Functiones et Approximatio
XXXIX.2 (2008), 179–189

ON THE CLASS NUMBER OF A COMPOSITUM OF REAL QUADRATIC FIELDS: AN APPROACH VIA CIRCULAR UNITS

Radan Kučera

Dedicated to Professor Władysław Narkiewicz
at the occasion of his seventieth birthday

Abstract: For a compositum k of quadratic number fields new explicit units are constructed by taking power-of-two roots of circular units. These units are used to obtain a result concerning the divisibility of the class number of k by a power of 2.

Keywords: compositum of real quadratic fields, class number, group of circular units.

1. Introduction

Let k be a compositum of quadratic number fields and let -1 not be a square in the genus field K of k in the narrow sense. This paper resumes the study of the group E of all units of k that started in [3], where a group of circular units C of k, slightly bigger than the Sinnott's one defined in [4], has been introduced and an explicit basis of C has been found. Using this basis, the index $[E : C]$ has been computed as a product of several factors, one of them being the class number h^+ of the maximal real subfield k^+ of k. This index formula has been used to get some divisibility relations for h^+ (see [3], [2], [1]). The aim of this paper is to try to improve results of [3] in the following direction: a new group of units $C_1 \subseteq K$ is defined by means of explicit generators. If K is real and $k \neq K$ then $C \subsetneq C_1 \subseteq E$, but in general (i.e., if K is imaginary) there are cases where C_1 is not a subgroup of E. Nevertheless C_1 still can be used to obtain divisibility relations for h^+ that are stronger than what is given by genus theory (if both $[k : \mathbb{Q}] > 2$ and $[K : k] > 2$). It seems to be interesting that the index $(E : C_1)$ is much easier to compute than $[E : C]$ (compare the index formulae given by Theorem 3.1 and by [3, Theorem 1]). The main results of this paper (see Theorems 3.2 and 4.1) can be summarized as follows:

2000 Mathematics Subject Classification: Primary 11R20, Secondary 11R27, 11R29
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.

Theorem 1.1. *If k is a compositum of real quadratic fields such that -1 is not a square in the genus field K of k in the narrow sense then the class number h of k is divisible by the following power of 2:*

$$\frac{[k:\mathbb{Q}]}{2}\cdot\left(\frac{[K:k]}{4}\right)^{([k:\mathbb{Q}]/2)-1}\ \Big|\ h\,.$$

Moreover, if K is real then even

$$2\cdot[k:\mathbb{Q}]\cdot\left(\frac{[K:k]}{4}\right)^{[k:\mathbb{Q}]/2}\ \Big|\ h\,.$$

To compare the strength of this result, let us notice that genus theory gives only $\frac{[K:k]}{2}\mid h$ and $[K:k]\mid h$, respectively.

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 (so k can be both real and imaginary). 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 uniquely determined $x\in\{2,-2\}$ 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

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

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 W be the group of roots of unity in k (it is easy to see that $\#W$ is 2 or 6). The paper [3] was devoted to the study of the group C generated by $W \cup \{\eta_S^\sigma;\, S \subseteq J,\, \sigma \in G\}$. The aim of this paper is to show that some power-of-two roots of the generators of C lie in K and to study the group C_1 of units generated by these roots. We shall be more specific in a moment. For any $S \subseteq J$ let D_S be the group generated by $\{\varepsilon_T;\, T \subseteq S\}$.

Lemma 2.1. *For any $S \subseteq J$ and any $\sigma \in G$ we have $\varepsilon_S^{1+\sigma} = \pm \prod_{T \subseteq S} \varepsilon_T^{2a_T}$ for suitable $a_T \in \mathbb{Z}$.*

Proof. This is a direct consequence of [3, Lemma 2], because $\varepsilon_S^{1+\sigma} = \varepsilon_S^2/\varepsilon_S^{1-\sigma}$. ■

Since -1 is not a square in K, the only power-of-two roots of unity in K are ± 1. Therefore the following proposition well defines $\varkappa_S \in K_S$ up to sign.

Proposition 2.1. *For any $S \subseteq J$ there is $\varkappa_S \in D_S$ such that $\varkappa_S^{[K_S:k_S]} = \pm \eta_S$.*

Proof. It is easy to see that $\mathrm{Gal}(K_S/k_S)$ is a subspace of the (multiplicative) vector space $\mathrm{Gal}(K_S/\mathbb{Q})$ over $\mathbb{F}_2$. Let $\alpha_1, \dots, \alpha_r$ be a basis of $\mathrm{Gal}(K_S/k_S)$, then $\eta_S = \mathrm{N}_{K_S/k_S}(\varepsilon_S) = \varepsilon_S^{(1+\alpha_1)\cdots(1+\alpha_r)}$ and $[K_S : k_S] = 2^r$. The proposition follows by means of induction with respect to r using Lemma 2.1. ■

Let C_1 be the group generated by $W \cup \{\varkappa_S^\sigma;\, S \subseteq J,\, \sigma \in G\}$.

Lemma 2.2. *For any $S \subseteq J$ and any $\sigma \in G$ we have $\varkappa_S^{1-\sigma} = \pm \prod_{T \subseteq S} \varkappa_T^{2a_T}$ for suitable $a_T \in \mathbb{Z}$.*

Proof. In the proof of [3, Lemma 3] we have derived the following formula

$$\eta_S^{1-\sigma} = \pm \prod_{T \subseteq S} \eta_T^{2a_T[K_S:k_S K_T]}\,,$$

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

$$(\varkappa_S^{1-\sigma})^{[K_S:k_S]} = \pm \prod_{T \subseteq S} \varkappa_T^{2a_T[K_S:k_S K_T][K_T:k_T]}\,.$$

We have $k_S \cap K_T = k \cap K_S \cap K_T = k \cap K_T = k_T$ and so $[K_T : k_T] = [k_S K_T : k_S]$. The lemma follows as the only power-of-two roots of unity in K are ± 1. ■

Let k^+ be the maximal real subfield of k and 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

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

hence n_{S_χ} is the conductor of χ.

Theorem 2.1. *The set $B = \{\varkappa_{S_\chi};\ \chi \in X,\ \chi \neq 1\}$ is a $\mathbb{Z}$-basis of C_1.*

Proof. Lemma 2.2 implies that C_1 is generated by $W \cup \{\varkappa_S;\ S \subseteq J\}$. Let us suppose that $S \subseteq J$ and that $S \neq S_\chi$ for all $\chi \in X$. In the proof of [3, Lemma 5] we have derived the following formula for such a set S; here $T \subseteq J$ and $\rho \in W$:

$$\rho\eta_S^2 = \prod_{p \in S \cap T} (\mathrm{N}_{k_S/k_{S\setminus\{p\}}}(\eta_S))^{[K_S:k_S K_{S\setminus\{p\}}]\prod_{q\in S\cap T, q<p}(-\sigma_q)}\ .$$

Due to [3, Lemma 4] we have

$$\mathrm{N}_{k_S/k_{S\setminus\{p\}}}(\eta_S) = \pm\eta_{S\setminus\{p\}}^{1-\mathrm{Frob}(|p|,k_{S\setminus\{p\}})}$$

where $\mathrm{Frob}(|p|, k_{S\setminus\{p\}})$ is the Frobenius automorphism of $|p|$ in $k_{S\setminus\{p\}}$ and so

$$\rho\varkappa_S^{2[K_S:k_S]} = \pm \prod_{p \in S \cap T} (\varkappa_{S\setminus\{p\}}^{1-\mathrm{Frob}(|p|,k_{S\setminus\{p\}})})^{[K_{S\setminus\{p\}}:k_{S\setminus\{p\}}][K_S:k_S K_{S\setminus\{p\}}]\prod_{q\in S\cap T, q<p}(-\sigma_q)}\ .$$

We have $[K_{S\setminus\{p\}} : k_{S\setminus\{p\}}][K_S : k_S K_{S\setminus\{p\}}] = [K_S : k_S]$ and Lemma 2.2 implies that

$$\rho\varkappa_S^{2[K_S:k_S]} = \pm\big(\prod_{T \subsetneq S} \varkappa_T^{2a_T}\big)^{[K_S:k_S]}$$

for suitable $a_T \in \mathbb{Z}$. Therefore

$$\rho_1 = \varkappa_S \prod_{T \subsetneq S} \varkappa_T^{-a_T}$$

is a root of unity in K such that $\rho_1^{2[K_S:k_S]} = \pm\rho^{-1} \in W$. This gives that $\rho_1 \in W$ because $\#W$ is 2 or 6 and -1 is not a square in K. Hence $B \cup W$ is a system of generators of C_1. The definition of C_1 implies that C_1 and C have the same $\mathbb{Z}$-rank. Moreover, [3, Theorem 1] states that the $\mathbb{Z}$-rank of C equals $(\#X) - 1$ and the theorem follows. ∎

Corollary 2.1. *The index of C in C_1 is equal to $[C_1 : C] = \prod_{\chi \in X}[K_{S_\chi} : k_{S_\chi}]$.*

Proof. [3, Theorem 1 and Lemma 5] gives that $\{\eta_{S_\chi};\ \chi \in X,\ \chi \neq 1\}$ is a $\mathbb{Z}$-basis of C. Proposition 2.1 implies that the transition matrix is the diagonal matrix $\mathrm{diag}([K_{S_\chi} : k_{S_\chi}])_{\chi\in X,\,\chi\neq 1}$. The corollary follows as the torsion subgroups of C and C_1 coincide. ∎

3. The index of $(E : C_1)$

The index $[E : C]$ is computed in [3, Theorem 1] by means of the class number h^+ of k^+. To get a lower bound for the divisibility of h^+ by a power of 2, it is enough to obtain a lower bound for the divisibility of the index $[E : C]$. Unfortunately this lower bound is not the index $[C_1 : C]$ because C_1 is not a subgroup of E in general. So we shall consider the intersection $C_1 \cap E = C_1 \cap k$.

Lemma 3.1. *For any $\varepsilon \in C_1$ and any $\sigma \in Gal(K/k)$ let $\chi_\varepsilon(\sigma) = \varepsilon^{1-\sigma}$. Then $\chi_\varepsilon : Gal(K/k) \to \{1, -1\}$ is a homomorphism. Moreover,*

$$\tilde{\chi} : C_1 \to \widehat{Gal(K/k)} \ ,$$

where $\tilde{\chi}(\varepsilon) = \chi_\varepsilon$, is a homomorphism whose kernel $\ker \tilde{\chi} = C_1 \cap E$.

Proof. For any $S \subseteq J$ we have $[K_S : k_S] = [kK_S : k] \mid [K : k]$ and so $\varepsilon^{[K:k]} \in C \subseteq k$. Thus $(\chi_\varepsilon(\sigma))^{[K:k]} = 1$ for any $\sigma \in \mathrm{Gal}(K/k)$ and so $\chi_\varepsilon(\sigma)$ is a power-of-two root of unity in K, i.e. ± 1. The lemma follows from the identities $\varepsilon^{1-\sigma\tau} = \varepsilon^{1-\sigma} \cdot (\varepsilon^{1-\tau})^\sigma$ and $(\varepsilon\rho)^{1-\sigma} = \varepsilon^{1-\sigma} \cdot \rho^{1-\sigma}$. ■

Corollary 3.1. *For any $S \subseteq J$ we have $\varkappa_S^2 \in E$ and so $[C_1 : C_1 \cap E] \mid 2^{[k^+:\mathbb{Q}]-1}$. Moreover the index $[C_1 : C_1 \cap E]$ divides the degree $[K : k]$, too.*

Proof. This follows from $\mathrm{rank}_{\mathbb{Z}} C_1 = [k^+ : \mathbb{Q}] - 1$ and $\#\widehat{\mathrm{Gal}(K/k)} = [K : k]$. ■

The following theorem computes the generalized index $(E : C_1) = \frac{[E:C]}{[C_1:C]}$. (The definition of the generalized index can be found in [4, page 187].) Let K' be the genus field in narrow sense of k^+. We shall start with a lemma:

Lemma 3.2. *We have*

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

Proof. If χ is the trivial character then $K_{S_\chi} = \mathbb{Q}$. Let $\chi \in X$ be a nontrivial character. Then $[K_{S_\chi} : \mathbb{Q}] = \#\mathrm{Gal}(K_{S_\chi}/\mathbb{Q})$ and $\dim_{\mathbb{F}_2} \mathrm{Gal}(K_{S_\chi}/\mathbb{Q}) = \#S_\chi$ equals the number of primes dividing the conductor n_{S_χ} of χ, which is equal to the number of primes that ramify in the quadratic field corresponding to χ. If χ runs over all nontrivial characters in X then the corresponding field runs over all quadratic subfields of k^+. For any prime q ramifying in $k^+/\mathbb{Q}$, let M_q be the inertia subfield of $k^+/\mathbb{Q}$ corresponding to q, i.e. the fixed field of the inertia subgroup of $\mathrm{Gal}(k^+/\mathbb{Q})$ corresponding to q. Then the prime q does not ramify in a quadratic subfield L of k^+ if and only if L is a subfield of M_q. The ramifying index of q in $k^+/\mathbb{Q}$ equals 2 and so the degree $[M_q : \mathbb{Q}] = [k^+ : \mathbb{Q}]/2$. Hence the inertia field M_q has exactly $([k^+ : \mathbb{Q}]/2) - 1$ quadratic subfields. Therefore q ramifies in exactly $[k^+ : \mathbb{Q}]/2$

quadratic subfields of k^+. As $\dim_{\mathbb{F}_2} \operatorname{Gal}(K'/\mathbb{Q})$ is equal to the number of primes q that ramify in k^+, we have

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

where the sum is taken over all primes q ramifying in $k^+/\mathbb{Q}$. ■

Theorem 3.1. *The generalized index* $(E : C_1)$ *is given by the formula*

$$(E : C_1) = \left(\frac{[K' : k^+]}{4}\right)^{-[k^+:\mathbb{Q}]/2} \cdot \frac{Qh^+}{2 \cdot [k^+ : \mathbb{Q}]} ,$$

where h^+ *is the class number of* k^+ *and* $Q = [E : W(E \cap k^+)]$ *is the Hasse unit index of* k *(so* $Q \in \{1, 2\}$ *and* $Q = 1$ *if* k *is real).*

Proof. [3, Theorem 1] gives

$$[E : C] = \left(\prod_{\chi\in X,\,\chi\neq 1} \frac{2 \cdot [k : k_{S_\chi}]}{[k : k^+]}\right) \cdot (\#X)^{-(\#X)/2} \cdot Qh^+ .$$

Using Corollary 2.1 and $\#X = [k^+ : \mathbb{Q}]$ we obtain

$$\begin{aligned}(E : C_1) &= [E : C]/[C_1 : C] \\ &= \left(\prod_{\chi\in X,\,\chi\neq 1} \frac{2 \cdot [k : k_{S_\chi}]}{[k : k^+] \cdot [K_{S_\chi} : k_{S_\chi}]}\right) \cdot [k^+ : \mathbb{Q}]^{-[k^+:\mathbb{Q}]/2} \cdot Qh^+ \\ &= \left(\prod_{\chi\in X} \frac{2 \cdot [k^+ : \mathbb{Q}]}{[K_{S_\chi} : \mathbb{Q}]}\right) \cdot [k^+ : \mathbb{Q}]^{-[k^+:\mathbb{Q}]/2} \cdot \frac{Qh^+}{2 \cdot [k^+ : \mathbb{Q}]}\end{aligned}$$

and Lemma 3.2 gives the theorem. ■

Corollary 3.2. *Let* C_2 *be the group generated by* $W \cup \{\varkappa_S^{2\sigma};\, S \subseteq J,\, \sigma \in G\}$*. Then* C_2 *is a subgroup of* E *of index*

$$[E : C_2] = \left(\frac{[K' : k^+]}{16}\right)^{-[k^+:\mathbb{Q}]/2} \cdot \frac{Qh^+}{4 \cdot [k^+ : \mathbb{Q}]} .$$

Proof. Corollary 3.1 gives $C_2 \subseteq E$. The index formula is given by Theorem 3.1 and the obvious equality $[C_1 : C_2] = 2^{[k^+:\mathbb{Q}]-1}$. ■

Theorem 3.2. *If* k *is real then the class number* h *of* k *is divisible by the following powers of 2:*

$$\frac{[k : \mathbb{Q}]}{2} \cdot \left(\frac{[K : k]}{4}\right)^{([k:\mathbb{Q}]/2)-1} \,\Big|\, h$$

and

$$4 \cdot [k : \mathbb{Q}] \cdot \left(\frac{[K : k]}{16}\right)^{[k:\mathbb{Q}]/2} \,\Big|\, h .$$

Proof. Theorem 3.1 gives

$$h = 2 \cdot [k:\mathbb{Q}] \cdot (E : C_1) \cdot \left(\frac{[K:k]}{4}\right)^{[k:\mathbb{Q}]/2}$$
$$= \frac{2 \cdot [k:\mathbb{Q}]}{[K:k]} \cdot [E : C_1 \cap E] \cdot \frac{[K:k]}{[C_1 : C_1 \cap E]} \cdot \left(\frac{[K:k]}{4}\right)^{[k:\mathbb{Q}]/2}$$

and Corollary 3.1 implies the former divisibility relation. The latter one is given by Corollary 3.2. ■

The following example shows that C_1 is not a subgroup of E in general:

Example 3.1. Let $k = \mathbb{Q}(\sqrt{21})$. Then $J = \{-3, -7\}$, $K = \mathbb{Q}(i\sqrt{3}, i\sqrt{7})$,

$$\varepsilon_J = (1 - \zeta_J)(1 - \zeta_J^4)(1 - \zeta_J^{16}) = \frac{i\sqrt{3} - i\sqrt{7}}{2},$$
$$\eta_J = \varepsilon_J^{1+\sigma_{-3}\sigma_{-7}} = \varepsilon_J \cdot \overline{\varepsilon_J} = -\varepsilon_J^2,$$
$$\varkappa_J = \pm\varepsilon_J.$$

Hence we have $C_1 = \langle -1, \varkappa_J \rangle$, $C = \langle -1, \eta_J \rangle$ and $[C_1 : C] = 2$ for this specific k. Theorem 3.1 gives $(E : C_1) = \frac{h}{2}$. It is easy to compute that $h = 1$ which implies $E = C$.

4. The case of real K

The rest of this paper is devoted to a special case of K being real. Our aim is to show that under this assumption we have $C_1 \subseteq E$. It is easy to see that K is real if and only if each $p \in J$ is positive.

We shall need the equivalence relation $\sim$ defined on the group of all units of K as follows: For any units x, y of K we write $x \sim y$ if and only if x/y is the square of a totally positive unit of K.

Lemma 4.1. *If K is real then we have:*
(a) *if $x \sim y$ and $u \sim v$ are units of K then $xu \sim yv$;*
(b) *if $x \sim y$ are units of K then $x^\sigma \sim y^\sigma$ for any $\sigma \in G$;*
(c) *$e^4 \sim 1$ for any unit e of K;*
(d) *$\varepsilon_{\{p\}}^2 \not\sim 1$ for any $p \in J$;*
(e) *$\varepsilon_S^2 \sim 1$ for any $S \subseteq J$, $\#S > 1$;*
(f) *$\varepsilon_S^{1-\sigma\tau} \sim \varepsilon_S^{1-\sigma} \cdot \varepsilon_S^{1-\tau}$ for any $S \subseteq J$ and any $\sigma, \tau \in G$.*

Proof. (a) The product of totally positive units is totally positive, too. (b) All conjugates of a totally positive unit are again totally positive. (c) As all conjugates of e belong to K, they are real, and so e^2 is totally positive. (d) [3, Lemma 1] gives $\varepsilon_{\{p\}}^{1+\sigma_p} = -1$ and so $\varepsilon_{\{p\}}$ is neither totally positive nor totally negative. (e) Due to its definition, ε_S is the norm of a nonzero number from an imaginary abelian field

$\mathbb{Q}^S$ to a real subfield K_S and so it is totally positive. (f) Using (a), this statement is equivalent to $\varepsilon_S^{(1-\sigma)(1-\tau)} \sim 1$. Due to [3, Lemma 2] we have $\varepsilon_S^{1-\sigma} = \pm \prod_{T\subseteq S} \varepsilon_T^{2a_T}$ for suitable $a_T \in \mathbb{Z}$ and, once again, [3, Lemma 2] implies

$$\Big(\prod_{T\subseteq S} \varepsilon_T^{a_T}\Big)^{1-\tau} = \pm \prod_{T\subseteq S} \varepsilon_T^{2b_T}$$

for suitable $b_T \in \mathbb{Z}$. Thus

$$\varepsilon_S^{(1-\sigma)(1-\tau)} = \Big(\pm \prod_{T\subseteq S} \varepsilon_T^{2b_T}\Big)^2$$

and (c) gives the result. ■

In the following lemma we shall consider the complete undirected graph on $S \subseteq J$ where for each $p, q \in S$, $p \neq q$, the edge between vertices p and q is labeled by the number $m_{(p,q)}$ which is defined by means of Legendre symbol as follows:

$$m_{(p,q)} = \frac{1-t_{p,q}}{2}, \qquad \text{where} \qquad t_{p,q} = \begin{cases} (\frac{p}{q}) & \text{if } q \text{ is odd,} \\ (\frac{2}{p}) & \text{if } q = 2. \end{cases}$$

Notice that the quadratic reciprocity law implies $m_{(p,q)} = m_{(q,p)}$ as we are assuming that each $p \in J$ is positive, i.e., either $p = 2$ or p is a prime congruent to 1 modulo 4. If H is a Hamiltonian path from p to q in S, i.e., $H = (p, r_1, \dots, r_{\#S-2}, q)$ such that $\{p, r_1, \dots, r_{\#S-2}, q\} = S$, then we put $m_H = m_{(p,r_1)} \cdot m_{(r_1,r_2)} \cdots m_{(r_{\#S-2},q)}$.

Lemma 4.2. *If K is real, $p \in S \subseteq J$, and $\#S > 1$ then*

$$\varepsilon_S^{1+\sigma_p} \sim \prod_{q\in S,\, q\neq p} \varepsilon_{\{q\}}^{2\sum_H m_H},$$

where the sum is taken over all Hamiltonian paths H from p to q in S.

Proof. If $S = \{p, q\}$ then [3, Lemma 1] gives

$$\varepsilon_S^{1+\sigma_p} = t_{p,q} \cdot \varepsilon_{\{q\}}^{1-\mathrm{Frob}(p,K_{\{q\}})} = \begin{cases} 1 & \text{if } t_{p,q} = 1, \\ -\varepsilon_{\{q\}}^{1-\sigma_q} = \varepsilon_{\{q\}}^2 & \text{if } t_{p,q} = -1, \end{cases}$$

which we wanted to show. Let us suppose that $\#S > 2$ and that the lemma has been proved for all $T \subsetneq S$. Then [3, Lemma 1] states

$$\varepsilon_S^{1+\sigma_p} = \varepsilon_{S\setminus\{p\}}^{1-\mathrm{Frob}(p,K_{S\setminus\{p\}})}.$$

It is easy to see that $\mathrm{Frob}(p, K_{S\setminus\{p\}}) = \prod_{q\in S\setminus\{p\}} \sigma_q^{m_{(p,q)}}$ and Lemma 4.1(f,e,b,a) implies

$$\varepsilon_S^{1+\sigma_p} \sim \prod_{q\in S\setminus\{p\}} \big(\varepsilon_{S\setminus\{p\}}^{1-\sigma_q}\big)^{m_{(p,q)}} \sim \prod_{q\in S\setminus\{p\}} \big(\varepsilon_{S\setminus\{p\}}^{1+\sigma_q}\big)^{m_{(p,q)}}.$$

The lemma follows from the induction hypothesis for $\varepsilon_{S\setminus\{p\}}^{1+\sigma_q}$ and Lemma 4.1(a). ■

Recall that we have seen in Lemma 2.1 that for any $S \subseteq J$ and any $\sigma \in G$ we have $\varepsilon_S^{1+\sigma} = \pm x^2$ for suitable $x \in D_S = \langle \varepsilon_T; T \subseteq S \rangle$. The following lemma states that this x satisfies $x^{1-\sigma} = 1$. Example 3.1 shows that the assumption of K being real cannot be avoided here.

Lemma 4.3. *If K is real, $S \subseteq J$, and $\sigma \in G$ then there is $x \in D_S$ such that $\varepsilon_S^{1+\sigma} = \pm x^2$ and $x^{1-\sigma} = 1$.*

Proof. If $S = \emptyset$ then $\varepsilon_S = 1$ and $x = \pm 1$. If $S = \{p\}$ then ε_S^σ is equal to either ε_S or $\varepsilon_S^{\sigma_p}$. In the former case $x = \pm \varepsilon_S$ and $x^{1-\sigma} = \varepsilon_S^{1-\sigma} = 1$, in the latter case [3, Lemma 1] gives $\varepsilon_S^{1+\sigma} = -1$ and $x = \pm 1$.

Finally, let $\#S > 1$. There is $T \subseteq S$ such that σ acts as $\prod_{p \in T} \sigma_p$ on K_S. Lemma 2.1 gives $x \in D_S$ such that $\varepsilon_S^{1+\sigma} = \pm x^2$ and Lemmas 4.1 and 4.2 imply

$$\pm x^2 = \varepsilon_S^{1+\prod_{p \in T} \sigma_p} \sim \varepsilon_S^{1-\prod_{p \in T} \sigma_p} \sim \prod_{p \in T} \varepsilon_S^{1-\sigma_p} \sim \prod_{p \in T} \varepsilon_S^{1+\sigma_p} \sim \prod_{p \in T} \prod_{q \in S,\, q \neq p} \varepsilon_{\{q\}}^{2 \sum_H m_H},$$

where the sum is taken over all Hamiltonian paths H from p to q in S. Hence there is a totally positive unit $y \in K$ such that

$$\pm x^2 = y^2 \cdot \prod_{q \in S} \varepsilon_{\{q\}}^{2 \sum_{p \in T,\, p \neq q} \sum_H m_H}.$$

As -1 is not a square in K this implies

$$x = \pm y \cdot \prod_{q \in S} \varepsilon_{\{q\}}^{\sum_{p \in T,\, p \neq q} \sum_H m_H}$$

and so

$$x^{1-\sigma} = y^{1-\sigma} \cdot \prod_{q \in S} \left(\varepsilon_{\{q\}}^{1-\sigma}\right)^{\sum_{p \in T,\, p \neq q} \sum_H m_H}.$$

We have

$$\varepsilon_{\{q\}}^{1-\sigma} = \begin{cases} 1 & \text{if } q \notin T, \\ \varepsilon_{\{q\}}^{1-\sigma_q} = -\varepsilon_{\{q\}}^2 & \text{if } q \in T. \end{cases}$$

Therefore

$$x^{1-\sigma} = y^{1-\sigma} \cdot \prod_{q \in T} \left(-\varepsilon_{\{q\}}^2\right)^{\sum_{p \in T,\, p \neq q} \sum_H m_H}.$$

As $(x^{1-\sigma})^2 = (\varepsilon_S^{1+\sigma})^{1-\sigma} = 1$ we have $x^{1-\sigma} = \pm 1$. Hence to prove the lemma we need to show that $x^{1-\sigma} > 0$. Since y is totally positive, $y^{1-\sigma} > 0$; moreover $\varepsilon_{\{q\}}^2 > 0$. Hence

$$\operatorname{sgn} x^{1-\sigma} = \prod_{q \in T} (-1)^{\sum_{p \in T,\, p \neq q} \sum_H m_H} = (-1)^{\sum_{q \in T} \sum_{p \in T,\, p \neq q} \sum_H m_H}.$$

We know that $m_H = m_{H^{\mathrm{op}}}$, where H^{op} is the path opposite to H. This implies that $\sum_{q\in T}\sum_{p\in T,\,p\neq q}\sum_H m_H = 2\sum_{q\in T}\sum_{p\in T,\,p<q}\sum_H m_H$ is even and so sgn $x^{1-\sigma} = 1$ and $x^{1-\sigma} > 0$. The lemma is proved. ■

Proposition 4.1. *If K is real then $\varkappa_S \in k_S$ for each $S \subseteq J$.*

Proof. We need to show that $\varkappa_S^{1-\sigma} = 1$ for each $\sigma \in \mathrm{Gal}(K_S/k_S)$. This is clear if $\sigma = 1$, so we can assume that $\sigma \neq 1$. Then there is a basis $\alpha_1, \ldots, \alpha_r$ of $\mathrm{Gal}(K_S/k_S)$ such that $\alpha_r = \sigma$. Lemma 2.1 implies that

$$\varepsilon_S^{(1+\alpha_1)\cdots(1+\alpha_{r-1})} = \pm y^{2^{r-1}}$$

with $y = \prod_{T\subseteq S} \varepsilon_T^{a_T}$ for suitable $a_T \in \mathbb{Z}$. Then

$$\pm\varkappa_S^{2^r} = \eta_S = \varepsilon_S^{(1+\alpha_1)\cdots(1+\alpha_{r-1})(1+\sigma)} = \left(\pm y^{2^{r-1}}\right)^{1+\sigma} = \left(y^{1+\sigma}\right)^{2^{r-1}} .$$

As -1 is not a square in K this implies

$$\pm\varkappa_S^2 = y^{1+\sigma} = \prod_{T\subseteq S} \left(\varepsilon_T^{1+\sigma}\right)^{a_T} .$$

Lemma 4.3 states that there are $x_T \in D_T$ such that $\varepsilon_T^{1+\sigma} = \pm x_T^2$ and $x_T^{1-\sigma} = 1$. Hence

$$\pm\varkappa_S^2 = \prod_{T\subseteq S} \left(\pm x_T^2\right)^{a_T}$$

and this implies

$$\varkappa_S = \pm \prod_{T\subseteq S} x_T^{a_T}$$

because -1 is not a square in K. Therefore

$$\varkappa_S^{1-\sigma} = \prod_{T\subseteq S} \left(x_T^{1-\sigma}\right)^{a_T} = 1 ,$$

which we wanted to prove. ■

Theorem 4.1. *If K is real then the class number h of k is divisible by the following power of 2:*

$$2\cdot[k:\mathbb{Q}]\cdot\left(\frac{[K:k]}{4}\right)^{[k:\mathbb{Q}]/2} \;\Big|\; h .$$

Proof. Proposition 4.1 implies that $C_1 \subseteq E$ and so $(E : C_1) = [E : C_1]$ is an integer. Theorem 3.1 gives

$$h = 2\cdot[k:\mathbb{Q}]\cdot[E:C_1]\cdot\left(\frac{[K:k]}{4}\right)^{[k:\mathbb{Q}]/2}$$

and the theorem follows. ■

References

[1] M. Bulant, *On the parity of the class number of the field* $Q(\sqrt{p}, \sqrt{q}, \sqrt{r})$, J. Number Theory **68** (1998), 72–86.

[2] R. Kučera, *On the parity of the class number of a biquadratic field*, J. Number Theory **52** (1995), 43–52.

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

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

Address: Přírodovědecká fakulta, Masarykova univerzita, Kotlářská 2, 611 37 Brno, Czech Republic

E-mail: kucera@math.muni.cz

Received: 23 October 2007; **revised:** 13 October 2008