,\, t<d} y_t^{2a_t}$$

for suitable integers a, a_t. But p is not a square in K, so a is even and

$$y_d = \pm p^{a/2} \cdot \prod_{t \mid d,\, t<d} y_t^{a_t}.$$

We have shown that $B \cup \{-1\}$ is a system of generators of Y.

Lemma 4.3 says $(y_d) = \mathfrak{p}^{d\alpha_d}$ as ideals of K, moreover $(p) = \mathfrak{p}^{N_K}$. As p splits completely in K, we have the G-module homomorphism $Y \to \mathbb{Z}[G]$ sending each $y \in Y$ to $\delta \in \mathbb{Z}[G]$ satisfying $(y) = \mathfrak{p}^\delta$. The image of Y is a submodule of finite index in the Stickelberger ideal $\mathcal{S}_K$, hence the $\mathbb{Z}$-rank of Y cannot be smaller than the $\mathbb{Z}$-rank of $\mathcal{S}_K$, which is equal to $1 + \frac{1}{2}[K : \mathbb{Q}]$ (see [4, Theorem 2.1]). But this equals the number of elements of B. Therefore B is multiplicatively independent over $\mathbb{Z}$. ∎

Lemma 4.7. *Let $y \in Y$ and $d \mid n$. If there is a positive integer r such that $y^{2^r} \in k_d$ then $y \in k_d$.*

Proof. It is enough to prove the lemma for $r = 1$ and to use induction. Assume $y^2 \in k_d$. Then for any $\sigma \in \mathrm{Gal}(K/k_d)$ we have $(y^2)^{1-\sigma} = 1$ and so $y^{1-\sigma} = \pm 1$. Lemma 4.5 gives that $y^{1-\sigma}$ belongs to a subgroup of Y generated by p and by y_t^2 for all $t \mid n$. Theorem 4.6 implies that this subgroup has no torsion and so $y^{1-\sigma} = 1$. ∎

Proposition 4.8. *For any $d \mid n$ there is $z_d \in k_d$ such that either*

$$z_d^{[K_d:k_d]} = \mathrm{N}_{K_d/k_d}(y_d)$$

or

$$z_d^{[K_d:k_d]} = p^{[K_d:k_d]/2} \cdot \mathrm{N}_{K_d/k_d}(y_d).$$

Proof. If $K_d = k_d$ there is nothing to prove. Assume that $K_d \neq k_d$ and so $[K_d : k_d]$ is even. As in the proof of Proposition 2.2, we choose a basis $\rho_1, \ldots, \rho_r$ of the (multiplicative) vector space $\mathrm{Gal}(K_d/k_d)$ over $\mathbb{F}_2$. Then $[K_d : k_d] = 2^r$ and

$$\mathrm{N}_{K_d/k_d}(y_d) = y_d^{(1+\rho_1)\cdots(1+\rho_r)}.$$

By induction on r using Lemma 4.5 we show that

$$y_d^{(1+\rho_1)\cdots(1+\rho_r)} = \Big(p^a \cdot \prod_{t|d} y_t^{2a_t}\Big)^{[K_d:k_d]/2}$$

for suitable integers a, a_t. We put

$$z_d = p^{-[-a/2]} \cdot \prod_{t|d} y_t^{a_t}$$

and one of the two equalities in the statement of the proposition follows depending on whether a is even or odd. As $z_d \in Y$ and $z_d^{[K_d:k_d]} \in k_d$, Lemma 4.7 gives $z_d \in k_d$. ∎

THEOREM 4.9. *The elements of $\mathcal{T}_k$ annihilate all ideal classes in the principal genus* PG_k *of* k.

Proof. As C has been chosen as an arbitrary class in PG_k it is enough to show that $\mathcal{T}_k \subseteq \mathcal{A}$, where $\mathcal{A}$ is the annihilator of C. We have $\mathcal{P} \in C$ and so $\mathcal{A} = \{\alpha \in \mathbb{Z}[G];\ \mathcal{P}^\alpha \text{ is principal}\}$. Sinnott proved that the Stickelberger ideal $\mathcal{S}_k$ is contained in $\mathcal{A}$.

On one hand, if $\sqrt{-3} \in k$ then $3 \mid n$ and $\beta_3 = \gamma_3 \in \mathcal{T}'_k$. On the other hand, if $\sqrt{-3} \notin k$ and $\sqrt{-3} \in K$ then $\beta_3 = N_k \in \mathcal{T}'_k$. Let us define $\beta_3 = 0$ in the last case, i.e., when $\sqrt{-3} \notin K$, just to avoid distinguishing the three cases. So in all cases we have $N_k, 3\beta_3 \in \mathcal{S}_k \subseteq \mathcal{A}$.

Proposition 2.4 gives that for any $d \mid n$ there are $u \in \{0,1\}$, $v \in \{0,1,2\}$ such that $\delta_d = \gamma_d + (u/2)N_k + v\beta_3 \in A_k$; moreover $v = 0$ if $3 \nmid d$. Theorem 3.1 states that $\{\gamma_d;\ \chi \in X',\ d = n_{S_\chi}\} \cup \{\frac{1}{2}N_k\}$ is a $\mathbb{Z}$-basis of $\mathcal{T}'_k$, hence

$$\{\delta_d;\ \chi \in X',\ d = n_{S_\chi}\} \cup \{N_k\}$$

is a $\mathbb{Z}$-basis of $\mathcal{T}_k = \mathcal{T}'_k \cap A_k$; notice that $\delta_3 = 3\beta_3$ if $\sqrt{-3} \in k$. Thus the theorem will be proved if we show that $\delta_d \in \mathcal{A}$ for any $d \mid n$.

Proposition 4.8 states

$$z_d^{[K_d:k_d]} = p^{[K_d:k_d]x/2} \cdot \mathrm{N}_{K_d/k_d}(y_d)$$

for suitable $x \in \{0,1\}$. Using Lemma 4.3 and Proposition 2.4 we have

$$\begin{aligned}(z_d^{[K_d:k_d]}) &= (p^{[K_d:k_d]x/2} \cdot \mathrm{N}_{K_d/k_d}(y_d)) \\ &= \mathcal{P}^{d\beta_d + [K_d:k_d](x/2)N_k} = \mathcal{P}^{[K_d:k_d](d\gamma_d + (x/2)N_k)}\end{aligned}$$

as ideals of k and so

$$(z_d) = \mathcal{P}^{d\gamma_d + (x/2)N_k}$$

which means $d\gamma_d + (x/2)N_k \in \mathcal{A}$, hence $d(\gamma_d + (x/2)N_k) \in \mathcal{A}$ as d is odd and $N_k \in \mathcal{A}$. We have mentioned that $3\beta_3 \in \mathcal{A}$ and that $3 \nmid d$ implies $v = 0$. Therefore $dv\beta_3 \in \mathcal{A}$ and so $d\delta_d = d(\gamma_d + (x/2)N_k + v\beta_3) \in \mathcal{A}$. It is easy to see that

$$[K_d : k_d]\delta_d = \beta_d + [K_d : k_d]((x/2)N_k + v\beta_3) \in \mathcal{S}'_k \cap A_k = \mathcal{S}_k \subseteq \mathcal{A}.$$

As d and $[K_d : k_d]$ are relatively prime we have obtained $\delta_d \in \mathcal{A}$ and the theorem is proved. ∎

Corollary 4.10. *The elements of $2\mathcal{T}_k$ annihilate the ideal class group Cl_k of k.*

Proof. The Galois group $\mathrm{Gal}(K/k)$ is 2-elementary and so the square of the Frobenius of any prime ideal of k is trivial on K. Thus the square of any ideal of k belongs to a class from the principal genus PG_k of k. ∎

Remark. The elements of the augmentation ideal I_G of $\mathbb{Z}[G]$ also map any class in Cl_k to a class in PG_k, so $I_G\mathcal{T}_k$ annihilates Cl_k. But these annihilators are in fact already obtained in Corollary 4.10 because Proposition 2.4 and Lemma 2.5 imply that for any $\sigma \in G_k$ and any $\delta \in \mathcal{T}_k$ we have either $(1-\sigma)\delta \in 2\mathcal{T}_k$ or $(1-\sigma)\delta + N_k \in 2\mathcal{T}_k$.

Proof of Theorem 1.1. Corollary 4.10 gives that $\mathcal{S}_k + 2\mathcal{T}_k$ annihilates Cl_k. Using δ_d defined in the proof of Theorem 4.9 we can describe a $\mathbb{Z}$-basis of $\mathcal{S}_k + 2\mathcal{T}_k$. We know (see [1, Lemma 22 and Theorem 3]) that

$$\{[K_d : k_d]\delta_d;\ \chi \in X',\ d = n_{S_\chi}\} \cup \{N_k\}$$

is a $\mathbb{Z}$-basis of $\mathcal{S}_k$ and (see the proof of Theorem 4.9) that

$$\{2\delta_d;\ \chi \in X',\ d = n_{S_\chi}\} \cup \{2N_k\}$$

is a $\mathbb{Z}$-basis of $2\mathcal{T}_k$. Therefore

$$\{\min(2, [K_d : k_d])\delta_d;\ \chi \in X',\ d = n_{S_\chi}\} \cup \{N_k\}$$

is a $\mathbb{Z}$-basis of $\mathcal{S}_k + 2\mathcal{T}_k$ and we can easily compute the index

$$[(\mathcal{S}_k + 2\mathcal{T}_k) : \mathcal{S}_k] = \prod_{\substack{\chi \in X',\, d = n_{S_\chi} \\ K_d \neq k_d}} \frac{[K_d : k_d]}{2},$$

which gives the index formula of Theorem 1.1 because $K_\chi = K_d$ and $k \cap K_\chi = k_d$ with $d = n_{S_\chi}$. ∎

Acknowledgements. The author was supported under the project 201/07/0191 of the Czech Science Foundation and the project MSM0021622409 of the Ministry of Education of the Czech Republic.

References

[1] R. Kučera, *On the Stickelberger ideal and circular units of a compositum of quadratic fields*, J. Number Theory 56 (1996), 139–166.
[2] —, *On the class number of a compositum of real quadratic fields: an approach via circular units*, Funct. Approx. Comment. Math. 39 (2008), 179–189.
[3] S. Lang, *Cyclotomic Fields I and II*, 2nd ed., Grad. Texts in Math. 121, Springer, New York, 1990.
[4] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.
[5] L. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, New York, 1982.

Radan Kučera
Faculty of Science
Masaryk University
Kotlářská 2
611 37 Brno, Czech Republic
E-mail: kucera@math.muni.cz

Received on 8.12.2008 (5883)