ACTA ARITHMETICA
139.2 (2009)

On the group of circular units of any compositum of quadratic fields

by

ZDENĚK POLICKÝ (Brno)

Introduction. The aim of this paper is to describe the group of circular units C of a compositum k of quadratic fields in the last case that has not been covered yet, namely when the ramification index e of 2 equals 4. It is easy to see that e always divides 4. If $e = 1$ or $e = 2$ we already know a basis of C and an explicit formula for the index of C in the full group of units E (see [2, Theorem 1] and [4, Proposition 1.4]). The main ingredient of these results was the observation that the action of the augmentation ideal of $\mathbb{Z}[G]$, where $G = \mathrm{Gal}(k/\mathbb{Q})$, on the quotient C/W, where W is the group of all roots of unity in k, gives squares in C/W. In other words, for any $\varepsilon \in C$ and any $\sigma \in G$ there is $\rho \in W$ and $\eta \in C$ such that $\varepsilon^{1-\sigma} = \rho\eta^2$. Unfortunately, this key property of the group of circular units of a compositum of quadratic field is not satisfied in the case $e = 4$ (see Example 8 below for $k = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$). Therefore if $e = 4$ we cannot use the same approach for k. Nevertheless, using the three maximal subfields of k whose ramification index at 2 is 2, we are able to describe an explicit maximal independent system of units in C. Let $\tilde{C}$ be the group generated by W and by this system. Then we can compute the index $[E : \tilde{C}]$ and give a reasonable upper bound for the index $[C : \tilde{C}]$ (see Theorem 7 and Proposition 5).

1. Definitions and basic results. Let k be a compositum of quadratic fields and let K be the genus field of k in the narrow sense. We assume that both -1 and 2 are squares in K. We put

$$J = \{-1, -2, 2\} \cup \{p \in \mathbb{Z};\ p \equiv 1 \pmod 4,\ |p| \text{ is a prime ramifying in } k\}.$$

2000 *Mathematics Subject Classification*: Primary 11R29; Secondary 11R27.
Key words and phrases: compositum of quadratic fields, circular units, the index of circular units, class number.

DOI: 10.4064/aa139-2-2

For any $p \in J$, let

$$n_{\{p\}} = \begin{cases} |p| & \text{if } p \notin \{-1, -2, 2\}, \\ 4 & \text{if } p = -1, \\ 8 & \text{if } p = \pm 2. \end{cases}$$

For any $S \subseteq J$ let n_S be the smallest common multiple of $n_{\{p\}}$ for all $p \in S$ (by convention $n_\emptyset = 1$), and

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

It is easy to see that $K_J = K$, $k_J = k$, and n_J is the conductor of k.

We call a subset $S \subseteq J$ *admissible* if S contains at most one of the numbers -1, 2, and -2. For any admissible set $S \subseteq J$ we define

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

and $\eta_S = \mathrm{N}_{K_S/k_S}(\varepsilon_S)$.

Let χ_2 and χ_{-2} be the unique even and odd Dirichlet character of conductor 8, respectively. For each $p \in J - \{2, -2\}$ let χ_p be the unique Dirichlet character of conductor $n_{\{p\}}$, so χ_p is odd if and only if $p < 0$.

Let X be the group of all even Dirichlet characters corresponding to k. Each $\chi \in X$ can be written in the form $\chi = \prod_{p \in S_\chi} \chi_p$ for a unique admissible set $S_\chi \subseteq J$. Then the conductor of χ is equal to n_{S_χ}.

It is easy to see that, for any admissible set $S \subseteq J$, a character $\chi \in X$ belongs to the set of Dirichlet characters corresponding to the field k_S if and only if $S_\chi \subseteq S$.

Let C be the group of circular units of k defined in [3]. This means that C is generated by W and by all conjugates of η_S, where $S \subseteq J$ (see the proof of Proposition 4 below). This group contains the Sinnott group of circular units C' of k but it can be slightly bigger. Lemma 3 in [2] implies that the Sinnott group is generated by

$$W \cup \{\eta_S;\, S \subseteq J,\, \# S > 1\} \cup \{\eta_p^2;\, p \in J,\, p > 0, \sqrt{p} \in k\}$$

and consequently $[C : C'] = 2^a$, where

$$0 \le a \le \# \{p \in J;\, p > 0,\, \sqrt{p} \in k\}.$$

Similarly, for any $S \subseteq J$ let C_S be the group of circular units of k_S defined in [3]. If S is admissible then the ramification index of 2 in k_S is not equal to 4 and so we know the following basis of C_S:

LEMMA 1. *If $S \subseteq J$ is admissible then a basis of C_S is formed by the set of all η_{S_χ} where $\chi \in X$ is non-trivial and satisfies $S_\chi \subseteq S$.*

Proof. If $-1 \notin S$ see [2, Lemma 5], otherwise see [4, Proposition 1.4]. ∎

Let W be the group of all roots of unity in k. Let $\tilde{C}$ be the subgroup of the multiplicative group $k^\times$ generated by W and by all conjugates of η_S for all admissible sets $S \subseteq J$. Let $G = \mathrm{Gal}(k/\mathbb{Q})$ be the Galois group of k.

Lemma 2. *For any $\varepsilon \in \tilde{C}$ and any $\sigma \in G$ there are $\rho \in W$ and $\eta \in \tilde{C}$ such that $\varepsilon^{1-\sigma} = \rho\eta^2$.*

Proof. Consider a conjugate of η_S for an admissible set $S \subseteq J$. If $-1 \notin S$ use [2, Lemma 2], otherwise use [4, Lemma 1.2]. ∎

Lemma 3. *The set $W \cup \{\eta_{S_\chi};\, \chi \in X,\, \chi \neq 1\}$ generates the group $\tilde{C}$.*

Proof. Lemma 2 gives that $\tilde{C}$ is as a group generated by W and by η_S for all admissible sets $S \subseteq J$. For any admissible set $S \subseteq J$ we can show that if $S \neq S_\chi$ for all $\chi \in X$ then η_S can be written as a multiplicative $\mathbb{Z}$-linear combination of η_L for $L \subsetneq S$ (modulo roots of unity). If $-1 \notin S$ use [2, Lemma 5], otherwise use [4, p. 1077]. ∎

2. The index of $\tilde{C}$ in C

Proposition 4. *The group C of circular units of k is generated by $\tilde{C}$ and by all conjugates of $\mathrm{N}_{\mathbb{Q}^S/k_S}(1-\zeta_S)$, where $S \subseteq J$ is not admissible, $S \neq \{-1, 2, -2\}$, and the ramification index of k_S at 2 is 4.*

Proof. Let E be the full group of units of k. By definition (see [3]), C is the intersection of E and a group D, where D is generated by -1, by $\sqrt{p}$ for all $p \in J$ such that $p > 0$ and $\sqrt{p} \in k$, and by all conjugates of $\mathrm{N}_{\mathbb{Q}^S/k_S}(1-\zeta_S)$ for all non-empty $S \subseteq J$.

For a non-empty $S \subseteq J$, it is well-known that $\mathrm{N}_{\mathbb{Q}^S/k_S}(1-\zeta_S)$ is a unit if and only if n_S is not a prime power. Moreover, if $p \in J$ and $p < 0$ then all units of $k_{\{p\}}$ are roots of unity. Therefore $\tilde{C}$ is the intersection of E and a group $\tilde{D}$, where $\tilde{D}$ is generated by -1, by $\sqrt{p}$ for all $p \in J$ such that $p > 0$ and $\sqrt{p} \in k$, and by all conjugates of $\mathrm{N}_{\mathbb{Q}^S/k_S}(1-\zeta_S)$ for all *admissible* non-empty $S \subseteq J$.

If S is not admissible and the ramification index of k_S at 2 is not 4 then $k_S = k_{S'}$ for a suitable admissible $S' \subseteq S$. Hence D is generated by $\tilde{D}$ and by $\mathrm{N}_{\mathbb{Q}^S/k_S}(1-\zeta_S)$ for all non-admissible $S \subseteq J$ such that the ramification index of k_S at 2 is 4. This norm is a unit unless $S = \{-1, 2, -2\}$ and $\sqrt{-1}, \sqrt{2} \in k$, in which case $k_S = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ is the eighth cyclotomic field. But the group of all units of the latter is generated by ζ_8 and by

$$\eta = \zeta_8^{-1} \cdot \frac{1-\zeta_8^3}{1-\zeta_8} = 1 + \zeta_8 + \zeta_8^{-1} = 1 + \sqrt{2}.$$

We have

$$\eta_{\{2\}} = \frac{1}{\sqrt{2}} \mathrm{N}_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2})}(1-\zeta_8) = \sqrt{2}-1 = \eta^{-1},$$

and the proposition follows. ∎

Proposition 5. *The group $\tilde{C}$ is of finite index in C and $[C:\tilde{C}] \le 2^n$, where n is the number of all $S \subseteq J$ such that $\{-1,2,-2\} \subsetneq S$ and the ramification index of k_S at 2 is 4. Moreover, the Galois action of G on $C/\tilde{C}$ is trivial.*

Proof. Let $T = J - \{-1,2,-2\}$. For any $x \in \{-1,2,-2\}$ let ρ_x be the generator of $\mathrm{Gal}(K/K_{T\cup\{x\}})$. For any $L \subseteq T$ we put $S = L \cup \{-1,2,-2\}$ and $\varepsilon = \mathrm{N}_{\mathbb{Q}^S/k_S}(1-\zeta_S)$. Then

$$\varepsilon^2 = \varepsilon^{1+\rho_{-1}} \cdot \varepsilon^{1+\rho_{-2}} \cdot (\varepsilon^{1+\rho_2})^{-\rho_{-1}}.$$

For any $x \in \{-1,2,-2\}$ we have

$$\varepsilon^{1+\rho_x} = \mathrm{N}_{\mathbb{Q}^S/k_{T\cup\{x\}}}(1-\zeta_S) = \eta_{T\cup\{x\}}$$

because $\mathrm{N}_{\mathbb{Q}^S/\mathbb{Q}^{T\cup\{x\}}}(1-\zeta_S) = 1-\zeta_{T\cup\{x\}}$. We have obtained $\varepsilon^2 \in \tilde{C}$ and for any $\sigma \in G$ Lemma 2 gives $\varepsilon^{2(1-\sigma)} \in W \cdot \tilde{C}^2$, which implies $\varepsilon^{1-\sigma} \in \tilde{C}$. The proposition follows by means of Proposition 4. ∎

3. A basis of $\tilde{C}$ and the index of $\tilde{C}$ in E

Theorem 6. *The set $\{\eta_{S_\chi};\ \chi \in X,\ \chi \ne 1\}$ is a $\mathbb{Z}$-basis of $\tilde{C}$, i.e. elements of this set are multiplicatively independent and together with W generate $\tilde{C}$.*

Proof. Proposition 5 gives that $\tilde{C}$ and C have the same $\mathbb{Z}$-rank. As the index $[E:C]$ is finite, $\tilde{C}$ and E have the same $\mathbb{Z}$-rank, and the $\mathbb{Z}$-rank of E is equal to the number of elements of the given set. The theorem follows from Lemma 3. ∎

Having a $\mathbb{Z}$-basis allows us to compute the index:

Theorem 7. *We have*

$$[E:\tilde{C}] = \Bigg(\prod_{\chi\in X,\,\chi\ne 1} \frac{2\cdot[k:k_{S_\chi}]}{[k:k^+]}\Bigg) \cdot |X|^{-|X|/2} \cdot Qh^+,$$

where k^+ is the maximal real subfield of k, $|X|$ means the number of characters in X, $Q = [E : W\cdot(E\cap k^+)]$ is the Hasse unit index of k, and h^+ is the class number of k^+.

Proof. This can be proved in the same way as Theorem 1 in [2]. ∎

The following example shows that the estimate of the index $[C : \tilde{C}]$ can be precise. It seems to be an interesting question whether this holds true in general.

Example 8. Let $k = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$. Then k is the 24th cyclotomic field. Sinnott's formula for the index of the group of circular units of a cyclotomic field (see [5, Theorem]) shows that the Sinnott's group of circular units of k equals E and so we also have $C = E$. Then [1, Theorem 6.1] gives the following $\mathbb{Z}$-basis of C: $\alpha = 1 - \zeta$, $\beta = 1 - \zeta^{19}$, $\gamma = (1 - \zeta^9)/(1 - \zeta^3)$. As β is a conjugate of α, we see that we obtain $\alpha \cdot \beta^{-1}$ by an action of the augmentation ideal on α. As both α and β belong to a basis we see that $\alpha \cdot \beta^{-1}$ is not a square modulo roots of unity in E. Theorem 6 states that $\eta_{\{2\}}$, $\eta_{\{-1,-3\}}$ and $\eta_{\{-2,-3\}}$ form a $\mathbb{Z}$-basis of $\tilde{C}$. We have

$$\begin{aligned} \eta_{\{2\}} &= (1 + \sqrt{2})^{-1} = \zeta^3 \cdot \gamma, \\ \eta_{\{-1,-3\}} &= 1 - \zeta^2 = \zeta \cdot \alpha \cdot \beta^{-1} \cdot \gamma, \\ \eta_{\{-2,-3\}} &= \alpha \cdot \beta. \end{aligned}$$

The determinant of the transition matrix gives the index $[C : \tilde{C}] = 2$ for k, which equals the upper bound given by Proposition 5.

This research was supported by the Grant Agency of the Czech Republic by the project 201/07/0191.

References

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

[2] —, *On the Stickelberger ideal and circular units of a compositum of quadratic fields*, ibid. 56 (1996), 139–166.

[3] —, *A note on Sinnott's definition of circular units of an abelian field*, ibid. 63 (1997), 403–407.

[4] Z. Polický, *On the index of circular units in the full group of units of a compositum of quadratic fields*, ibid. 128 (2008), 1074–1090.

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

Department of Mathematics and Statistics
Faculty of Science
Masaryk University
Kotlářská 2
611 37 Brno, Czech Republic
E-mail: alize@seznam.cz

Received on 4.10.2008
and in revised form on 13.12.2008 (5817)