Tatra Mt. Math. Publ. **20** (2000), 99–110

TATRA MOUNTAINS
Mathematical Publications

ON THE STICKELBERGER IDEAL AND CIRCULAR UNITS OF SOME GENUS FIELDS

Radan Kučera

ABSTRACT. The Stickelberger ideal and the group of circular units of a compositum of imaginary fields of prime power conductors are studied. Bases of these structures are found and formulae for the first and second factor of the class number are derived.

1. Introduction. The Stickelberger ideal and the group of circular units of abelian fields were introduced by Sinnott in his series of two papers [S1] and [S2], where he also derived formulae for the indices of the Stickelberger ideal and of the group of circular units. (By abelian field we mean a finite Galois extension of the rational numbers with abelian Galois group.) Unfortunately, these formulae are not fully explicit in general, since they contain indices of Sinnott modules. Sinnott was successful in computing the indices of these modules only for some classes of abelian fields. His results on these indices are based mostly on cohomological computations.

Besides this cohomological way, there is also an elementary way of studying the Stickelberger ideal and the group of circular units, which is based on explicit description of $\mathbb{Z}$-bases. At first this method was used by Skula who gave a $\mathbb{Z}$-basis of the Stickelberger ideal of the p^nth cyclotomic field (p being an odd prime) to obtain an elementary proof of Iwasawa's class number formula (see [S]). Similarly, in [K2] we have used results of [K1] to construct explicit bases of the Stickelberger ideal and of the group of circular units for any cyclotomic field. Later on, a similar construction for some composita of quadratic fields enabled us to compute explicit formulae for the indices of the Stickelberger ideal and the circular units of these fields (see [K3]).

2000 Mathematics Subject Classification: 11R20.
Keywords: circular (cyclotomic) units, Stickelberger ideal.

This research is supported by the grant 201/97/0433 of the Grant Agency of the Czech Republic.

The aim of this paper is to show that although [K1] was written to cover the cyclotomic case, it can be also used in a more general situation: for any abelian field K such that

1. the Galois group of K is the direct product of its inertia groups, and
2. any maximal subfield of K ramified at precisely one (finite) prime is imaginary.

It is easy to see that such a field can be characterized as a compositum K of a finite number of imaginary subfields of cyclotomic fields with prime power conductor.

In this paper we shall construct bases of the group of circular units and of the Stickelberger ideal for fields of the given type. By means of this basis we shall show that, for a field of this type, Washington's definition of cyclotomic units [W, page 143] coincides with Sinnott's definition of circular units. This can be said also in another way: circular units for fields of this type satisfy Galois descent. Moreover, we shall obtain formulae for the first and the second factor of the class number of such a field in the form of a determinant.

2. Circular units. Let $K = \prod_{p\in J} K_p$, where J is a non-empty finite set of primes and, for any $p \in J$, K_p is an imaginary abelian field of conductor p^{t_p} for a suitable positive integer t_p. For convenience we suppose K to be contained in the complex field $\mathbb{C}$.

For any $S \subseteq J$, let (by convention, $n_\emptyset = 1$ and $K_\emptyset = \mathbb{Q}$)

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

It is easy to see that n_J is the conductor of K. Let us define $\varepsilon_\emptyset = -1$ and $\varepsilon_S = \mathrm{N}_{\mathbb{Q}^S/K_S}(1-\zeta_S)$ for any $S \subseteq J$, $S \neq \emptyset$.

Let E, W, and C be the group of units of K, the group of roots of unity in K, and the Sinnott group of circular units of K, respectively. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ be the Galois group of K and let D be the subgroup of the multiplicative group $K^\times$ generated by $\{\varepsilon_S^\sigma\colon S \subseteq J, \sigma \in G\}$. Then we have

Lemma 1. *$C = E \cap D$.*

Proof. Let $\zeta_n = e^{2\pi i/n}$ for any positive integer n. Lettl proved that $C = E \cap D'$, where D' is generated by

$$\left\{-1, \mathrm{N}_{\mathbb{Q}(\zeta_n)/K\cap\mathbb{Q}(\zeta_n)}(1-\zeta_n^a)\colon 1 < n \mid n_J,\, (a,n) = 1\right\}$$

(see [L]). Let us fix a divisor $n > 1$ of n_J. Then $n = \prod_{p\in S} p^{i_p}$, where $0 < i_p \le t_p$ for each $p \in S \subseteq J$ and $S \neq \emptyset$. It is a well-known fact that

$$1-\zeta_n = \mathrm{N}_{\mathbb{Q}^S/\mathbb{Q}(\zeta_n)}(1-\zeta_S),$$

so

$$\mathrm{N}_{\mathbb{Q}(\zeta_n)/K\cap\mathbb{Q}(\zeta_n)}(1-\zeta_n)=\mathrm{N}_{\mathbb{Q}^S/K\cap\mathbb{Q}(\zeta_n)}(1-\zeta_S)=\prod_{\sigma\in\mathrm{Gal}(K^S/K\cap\mathbb{Q}(\zeta_n))}\varepsilon_S^{\sigma}.$$

Hence $D=D'$ and the lemma follows. □

In order to obtain a basis of C we shall use the results of [K1] in the same way as in [K2].

For any $p\in J$, let $T_p=\mathrm{Gal}\big(K/K_{J\setminus\{p\}}\big)$ be the inertia group of p in G, $e_p=\frac{1}{\#T_p}\sum_{\tau\in T_p}\tau\in\mathbb{Q}[G]$ be the corresponding idempotent and $\lambda_p=\mathrm{Frob}\,(p,K)^{-1}$, where $\mathrm{Frob}\,(p,K)\in G$ is an extension of the Frobenius automorphism of p in $K_{J\setminus\{p\}}/\mathbb{Q}$, so $e_p\lambda_p\in\mathbb{Q}[G]$ is well-defined. For any $p\in J$ we need to consider the abelian semigroup $T_p^*=T_p\cup\{g_p^*\}$ which is obtained from T_p by adding a new element g_p^* and putting $\tau g_p^*=g_p^*$ for any $\tau\in T_p^*$.

We shall need an induction. Let $p_1,\dots,p_n$ be the elements of J. For any $i\in\{0,\dots,n\}$ let

$$G_i=\prod_{k=1}^{i}T_{p_k}^*\prod_{k=i+1}^{n}T_{p_k}$$

and $a_i\colon G_i\to\mathbb{Q}[G]$ be defined in the following way: $a_0(\tau)=\tau$ for any $\tau\in G_0=G$ and

$$a_i(\tau)=(1-e_{p_i}\lambda_{p_i})a_{i-1}(\tau),$$
$$a_i(g_{p_i}^*\tau)=\big(\#T_{p_i}\big)e_{p_i}a_{i-1}(\tau)$$

for any $i\in\{1,\dots,n\}$ and $\tau\in G_{i-1}$.

Let us consider the homomorphisms $\ell\colon K^\times\to\mathbb{R}[G]$ and $h\colon\mathbb{R}[G]\to\mathbb{R}[G]$ defined by

$$\ell(\alpha)=\sum_{\tau\in G}\log|\alpha^\tau|\tau^{-1},\qquad h(x)=(1-e)x$$

for any $\alpha\in K^\times$ and any $x\in\mathbb{R}[G]$, where $e=\frac{1}{[K:\mathbb{Q}]}\sum_{\tau\in G}\tau=\prod_{i=1}^{n}e_{p_i}$.

Let $\Phi\colon\mathbb{Q}[G]\to\mathbb{R}[G]$ be the G-module homomorphism determined by

$$\Phi(1)=\tfrac12(1-e)\sum_{S\subseteq J}\frac{1}{[K_{J\setminus S}:\mathbb{Q}]}\,\ell\Big(\varepsilon_S^{\prod_{p\in J\setminus S}\lambda_p}\Big).$$

Lemma 2. *For any $i\in\{0,\dots,n\}$ and any $\sigma\in G_i$ we have*

$$\Phi\big(a_i(\sigma)\big)=\tfrac12(1-e)\sum_{\{p_1,\dots,p_i\}\subseteq S\subseteq J}\frac{1}{[K_{J\setminus S}:\mathbb{Q}]}\,\ell\Big(\varepsilon_{S\setminus T}^{\tau\prod_{p\in J\setminus S}\lambda_p}\Big),$$

where $T=\{p\in J\colon \sigma g_p^*=\sigma\}$ *and* $\tau\in G$ *satisfies* $\sigma=\tau\prod\limits_{p\in T} g_p^*$.

P r o o f . This can be proved by induction with respect to i (similarly as Lemma 4.1 in [K2]). □

LEMMA 3. *Let* $j\in G$ *be the complex conjugation on* K *and* U *be the additive subgroup of* $\mathbb{Q}[G]$ *generated by* $\{a_n(\sigma)\colon \sigma\in G_n\}$. *Then*

$$h\big(\ell(D)\big)=\Phi\big((1+j)U\big).$$

P r o o f . Lemma 2 implies

$$\Phi\Bigg((1+j)\,a_n\Big(\tau\prod_{p\in T} g_p^*\Big)\Bigg)=(1-e)\,\ell\big(\varepsilon_{J\setminus T}^{\tau}\big)$$

for any $\tau\in G$ and any $T\subseteq J$, and the lemma follows. □

LEMMA 4. *The group* $\ell(D)\cap\ker h$ *is generated by* $\big\{\frac12\ell(p)\colon p\in J\big\}$.

P r o o f . Let us fix $p\in J$ and a system H of representatives of

$$\mathrm{Gal}(K_p/\mathbb{Q})/\,\mathrm{Gal}\big(K_p/K_p^+\big),$$

where K_p^+ is the maximal real subfield of K_p. It is easy to see that

$$\sum_{\tau\in H}\ell\big(\varepsilon_{\{p\}}^{\tau}\big)=\tfrac12\sum_{\tau\in\mathrm{Gal}(K_p/\mathbb{Q})}\ell\big(\varepsilon_{\{p\}}^{\tau}\big)=\tfrac12\ell(p)\in\ell(D)\cap\ker h.$$

The rest of the Lemma can be proved similarly as Lemma 2.6 in [K2]. □

Now we can use the result of [K1] for the construction of a basis of C. The Galois group G is the direct product $\prod\limits_{p\in J} T_p$, so we can define $j_p\in T_p$ by the equality $j=\prod\limits_{p\in J} j_p$ (recall that $j\in G$ is the complex conjugation). For each $p\in J$, let us choose and fix a system T_p' of representatives of $T_p/\{1,j_p\}$ in such a way that $1\in T_p'$. We shall need the following sets $M_+,M_-\subseteq\prod\limits_{p\in J} T_p^*$ (an empty product is considered to be 1):

$$\begin{aligned}M_\pm=&\left(\prod_{i=1}^{n}\big(T_{p_i}^*\setminus\{j_{p_i}\}\big)\right)\\ &\Bigg\backslash\left(N_\pm\cup\bigcup_{k=1}^{n}\Big(\prod_{i=1}^{k-1}\big(T_{p_i}^*\setminus\{j_{p_i}\}\big)\Big)\Big(T_{p_k}\setminus\big(T_{p_k}'\cup\{j_{p_k}\}\big)\Big)\Big(\prod_{i=k+1}^{n}\{1,g_{p_i}^*\}\Big)\right),\end{aligned}$$

where $N_\pm = \Big\{ \prod_{p\in S} g_p^* \colon S \subseteq J,\ (-1)^{\#(J\setminus S)} = \mp 1 \Big\}$.

For any $\sigma \in \prod_{p\in J} T_p^*$, we define $\eta_\sigma \in C$ as follows: let $T = \{p\in J \colon \sigma g_p^* = \sigma\}$ and let $\tau\in G$ satisfy $\sigma = \tau \prod_{p\in T} g_p^*$; then

$$\eta_\sigma = \begin{cases} \varepsilon_{J\setminus T}^{\tau} & \text{if } \#T \neq n-1\,, \\ \varepsilon_{J\setminus T}^{\tau-1} & \text{if } \#T = n-1\,. \end{cases}$$

Theorem 1. *The set*

$$B = \Big\{ \eta_\sigma \colon \sigma\in M_+,\ \sigma \neq \prod_{p\in J} g_p^* \Big\}$$

is a basis of (the non-torsional part of) C, considered as a $\mathbb{Z}$-module.

P r o o f. By the Theorem in [K1], $\{(1+j)a_n(\sigma)\colon \sigma\in M_+\}$ is a basis of the $\mathbb{Z}$-module $(1+j)U$. By Lemma 3, we obtain that $\big\{\Phi\big((1+j)a_n(\sigma)\big)\colon \sigma\in M_+\big\}$ is a system of generators of $h\big(\ell(D)\big)$ considered as a $\mathbb{Z}$-module. From the proof of Lemma 3 we have

$$\Phi\Bigg((1+j)a_n\Big(\tau\prod_{p\in T} g_p^*\Big)\Bigg) = h\Big(\ell\big(\varepsilon_{J\setminus T}^{\tau}\big)\Big)$$

for any $\tau\in G$ and any $T\subseteq J$.

Let $p\in J$. We have $\tau \prod_{q\in J\setminus\{p\}} g_q^* \in M_+$ for any $\tau\in T_p'\setminus\{1\}$ and

$$\sum_{\tau\in T_p'} \ell\big(\varepsilon_{\{p\}}^{\tau}\big) = \tfrac12 \ell(p)\,.$$

Hence, Lemma 4 implies that

$$\big\{\ell\big(\varepsilon_{\{p\}}\big)\colon p\in J\big\} \cup \big\{\ell(\eta_\sigma)\colon \sigma\in M_+\big\}$$

is a system of generators of $\ell(D)$.

Therefore, by Lemma 1, for any $\alpha\in C$ there are $x_p, y_\sigma\in\mathbb{Z}$ such that

$$\ell(\alpha) = \sum_{p\in J} x_p \ell\big(\varepsilon_{\{p\}}\big) + \sum_{\sigma\in M_+} y_\sigma \ell(\eta_\sigma)\,.$$

Because

$$\big(\log \mathrm{N}_{K/\mathbb{Q}}(\beta)\big) \sum_{\tau\in G}\tau = \ell(\beta)\sum_{\tau\in G}\tau$$

for any $\beta \in K^\times$, we obtain

$$0 = \big(\log \mathrm{N}_{K/\mathbb{Q}}(\alpha)\big)\sum_{\tau\in G}\tau = \Bigg(\sum_{p\in J} x_p \log \mathrm{N}_{K/\mathbb{Q}}(\varepsilon_{\{p\}}) + \sum_{\sigma\in M_+} y_\sigma \log \mathrm{N}_{K/\mathbb{Q}}(\eta_\sigma)\Bigg)\sum_{\tau\in G}\tau$$
$$= \Bigg(\log \prod_{p\in J} p^{x_p[K:K_p]}\Bigg)\sum_{\tau\in G}\tau\,.$$

Hence $x_p = 0$ for each $p \in J$. Moreover, $\ell(\eta_\sigma) = 0$ for $\sigma = \prod_{p\in J} g_p^*$, so $\ell(B)$ is a system of generators of $\ell(C)$.

Because C is of finite index in E (by [S2]), the $\mathbb{Z}$-rank of C is $\frac{1}{2}[K:\mathbb{Q}]-1 = \#B$ and the theorem follows, since $C \cap \ker \ell$ is the group of roots of unity in K (see, e.g., [B-S, Chap. II, Sect. 3, Theorem 2]). □

The knowledge of a basis of C gives the determinant formula for the index $[E\colon C]$. We can use the basis B of Theorem 1 and compare this formula with results of Sinnott to obtain the following class number formula.

THEOREM 2. *Let h^+ be the class number of the maximal real subfield K^+ of K and let $G^+ = \mathrm{Gal}(K^+/\mathbb{Q})$. Then*

$$h^+ = \frac{2^{-a}}{Q\,\mathrm{Reg}(K)}\Big|\det\big(2\log|\varepsilon^\tau|\big)_{\varepsilon\in B,\,\tau\in G^+\setminus\{1\}}\Big|,$$

where $\mathrm{Reg}(K)$ and $Q = \big[E\colon (E\cap K^+)W\big]$ are the regulator and the Hasse unit index of K, respectively, and $a = 0$ if $n = 1$ and $a = 2^{n-2}-n$ if $n > 1$ (recall that $n = \#J$).

P r o o f . Theorem 4.1 of [S2] gives

$$[E:C] = h^+Q2^{-g'}\,\frac{\prod_{p\in J}[K_p:\mathbb{Q}]}{[K:\mathbb{Q}]}\,\big(e^+R : e^+U\big)\,,$$

where $R = \mathbb{Z}[G]$, U is the Sinnott module of K (for the definition of U see [S2]), $e^+ = \frac{1}{2}(1+j)$ and $g' = n$ by Proposition 4.1 of [S2]. So

$$[E:C] = h^+Q2^{-n}\big(e^+R : e^+U\big)\,.$$

Because G is the direct product of its inertia groups and K_p is imaginary for each $p \in J$, we can use Theorem 5.4 of [S2] (with $H = \{1, j\}$) for the computation of the index $(e^+R\colon e^+U)$. By this theorem

$$\big(R'\colon U'\big) = \begin{cases} 1 & \text{if } n = 1\,, \\ 2^{2^{n-2}-1} & \text{if } n > 1\,, \end{cases}$$

where $R' = \mathbb{Z}\big[\mathrm{Gal}(K^+/\mathbb{Q})\big]$ and U' is the Sinnott module of K^+. We have

$$\begin{aligned}\big(e^+R : e^+U\big) &= \big((1+j)R : (1+j)U\big)\\ &= \big(\mathrm{cor}_{K/K^+} R' : \mathrm{cor}_{K/K^+} U'\big)\,\big(\mathrm{cor}_{K/K^+} U' : (1+j)U\big)\\ &= 2(R' : U')\,,\end{aligned}$$

because cor_{K/K^+} is an injective homomorphism (for the definition of cor, see [S2]), $\mathrm{cor}_{K/K^+} R' = (1+j)R$, and $\big(\mathrm{cor}_{K/K^+} U' : (1+j)U\big) = 2$ by (5.32) of [S2].

On the other hand, Theorem 1 gives

$$[E\colon C] = \frac{1}{\mathrm{Reg}(K)}\Big|\det\big(2\log|\varepsilon^\tau|\big)_{\varepsilon\in B,\,\tau\in G^+\setminus\{1\}}\Big|$$

and the theorem follows. □

Let C' be the group of cyclotomic units of K defined in [W, page 143], namely the intersection of K and the group of circular units in the smallest cyclotomic field containing K. It is easy to show that $C \subseteq C'$ for any abelian field and it is not difficult to construct abelian fields for which $C \neq C'$. By means of Theorem 1 we can compare both groups for the field K considered in this section.

Proposition. $C = C'$.

Proof. The smallest cyclotomic field containing K is the field $\widetilde{K} = \mathbb{Q}^J$. Let $\widetilde{G} = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ and $\tilde{j} \in \widetilde{G}$ be the complex conjugation. Similarly, let $\widetilde{T}_p$, $\tilde{j}_p$, $\tilde{g}_p^*$, and $\widetilde{T}_p^*$ mean T_p, j_p, g_p^*, and T_p^*, respectively, when considering $\widetilde{K}$ instead of K. Let $r\colon \prod_{p\in J}\widetilde{T}_p^* \to \prod_{p\in J} T_p^*$ be the semigroup homomorphism satisfying $r(\tilde{g}_p^*) = g_p^*$ for any $p \in J$, and $r(\tau) = \mathrm{res}_{\widetilde{K}/K}\,\tau$ for any $\tau \in \widetilde{G}$. For any $p \in J$, let $\widetilde{T}_p' = \{\tau \in \widetilde{T}_p \colon r(\tau) \in T_p'\}$. It is easy to see that $\widetilde{T}_p'$ is a system of representatives of $\widetilde{T}_p/\{1,\tilde{j}_p\}$ such that $1 \in \widetilde{T}_p'$. Let $\widetilde{M}_+ \subseteq \prod_{p\in J}\widetilde{T}_p^*$ be the set M_+ when considering $\widetilde{K}$ instead of K (defined by means of these sets $\widetilde{T}_p'$).

Because $r\big(\widetilde{T}_p^* \setminus \{\tilde{j}_p\}\big) \subseteq T_p^*$ and $r\big(\widetilde{T}_p \setminus \big(\widetilde{T}_p' \cup \{\tilde{j}_p\}\big)\big) \subseteq T_p \setminus T_p'$, it is easy to check that if $\sigma \in \prod_{p\in J}\widetilde{T}_p^*$ satisfies $r(\sigma) \in M_+$ then $\sigma \in \widetilde{M}_+$.

Let $\tilde{\eta}_\sigma$ mean η_σ when considering $\widetilde{K}$ instead of K, namely

$$\tilde{\eta}_\sigma = \begin{cases} 1 - \zeta_{J\setminus T}^{\tau} & \text{if } \#T \neq n-1\,,\\ (1-\zeta_{J\setminus T})^{\tau-1} & \text{if } \#T = n-1 \end{cases}$$

for any $T \subseteq J$ and any $\tau \in \widetilde{G}$, where $\sigma = \tau\prod_{p\in T}\tilde{g}_p^*$.

For any $T \subseteq J$ and any $\tau \in G$, let us denote $\sigma = \tau\omega$, where $\omega = \prod_{p\in T} g_p^*$. It is easy to see that

$$\eta_\sigma = \begin{cases} \prod\limits_{x\in X,\, r(x)=\sigma} \tilde{\eta}_x & \text{if } \#T \neq n-1\,, \\ \prod\limits_{x\in X,\, r(x)=\sigma} \tilde{\eta}_x \cdot \prod\limits_{x\in X,\, r(x)=\omega} \tilde{\eta}_x^{-1} & \text{if } \#T = n-1\,, \end{cases} \tag{1}$$

where $X = \prod_{p\in J} \widetilde{T}_p^*$.

Now we can prove the Proposition. It is enough to show that $C' \subseteq C$. Let us suppose $\alpha \in C'$. Then, by Theorem 1,

$$\alpha = \rho \prod_{x\in\widetilde{M}_+} \tilde{\eta}_x^{a_x} \tag{2}$$

for some $a_x \in \mathbb{Z}$ and some root of unity ρ. Because $\alpha \in K$, we have $\alpha^{[\mathbb{Q}^J:K]} = \mathrm{N}_{\mathbb{Q}^J/K}(\alpha) \in C$, hence, again by Theorem 1,

$$\alpha^{[\mathbb{Q}^J:K]} = \rho' \prod_{\sigma\in M_+} \eta_\sigma^{b_\sigma}\,.$$

If we substitute η_σ by means of (1) and compare the obtained expression with (2), we get that $[\mathbb{Q}^J : K]$ divides b_σ for each $\sigma \in M_+$, so $\alpha \in C$ and the Proposition is proved. □

3. Stickelberger ideal. Let us keep the notation of the previous section. Let $\mathcal{S}$ be the Stickelberger ideal of K, i.e., $\mathcal{S} = \mathcal{S}' \cap \mathbb{Z}[G]$, where $\mathcal{S}'$ is the additive subgroup of $\mathbb{Q}[G]$ generated by $\{\theta_n'(a)\colon a, n \in \mathbb{Z}, n \geq 1\}$ (for the definition of $\theta_n'(a)$ see [S2] or Section 6 of [K3]). Let $N = \sum_{\tau\in G} \tau$ and, for any $S \subseteq J$, let

$$\gamma_S = \theta_{n_S}'(-1) - \tfrac{1}{2}[\mathbb{Q}^S : K_S]N\,.$$

Lemma 5. *$\mathcal{S}'$ is the additive subgroup of $\mathbb{Q}[G]$ generated by*

$$\{\sigma\gamma_S\colon S \subseteq J,\, \sigma \in G\} \cup \{\tfrac{1}{2}N\}\,.$$

Proof. The remark at the end of Section 6 of [K3] states that $\mathcal{S}'$ is the additive subgroup of $\mathbb{Q}[G]$ generated by

$$\{\sigma\theta_n'(-1)\colon 1 < n \mid n_J,\, \sigma \in G\} \cup \{\tfrac{1}{2}N\}\,.$$

Let us fix a divisor $n > 1$ of n_J. Then $n = \prod_{p\in S} p^{i_p}$, where $0 < i_p \leq t_p$ for each $p \in S \subseteq J$ and $S \neq \emptyset$. Let $\mathbb{Q}^{(n)}$ be the nth cyclotomic field. Lemma 12 of [K3] implies by induction that there is $x \in \mathbb{Z}$ such that

$$\theta_n(-1) = \mathrm{res}_{\mathbb{Q}^S/\mathbb{Q}^{(n)}}\, \theta_{n_S}(-1) + \frac{x}{2} \sum_{\tau\in \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q})} \tau\,,$$

hence

$$\begin{aligned}
\theta'_n(-1) &= \operatorname{cor}_{K/K\cap\mathbb{Q}^{(n)}} \operatorname{res}_{\mathbb{Q}^{(n)}/K\cap\mathbb{Q}^{(n)}} \theta_n(-1) \\
&= \frac{x[\mathbb{Q}^{(n)} : K\cap\mathbb{Q}^{(n)}]}{2}\, N + \operatorname{cor}_{K/K\cap\mathbb{Q}^{(n)}} \operatorname{res}_{\mathbb{Q}^S/K\cap\mathbb{Q}^{(n)}} \theta_{n_S}(-1) \\
&= \frac{x[\mathbb{Q}^{(n)} : K\cap\mathbb{Q}^{(n)}]}{2}\, N \\
&\quad + \operatorname{cor}_{K/K_S} \operatorname{cor}_{K_S/K\cap\mathbb{Q}^{(n)}} \operatorname{res}_{K_S/K\cap\mathbb{Q}^{(n)}} \operatorname{res}_{\mathbb{Q}^S/K_S} \theta_{n_S}(-1) \\
&= \frac{x[\mathbb{Q}^{(n)} : K\cap\mathbb{Q}^{(n)}]}{2}\, N \\
&\quad + \operatorname{cor}_{K/K_S}\left(\big(\operatorname{res}_{\mathbb{Q}^S/K_S} \theta_{n_S}(-1)\big) \sum_{\sigma\in\operatorname{Gal}(K_S/K\cap\mathbb{Q}^{(n)})} \sigma\right)
\end{aligned}$$

by Lemma 13 of [K3]. For any $\sigma \in \operatorname{Gal}\big(K_S/K\cap\mathbb{Q}^{(n)}\big)$, let us choose and fix $\sigma' \in G$ such that $\operatorname{res}_{K/K_S} \sigma' = \sigma$. Then

$$\theta'_n(-1) = \frac{x[\mathbb{Q}^{(n)} : K\cap\mathbb{Q}^{(n)}]}{2}\, N + \sum_{\sigma\in\operatorname{Gal}(K_S/K\cap\mathbb{Q}^{(n)})} \sigma'\big(\gamma_S + \tfrac{1}{2}[\mathbb{Q}^S : K_S]N\big)$$

and the lemma follows. □

Let $\Psi\colon \mathbb{Q}[G] \to \mathbb{Q}[G]$ be the G-module homomorphism determined by

$$\Psi(1) = \frac{1}{2}\sum_{S\subseteq J} \frac{1}{[K_{J\setminus S} : \mathbb{Q}]}\, \gamma_S \prod_{p\in J\setminus S} \lambda_p\,.$$

Lemma 6. *For any $i \in \{0,\dots,n\}$ and any $\sigma \in G_i$ we have*

$$\Psi\big(a_i(\sigma)\big) = \frac{1}{2}\sum_{\{p_1,\dots,p_i\}\subseteq S\subseteq J} \frac{1}{[K_{J\setminus S} : \mathbb{Q}]}\, \tau\gamma_{S\setminus T} \prod_{p\in J\setminus S} \lambda_p\,,$$

where $T = \{p \in J\colon \sigma g_p^* = g_p^*\}$ and $\tau \in G$ satisfies $\sigma = \tau \prod_{p\in T} g_p^*$.

P r o o f . This can be proved similarly as Lemma 4.1 in [K2] if we show that γ_S satisfies the distribution relations, namely that for any $S \subseteq J$ and any $p \in S$ we have

$$\sum_{\tau\in T_p} \tau\gamma_S = (1-\lambda_p)\gamma_{S\setminus\{p\}}\,.$$

Let us suppose that $p \in S \subseteq J$. Then

$$\begin{aligned}\sum_{\tau\in T_p} \tau\gamma_S &= -\tfrac{1}{2}[\mathbb{Q}^S : K_S](\#T_p)N + \sum_{\tau\in T_p} \tau\theta'_{n_S}(-1)\\ &= -\tfrac{1}{2}[\mathbb{Q}^S : K_{S\setminus\{p\}}]N\\ &\quad + \operatorname{cor}_{K/K_S}\operatorname{cor}_{K_S/K_{S\setminus\{p\}}}\operatorname{res}_{K_S/K_{S\setminus\{p\}}}\operatorname{res}_{\mathbb{Q}^S/K_S}\theta_{n_S}(-1)\end{aligned}$$

by Lemma 13 of [K3], because $\operatorname{res}_{K/K_S}$ gives a bijection of T_p onto $\operatorname{Gal}\big(K_S/K_{S\setminus\{p\}}\big)$. Hence

$$\sum_{\tau\in T_p} \tau\gamma_S = -\tfrac{1}{2}\big[\mathbb{Q}^S : K_{S\setminus\{p\}}\big]N + \operatorname{cor}_{K/K_{S\setminus\{p\}}}\operatorname{res}_{\mathbb{Q}^{S\setminus\{p\}}/K_{S\setminus\{p\}}}\operatorname{res}_{\mathbb{Q}^S/\mathbb{Q}^{S\setminus\{p\}}}\theta_{n_S}(-1)\,.$$

Lemma 12 of [K3] implies by induction that

$$\begin{aligned}\operatorname{res}_{\mathbb{Q}^S/\mathbb{Q}^{S\setminus\{p\}}}\theta_{n_S}(-1) &= \Big(1-\operatorname{Frob}\big(p,\mathbb{Q}^{S\setminus\{p\}}\big)^{-1}\Big)\theta_{n_{S\setminus\{p\}}}(-1)\\ &\quad + \frac{1}{2}\big[\mathbb{Q}^S : \mathbb{Q}^{S\setminus\{p\}}\big]\sum_{\sigma\in\operatorname{Gal}(\mathbb{Q}^{S\setminus\{p\}}/\mathbb{Q})}\sigma\,,\end{aligned}$$

which implies the desired equality.

For any $\sigma \in \prod_{p\in J} T_p^*$ we define $\beta_\sigma \in \mathcal{S}'$ as follows: let $T = \{p\in J\colon \sigma g_p^* = \sigma\}$ and let $\tau \in G$ satisfy $\sigma = \tau\prod_{p\in T} g_p^*$; then $\beta_\sigma = \tau\gamma_{J\setminus T}$.

Consider the set $M_- \subseteq \prod_{p\in J} T_p^*$ which was defined before Theorem 1. □

THEOREM 3. *The set $B' = \{\frac{1}{2}N\}\cup\{\beta_\sigma\colon \sigma\in M_-\}$ is a basis of $\mathcal{S}'$.*

P r o o f . Because

$$(1+j)\gamma_S = \theta'_{n_S}(-1) + \theta'_{n_S}(1) - [\mathbb{Q}^S : K_S]N = 0$$

for any $S \subseteq J$, Lemma 6 implies $\Psi\big((1-j)a_n(\sigma)\big) = \beta_\sigma$ for any $\sigma \in \prod_{p\in J} T_p^*$. Therefore

$$\mathcal{S}' = \tfrac{1}{2}N\mathbb{Z} + \Psi\big((1-j)U\big)$$

by Lemma 5. The Theorem in [K1] states that $\{(1-j)a_n(\sigma)\colon \sigma\in M_-\}$ is a basis of the $\mathbb{Z}$-module $(1-j)U$, hence B' is a system of generators of $\mathcal{S}'$.

Let $A = \{\alpha\in\mathbb{Z}[G]\colon (1+j)\alpha\in N\mathbb{Z}\}$. Because $\mathcal{S}$ is of finite index in $\mathcal{S}'$ and also in A (by [S2]), $\operatorname{rank}_{\mathbb{Z}}\mathcal{S}' = \operatorname{rank}_{\mathbb{Z}} A = \frac{1}{2}[K:\mathbb{Q}] + 1 = \#B'$ and the theorem follows. □

Remark. In fact, Theorem 3 describes only a basis of $\mathcal{S}'$ instead of a basis of the Stickelberger ideal. But it is not difficult to construct such a basis in any concrete case, since $\mathcal{S}'/\mathcal{S} \cong W$ by Proposition 2.1 of [S2]. Nevertheless, this construction for the general case is too technical, so we shall not include it here.

Similarly as for circular units, we shall use the basis B' of Theorem 3 and compare the corresponding determinant formula with the results of Sinnott to obtain the class number formula for the relative class number of K.

For any $\sigma \in \prod_{p\in J} T_p^*$ and any $\tau \in G$ we define $x_{\sigma,\tau} \in \mathbb{Q}$ as follows: let $S = \{p \in J\colon \sigma g_p^* \neq \sigma\}$ and let $\omega \in G$ and $a \in \mathbb{Z}$ satisfy $\sigma = \omega \prod_{p\in J\setminus S} g_p^*$ and $\zeta_S^a = \zeta_S^\omega$. Then we put

$$x_{\sigma,\tau} = \sum_t \left(\left\langle \tfrac{at}{n_S}\right\rangle - \tfrac{1}{2}\right),$$

where $\langle x\rangle$ is the fractional part of the rational number x ($0 \le \langle x\rangle < 1$, $x - \langle x\rangle \in \mathbb{Z}$) and the sum is taken over all positive integers $t < n_S$ which are relatively prime to n_S such that $\mathrm{res}_{\mathbb{Q}^S/K_S}\,\sigma_t = \mathrm{res}_{K/K_S}\,\tau$ for the automorphism σ_t of $\mathbb{Q}^S$ determined by $\zeta_S^{\sigma_t} = \zeta_S^t$.

Theorem 4. *Let h^- be the relative class number of K and let G^- be a system of representatives of $G/\{1,j\}$. Then*

$$h^- = Qw2^{-b}\left|\det(x_{\sigma,\tau})_{\sigma\in M_-,\,\tau\in G^-}\right|,$$

where $w = \#W$ is the number of roots of unity in K, $Q = [E : (E\cap K^+)W]$ is the Hasse unit index of K, and $b = 0$ if $n = 1$ and $b = 2^{n-2}$ if $n > 1$ (recall that $n = \#J$).

Proof. Theorem 2.1 of [S2] gives

$$[A : \mathcal{S}] = \frac{h^-}{Q}(e^-R : e^-U),$$

where $R = \mathbb{Z}[G]$, U is the Sinnott module of K, $e^- = \frac{1}{2}(1-j)$, and $A = \{\alpha \in \mathbb{Z}[G]\colon (1+j)\alpha \in N\mathbb{Z}\}$. Similarly as in the proof of Theorem 2 we can use Theorem 5.4 of [S2] for the computation of the index $(e^-R : e^-U)$. By (5.34) and (5.35) of [S2] if $n > 1$ and by Theorem 5.1 of [S2] if $n = 1$ we obtain $(e^-R : e^-U) = 2^b$. Proposition 2.1 of [S2] gives $[\mathcal{S}' : \mathcal{S}] = w$, therefore

$$(A : \mathcal{S}') = \frac{2^b h^-}{Qw}.$$

It is easy to see that

$$\{(1-j)\tau\colon \tau \in G^-\} \cup \Big\{\sum_{\tau\in G^-} \tau\Big\}$$

is a basis of A and that

$$\tfrac{1}{2}N = -\sum_{\tau\in G^-}\tfrac{1}{2}(1-j)\tau + \sum_{\tau\in G^-}\tau\,.$$

Let us fix $\sigma \in M_-$. Let $S = \{p \in J\colon \sigma g_p^* \neq \sigma\}$ and let $\omega \in G$ and $a \in \mathbb{Z}$ satisfy $\sigma = \omega \prod\limits_{p\in J\setminus S} g_p^*$ and $\zeta_S^a = \zeta_S^\omega$. From the definitions of γ_S and $\theta'_n(a)$ (see Section 6 of [K3]) we easily find that

$$\beta_\sigma = \omega\gamma_S = -\tfrac{1}{2}[\mathbb{Q}^S : K_S]N + \theta'_{n_S}(-a) = \sum_{\tau\in G} x_{\sigma,\tau}\tau = \sum_{\tau\in G^-} x_{\sigma,\tau}(1-j)\tau\,.$$

Thus, Theorem 3 gives

$$(A : \mathcal{S}') = \left|\det(x_{\sigma,\tau})_{\sigma\in M_-,\,\tau\in G^-}\right|$$

and the theorem follows. □

Acknowledgements. I am grateful to the unknown referee for his/her careful reading of the manuscript and many valuable suggestions.

REFERENCES

[B–S] BOREVICH, Z. I.—SHAFAREVICH, R. I.: *Number Theory*, Academic Press, New York, 1966.

[K1] KUČERA, R.: *On bases of odd and even universal ordinary distributions*, J. Number Theory **40** (1992), 264–283.

[K2] KUČERA, R.: *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field*, J. Number Theory **40** (1992), 284–316.

[K3] KUČERA, R.: *On the Stickelberger ideal and circular units of a compositum of quadratic fields*, J. Number Theory **56** (1996), 139–166.

[L] LETTL, G.: *A note on Thaine's circular units*, J. Number Theory **35** (1990), 224–226.

[S] SKULA, L.: *Another proof of Iwasawa's class number formula*, Acta Arith. **39** (1981), 1–6.

[S1] SINNOTT, W.: *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. **108** (1978), 107–134.

[S2] SINNOTT, W.: *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181–234.

[W] WASHINGTON, L. C.: *Introduction to Cyclotomic Fields*, Springer–Verlag, New York, 1982.

Received November 8, 1999

Department of Mathematics
Masaryk University
Janáčkovo nám. 2a
CZ–662 95 Brno
CZECH REPUBLIC
E-mail: kucera@math.muni.cz