ACTA ARITHMETICA
LXVII.2 (1994)

Different groups of circular units of a compositum of real quadratic fields

by

RADAN KUČERA (Brno)

1. Introduction. There are many different definitions of the group of circular units of a real abelian field. The aim of this paper is to study their relations in the special case of a compositum k of real quadratic fields such that -1 is not a square in the genus field K of k in the narrow sense.

The reason why fields of this type are considered is as follows. In such a field it is possible to define a group C of units (slightly bigger than Sinnott's group of circular units) such that the Galois group acts on $C/(\pm C^2)$ trivially (see [K, Lemma 2]).

Due to this key property we can easily compare different groups of circular units (see the conclusion of this paper).

2. The group C and the Sinnott group C'. Let k be a compositum of quadratic fields and suppose -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 $k = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_s})$, where $d_1, \ldots, d_s$ with $s \geq 1$ are square-free positive integers all congruent to 1 modulo 4, or 2 ramifies in k and there is a unique $x \in \{2, -2\}$ such that $k = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_s})$, where $d_1, \ldots, d_s$ with $s \geq 1$ are square-free positive integers such that $d_i \equiv 1 \pmod 4$ or $d_i \equiv x \pmod 8$ for each $i \in \{1, \ldots, s\}$. 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

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

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)

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

It is easy to see that $K_J = K$ and that n_J is the conductor of k. Let us define

$$\varepsilon_S = \begin{cases} 1 & \text{if } S = \emptyset, \\ \frac{1}{\sqrt{p}} \mathrm{N}_{\mathbb{Q}^S/K_S}(1-\zeta_S) & \text{if } S = \{p\}, \\ \mathrm{N}_{\mathbb{Q}^S/K_S}(1-\zeta_S) & \text{if } \#S > 1, \end{cases}$$

$k_S = k \cap K_S$ and $\eta_S = \mathrm{N}_{K_S/k_S}(\varepsilon_S)$ for any $S \subseteq J$. It is easy to see that ε_S and η_S are units in K_S and k_S, respectively.

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 $\{\sigma_p : p \in J\}$. Let

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

where $\widehat{G}$ is the character group of G. Then X can be viewed also as the group of all Dirichlet characters corresponding to k. For any $\chi \in X$ let

$$S_\chi = \{p \in J : \chi(\sigma_p) = -1\}.$$

Let C be the group generated by -1 and by

$$\{\eta_S^\sigma : S \subseteq J,\ \sigma \in G\}.$$

Let C' be the Sinnott group of circular units of k, i.e., the group of units in the group generated by -1 and

$$\{\mathrm{N}_{\mathbb{Q}^S/\mathbb{Q}^S\cap k}(1-\zeta_S)^\sigma : \sigma \in G,\ S \subseteq J,\ S \neq \emptyset\}$$

(see [L]). When we speak about a basis of a group of units we always have in mind a basis of the non-torsion part.

Proposition 1. *The set* $\{\eta_{S_\chi} : \chi \in X,\ \chi \neq 1\}$ *is a basis of* C *and*

$$[E : C] = \Big(\prod_{\substack{\chi\in X\\ \chi\neq 1}} (2\cdot[k : k_{S_\chi}])\Big)\cdot[k:\mathbb{Q}]^{-[k:\mathbb{Q}]/2}\cdot h,$$

where h *is the class number of* k *and* E *is the full group of units in* k. *The set*

$$\{\eta_{S_\chi} : \chi \in X,\ \#S_\chi > 1\} \cup \{\eta_{S_\chi}^2 : \chi \in X,\ \#S_\chi = 1\}$$

is a basis of C' *and* $[C : C'] = 2^a$, *where*

$$a = \#\{p \in J : \sqrt{p} \in k\} = \#\{\chi \in X : \#S_\chi = 1\}.$$

P r o o f. The results concerning C were proved in [K, Theorem 1]. It was proved in [K, Section 4] that C' is generated by

$$\{-1\} \cup \{\eta_S : S \subseteq J,\ \#S > 1\} \cup \{\eta^2_{\{p\}} : p \in J,\ p > 0,\ \sqrt{p} \in k\}.$$

It was shown in [K, proof of Lemma 5] that for any $S \subseteq J$ such that $S \neq S_\chi$ for all $\chi \in X$ there are $a_T \in \mathbb{Z}$ satisfying

$$\eta_S = \pm \prod_{T \subsetneq S} \eta_T^{a_T}.$$

But η_T is totally positive if $\#T > 1$ (it is a norm from an imaginary abelian field to a real one) while $\eta_{\{p\}}^{1+\sigma_p} = -1$ for any $p \in J$ such that $\sqrt{p} \in k$ due to [K, Lemma 1]. Thus $a_{\{p\}}$ is even for all such p and the proposition follows.

3. The groups defined by Hasse, Leopoldt, Gras and Gillard. To define all groups we are interested in we shall follow Gillard's paper [G]. Let F be a real abelian field. Let ξ be a non-principal $\mathbb{Q}$-irreducible $\mathbb{Q}$-character on $\mathrm{Gal}(F/\mathbb{Q})$ with kernel denoted by $\ker\xi$ (i.e., ξ is the sum of all linear characters $\mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{C}^\times$ with kernel equal to $\ker\xi$). Let F_ξ denote the subfield of F corresponding to $\ker\xi$, f_ξ the conductor of F_ξ and $G_\xi = \mathrm{Gal}(F_\xi/\mathbb{Q})$. It is easy to see that G_ξ is a cyclic group. Let $\zeta_n = e^{2\pi i/n}$ for any positive integer n. Then we define

$$\theta_\xi = \prod_\sigma (\zeta_{2f_\xi} - \zeta_{2f_\xi}^{-1})^{\bar\sigma}$$

where the product is taken over all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{f_\xi})^+/F_\xi)$ and $\bar\sigma$ means an extension of σ to $\mathbb{Q}(\zeta_{2f_\xi})$. Thus θ_ξ is well-defined up to sign and

$$(-1)^{s(\xi)}\theta_\chi^2 = \mathrm{N}_{\mathbb{Q}(\zeta_{f_\xi})/F_\xi}(1 - \zeta_{f_\xi}) \in F_\xi,$$

where $s(\xi) = [\mathbb{Q}(\zeta_{f_\xi})^+ : F_\xi]$. For any $\alpha \in G_\xi$ fix some $\sqrt{(\theta_\varepsilon^2)^\alpha}$ and denote it by θ_ξ^α. This definition can be extended to $\alpha \in \mathbb{Z}[G_\xi]$ by linearity.

Suppose that for any such $\xi \neq 1$ we have an ideal $I_\xi \subseteq \mathbb{Z}[G_\xi]$. Then we can consider the group $\prod_{\xi\neq 1}\{\pm\theta_\xi^\alpha : \alpha \in I_\xi\}$. For some special choices of I_ξ we obtain the following interesting groups. The *Leopoldt group of formal cyclotomic units* $C^{(0)}$ is obtained if I_ξ is the ideal generated by

$$\gamma_\xi = \prod_{p\mid n}(1 - \sigma^{n/p}),$$

where σ is a generator of the cyclic group G_ξ of order n, and p in the product runs through all primes dividing n. We obtain the *Hasse group* $C^{(1)}$ if I_ξ is the augmentation ideal of $\mathbb{Z}[G_\xi]$ (i.e., I_ξ is generated by $\sigma - 1$, where σ denotes a generator of G_ξ). We get the *Gillard group* $C^{(2)}$ if

$$I_\xi = \{\alpha \in \mathbb{Z}[G_\xi] : \theta_\xi^\alpha \text{ is a unit in } F\}$$

and the *Gras group* $C^{(3)}$ (for F not necessarily cyclic) if

$$I_\xi = \{\alpha \in \mathbb{Z}[G_\xi] : \theta_\xi^\alpha \text{ is a unit in } F_\xi\}.$$

Finally, the *Leopoldt group of cyclotomic units* H is the intersection $E \cap C^{(4)}$, where $C^{(4)}$ is obtained if $I_\xi = \mathbb{Z}[G_\xi]$.

Now, consider these groups for F being our field k. So we need not distinguish between linear characters and $\mathbb{Q}$-irreducible $\mathbb{Q}$-characters. For any $\chi \in X$, $\chi \neq 1$, the field F_χ is a quadratic subfield of k_{S_χ}. The conductor of F_χ is $f_\chi = n_{S_\chi}$, so $\zeta_{f_\chi} = \zeta_{S_\chi}$. Moreover, $s(\chi) = \frac{1}{4}\varphi(f_\chi)$ is odd if and only if $S_\chi = \{p\}$ and $p = 2$ or $|p| = p \equiv 5 \pmod 8$ or if $S_\chi = \{p, q\}$ and $p \neq q$ are odd and negative. If $S_\chi = \{p\}$ then $p > 0$, $k_{S_\chi} = K_{S_\chi} = F_\chi = \mathbb{Q}(\sqrt{p})$ and

$$(-1)^{s(\chi)}\theta_\chi^2 = \mathrm{N}_{\mathbb{Q}^{S_\chi}/F_\chi}(1 - \zeta_{S_\chi}) = \sqrt{p} \cdot \varepsilon_{S_\chi}.$$

On the other hand, if $\# S_\chi > 1$ then

$$(-1)^{s(\chi)}\theta_\chi^2 = \mathrm{N}_{\mathbb{Q}^{S_\chi}/F_\chi}(1 - \zeta_{S_\chi}) = \mathrm{N}_{k_{S_\chi}/F_\chi}(\eta_{S_\chi}). \tag{1}$$

Fix some $\sigma_\chi \in \mathrm{Gal}(k_{S_\chi}/\mathbb{Q}) \setminus \mathrm{Gal}(k_{S_\chi}/F_\chi)$ for any $\chi \in X$, $\chi \neq 1$. Then $\mathrm{Gal}(F_\chi/\mathbb{Q}) = \{1, \sigma_\chi|_{F_\chi}\}$. It is easy to see that $C^{(0)} = C^{(1)}$ is generated by -1 and by

$$\{\theta_\chi^{1-\sigma_\chi} : \chi \in X,\ \chi \neq 1\}$$

and that this set is a basis because the number of elements involved is precisely the $\mathbb{Z}$-rank. If $S_\chi = \{p\}$ then

$$(\theta_\chi^2)^{1-\sigma_\chi} = (\sqrt{p}\,\varepsilon_{\{p\}})^{1-\sigma_p} = \frac{p\varepsilon_{\{p\}}^2}{(\sqrt{p}\,\varepsilon_{\{p\}})^{1+\sigma_p}} = \varepsilon_{\{p\}}^2 = \eta_{\{p\}}^2$$

by [K, Lemma 1] and because $K_{S_\chi} = k_{S_\chi}$. Let us concentrate on the case where $\# S_\chi > 1$. Then

$$(\theta_\chi^2)^{1-\sigma_\chi} = \mathrm{N}_{k_{S_\chi}/F_\chi}(\eta_{S_\chi})^{1-\sigma_\chi} = \frac{\mathrm{N}_{k_{S_\chi}/F_\chi}(\eta_{S_\chi})^2}{\mathrm{N}_{k_{S_\chi}/\mathbb{Q}}(\eta_{S_\chi})} = \mathrm{N}_{k_{S_\chi}/F_\chi}(\eta_{S_\chi})^2,$$

because $\mathrm{N}_{k_{S_\chi}/\mathbb{Q}}(\eta_{S_\chi}) = \mathrm{N}_{\mathbb{Q}^{S_\chi}/\mathbb{Q}}(1 - \zeta_{S_\chi}) = 1$. Therefore (recall that θ_χ can be outside of k_{S_χ} and that $\theta_\chi^{1-\sigma_\chi}$ is determined only up to sign in this case)

$$\theta_\chi^{1-\sigma_\chi} = \pm \mathrm{N}_{k_{S_\chi}/F_\chi}(\eta_{S_\chi}). \tag{2}$$

Let $\sigma \in \mathrm{Gal}(k_{S_\chi}/F_\chi)$, so $\chi(\sigma)=1$. Choose $T \subseteq S_\chi$ such that $\sigma = \prod_{p \in T} \sigma_p|_{k_{S_\chi}}$. Then

$$1 = \chi(\sigma) = \prod_{p \in T} \chi(\sigma_p) = (-1)^{\# T},$$

and

$$\eta_{S_\chi}^{1-\sigma} = \eta_{S_\chi}^{1-\Pi_{p\in T}\sigma_p} = \prod_{p\in T} (\eta_{S_\chi}^{1+\sigma_p})^{\Pi_{q\in T,\, q<p}(-\sigma_q)}.$$

Of course,

$$\begin{aligned}\eta_{S_\chi}^{1+\sigma_p} &= \mathrm{N}_{K_{S_\chi}/K_{S_\chi\setminus\{p\}}}(\eta_{S_\chi}) = \mathrm{N}_{k_{S_\chi}K_{S_\chi\setminus\{p\}}/K_{S_\chi\setminus\{p\}}}(\eta_{S_\chi})^{[K_{S_\chi}:k_{S_\chi}K_{S_\chi\setminus\{p\}}]} \\ &= (\pm\eta_{S_\chi\setminus\{p\}}^{1-\mathrm{Frob}(|p|,k_{S_\chi\setminus\{p\}})})^{[K_{S_\chi}:k_{S_\chi}K_{S_\chi\setminus\{p\}}]}\end{aligned}$$

by [K, Lemma 4], because $k_{S_\chi} \cap K_{S_\chi\setminus\{p\}} = k_{S_\chi\setminus\{p\}}$. Therefore

$$\eta_{S_\chi}^{1-\sigma} = \pm \prod_{R\subsetneq S_\chi} \eta_R^{2a_R}$$

for suitable integers a_R due to Lemma 3 of [K]. So

$$(3)\qquad \begin{aligned}\theta_\chi^{1-\sigma_\chi} &= \pm\mathrm{N}_{k_{S_\chi}/F_\chi}(\eta_{S_\chi}) \\ &= \pm \prod_{\sigma\in\mathrm{Gal}(k_{S_\chi}/F_\chi)} \eta_{S_\chi}^{\sigma} = \eta_{S_\chi}^{[k_{S_\chi}:F_\chi]} \cdot \Big(\pm \prod_{R\subsetneq S_\chi} \eta_R^{2b_R}\Big)\end{aligned}$$

for suitable integers b_R. But $\{\eta_{S_\chi} : \chi \in X,\ \chi \neq 1\}$ is a basis of C and if some η_R is not in this basis then it can be written as a combination of $\eta_{R'}$, where $R' \subsetneq R$ (see [K, Theorem 1 and the proof of Lemma 5]). We have proved the following

PROPOSITION 2. *The set* $\{\theta_\chi^{1-\sigma_\chi} : \chi \in X,\ \chi \neq 1\}$ *is a basis of* $C^{(0)} = C^{(1)} \subseteq C$ *and*

$$[C : C^{(0)}] = \prod_{\substack{\chi\in X\\ \chi\neq 1}} [k_{S_\chi} : F_\chi] = \prod_{\substack{\chi\in X\\ \chi\neq 1}} \big(\tfrac{1}{2}[k_{S_\chi} : \mathbb{Q}]\big).$$

For studying $C^{(2)}$ and $C^{(3)}$ we need to know when $\theta_\chi \in k$ and $\theta_\chi \in F_\chi$, respectively. We shall suppose that $\#S_\chi > 1$, because θ_χ is not a unit if $\#S_\chi = 1$. If $s(\chi)$ is odd then $-\theta_\chi^2 = \mathrm{N}_{\mathbb{Q}^{S_\chi}/F_\chi}(1 - \zeta_{S_\chi}) > 0$, so θ_χ is pure imaginary and $\theta_\chi \notin k$. Suppose now that $s(\chi)$ is even. Recall that χ can be considered as an even Dirichlet character modulo $f_\chi = n_{S_\chi}$. We need to distinguish two cases.

First, suppose that n_{S_χ} is odd. Let $q = \min S_\chi$ and write $|q| - 1 = 2^b \cdot c$ with c odd. Let ψ be a Dirichlet character modulo $|q|$ of order 2^b, so $\psi(-1) = -1$, and let

$$A = \{a \in \mathbb{Z} : 1 \le a \le f_\chi,\ \chi(a) = 1,\ (\psi(a) = 1 \text{ or } \operatorname{Im}\psi(a) > 0)\}.$$

It is easy to see that for any $\sigma \in \mathrm{Gal}((\mathbb{Q}^{S_\chi})^+/F_\chi)$ there is precisely one $a \in A$ such that σ is the restriction to $(\mathbb{Q}^{S_\chi})^+$ of the automorphism of $\mathbb{Q}^{S_\chi}$

sending ζ_{S_χ} to $\zeta_{S_\chi}^a$. Therefore

$$\theta_\chi = \prod_{a\in A} (\xi^a - \xi^{-a}),$$

where $\xi = \zeta_{S_\chi}^{(1+f_\chi)/2}$. We want to prove that $\theta_\chi \in F_\chi$. Choose any $\sigma \in \mathrm{Gal}(\mathbb{Q}^{S_\chi}/F_\chi)$. If y is determined by $\sigma(\zeta_{S_\chi}) = \zeta_{S_\chi}^y$ then we define

$$A_1 = \{a \in A : \psi(ay) = 1 \text{ or } \operatorname{Im}\psi(ay) > 0\},$$
$$A_2 = \{a \in A : \psi(ay) = -1 \text{ or } \operatorname{Im}\psi(ay) < 0\}.$$

Because $\chi(y) = 1$ and $\chi(-1) = 1$, the mapping $f : A \to A$ defined by $f(a) \equiv ay \pmod{f_\chi}$ if $a \in A_1$, and $f(a) \equiv -ay \pmod{f_\chi}$ if $a \in A_2$, is a permutation. Therefore

$$\begin{aligned}\sigma(\theta_\chi) &= \prod_{a\in A} (\xi^{ay} - \xi^{-ay}) \\ &= \Big(\prod_{a\in A_1} (\xi^{f(a)} - \xi^{-f(a)})\Big)\Big(\prod_{a\in A_2} (-1)(\xi^{f(a)} - \xi^{-f(a)})\Big) \\ &= (-1)^{\#A_2} \cdot \theta_\chi.\end{aligned}$$

It is easy to see that $\#A = \frac{1}{4}\varphi(f_\chi) = s(\chi)$ and that $\#\{a \in A : \psi(a) = \psi(a_0)\} = 2^{1-b}s(\chi)$ for any fixed $a_0 \in A$. But A_2 is a disjoint union of such sets involving some a_0, so $2^{1-b}s(\chi) \mid (\#A_2)$. If $q < 0$ then $|q| \equiv 3 \pmod 4$, so $b = 1$, $s(\chi) \mid (\#A_2)$ and $\#A_2$ is even. If $q > 0$ then also $q' = \min(S_\chi \setminus \{q\}) > q > 0$ (recall $\#S_\chi > 1$) and $q' \equiv 1 \pmod 4$. Thus

$$2^{1-b}s(\chi) = 2^{-1-b}\varphi(f_\chi) = c\frac{q'-1}{2} \prod_{p\in S_\chi\setminus\{q,q'\}} \varphi(p) \equiv 0 \pmod 2$$

and $\#A_2$ is again even. We have proved that $\theta_\chi \in F_\chi$ if n_{S_χ} is odd and either $\#S_\chi > 2$ or $S_\chi = \{p, q\}$ with $p > 0$ and $q > 0$.

Now, suppose that n_{S_χ} is even. Then $n_{S_\chi} = 8n$ for some odd $n > 1$ and $s(\chi) = \varphi(n)$. Directly from the definition we have

$$\theta_\chi = \prod_a (\zeta_{16n}^a - \zeta_{16n}^{-a}), \tag{4}$$

where the product is taken over all integers a satisfying $0 < a < 16n$ and $\chi(a) = 1$ which are congruent to 1 or to 5 modulo 16. It is easy to see that there is $y \equiv 5 \pmod{16}$ such that $\chi(y) = 1$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{16n})/\mathbb{Q})$ be determined by $\zeta_{16n}^\sigma = \zeta_{16n}^y$. Then $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{16n})/F_\chi)$ and

$$\theta_\chi^{\sigma-1} = \Big(\prod_{\substack{0<a<16n \\ \chi(a)=1 \\ a\equiv 5,9 \,(\mathrm{mod}\, 16)}} (\zeta_{16n}^a - \zeta_{16n}^{-a})\Big)\Big(\prod_{\substack{0<a<16n \\ \chi(a)=1 \\ a\equiv 1,5 \,(\mathrm{mod}\, 16)}} (\zeta_{16n}^a - \zeta_{16n}^{-a})\Big)^{-1}.$$

Of course, $a\equiv 9 \pmod{16}$ if and only if $a\pm 8n\equiv 1 \pmod{16}$, so

$$\theta_\chi^{\sigma-1}=(-1)^{\#\{a\in\mathbb{Z}:0<a<16n,\,\chi(a)=1,\,a\equiv 9\,(\mathrm{mod}\,16)\}}=(-1)^{\varphi(n)/2}.$$

Consider any automorphism $\tau\in\mathrm{Gal}(\mathbb{Q}(\zeta_{16n})/F_\chi)$ and let $x\in\mathbb{Z}$ be such that $\zeta_{16n}^\tau=\zeta_{16n}^x$, so $\chi(x)=1$. If $x\equiv 1 \pmod 4$ then there is $j\in\{1,\dots,4\}$ satisfying $5^jx\equiv 1 \pmod{16}$, so $y^jx\equiv 1 \pmod{16}$ and $\sigma^j\tau$ acts on θ_χ identically, because it only permutes the terms in the product (4). Thus in this case

$$\theta_\chi^{\tau-1}=\theta_\chi^{\sigma^j\tau-1}\big(\theta_\chi^{\sigma-1}\big)^{-(\sigma^{j-1}+\ldots+1)\tau}=(-1)^{j\varphi(n)/2}.$$

On the other hand, if $x\equiv -1 \pmod 4$ then we can consider $\tau'\in\mathrm{Gal}(\mathbb{Q}(\zeta_{16n})/F_\chi)$ satisfying $\zeta_{16n}^{\tau'}=\zeta_{16n}^{-x}$ (recall that $\chi(-1)=1$ because F_χ is real). Because

$$(\zeta_{16n}^a-\zeta_{16n}^{-a})^\tau=-(\zeta_{16n}^a-\zeta_{16n}^{-a})^{\tau'}$$

and there is an even number of terms in the product (4), we have $\theta_\chi^\tau=\theta_\chi^{\tau'}$.

We have proved that $\theta_\chi\in F_\chi$ if and only if $\varphi(n)$ is divisible by 4. If $\#S_\chi>2$ then there are at least two different primes dividing n and $4\mid\varphi(n)$. If $S_\chi=\{2,p\}$ then $\sqrt{2p}\in k$, so $p>0$ and $n=p\equiv 1 \pmod 4$, hence again $4\mid\varphi(n)$. Finally, if $S_\chi=\{-2,p\}$ then $\sqrt{-2p}\in k$, so $p<0$ and $n=-p\equiv 3 \pmod 4$, in which case 4 does not divide $\varphi(n)$. We shall prove that in the last case even $\theta_\chi\notin k$. Indeed, if $\tau\in\mathrm{Gal}(\mathbb{Q}(\zeta_{16n})/F_\chi(\sqrt{2}))$ and if $x\in\mathbb{Z}$ satisfies $\zeta_{16n}^\tau=\zeta_{16n}^x$ then $x\equiv\pm1 \pmod 8$ and $\theta_\chi^{\tau-1}=1$ by the previous computation. But this means that $\theta_\chi\in F_\chi(\sqrt{2})$. So $\sqrt{2}\in F_\chi(\theta_\chi)\subseteq K_J(\theta_\chi)$ but $\sqrt{2}\notin K_J$, because $\sqrt{-1}\notin K_J$ and $\sqrt{-2}\in K_J$ in this case. Thus $K_J\neq K_J(\theta_\chi)$, which implies $\theta_\chi\notin k\subseteq K_J$.

PROPOSITION 3. *Let $J^+=\{p\in J:p>0\}$ and $J^-=\{p\in J:p<0\}$. Then the set*

$$\{\theta_\chi:\chi\in X,\ \#S_\chi\ge 2,\ S_\chi\subseteq J^+ \text{ if } \#S_\chi=2\}\\ \cup\{\theta_\chi^{1-\sigma_\chi}:\chi\in X,\ \#S_\chi=1 \text{ or } 2,\ S_\chi\subseteq J^- \text{ if } \#S_\chi=2\}$$

is a basis of $C^{(2)}=C^{(3)}$. The set

$$\{\theta_\chi:\chi\in X,\ [k_{S_\chi}:\mathbb{Q}]>2\}\cup\{\theta_\chi^{1-\sigma_\chi}:\chi\in X,\ [k_{S_\chi}:\mathbb{Q}]=2\}$$

is a basis of $C^{(2)}\cap C$. Moreover, $[C^{(2)}:C^{(0)}]=2^b$ and $[C^{(2)}:C^{(2)}\cap C]=2^c$, where

$$b=\#\{\chi\in X:\#S_\chi\ge 2,\ S_\chi\subseteq J^+ \text{ if } \#S_\chi=2\},$$
$$c=\#\{\chi\in X:\#S_\chi\ge 2,\ [k_{S_\chi}:\mathbb{Q}]=2,\ S_\chi\subseteq J^+ \text{ if } \#S_\chi=2\}.$$

P r o o f. Let $\chi \in X$, $\chi \neq 1$. We have shown in the previous computation that $\theta_\chi \in k$ if and only if $\theta_\chi \in F_\chi$, and that this is the case if and only if $\#S_\chi > 1$ and $S_\chi \subseteq J^+$ if $\#S_\chi = 2$. Thus $C^{(2)} = C^{(3)}$. If $\#S_\chi > 1$ then $\theta_\chi^2 = \pm\theta_\chi^{1-\sigma_\chi}$ by (1) and (2), so a basis of $C^{(2)}$ can have the above described form.

If $k_{S_\chi} = F_\chi$, then $\theta_\chi^{1-\sigma_\chi} = \pm\eta_{S_\chi}$ by (2). If $k_{S_\chi} \neq F_\chi$ then $\#S_\chi > 1$ and

$$\theta_\chi = \pm\eta_{S_\chi}^{[k_{S_\chi}:F_\chi]/2} \cdot \prod_{R \subsetneq S_\chi} \eta_R^{b_R} \tag{5}$$

for suitable $b_R \in \mathbb{Z}$ by (3). But $\{\eta_{S_\chi} : \chi \in X, \chi \neq 1\}$ is a basis of C by Proposition 1, hence

$$\begin{aligned}&\{\theta_\chi : \chi \in X,\ \#S_\chi \geq 2,\ k_{S_\chi} \neq F_\chi,\ S_\chi \subseteq J^+ \text{ if } \#S_\chi = 2\}\\ &\quad \cup \{\theta_\chi^{1-\sigma_\chi} : \chi \in X, \chi \neq 1, (k_{S_\chi} = F_\chi \text{ or } \#S_\chi = 1\\ &\qquad\qquad\qquad\qquad \text{or } (\#S_\chi = 2 \text{ and } S_\chi \subseteq J^-))\}\end{aligned}$$

is a basis of $C^{(2)} \cap C$, because if $\chi \in X$ satisfies $k_{S_\chi} = F_\chi$, then $S_{\chi'} \not\subseteq S_\chi$ for any $\chi' \in X$ such that $1 \neq \chi' \neq \chi$. Of course, if $\#S_\chi = 1$ then $k_{S_\chi} = F_\chi$. If $\#S_\chi = 2$ and $S_\chi \subseteq J^-$, then again $k_{S_\chi} = F_\chi$. It is clear that $k_{S_\chi} = F_\chi$ if and only if $[k_{S_\chi} : \mathbb{Q}] = 2$. Hence this basis is of the stated form and the proposition follows.

Let us study Leopoldt's group H now. We have seen that $\theta_\chi \in E$ for any $\chi \in X$ such that $\#S_\chi > 2$ or such that $\#S_\chi = 2$ and $S_\chi \subseteq J^+$. Moreover, if $S_\chi = \{p\}$ then θ_χ has non-zero $|p|$-adic valuation. Therefore H is generated by -1 and

$$\begin{aligned}&\{\theta_\chi : \chi \in X,\ \#S_\chi \geq 2,\ S_\chi \subseteq J^+ \text{ if } \#S_\chi = 2\}\\ &\qquad \cup \{\theta_\chi^{1-\sigma_\chi} : \chi \in X,\ \#S_\chi = 1\} \cup \Big\{\prod_{\chi \in X_1} \theta_\chi^{a_\chi} \in k : a_\chi \in \mathbb{Z}\Big\},\end{aligned}$$

where $X_1 = \{\chi \in X : \#S_\chi = 2,\ S_\chi \subseteq J^-\}$, because $\theta_\chi^{1+\sigma_\chi}$ is a root of unity for $\chi \in X_1$. Thus we need to find when $\prod_{\chi \in X_1} \theta_\chi^{a_\chi} \in k$ for $a_\chi \in \mathbb{Z}$.

First, suppose that $\chi \in X_1$ and that $S_\chi = \{p, q\}$ with p and q odd. Then

$$\theta_\chi = \prod_{\substack{1 \leq a \leq pq \\ (\frac{a}{|p|}) = (\frac{a}{|q|}) = 1}} (\xi^a - \xi^{-a}) \in K_{\{p,q\}},$$

where $\xi = \zeta_{\{p,q\}}^{(1+pq)/2}$. The complex conjugation on $K_{\{p,q\}}$ is $\sigma_p\sigma_q$, so

$$\theta_\chi^{\sigma_p\sigma_q} = \prod_{\substack{1 \leq a \leq pq \\ (\frac{a}{|p|}) = (\frac{a}{|q|}) = 1}} (\xi^{-a} - \xi^a) = -\theta_\chi,$$

because $|p| \equiv |q| \equiv 3 \pmod 4$. Hence if $\sigma = \prod_{p\in S} \sigma_p \in \mathrm{Gal}(K_J/k)$ for some $S \subseteq J$, then

$$\theta_\chi^\sigma = \begin{cases} \theta_\chi & \text{if } S_\chi \cap S = \emptyset, \\ -\theta_\chi & \text{if } S_\chi \subseteq S \end{cases}$$

(it is clear that $\#(S_\chi \cap S) = 1$ is not possible because $\mathbb{Q}(\sqrt{pq}) = F_\chi \subseteq k$).

Now, suppose that $\chi \in X_1$ and that $S_\chi = \{-2, q\}$. Then $\theta_\chi \notin K_J$ but $\theta_\chi \in K_J(\sqrt{2})$. It is clear that $K_J(\sqrt{2}) = K_J(\sqrt{-1})$ in this case. So we need to extend our automorphisms σ_p to $K_J(\sqrt{-1})$: for any $p \in J$ let σ'_p be the non-trivial automorphism in $\mathrm{Gal}(K_J(\sqrt{-1})/K_{J\setminus\{p\}}(\sqrt{-1}))$, and let σ_{-1} be the non-trivial automorphism in $\mathrm{Gal}(K_J(\sqrt{-1})/K_J)$. Then

$$\zeta_{\{-2\}}^{\sigma'_q} = \zeta_{\{-2\}}, \quad \zeta_{\{-2\}}^{\sigma'_{-2}} = \zeta_{\{-2\}}^5 \quad \text{and} \quad \zeta_{\{-2\}}^{\sigma_{-1}} = \zeta_{\{-2\}}^3,$$

so $\theta_\chi^{\sigma'_{-2}} = \theta_\chi^{\sigma_{-1}} = -\theta_\chi$, while $\theta_\chi^{\sigma'_q} = \theta_\chi$, due to the computations preceding Proposition 3.

Suppose that $\sigma = \prod_{p\in S} \sigma_p \in \mathrm{Gal}(K_J/k)$ for some $S \subseteq J$. Then we have two extensions of σ to $K_J(\sqrt{-1})$, namely σ' and $\sigma'\sigma_{-1}$, where $\sigma' = \prod_{p\in S} \sigma'_p$, and

$$(6) \qquad \begin{aligned} \Big(\prod_{\chi\in X_1} \theta_\chi^{a_\chi}\Big)^{\sigma'} &= (-1)^{\Sigma_{\chi\in X_1,\, S_\chi\subseteq S} a_\chi} \prod_{\chi\in X_1} \theta_\chi^{a_\chi}, \\ \Big(\prod_{\chi\in X_1} \theta_\chi^{a_\chi}\Big)^{\sigma_{-1}} &= (-1)^{\Sigma_{\chi\in X_2} a_\chi} \prod_{\chi\in X_1} \theta_\chi^{a_\chi}, \end{aligned}$$

where $X_2 = \{\chi \in X_1 : -2 \in S_\chi\}$.

Consider the equivalence relation on J^- defined by

$$p \sim q \quad \text{if and only if} \quad \sqrt{pq} \in k.$$

Let us show that if $p \neq q$ then $p \sim q$ if and only if there is $\chi \in X_1$ such that $S_\chi = \{p, q\}$. Indeed, if $\chi \in X_1$ and $S_\chi = \{p, q\}$, then $\mathbb{Q}(\sqrt{pq}) = F_\chi \subseteq k$, so $p \sim q$. On the other hand, if $\sqrt{pq} \in k$ for $p, q \in J^-$, $p \neq q$, then $\chi \in \widehat{G}$ defined by

$$\chi(\sigma_t) = \begin{cases} -1 & \text{if } t \in \{p, q\}, \\ 1 & \text{if } t \in J \setminus \{p, q\}, \end{cases}$$

satisfies $\chi(\sigma) = 1$ for any $\sigma \in \mathrm{Gal}(K_J/\mathbb{Q}(\sqrt{pq}))$, hence $\chi \in X$ and $S_\chi = \{p, q\}$. It is easy to see that if

$$\sigma = \prod_{p\in S} \sigma_p \in \mathrm{Gal}(K_J/k),$$

then for any class $T \in J^-/\!\sim$ either $T \subseteq S$ or $T \cap S = \emptyset$. If $X_2 = \{\chi \in X_1 : -2 \in S_\chi\}$ is not empty, fix $\chi_0 \in X_2$. Then (6) implies that $\theta_\chi\theta_{\chi_0} \in k$ for any $\chi \in X_2$. For any class $T \in (J^- \setminus \{-2\})/\!\sim$ satisfying $\#T > 1$, fix $\chi_T \in X_1$

such that $S_{\chi_T} \subseteq T$. Then (6) implies that $\theta_\chi \theta_{\chi_T} \in k$ for any $\chi \in X_1$, where $T \in (J^- \setminus \{-2\})/{\sim}$ satisfies $S_\chi \subseteq T$. Hence we need only find when

$$\prod_{\substack{T\in (J^-\setminus\{-2\})/\sim \\ \#T>1}} \theta_{\chi_T}^{a_T} \in k,$$

where $a_T \in \mathbb{Z}$.

Let J_0 be the union of all $T \in (J^- \setminus \{-2\})/{\sim}$ such that $\#T > 1$. If $J_0 = \emptyset$ then $X_1 = X_2$, $\#X_2 \le 1$ and $H = C^{(2)}$. Suppose that $J_0 \ne \emptyset$. Then $\sim$ can be considered as an equivalence relation on J_0 and $\theta_\chi \in K_{J_0}$ for any $\chi \in X_1 \setminus X_2$. So (6) implies that

$$\prod_{T\in J_0/\sim} \theta_{\chi_T}^{a_T} \in k \quad \text{if and only if} \quad \sum_{\substack{T\in J_0/\sim \\ T\subseteq S}} a_T \equiv 0 \pmod 2$$

$$\text{for all } S \subseteq J_0 \text{ such that } \prod_{p\in S} \sigma_p \in \mathrm{Gal}(K_{J_0}/k_{J_0}).$$

Choose $S_1, \dots, S_l \subseteq J_0$ such that the restrictions of

$$\tau_1 = \prod_{p\in S_1} \sigma_p, \ \dots, \ \tau_l = \prod_{p\in S_l} \sigma_p$$

form a basis of the (multiplicative) vector space $\mathrm{Gal}(K_{J_0}/k_{J_0})$ over $\mathbb{F}_2$. We shall prove that the equations

$$\sum_{\substack{T\in J_0/\sim \\ T\subseteq S_i}} x_T = 0, \qquad i = 1, \dots, l, \tag{7}$$

over $\mathbb{F}_2$ are linearly independent. Indeed, suppose that there is $L \subseteq \{1, \dots, l\}$ such that

$$\#\{i \in L : T \subseteq S_i\} \equiv 0 \pmod 2$$

for all $T \in J_0/{\sim}$. Now, for any $p \in J_0$ there is $T \in J_0/{\sim}$ such that $p \in T$. But for any $i \in \{1, \dots, l\}$, we have $p \in S_i$ if and only if $T \subseteq S_i$. Therefore $\#\{i \in L : p \in S_i\}$ is even for all $p \in J_0$. Thus

$$\prod_{i\in L} \tau_i = \prod_{p\in J_0} \sigma_p^{\#\{i\in L: p\in S_i\}} = 1.$$

But this means that $L = \emptyset$ because $\tau_1, \dots, \tau_l$ is a basis. The equations in (7) are then linearly independent. So there are l classes $C_1, \dots, C_l \in J_0/{\sim}$ such that (7) is equivalent to

$$x_{C_i} = \sum_{T\in R} b_{T,i} x_T, \qquad i = 1, \dots, l, \tag{8}$$

for suitable elements $b_{T,i} \in \mathbb{F}_2$, where $R = (J_0/{\sim}) \setminus \{C_1, \dots, C_l\}$. Thus $\prod_{T\in J_0/\sim} \theta_{\chi_T}^{a_T}$ with $a_T \in \mathbb{Z}$ is in k if and only if $x_T = a_T + 2\mathbb{Z}$ is a solution of (8), where we have identified $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Therefore

$$\begin{aligned}&\{\theta_\chi : \chi \in X,\ \#S_\chi \ge 2,\ S_\chi \subseteq J^+ \text{ if } \#S_\chi = 2\}\\ &\ \cup \{\theta_\chi^{1-\sigma_\chi} : \chi \in X,\ \#S_\chi = 1\} \cup \{\theta_\chi \theta_{\chi_0} : \chi \in X_2\}\\ &\ \cup \{\theta_\chi \theta_{\chi_T} : \chi \in X_1 \setminus X_2,\ T \in (J^- \setminus \{-2\})/\!\sim \text{ with } S_\chi \subseteq T,\ \chi \ne \chi_T\}\\ &\ \cup \Big\{\theta_{\chi_T} \prod_{i=1}^{l} \theta_{\chi_{C_i}}^{b_{T,i}} : T \in R\Big\} \cup \{\theta_{\chi_{C_i}}^2 : i = 1, \ldots, l\}\end{aligned}$$

is a basis of H, where each element $b_{T,i} \in \mathbb{F}_2$, used in (8), is understood as the integer 0 or 1.

Proposition 4. *Let* $J^- = \{p \in J : p < 0\}$, $J_0 = \{p \in J^- \setminus \{-2\} : \sqrt{pq} \in k$ *for some* $q \in J^- \setminus \{-2\}$ *with* $q \ne p\}$ *and* $d = \#\{\chi \in X : \#S_\chi = 2,\ S_\chi \subseteq J^-\}$. *Let* $d_0 = 1$ *if there is an odd* $p \in J^-$ *such that* $\sqrt{-2p} \in k$, *and* $d_0 = 0$ *otherwise. Then*

$$[H : C^{(2)}] = \frac{2^{d-d_0}}{[K_{J_0} : k_{J_0}]}.$$

Moreover, $H \cap C = C^{(2)} \cap C$.

Proof. The former equality can be obtained directly by comparing the basis of $C^{(2)}$ (see Proposition 3) with the basis of H described above. To prove the latter equality, let us compare the basis of H with the basis of C (see Proposition 1). If $\#S_\chi = 1$ then $\theta_\chi^{1-\sigma_\chi} = \pm\eta_{S_\chi}$, which is an element (up to sign) of both bases. So we need to find when

$$\varepsilon = \prod_{\substack{\chi \in X\\ \#S_\chi > 1}} \theta_\chi^{c_\chi} \in k$$

with $c_\chi \in \mathbb{Z}$ is an element of C. We shall prove that $\varepsilon \in C$ if and only if $c_\chi [k_{S_\chi} : F_\chi]$ is even for all $\chi \in X$ with $\#S_\chi > 1$.

Fix some linear ordering $\prec$ on X such that

$$S_\chi \subseteq S_\psi \Rightarrow \chi \prec \psi$$

for any $\chi, \psi \in X$. As we mentioned in the proof of Proposition 1, for any $S \subseteq J$ such that $S \ne S_\chi$ for all $\chi \in X$, there are $a_T \in \mathbb{Z}$ satisfying

$$\eta_S = \pm \prod_{T \subsetneq S} \eta_T^{a_T}.$$

Therefore (3) implies that for any $\chi \in X$ such that $\#S_\chi > 1$,

$$\theta_\chi^2 = \pm\eta_{S_\chi}^{[k_{S_\chi} : F_\chi]} \cdot \prod_{\substack{\psi \in X \setminus \{1\}\\ \psi \prec \chi}} \eta_{S_\psi}^{2b_{\chi,\psi}}$$

for suitable integers $b_{\chi,\psi}$. Thus, with respect to the basis of C, ε^2 has the following form:

$$\varepsilon^2 = \prod_{\substack{\chi\in X\\ \#S_\chi>1}} \theta_\chi^{2c_\chi} = \pm \prod_{\substack{\chi\in X\\ \#S_\chi>1}} \Big(\eta_{S_\chi}^{c_\chi[k_{S_\chi}:F_\chi]} \cdot \prod_{\substack{\psi\in X\setminus\{1\}\\ \psi\prec\chi}} \eta_{S_\psi}^{2c_\chi b_{\chi,\psi}}\Big).$$

It is easy to see that $\varepsilon \in C$ if and only if the exponent of η_{S_ψ} in this expression is even for each $\psi \in X \setminus \{1\}$. This exponent is

$$\sum_{\substack{\chi\in X\\ \psi\prec\chi}} 2c_\chi b_{\chi,\psi} \quad \text{or} \quad c_\psi[k_{S_\psi} : F_\psi] + \sum_{\substack{\chi\in X\\ \psi\prec\chi}} 2c_\chi b_{\chi,\psi}$$

depending on whether $\#S_\psi = 1$ or $\#S_\psi > 1$. Hence $\varepsilon \in C$ if and only if $c_\chi[k_{S_\chi} : F_\chi]$ is even for all $\chi \in X$ with $\#S_\chi > 1$.

Now we can use the basis of H described before the proposition to obtain the following basis of $H \cap C$:

$$\{\theta_\chi : \chi \in X,\ \#S_\chi \ge 2,\ k_{S_\chi} \ne F_\chi\} \cup \{\theta_\chi^{1-\sigma_\chi} : \chi \in X,\ \#S_\chi = 1\} \\ \cup \{\theta_\chi^2 : \chi \in X,\ \#S_\chi \ge 2,\ k_{S_\chi} = F_\chi\},$$

because $k_{S_\chi} = F_\chi$ for any $\chi \in X_1$. But that is (maybe, up to some signs) the basis of $C^{(2)} \cap C$ given in Proposition 3.

4. Sinnott's group of square roots and Washington's group. Let C'_1 be the group defined in [S, p. 209], namely

$$C'_1 = \{\varepsilon \in E : \varepsilon^2 \in C'\}.$$

Similarly, define

$$C_1 = \{\varepsilon \in E : \varepsilon^2 \in C\}.$$

Finally, let C'' be the group of cyclotomic units defined in [W, p. 143], namely the intersection of E and the group of cyclotomic units in the smallest cyclotomic field containing k.

Proposition 5. $C_1 = C'_1$.

Proof. Because $C' \subseteq C$, we have $C'_1 \subseteq C_1$ directly from the definitions. Suppose that $\varepsilon \in C_1$. Then $\varepsilon \in E$ and $\varepsilon^2 \in C$. By comparing the bases of C' and C in Proposition 1, we see that there are $\varepsilon' \in C'$ and $S \subseteq \{p \in J : \sqrt{p} \in k\}$ such that

$$\varepsilon^2 = \varepsilon' \prod_{p\in S} \eta_{\{p\}}.$$

But C' is generated by -1 and norms from imaginary abelian fields to real ones, so ε' is totally positive or totally negative. If $q \in S$ then

$$\Big(\prod_{p\in S}\eta_{\{p\}}\Big)^{1-\sigma_q} = \eta_{\{q\}}^{1-\sigma_q} = -\eta_{\{q\}}^2 < 0$$

by Lemma 1 of [K]. Of course, ε^2 is totally positive. Therefore $S=\emptyset$ and $\varepsilon^2 = \varepsilon' \in C'$. So $\varepsilon \in C_1'$ and the proposition follows.

LEMMA. *Let $S \subseteq J$. If $\#S = 1$ then η_S is a cyclotomic unit in the n_S-th cyclotomic field. If $\#S > 1$ then η_S or $-\eta_S$ is the square of a cyclotomic unit in the n_S-th cyclotomic field and $\sqrt{\eta_S}$ is in the maximal real subfield of $K_S(\sqrt{-1})$.*

Proof. We shall distinguish two cases depending on the parity of n_S. First, suppose that n_S is odd. Let $\xi = \zeta_S^{(1+n_S)/2}$; then

$$\alpha = \mathrm{N}_{\mathbb{Q}^S/K_S^+}(1-\zeta_S) = \mathrm{N}_{\mathbb{Q}^S/K_S^+}(-\xi)\mathrm{N}_{\mathbb{Q}^S/K_S^+}(\xi-\xi^{-1}) = \mathrm{N}_{\mathbb{Q}^S/K_S^+}(\xi-\xi^{-1}),$$

where we have used the fact that $\mathrm{N}_{\mathbb{Q}^S/K_S^+}(-\xi)$ is a totally positive root of unity. First, let $S=\{p\}$. Then

$$\eta_S = \begin{cases} \pm 1 & \text{if } \sqrt{p}\notin k,\\ \frac{1}{\sqrt{p}}\alpha & \text{if } \sqrt{p}\in k.\end{cases}$$

Of course, $p>0$ in the latter case, so $p \equiv 1 \pmod 4$, $\alpha^{1+\sigma_p} = p$ (by Lemma 1 of [K]) and

$$\eta_S^2 = \alpha^{1-\sigma_p} = \prod_{a=1}^{p-1}(\xi^a - \xi^{-a})^{(\frac{a}{p})} = \Big(\prod_{a=1}^{(p-1)/2}(\xi^a-\xi^{-a})^{(\frac{a}{p})}\Big)^2,$$

which is the square of a cyclotomic unit in the pth cyclotomic field.

Now, suppose that $\#S>1$ and that K_S is imaginary. Then

$$\begin{aligned}\alpha &= \mathrm{N}_{K_S/K_S^+}(\mathrm{N}_{\mathbb{Q}^S/K_S}(\xi-\xi^{-1}))\\ &= (-1)^{[\mathbb{Q}^S:\,K_S]}\mathrm{N}_{\mathbb{Q}^S/K_S}(\xi-\xi^{-1})^2.\end{aligned}$$

Let $\tau_0,\dots,\tau_l$ be a basis of the (multiplicative) vector space $\mathrm{Gal}(K_S/k_S)$ over $\mathbb{F}_2$, where τ_0 is the complex conjugation. Let L be the subfield of K_S whose Galois group is generated by $\tau_1,\dots,\tau_l$. Then

$$\eta_S = \mathrm{N}_{K_S^+/k_S}(\alpha) = \mathrm{N}_{K_S/L}(\alpha) = (-1)^{[\mathbb{Q}^S:\,L]}\mathrm{N}_{\mathbb{Q}^S/L}(\xi-\xi^{-1})^2.$$

Therefore $\sqrt{\eta_S}\in L(\sqrt{-1}) \subseteq K_S(\sqrt{-1})$. Moreover, η_S is totally positive, so $\sqrt{\eta_S}$ is real. The lemma follows in this case because $\mathrm{N}_{\mathbb{Q}^S/L}(\xi-\xi^{-1})$ is a cyclotomic unit in the n_Sth cyclotomic field.

Now, suppose that $\#S > 1$ and that K_S is real. Then all $p \in S$ are positive and

$$\alpha = \prod_{a\in A} (\xi^a - \xi^{-a}),$$

where

$$A = \left\{a \in \mathbb{Z} : 1 \le a \le n_S,\ \left(\tfrac{a}{p}\right) = 1 \text{ for all } p \in S\right\}.$$

Choose $q \in S$ and write $q - 1 = 2^b \cdot c$ with c odd. Let ψ be a Dirichlet character modulo q of order 2^b, so $\psi(-1) = -1$, and let

$$B = \{a \in A : \psi(a) = 1 \text{ or } \operatorname{Im}\psi(a) > 0\}.$$

Then $A = B \cup \{n_S - a : a \in B\}$ is a disjoint union, so

$$\alpha = (-1)^{\#B} \prod_{a\in B} (\xi^a - \xi^{-a})^2.$$

Of course,

$$\#B = \frac{1}{2}(\#A) = \frac{1}{2}\prod_{p\in S}\frac{p-1}{2}$$

is even. Let

$$\beta = \prod_{a\in B} (\xi^a - \xi^{-a}).$$

We shall show that $\beta \in K_S$, which means

$$\beta = \prod_{a\in B} (\xi^{ay} - \xi^{-ay}) \qquad \text{for any } y \in A.$$

Fix $y \in A$ and define the mapping $g : B \to B$ by the following congruence modulo n_S: for any $a \in B$,

$$g(a) \equiv \begin{cases} ay & \text{if } \psi(ay) = 1 \text{ or } \operatorname{Im}\psi(ay) > 0,\\ -ay & \text{if } \psi(ay) = -1 \text{ or } \operatorname{Im}\psi(ay) < 0.\end{cases}$$

It is easy to see that g is a permutation and that

$$\prod_{a\in B} (\xi^{ay} - \xi^{-ay}) = (-1)^{\#B'} \prod_{a\in B} (\xi^{g(a)} - \xi^{-g(a)}) = (-1)^{\#B'}\beta,$$

where $B' = \{a \in B : g(a) \equiv -ay \pmod{n_S}\}$. We have

$$\#\{a \in A : \psi(a) = \psi(a_0)\} = 2^{1-b}(\#A)$$

for any fixed $a_0 \in A$. But B' is a disjoint union of such sets involving some a_0, so $\#B'$ is divisible by

$$2^{1-b}(\#A) = c \prod_{p\in S\setminus\{q\}} \frac{p-1}{2},$$

which is even. Thus $\beta \in K_S$ and $\eta_S = \mathrm{N}_{K_S/k_S}(\alpha) = \mathrm{N}_{K_S/k_S}(\beta)^2$. The lemma is proved if n_S is odd because β is a cyclotomic unit in the n_Sth cyclotomic field.

Now, let us deal with the case of n_S being even. If $S = \{-2\}$ then $\eta_S = 1$. If $S = \{2\}$ then $\eta_S = -1 + \sqrt{2}$ or $\eta_S = -1$ depending on whether $\sqrt{2} \in k$ or not. It is easy to check that

$$-1 + \sqrt{2} = -\zeta_{\{2\}}(1 - \zeta_{\{2\}})(1 - \zeta_{\{2\}}^3)^{-1}$$

is a cyclotomic unit in the eighth cyclotomic field.

Now, suppose that $\#S > 1$. Then

$$\varepsilon_S = \prod_a (1 - \zeta_S^a),$$

where the product is taken over all positive integers $a < n_S$ satisfying $\left(\frac{a}{|p|}\right) = 1$ for all odd $p \in S$ such that $a \equiv \pm 1 \pmod 8$ if $2 \in S$ or $a \equiv 1, 3 \pmod 8$ if $-2 \in S$. Let $\xi = e^{\pi i/n_S}$, so $\xi^2 = \zeta_S$.

First, suppose that K_S is imaginary. Let τ be the complex conjugation on $\mathbb{Q}(\xi)$. Because $n_S \equiv 8 \pmod{16}$, we have

$$\varepsilon_S^{1+\tau} = \prod_a (1 - \zeta_S^a)(1 - \zeta_S^{-a}) = \prod_a (-(\xi^a - \xi^{-a})^2),$$

where the products are taken over all positive integers $a < 2n_S$ satisfying $\left(\frac{a}{|p|}\right) = 1$ for all odd $p \in S$ such that $a \equiv \pm 1 \pmod{16}$ if $2 \in S$ or $a \equiv 1, 3 \pmod{16}$ if $-2 \in S$. The number of terms in these products is even, so $\varepsilon_S^{1+\tau} = \beta^2$, where

$$\beta = \prod_a (\xi^a - \xi^{-a}), \tag{9}$$

with a running through the same set as above. We need to prove that $\beta \in (K_S(\sqrt{-1}))^+$. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi)/K_S(\sqrt{-1}))$ there is an integer y satisfying $y \equiv 1 \pmod 8$ and $\left(\frac{y}{p}\right) = 1$ for all odd $p \in S$ such that $\xi^\sigma = \xi^y$. It is clear that if $y \equiv 1 \pmod{16}$ then σ only permutes the terms in the product (9), so $\beta^\sigma = \beta$ in this case. If $y \equiv 9 \pmod{16}$ then $y' = y + n_S \equiv 1 \pmod{16}$ and $\xi^{y'} = -\xi^y$. Moreover, $\left(\frac{y'}{p}\right) = 1$ for all odd $p \in S$, so

$$\beta^\sigma = \prod_a (\xi^{ay} - \xi^{-ay}) = \prod_a (-(\xi^{ay'} - \xi^{-ay'})) = \beta$$

in this case, too. It is easy to see that β is real, so $\beta \in (K_S(\sqrt{-1}))^+$. It is clear that β is a cyclotomic unit in the n_Sth cyclotomic field and the lemma is proved in this case, since $\eta_S = \mathrm{N}_{K_S^+/k_S}(\beta^2)$.

Finally, suppose that K_S is real. Then all $p \in S$ are positive and

$$\varepsilon_S = \prod_a (1 - \zeta_S^a)(1 - \zeta_S^{-a}) = \prod_a (-(\xi^a - \xi^{-a})^2)$$

with the products taken over all positive integers $a < n_S$ such that $a \equiv 1 \pmod 8$ and $\left(\frac{a}{p}\right) = 1$ for all odd $p \in S$. The number of terms in these products is even, so $\varepsilon_S = \beta^2$, where

$$\beta = \prod_a (\xi^a - \xi^{-a}), \tag{10}$$

where a in the product runs through all integers satisfying $0 < a < 2n_S$ and $a \equiv 1 \pmod{16}$ such that $\left(\frac{a}{p}\right) = 1$ for all odd $p \in S$. Let us show that $\beta \in K_S$. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi)/K_S)$ there is an integer y satisfying $\xi^\sigma = \xi^y$ such that $y \equiv \pm 1 \pmod 8$ and $\left(\frac{y}{p}\right) = 1$ for all odd $p \in S$. It is clear that if $y \equiv 1 \pmod{16}$ then σ only permutes the terms in the product (10). If $y \equiv 9 \pmod{16}$ then σ also changes the sign of each term in (10). But the number of terms in the product (10) is even, so $\beta^\sigma = \beta$ in both previous cases. If $y \equiv -1 \pmod 8$ then we have proved that $\beta^{\tau\sigma} = \beta$, where τ is the complex conjugation on $\mathbb{Q}(\xi)$. But β is real, so $\beta \in K_S$. It is clear that β is a cyclotomic unit in the n_Sth cyclotomic field and the lemma is proved.

PROPOSITION 6. *Let $2^g = [C' : \{1, -1\} \times (C_1')^2]$. Then $H \subseteq C_1' \subseteq C''$ and*

$$[C_1' : C'] = 2^{[k:\mathbb{Q}]-1-g}.$$

Moreover, 2^g is a divisor of $[K_J : k]$.

Proof. The fact that $[C' : \{1, -1\} \times (C_1')^2]$ is a power of 2 follows from the inclusion $C' \subseteq C_1'$. By (1) and (2) we have $\theta_\chi^2 = \pm\theta_\chi^{1-\sigma_\chi}$ for any $\chi \in X$ such that $\#S_\chi > 1$. The form of the basis of H before Proposition 4 gives $H \subseteq C_1$, because $\theta_\chi^{1-\sigma_\chi} \in C$ by Proposition 2. But $C_1 = C_1'$ by Proposition 5.

Let $\varepsilon \in C_1'$. Then $\varepsilon \in E$ and $\varepsilon^2 \in C'$. The Lemma gives that any element of the basis of C' given in Proposition 1 is (up to sign) the square of a cyclotomic unit in the n_Jth cyclotomic field. Thus ε is a cyclotomic unit in this field and $\varepsilon \in C''$.

The formula follows from

$$2^g \cdot [C_1' : C'] = [C_1' : \{1, -1\} \times (C_1')^2] = 2^{[k:\mathbb{Q}]-1}.$$

It remains to show that 2^g is a divisor of $[K_J : k]$. Let C_0' be the group of totally positive elements of C'. Proposition 1 gives that

$$\{\eta_{S_\chi} : \chi \in X,\ \#S_\chi > 1\} \cup \{\eta_{S_\chi}^2 : \chi \in X,\ \#S_\chi = 1\}$$

generates C_0'. The Lemma implies that $\sqrt{\varepsilon} \in (K_J(\sqrt{-1}))^+$ for any $\varepsilon \in C_0'$. Of course,

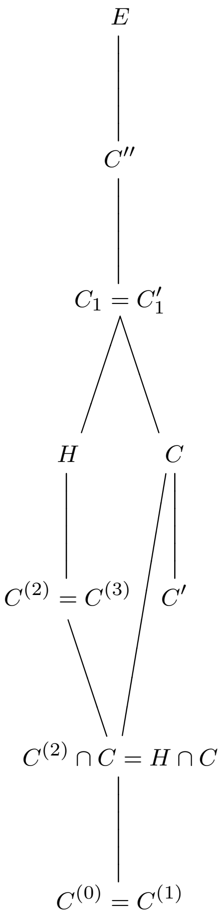
$$(C_1')^2 = \{\varepsilon \in C_0' : \sqrt{\varepsilon} \in k\}.$$

Because $C' = \{1,-1\} \times C'_0$ we have

$$2^g = [C'_0 : (C'_1)^2] \mid [(K_J(\sqrt{-1}))^+ : k] = [K_J : k].$$

The proposition is proved.

5. Conclusion. Let us put together all the propositions. We have shown that the groups of cyclotomic units we are interested in form the following ordered set with respect to inclusion.



$a = \#\{\chi \in X : \#S_\chi = 1\}$,

$b = \#\{\chi \in X : \#S_\chi \geq 2,\ S_\chi \subseteq J^+ \text{ if } \#S_\chi = 2\}$,

$c = \#\{\chi \in X : \#S_\chi \geq 2,\ [k_{S_\chi} : \mathbb{Q}] = 2,\ S_\chi \subseteq J^+ \text{ if } \#S_\chi = 2\}$,

$d = \#\{\chi \in X : \#S_\chi = 2,\ S_\chi \subseteq J^-\}$,

so $a + b + d = [k : \mathbb{Q}] - 1$;

$J^+ = \{p \in J : p > 0\}$,

$J^- = \{p \in J : p < 0\}$,

$J_0 = \{p \in J^- : p \text{ odd},\ \sqrt{pq} \in k \text{ for some odd } q \in J^- \text{ with } q \neq p\}$,

$$d_0 = \begin{cases} 1 & \text{if there is an odd } p \in J^- \text{ such that } \sqrt{-2p} \in k, \\ 0 & \text{otherwise,} \end{cases}$$

$g \in \mathbb{Z},\ 0 \leq g \leq b + d,\ 2^g \mid [K_J : k]$;

$$[E : C_1] = 2^{g-b-d}\Big(\prod_{\substack{\chi \in X \\ \chi \neq 1}} (2 \cdot [k : k_{S_\chi}])\Big) \cdot [k : \mathbb{Q}]^{-[k:\mathbb{Q}]/2} \cdot h,$$

$[C_1 : C] = 2^{b+d-g}$,

$[C : C'] = 2^a$,

$$[C_1 : H] = 2^{d_0 - g}[K_{J_0} : k_{J_0}] \prod_{\substack{\chi \in X \\ \chi \neq 1}} (\tfrac{1}{2} \cdot [k_{S_\chi} : \mathbb{Q}]),$$

$[H : C^{(2)}] = 2^{d - d_0}[K_{J_0} : k_{J_0}]^{-1}$,

$[C^{(2)} : C^{(2)} \cap C] = 2^c$,

$[C^{(2)} \cap C : C^{(0)}] = 2^{b-c}$,

$$[C : C^{(2)} \cap C] = 2^{c-b} \prod_{\substack{\chi \in X \\ \chi \neq 1}} (\tfrac{1}{2} \cdot [k_{S_\chi} : \mathbb{Q}]).$$

Acknowledgments. I am very grateful to Claude Levesque for helpful discussions and many remarks which improved this paper. This paper was written during my stay at Université Laval in Québec as a post-doctoral fellow (through grants from Université Laval and Centre interuniversitaire en calcul mathématique algébrique).

References

[G] R. Gillard, *Remarques sur les unités cyclotomiques et les unités elliptiques*, J. Number Theory 11 (1979), 21–48.

[K] R. Kučera, *On the Stickelberger ideal and circular units of a compositum of quadratic fields*, preprint.

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

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

[W] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

DEPARTMENT OF MATHEMATICS
MASARYK UNIVERSITY
JANÁČKOVO NÁM. 2A
662 95 BRNO, CZECH REPUBLIC
E-mail: KUCERA@MATH.MUNI.CZ

Received on 17.3.1993 (2396)