On the index of circular units in the full group of units of a compositum of quadratic fields

Zdeněk Polický 1

Department of Mathematics, Faculty of Science, Masaryk University,
Janáčkovo nám. 2a, 602 00 Brno, Czech Republic

Received 21 November 2006; revised 21 July 2007

Available online 25 October 2007

Communicated by J.S. Hsia

Abstract

For a compositum of quadratic fields \( k = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_s}) \), where \( d_1, \ldots, d_s \) are square-free odd integers and \( d_1 \equiv 3 \pmod{4} \), we study the group \( C \) of circular units of \( k \). We construct a basis of \( C \), compute the index of \( C \) in the full group of units of \( k \) and derive a lower bound for the divisibility of this index by a power of 2. These results give a lower bound for the divisibility of the class number of the maximal real subfield of \( k \) by a power of 2.

Keywords: Compositum of quadratic fields; Circular units; Index of circular units; Class number

Introduction

Let \( k \) be a compositum of a finite number of quadratic fields and let \( K \) be the genus field of \( k \) in narrow sense. We assume that \(-1\) is a square in \( K \) but \( 2 \) is not a square in \( K \).

The aim of this paper is to construct a group \( C \) of circular units of \( k \), which is slightly larger than the Sinnott’s group given in [2]. We find a basis of \( C \) and compute the index of \( C \) in the group \( E \) of all units of \( k \) (see Proposition 1.4). The main result of this paper is a lower bound for the divisibility of \([E : C]\) by a power of 2 (see Theorem 4.2). These results give a lower bound for the divisibility of the class number of the maximal real subfield of \( k \) by a power of 2.

1 Supported by the Grant Agency of the Czech Republic (Methods of Theory of Numbers, 201/04/381).

E-mail address: alize@seznam.cz.

MSC: primary 11R29; secondary 11R27
This paper can be understood as a counterpart of [1] where such a task has been done for the case $-1$ not being a square in $K$. Thus this paper together with [1] cover all composita of quadratic fields whose ramification index at 2 is not 4.

1. Definition of $C$

Let $k$ be a compositum of quadratic fields and let $K$ be the genus field of $k$ in narrow sense. We assume that $\sqrt{-1} \in K$ and $\sqrt{2} \notin K$. We define a set $J$ of signed primes ramifying in $k$ as follows

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

For any $p \in J$, let us define

$$n_{\{p\}} = \begin{cases} |p| & \text{if } p \text{ is odd,} \\ 4 & \text{if } p = -2, \end{cases} \quad K_{\{p\}} = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \text{ is odd,} \\ \mathbb{Q}(\sqrt{-1}) & \text{if } p = -2. \end{cases}$$

For any $L \subseteq J$ let us denote $n_L = \prod_{p \in L} n_{\{p\}}$, $K_L = \prod_{p \in L} K_{\{p\}}$ if $L \neq \emptyset$ and $K_\emptyset = \mathbb{Q}$, and finally $Q_L^L = \mathbb{Q}(\zeta_L)$, where $\zeta_L = e^{2\pi i/n_L}$ is a primitive $n_L$th root of unity. It is easy to see that $K_J$ equals $K$.

For any $L \subseteq J$ let us now define

$$\epsilon_L = \begin{cases} 1 & \text{if } L = \emptyset, \\ \frac{1}{\sqrt{p}}N_{Q_L^L/K_L}(1 - \zeta_L) & \text{if } L = \{p\}, \; p \neq -2, \\ i & \text{if } L = \{-2\}, \\ N_{Q_L^L/K_L}(1 - \zeta_L) & \text{if } \#L > 1, \end{cases}$$

and $\eta_L = N_{K_L/k_L}(\epsilon_L)$ where $k_L = k \cap K_L$. It is easy to see that all $\epsilon_L$ are units of $K_L$.

For any $p \in J$ let $\sigma_p$ be the generator of $\text{Gal}(K_J/K_{J \setminus \{p\}})$. Then we denote $G = \text{Gal}(K_J/\mathbb{Q})$.

**Lemma 1.1.** Let $p \in L \subseteq J$. Then

$$N_{K_L/K_{L \setminus \{p\}}}(\epsilon_L) = \begin{cases} -\text{sgn } p & \text{if } L = \{p\}, \\ t_{p,q} \cdot \text{Frob}(|p|, K_{\{q\}}) \cdot \epsilon_{\{q\}} & \text{if } L = \{p, q\}, \; p \neq q, \; q \neq -2, \\ 1 & \text{if } L = \{p, -2\}, \; |p| \equiv 1 \pmod{4}, \\ -i & \text{if } L = \{p, -2\}, \; |p| \equiv 3 \pmod{4}, \\ \text{Frob}(|p|, K_{L \setminus \{p\}}) \cdot \epsilon_{L \setminus \{p\}} & \text{if } \#L > 2, \end{cases}$$

where sgn $p$ means the sign of $p$, $\text{Frob}(|p|, K_{\{q\}})$ is the Frobenius automorphism of $|p|$ in $K_{L \setminus \{p\}}/\mathbb{Q}$ and $t_{p,q}$ is defined by means of the Legendre symbol as follows:

$$t_{p,q} = \left( \frac{|p|}{|q|} \right).$$
Proof. At first, let us suppose \( \#L > 1 \). Then

\[
N_{K_L/K_{L\setminus \{p\}}} (\xi_L) = N_{Q_{L\setminus \{p\}}/K_{L\setminus \{p\}}} (N_{Q_{L\setminus \{p\}}/Q_{L\setminus \{p\}}} (1 - \xi_L))
\]

\[= N_{Q_{L\setminus \{p\}}/K_{L\setminus \{p\}}} (\xi_L) \left( (1 - \xi_L) \right)^{1 - \text{Frob}^{-1}(|p|, Q_{L\setminus \{p\}})}
\]

\[= N_{Q_{L\setminus \{p\}}/K_{L\setminus \{p\}}} (1 - \xi_L) \left( \xi_L \right)^{1 - \text{Frob}(|p|, K_{L\setminus \{p\}})},
\]

because \( \text{Frob}^2(|p|, K_{L\setminus \{p\}}) \) is the identity. So the lemma is proved if \( \#L > 2 \). If \( L = \{p, -2\} \) then

\[
N_{Q_{\{-2\}}/K_{\{-2\}}} (1 - \xi_{\{-2\}}) = 1 - i
\]

and the third and fourth case of the lemma follows from

\[
(1 - i)^{1 - \text{Frob}(|p|, K_{\{-2\}})} = \begin{cases} 
1 & \text{if } |p| \equiv 1 \pmod{4}, \\
-i & \text{if } |p| \equiv 3 \pmod{4}.
\end{cases}
\]

Similarly by using \( (\sqrt{q})^{1 - \text{Frob}(|p|, K_{\{q\}})} = t_{p,q} \) we prove the second case. If \( L = \{p\} \) the lemma follows easily. \( \square \)

Lemma 1.2. Let \( L \subseteq J, \sigma \in G \). Then

\[
\xi_{L}^{1 - \sigma} = \varrho \prod_{S \subseteq L} \xi_{S}^{2a_{S}}
\]

for suitable \( a_{S} \in \mathbb{Z} \), where \( \varrho \in \{1, -1, i, -i\} \) depends on the choice of \( L \) and \( \sigma \).

Proof. This can be proved in the same way as Lemma 2 of [1]. \( \square \)

Lemma 1.3. Let \( L \subseteq J, \sigma \in G \). Then

\[
\eta_{L}^{1 - \sigma} = \varrho \prod_{S \subseteq L} \eta_{S}^{2a_{S}},
\]

for suitable \( a_{S} \in \mathbb{Z} \), where \( \varrho \in \{1, -1, i, -i\} \cap k \) depends on the choice of \( L \) and \( \sigma \).

Proof. This is a corollary of Lemma 1.2 and of the fact that \( \eta_{S} \in k \) implies \( \varrho \in k \). \( \square \)

Now let us denote \( W \) the group of roots of unity of \( k \). Since \( k \) is a compositum of quadratic fields then it is not difficult to prove that \( \#W \mid 24 \). Moreover, we assume that \( \sqrt{2} \notin K_{J} \) and so \( \#W \mid 12 \). Further, we need to define the set \( X \) as follows:

\[
X = \{ \xi \in \hat{G}; \xi(\sigma) = 1 \text{ for all } \sigma \in \text{Gal}(K_{J}/k^{+}) \},
\]

where \( \hat{G} \) is the group of characters of \( G \). Then \( X \) can be viewed as the group of all Dirichlet characters corresponding to the maximal real subfield \( k^{+} \) of \( k \). For any \( \xi \in X \) let us define

\[
L_{\xi} = \{ p \in J; \xi(\sigma_{p}) = -1 \}.
\]
Finally, let $C$ denote the group generated by $W$ and by $\{\eta_L^\sigma : L \subseteq J, \sigma \in G\}$ and let $E$ denote the full group of units of $k$. Notice that $C$ contains Sinnott’s group of circular units defined in [2]. It can be shown that these two groups do not coincide in general.

**Proposition 1.4.** Let $B = \{\eta_{L,\xi} : \xi \in X, \xi \neq 1\}$. Then $B$ is a basis of non-torsion part of $C$ and moreover

$$[E : C] = \left( \prod_{\xi \in X, \xi \neq 1} \frac{2 \cdot [k : k_{L,\xi}]}{[k : k^+]^2} \right) \cdot (\#X)^{-\frac{1}{2}(\#X)} \cdot Q h^+,$$

where $Q = [E : E^+W]$ is the Hasse unit index ($Q = 1$ if $k$ is real) and $h^+$ is the class number of $k^+$.

**Proof.** This can be proved in the same way as Theorem 1 and Lemma 5 of [1].

2. **Circular units that are squares in $K$**

For any $\epsilon \in C$ and any $\sigma \in G$ Lemma 1.2 implies that $\epsilon^{1-\sigma}$ is up to a root of unity the square of a unit in $C$. But $\#W | 12$ and so any $\rho \in W$ can be uniquely written in the form $\rho = \Delta \cdot (\delta \cdot \varphi)^2$, where $\Delta, \delta \in \{1, i\}$ and $\varphi^3 = 1$. Moreover, if $\#W | 4$ then $\varphi = 1$ and if $\#W | 6$ then $\Delta = 1$. Therefore we have the identity

$$\epsilon^{1-\sigma} = \Delta(\sigma, \epsilon) \cdot (\delta(\sigma, \epsilon) \cdot \varphi(\sigma, \epsilon) \cdot \psi(\sigma, \epsilon))^2,$$

where $\Delta(\sigma, \epsilon), \delta(\sigma, \epsilon) \in \{1, i\}$, $\varphi(\sigma, \epsilon) \in \{1, \zeta_3, \zeta_3^2\}$ and $\psi(\sigma, \epsilon)$ belongs to the group generated by the set $B$. Moreover, $\Delta(\sigma, \epsilon), \delta(\sigma, \epsilon), \varphi(\sigma, \epsilon)$ and $\psi(\sigma, \epsilon)$ are uniquely determined by the previous identity.

**Lemma 2.1.** Let $\sigma \in G$. Then $\Delta(\sigma, \cdot)^2$ and $\psi(\sigma, \cdot)$ are homomorphisms, i.e., for any $\epsilon, \eta \in C$

$$\Delta(\sigma, \epsilon \eta)^2 = (\Delta(\sigma, \epsilon) \Delta(\sigma, \eta))^2,$$

$$\psi(\sigma, \epsilon \eta) = \psi(\sigma, \epsilon) \psi(\sigma, \eta).$$

**Proof.** The lemma follows from the identity $(\epsilon \eta)^{1-\sigma} = \epsilon^{1-\sigma} \eta^{1-\sigma}$ and from the definition of $\epsilon^{1-\sigma}$ in the form as above.

**Lemma 2.2.** Let $\sigma, \tau \in G$ and $\epsilon \in C$. Then

$$\Delta(\sigma \tau, \epsilon)^2 = (\Delta(\sigma, \epsilon) \Delta(\tau, \epsilon))^2.$$
and by decomposing $\varepsilon^{1-\sigma}$ as in the beginning of this section it is easy to see that $\Delta(\sigma, \varepsilon) \Delta(\tau, \varepsilon)^{\sigma} / \Delta(\sigma \tau, \varepsilon) \in \{ \pm 1, \pm i \}$ is a square in $k$. The identity follows because $\pm i$ is not a square in $k$ and $\Delta(\tau, \varepsilon)^{\sigma} = \pm \Delta(\tau, \varepsilon)$. □

**Proposition 2.3.** Let $\varepsilon \in E$ be such that there exists a function $f : G \to K_J$ satisfying $\varepsilon^{1-\sigma} = f(\sigma)^2$ for any $\sigma \in G$. If there exists a function $g : G \to \{-1, 1\}$ such that $fg$ is a crossed homomorphism, i.e., for all $\sigma, \tau \in G$

$$f(\sigma \tau)g(\sigma \tau) = f(\sigma)g(\sigma)(f(\tau)g(\tau))^\sigma,$$

then $\varepsilon$ or $2\varepsilon$ is a square in $K_J$.

**Proof.** Similarly as in [1, Proposition 2], we can show that there is $\alpha \in K^*_J$ and $b \in \mathbb{Q}^*$ such that $b = \varepsilon \alpha^2$ and that $\pm b = c^2 \prod_{p \in L} p$ for a suitable $c \in \mathbb{Q}^*$ and $L \subseteq J$. The proposition follows from the fact that $\sqrt{-1} \in K_J$ and $\sqrt{p} \in K_J$ for all $p \in J$, $p \neq -2$. □

**Remark 2.4.** The sufficient condition of Proposition 2.3 is also necessary. If $\varepsilon = \eta^2$ or $2\varepsilon = \eta^2$ for a suitable $\eta \in K_J$ then $f(\sigma) = \eta^{1-\sigma}$ satisfies $\varepsilon^{1-\sigma} = f(\sigma)^2$ and for any $f : G \to K_J$ with $f(\sigma)^2 = \varepsilon^{1-\sigma}$ we have the function $g : G \to \{-1, 1\}$ determined by $g(\sigma) = \eta^{1-\sigma} / f(\sigma)$, such that $fg$ is a crossed homomorphism.

Now let us denote for any $\sigma, \tau \in G$ and for any $\varepsilon \in C$

$$\langle \sigma, \tau \rangle_\varepsilon = \Delta(\sigma, \psi(\tau, \varepsilon))^2.$$

**Lemma 2.5.** Let $\sigma, \tau \in G$ and $\varepsilon \in C$. Then

$$\langle \sigma, \tau \rangle_{\varepsilon \eta} = \langle \sigma, \tau \rangle_\varepsilon \langle \sigma, \tau \rangle_\eta.$$

**Proof.** The lemma follows immediately from Lemma 2.1. □

**Proposition 2.6.** Let $\varepsilon \in C$. Then $\varepsilon$ or $2\varepsilon$ is a square in $K_J$ if and only if the following conditions are satisfied for any $\sigma, \tau \in G$:

1. (C1) $(\Delta(\sigma, \varepsilon))^2 = 1$,
2. (C2) $\langle \sigma, \sigma \rangle_\varepsilon = 1$,
3. (C3) $\langle \sigma, \tau \rangle_\varepsilon = \langle \tau, \sigma \rangle_\varepsilon$,
4. (C4) $\delta(\sigma, \varepsilon)^{1-1} \cdot \delta(\tau, \psi(\sigma, \varepsilon))^2 = \delta(\tau, \psi(\sigma, \varepsilon))^2$,
5. (C5) $\delta(\sigma, \varepsilon)^{\sigma + 1} \cdot \delta(\sigma, \psi(\sigma, \varepsilon))^2 = 1$.

**Proof.** At first, let us suppose that there is $\gamma \in K_J$ such that $\varepsilon = \gamma^2$ or $\varepsilon = 2\gamma^2$. Then

$$(\gamma^{1-\sigma})^2 = \varepsilon^{1-\sigma} = \Delta(\sigma, \varepsilon) \cdot (\delta(\sigma, \varepsilon) \cdot \psi(\sigma, \varepsilon))^2,$$

and easily $\Delta(\sigma, \varepsilon)$ is a square in $K_J$. It follows immediately that we have the condition (C1) because $i$ is not a square in $K_J$. Therefore (1) implies

$$\gamma^{1-\sigma} = \pm \delta(\sigma, \varepsilon) \cdot \psi(\sigma, \varepsilon) \cdot \psi(\sigma, \varepsilon).$$
It is easy to see that
\[
(\delta(\sigma, \epsilon))^{1-\tau} = \begin{cases} 
\delta(\sigma, \epsilon)^2 & \text{if } i^\tau = -i, \\
1 & \text{otherwise}
\end{cases}
\]
and that \(\varphi(\sigma, \epsilon)^{1-\tau}\) is a third root of unity, so a square in \(K_J\). Then substituting
\[
\psi(\sigma, \epsilon)^{1-\tau} = \Delta(\tau, \psi(\sigma, \epsilon)) \cdot (\delta(\tau, \psi(\sigma, \epsilon)) \cdot \varphi(\tau, \psi(\sigma, \epsilon)) \cdot \psi(\tau, \psi(\sigma, \epsilon)))^2
\]
for \(\tau = \sigma\) to the identity obtained from (2) by the application of \(1 - \sigma\), we deduce that \(\Delta(\sigma, \psi(\sigma, \epsilon))\) is a square in \(K_J\) but \(i\) is not a square in \(K_J\). So the condition (C2) follows. Similarly we substitute (3) to the identity \(\gamma^{(1-\sigma)(1-\tau)} = \gamma^{(1-\tau)(1-\sigma)}\). Since \(\varphi(\cdot, \cdot)\) is a third root of unity then
\[
\frac{\varphi(\sigma, \epsilon)^{1-\tau} \cdot \varphi(\tau, \psi(\sigma, \epsilon))^2}{\varphi(\tau, \epsilon)^{1-\sigma} \cdot \varphi(\sigma, \psi(\tau, \epsilon))^2} = 1
\]
and consequently
\[
\frac{\delta(\sigma, \epsilon)^{1-\tau} \cdot \Delta(\tau, \psi(\sigma, \epsilon)) \cdot (\delta(\tau, \psi(\sigma, \epsilon)) \cdot \psi(\tau, \psi(\sigma, \epsilon)))^2}{\delta(\tau, \epsilon)^{1-\sigma} \cdot \Delta(\sigma, \psi(\tau, \epsilon)) \cdot (\delta(\sigma, \psi(\tau, \epsilon)) \cdot \psi(\sigma, \psi(\tau, \epsilon)))^2} = 1.
\]

By using the same arguments as above we deduce
\[
\frac{\Delta(\tau, \psi(\sigma, \epsilon))}{\Delta(\sigma, \psi(\tau, \epsilon))} = 1
\]
because this is a square in \(K_J\). So the condition (C3) follows. By the same way the identity \(\gamma^{(1-\sigma)(1-\tau)} = \gamma^{(1-\tau)(1-\sigma)}\) gives that
\[
\left(\frac{\psi(\tau, \psi(\sigma, \epsilon))}{\psi(\sigma, \psi(\tau, \epsilon))}\right)^2 \in W.
\]
Since \(\psi(\cdot, \cdot)\) belongs to the non-torsion group generated by \(B\) then
\[
\frac{\psi(\tau, \psi(\sigma, \epsilon))}{\psi(\sigma, \psi(\tau, \epsilon))} = 1.
\]
Moreover, as \(\delta(\cdot, \cdot)\) is a fourth root of unity, then
\[
\frac{\delta(\sigma, \epsilon)^{1-\tau} \cdot \delta(\tau, \psi(\sigma, \epsilon))^2}{\delta(\tau, \epsilon)^{1-\sigma} \cdot \delta(\sigma, \psi(\tau, \epsilon))^2} = 1
\]
which implies (C4). To prove the last condition compare (1) and
\[
\gamma^{(1-\sigma)^2} = \delta(\sigma, \epsilon)^{1-\sigma} \cdot \varphi(\sigma, \epsilon)^{1-\sigma} \cdot (\delta(\sigma, \psi(\sigma, \epsilon)) \cdot \varphi(\sigma, \psi(\sigma, \epsilon)) \cdot \psi(\sigma, \psi(\sigma, \epsilon)))^2.
\]
Hence using the same facts as in proving the previous condition we have the last one.
On the other hand, suppose that the conditions (C1)–(C5) are satisfied. Let us denote \( f(\sigma) = \delta(\sigma, \epsilon) \varphi(\sigma, \epsilon) \psi(\sigma, \epsilon) \) for any \( \sigma \in G \). Hence, the condition (C1) implies \( \epsilon^{1-\sigma} = f(\sigma)^2 \). Then

\[
1 = \frac{\epsilon^{1-\sigma}}{\epsilon^{1-\sigma}(\epsilon^{1-\sigma})^\sigma} = \left( \frac{f(\sigma)}{(f(\sigma))(f(\tau))^{\sigma}} \right)^2.
\]

Let us denote \( \chi_{\epsilon}(\sigma, \tau) = \frac{f(\sigma \tau)}{f(\sigma)^{\sigma} f(\tau)^{\tau}} \). The previous identity implies \( \chi_{\epsilon}(\sigma, \tau) = \pm 1 \). By substituting

\[
\psi(\tau, \epsilon)^{1-\sigma} = \Delta(\sigma, \psi(\tau, \epsilon)) \cdot (\delta(\sigma, \psi(\tau, \epsilon)) \cdot \varphi(\sigma, \psi(\tau, \epsilon)) \cdot \psi(\sigma, \psi(\tau, \epsilon)))^2
\]

to the identity \( \chi_{\epsilon}(\sigma, \tau) = \frac{f(\sigma \tau)f(\tau)^{\tau}}{f(\sigma)^{\sigma} f(\tau)^{\tau}} \) and using the facts that \( \varphi(\sigma, \epsilon) \) is a third root of unity and \( \psi(\sigma, \epsilon) \) belongs to a non-torsion group, we deduce that

\[
\chi_{\epsilon}(\sigma, \tau) = \delta(\sigma, \epsilon) \cdot \delta(\tau, \epsilon)^{-\sigma} \cdot \delta(\sigma, \epsilon)^{-1} \cdot \delta(\sigma, \psi(\tau, \epsilon))^2 \cdot \Delta(\sigma, \psi(\tau, \epsilon)).
\]

The conditions (C2) and (C5) imply \( \chi_{\epsilon}(\sigma, \sigma) = 1 \). Since the conditions (C3) and (C4) are satisfied we have \( \chi_{\epsilon}(\sigma, \tau) = \chi_{\epsilon}(\tau, \sigma) \). This identity states that \( f(\sigma)^\tau \cdot f(\tau) = f(\tau)^\sigma \cdot f(\sigma) \) for any \( \sigma, \tau \in G \). Hence for any \( \rho \in G \)

\[
\chi_{\epsilon}(\sigma \rho, \tau) \cdot \chi_{\epsilon}(\sigma, \rho) = \frac{f(\sigma \rho \tau)}{f(\sigma \rho)^{\sigma} f(\tau)^{\rho}} \cdot \frac{f(\sigma \rho)}{f(\sigma)^{\rho} f(\rho)} = \frac{f(\sigma \rho \tau)}{(f(\tau)^{\sigma} f(\sigma))^{\rho} f(\rho)} \cdot \frac{f(\sigma \rho)}{f(\rho)^{\rho}}
\]

\[
= \chi_{\epsilon}(\rho \tau, \sigma) \cdot \chi_{\epsilon}(\rho, \tau).
\]

Let us fix a basis \( \sigma_1, \ldots, \sigma_l \) of \( G \). So for any \( \sigma \in G \) there is a unique \( V(\sigma) \subseteq \{1, \ldots, n\} \) such that \( \sigma = \prod_{i \in V(\sigma)} \sigma_i \). We define the mapping \( g : G \to \{-1, 1\} \) by

\[
g(\sigma) = \prod_{i \in V(\sigma)} \chi_{\epsilon} \left( \prod_{j \in V(\sigma), j \prec i} \sigma_j, \sigma_i \right).
\]

Let us show that for any linear ordering \( \prec \) on \( \{\sigma_1, \ldots, \sigma_l\} \) we have

\[
g(\sigma) = \prod_{i \in V(\sigma)} \chi_{\epsilon} \left( \prod_{j \in V(\sigma), j \prec \sigma_i} \sigma_j, \sigma_i \right).
\]

Indeed, any linear ordering can be obtained from the initial ordering \( \sigma_1 \prec \cdots \prec \sigma_n \) by a finite number of interchanges of neighbors. If two orderings \( \prec \) and \( \ll \) differ just by the interchange of the couple of neighbors \( \sigma_i, \sigma_j \) (i.e. \( \sigma_i \prec \sigma_j \) but \( \sigma_i \ll \sigma_j \) and for all \( \{\sigma_k, \sigma_l\} \neq \{\sigma_i, \sigma_j\} \) we have \( \sigma_k \prec \sigma_l \) if and only if \( \sigma_k \ll \sigma_l \)) then the right-hand sides of (6) are different for \( \prec \) and \( \ll \) only if both \( i, j \in V(\sigma) \) in which case the corresponding products differ just in two factors: the former has factors \( \chi_{\epsilon}(\tau, \sigma_i) \cdot \chi_{\epsilon}(\tau \sigma_i, \sigma_j) \) while the latter has \( \chi_{\epsilon}(\tau, \sigma_j) \cdot \chi_{\epsilon}(\tau \sigma_j, \sigma_i) \), where

\[
\tau = \prod_{k \in V(\sigma), \sigma_k \ll \sigma_i} \sigma_k.\]
We shall show that for any $\sigma, \tau \in G$ we have
\[ \chi_\varepsilon(\sigma, \tau) = g(\sigma)g(\tau)g(\sigma \tau). \] (7)

We shall use the induction with respect to $|V_\tau|$. If $V_\tau = \emptyset$ then $\tau = 1$ and $\chi_\varepsilon(\sigma, 1) = 1 = g(\sigma)^2$. So let us assume that $|V_\tau| = m > 0$ and that the result has been proved for all $\tau$ with $|V_\tau| < m$. Let us choose $i \in V_\tau$ and write $\tau = \sigma_i \tau'$, so $|V'_\tau| = m - 1$. Using (5), the induction hypothesis for $\tau'$, $g(\sigma_i) = 1$ given by (6), we obtain
\[ \chi_\varepsilon(\sigma, \tau) = \chi_\varepsilon(\sigma, \sigma_i \tau') = \chi_\varepsilon(\sigma, \tau') \cdot \chi_\varepsilon(\sigma, \sigma_i)^2 \cdot \chi_\varepsilon(\sigma, \sigma_i) \]
\[ = g(\tau') \cdot g(\sigma \tau') \cdot g(\sigma \sigma_i) \cdot \chi_\varepsilon(\sigma, \sigma_i). \]

So we need to show that $g(\sigma) = g(\sigma \sigma_i) \cdot \chi_\varepsilon(\sigma, \sigma_i)$. On one hand, if $i \notin V_\sigma$ this easily follows from the definition of $g$. On the other hand, if $i \in V_\sigma$ then for $\sigma' = \sigma_i$, we have $V_{\sigma'} = V_\sigma - \{i\}$ and $g(\sigma) = g(\sigma') \cdot \chi_\varepsilon(\sigma_i, \sigma')$. Using (5) and $\chi_\varepsilon(\sigma_i, \sigma_i) = 1$ we have
\[ \chi_\varepsilon(\sigma, \sigma_i) = \chi_\varepsilon(\sigma', \sigma_i) = \chi_\varepsilon(\sigma', \sigma_i) \cdot \chi_\varepsilon(\sigma', \sigma_i)^2 \cdot \chi_\varepsilon(\sigma, \sigma_i) = \chi_\varepsilon(\sigma', \sigma_i). \]

The definition of $\chi_\varepsilon(\sigma, \tau)$ and (7) give that $fg$ is a crossed homomorphism and Proposition 2.3 gives that $\varepsilon$ or $2\varepsilon$ is a square in $K_J$. The proposition is proved. \qed

3. The index of $[C : D''']$

In this section we study the set $D'''$ of all units $\varepsilon \in C$ that satisfy all conditions (C1)–(C5) of Proposition 2.6. Our aim is to show that $D'''$ is a subgroup of $C$ and to compute its index.

Lemma 3.1. Let $\varepsilon \in C$ and let $\sigma, \tau \in G$. Then
\[ \langle \cdot, \tau \rangle_\varepsilon : G \rightarrow \{-1, 1\}, \]
\[ \langle \sigma, \cdot \rangle_\varepsilon : G \rightarrow \{-1, 1\} \]
are homomorphisms.

Proof. The first identity follows from Lemma 2.2. The identity $\varepsilon^{1-\rho \tau} = \varepsilon^{1-\rho} (\varepsilon^{1-\tau})^\rho$ gives that $\psi(\rho, \varepsilon)^{-2} \psi(\rho, \varepsilon)^2 \psi(\tau, \varepsilon)^{2\rho} \in W$. Then by substituting
\[ \psi(\tau, \varepsilon)^{1-\rho} = \Delta(\rho, \psi(\tau, \varepsilon))(\delta(\rho, \psi(\tau, \varepsilon) \cdot \varphi(\rho, \psi(\tau, \varepsilon)) \cdot \psi(\rho, \psi(\tau, \varepsilon)))^2 \]
to the latter identity we have
\[ \left(\frac{\psi(\rho, \varepsilon)^2 \psi(\tau, \varepsilon)}{\psi(\rho \tau, \varepsilon)}\right)^2 \cdot \psi(\rho, \psi(\tau, \varepsilon))^{-4} \in W. \]
Since the group generated by \( B \) has no torsion then
\[
\frac{\psi(\rho, \varepsilon) \psi(\tau, \varepsilon)}{\psi(\rho \tau, \varepsilon)} \cdot \psi(\rho, \psi(\tau, \varepsilon))^{-2} = 1
\]
and by applying \( \Delta(\sigma, \cdot)^2 \) to this relation, Lemma 2.1 gives the second identity.  

**Lemma 3.2.** Let us denote \( r_{\sigma, \tau}(\varepsilon) = \langle \sigma, \tau \rangle_\varepsilon \langle \tau, \sigma \rangle_\varepsilon \). Then
\[
\begin{align*}
r_{\sigma, \tau}(\varepsilon \eta) &= r_{\sigma, \tau}(\varepsilon) r_{\sigma, \tau}(\eta), \\
r_{\rho \sigma, \tau}(\varepsilon) &= r_{\rho, \tau}(\varepsilon) r_{\sigma, \tau}(\varepsilon), \\
r_{\rho, \sigma \tau}(\varepsilon) &= r_{\rho, \sigma}(\varepsilon) r_{\rho, \tau}(\varepsilon)
\end{align*}
\]
for all \( \sigma, \rho, \tau \in G \) and for all \( \varepsilon, \eta \in C \).

**Proof.** The first identity follows from Lemma 2.5. The second and the third ones are easy corollaries of Lemma 3.1.

Let us now define a subgroup of the group of circular units \( C \). Recall that Lemmas 2.1, 2.5 and 3.2 state that \( \Delta(\sigma, \cdot)^2, \langle \sigma, \sigma \rangle, r_{\sigma, \tau}(\cdot) \) are homomorphisms \( C \to \{-1, 1\} \).

**Definition 3.3.** Let \( D \) be the intersection of the kernels of the following homomorphisms \( C \to \{-1, 1\} : \Delta(\sigma, \cdot)^2, \langle \sigma, \sigma \rangle, \) for all \( \sigma \in G \) and \( r_{\sigma, \tau}(\cdot) \) for all \( \sigma, \tau \in G \).

**Remark 3.4.** Notice that \( D \) is the subgroup of all units in \( C \) satisfying the conditions (C1)–(C3) of Proposition 2.6.

**Lemma 3.5.** Let \( 2^l = [k : \mathbb{Q}] \). Then
\[
[C : D] = 2^a,
\]
where \( a \leq 2l + \left(\frac{d}{2}\right) - 1 \) if \( \sqrt{-1} \in k \), \( a \leq l + \left(\frac{d}{2}\right) - 1 \) if \( \sqrt{-1} \notin k \) and \( k \) is imaginary, and \( a \leq l + \left(\frac{d}{2}\right) \) if \( k \) is real.

**Proof.** Let \( \tau_1, \ldots, \tau_l \in G \) be such that their restrictions to \( k \) are generators of \( \text{Gal}(k/\mathbb{Q}) \). If the restrictions of \( \sigma, \tau \in G \) to \( k \) coincide then \( \Delta(\sigma, \varepsilon) = \Delta(\tau, \varepsilon) \) and \( \psi(\sigma, \varepsilon) = \psi(\tau, \varepsilon) \) for any \( \varepsilon \in C \). So \( D \) is the intersection of the kernels \( \Delta(\sigma, \cdot)^2, \langle \sigma, \sigma \rangle, \) and \( r_{\sigma, \tau}(\cdot) \), where \( \sigma, \tau \) runs over the subgroup of \( G \) generated by \( \tau_1, \ldots, \tau_l \). Moreover, using Lemmas 2.2, 3.1 and 3.2 we obtain that \( D \) is the intersection of the kernels of \( \Delta(\tau_i, \cdot)^2, \langle \tau_i, \tau_j \rangle \). for \( 1 \leq i \leq l \) and \( r_{\tau_i, \tau_j}(\cdot) \), for \( 1 \leq i < j \leq l \). If \( \sqrt{-1} \notin k \) then \( \Delta(\tau_i, \cdot) = 1 \). The lemma follows from observation that if \( k \) is imaginary and \( \tau_1 \) is the complex conjugation then \( \psi(\tau_1, \varepsilon) = 1 \) and so \( \langle \tau_1, \tau_1 \rangle_\varepsilon = 1 \) for all \( \varepsilon \in C \).  

**Lemma 3.6.** Let us denote
\[
s_{\sigma, \tau}(\varepsilon) = \delta(\tau, \varepsilon)^{\sigma^{-1}} \cdot \delta(\sigma, \psi(\tau, \varepsilon))^2 \cdot \delta(\sigma, \varepsilon)^{\tau^{-1}} \cdot \delta(\tau, \psi(\sigma, \varepsilon))^2.
\]
Then

\[
\begin{align*}
    s_{\sigma, \tau}(\varepsilon \eta) &= s_{\sigma, \tau}(\varepsilon)s_{\sigma, \tau}(\eta), \\
    s_{\rho, \sigma, \tau}(\varepsilon) &= s_{\rho, \tau}(\varepsilon)s_{\sigma, \tau}(\varepsilon), \\
    s_{\rho, \sigma \tau}(\varepsilon) &= s_{\rho, \sigma}(\varepsilon)s_{\rho, \tau}(\varepsilon)
\end{align*}
\]

for any \(\sigma, \tau, \rho \in G\) and \(\varepsilon, \eta \in D\).

**Proof.** It is easy to see that

\[
\delta(\sigma, \varepsilon)^{t^{-1}} = \begin{cases} 
\delta(\sigma, \varepsilon)^2 & \text{if } i^t = -i, \\
1 & \text{otherwise.}
\end{cases}
\]

We deduce from the relation \((\varepsilon \eta)^{1-\sigma} = \varepsilon^{1-\sigma} \eta^{1-\sigma}\) that

\[
\Delta(\sigma, \varepsilon \eta)\delta(\sigma, \varepsilon \eta)^2 = \Delta(\sigma, \varepsilon)\delta(\sigma, \varepsilon)^2 \Delta(\sigma, \eta)\delta(\sigma, \eta)^2.
\]

Since \(\Delta(\sigma, \varepsilon) = 1\) for all \(\varepsilon \in D\) then \(\delta(\sigma, \varepsilon \eta)^2 = \delta(\sigma, \varepsilon)^2 \delta(\sigma, \eta)^2\), hence \(\delta(\sigma, \varepsilon \eta)^{1-\tau} = \delta(\sigma, \varepsilon)^{1-\tau} \delta(\sigma, \eta)^{1-\tau}\). Interchanging \(\sigma\) and \(\tau\) gives \(\delta(\tau, \varepsilon \eta)^{1-\sigma} = \delta(\tau, \varepsilon)^{1-\sigma} \delta(\tau, \eta)^{1-\sigma}\).

Moreover, Lemma 2.1 states that \(\psi(\tau, \varepsilon \eta)^{1-\sigma} = \psi(\tau, \varepsilon)^{1-\sigma} \psi(\tau, \eta)^{1-\sigma}\) and consequently we deduce from this relation that

\[
\Delta(\sigma, \psi(\tau, \varepsilon \eta))\delta(\sigma, \psi(\tau, \varepsilon \eta))^2 \\
= \Delta(\sigma, \psi(\tau, \varepsilon))\delta(\sigma, \psi(\tau, \varepsilon))^2 \Delta(\sigma, \psi(\tau, \eta)) \cdot \delta(\sigma, \psi(\tau, \eta))^2.
\]

Similarly, interchanging \(\sigma\) and \(\tau\),

\[
\Delta(\tau, \psi(\sigma, \varepsilon \eta))\delta(\tau, \psi(\sigma, \varepsilon \eta))^2 \\
= \Delta(\tau, \psi(\sigma, \varepsilon))\delta(\tau, \psi(\sigma, \varepsilon))^2 \Delta(\tau, \psi(\sigma, \eta)) \cdot \delta(\tau, \psi(\sigma, \eta))^2.
\]

Since \(\varepsilon \in D\) we have \(r_{\sigma, \tau}(\varepsilon) = 1\) which means

\[
\Delta(\sigma, \psi(\tau, \varepsilon)) = \Delta(\tau, \psi(\sigma, \varepsilon)).
\]

Similarly \(\eta \in D\) gives

\[
\Delta(\sigma, \psi(\tau, \eta)) = \Delta(\tau, \psi(\sigma, \eta))
\]

and \(\varepsilon \eta \in D\) gives

\[
\Delta(\sigma, \psi(\tau, \varepsilon \eta)) = \Delta(\tau, \psi(\sigma, \varepsilon \eta)).
\]

Putting things together we obtain

\[
\frac{\delta(\sigma, \psi(\tau, \varepsilon \eta))^2}{\delta(\tau, \psi(\sigma, \varepsilon \eta))^2} = \frac{\delta(\sigma, \psi(\tau, \varepsilon))^2}{\delta(\tau, \psi(\sigma, \varepsilon))^2} \cdot \frac{\delta(\sigma, \psi(\tau, \eta))^2}{\delta(\tau, \psi(\sigma, \eta))^2}.
\]
The first identity follows.
Since \( \sigma \rho - 1 = \sigma - 1 + (\rho - 1)\sigma \) then
\[
\delta(\tau, \varepsilon)^{\sigma \rho - 1} = \delta(\tau, \varepsilon)^{\sigma - 1}\delta(\tau, \varepsilon)^{\rho - 1}. \tag{i}
\]
Further, we use the identity
\[
1 = \frac{\varepsilon^{1, \sigma} \cdot (\varepsilon^{1-\rho})^{(\sigma - 1)} \cdot \varepsilon^{1-\rho}}{\varepsilon^{1-\sigma \rho}}. \tag{8}
\]
At first, we express
\[
(\varepsilon^{1-\rho})^{(\sigma - 1)} = \Delta(\rho, \varepsilon)^{\sigma - 1} \cdot \varphi(\rho, \varepsilon)^{2(\sigma - 1)} \cdot \psi(\rho, \varepsilon)^{2(\sigma - 1)}
\]
and consequently we substitute \( \psi(\rho, \varepsilon)^{2(1-\sigma)} \) in the relation (8) by the identity
\[
(\psi(\rho, \varepsilon)^{1-\sigma})^2 = (\Delta(\sigma, \psi(\rho, \varepsilon)) \cdot (\varphi(\sigma, \psi(\rho, \varepsilon)) \cdot \psi(\sigma, \psi(\rho, \varepsilon)))^2)^2. \tag{9}
\]
Since \( \psi(\cdot, \cdot) \) is a third root of unity, \( \Delta(\sigma, \varepsilon) = \Delta(\rho, \varepsilon) = \Delta(\sigma \rho, \varepsilon) = 1 \) as \( \varepsilon \in D \), and \( \psi(\cdot, \cdot) \) belongs to the non-torsion group then we obtain from (8) the identity
\[
\delta(\sigma \rho, \varepsilon)^2 = \delta(\sigma, \varepsilon)^2 \delta(\rho, \varepsilon)^2 \Delta(\sigma, \psi(\rho, \varepsilon))^2. \tag{9}
\]
In both cases, independently whether \( i^\tau = -i \) or \( i^\tau = i \), this gives
\[
\delta(\sigma \rho, \varepsilon)^{\tau - 1} = \delta(\sigma, \varepsilon)^{\tau - 1} \delta(\rho, \varepsilon)^{\tau - 1} \Delta(\sigma, \psi(\rho, \varepsilon))^{\tau - 1}. \tag{ii}
\]
By putting \( \psi(\tau, \varepsilon) \) instead of \( \varepsilon \) in the relation (8) we obtain the identity
\[
1 = \frac{\psi(\tau, \varepsilon)^{1-\sigma} \cdot (\psi(\tau, \varepsilon)^{1-\rho})^{(\sigma - 1)} \cdot \psi(\tau, \varepsilon)^{1-\rho}}{\psi(\tau, \varepsilon)^{1-\sigma \rho}}. \tag{10}
\]
As before, we express
\[
(\psi(\tau, \varepsilon)^{1-\rho})^{(\sigma - 1)} = \Delta(\rho, \psi(\tau, \varepsilon))^{\sigma - 1} \cdot \varphi(\rho, \psi(\tau, \varepsilon))^{2(\sigma - 1)} \cdot \psi(\rho, \psi(\tau, \varepsilon))^{2(\sigma - 1)}.
\]
Hence, substituting
\[
(\psi(\rho, \psi(\tau, \varepsilon))^{1-\sigma})^2 = \Delta(\sigma, \psi(\rho, \psi(\tau, \varepsilon)))^2 \cdot \varphi(\sigma, \psi(\rho, \psi(\tau, \varepsilon)))^4 \cdot \psi(\sigma, \psi(\rho, \psi(\tau, \varepsilon)))^4
\]
to the identity (10) similarly as in previous case we obtain
\[
\delta(\sigma \rho, \psi(\tau, \varepsilon))^2 = \delta(\sigma, \psi(\tau, \varepsilon))^2 \delta(\rho, \psi(\tau, \varepsilon))^2 \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^{\sigma - 1} \cdot \frac{\Delta(\sigma, \psi(\tau, \varepsilon)) \Delta(\rho, \psi(\tau, \varepsilon))}{\Delta(\sigma \rho, \psi(\tau, \varepsilon))} \cdot \Delta(\sigma, \psi(\rho, \psi(\tau, \varepsilon)))^2. \tag{iii}
\]
Finally, we express \( \psi(\sigma, \psi(\rho, \varepsilon)) \) and \( \psi(\cdot, \varepsilon) \) in the relation
\[
\left( \frac{\psi(\sigma, \varepsilon)\psi(\rho, \varepsilon)}{\psi(\sigma \rho, \varepsilon)} \right)^{1-\tau} = \psi(\sigma, \psi(\rho, \varepsilon))^{2(1-\tau)}
\]
which was obtained in the proof of Lemma 2.2. Since again \( \psi(\cdot, \cdot) \) belongs to the non-torsion group and \( \psi(\cdot, \cdot) \) is a third root of unity then we have
\[
\delta(\tau, \psi(\sigma, \varepsilon)) = \delta(\tau, \psi(\rho, \varepsilon))^{2(1-\tau)} \cdot \delta(\tau, \psi(\sigma, \psi(\rho, \varepsilon)))^2.
\]
(iv)

At first, expressing the relation \( \psi(\rho, \varepsilon)^{(1-\tau)(\sigma-1)} = \psi(\rho, \varepsilon)^{1-\sigma(\tau-1)} \) as before we deduce that
\[
\frac{\Delta(\tau, \psi(\sigma, \varepsilon)) \Delta(\tau, \psi(\rho, \varepsilon))}{\Delta(\tau, \psi(\sigma \rho, \varepsilon))} = 1.
\]
Since \( \Delta(\tau, \psi(\rho, \varepsilon))^\sigma = \Delta(\tau, \psi(\sigma, \rho, \varepsilon))^{-\sigma} \) as \( \varepsilon \in D \), we obtain that the identity (11) is equivalent to
\[
\Delta(\sigma, \psi(\tau, \psi(\rho, \varepsilon))) \Delta(\sigma, \psi(\rho, \psi(\tau, \varepsilon)))^{-2} = 1.
\]
Hence, using the relation \( \varepsilon^{(1-\rho)(1-\tau)} = \varepsilon^{(1-\tau)(1-\rho)} \) it is easy to see that \( \psi(\tau, \psi(\rho, \varepsilon)) = \psi(\rho, \psi(\tau, \varepsilon)) \) which gives exactly what we need. The second identity of the lemma follows. The third one is a consequence of the second one using the symmetry \( s_{\sigma, \tau}(\varepsilon) = s_{\tau, \sigma}(\varepsilon) \).

Now we need to define another subgroup of \( C \). Recall that Lemma 3.6 states that \( s_{\sigma, \tau}(\cdot) \) is a homomorphism \( D \to \{-1, 1\} \) for each \( \sigma, \tau \in G \).

**Definition 3.7.** Let \( D' \) be the intersection of the kernels of the homomorphisms \( s_{\sigma, \tau}(\cdot) : D \to \{-1, 1\} \) for all \( \sigma, \tau \in G \).

**Remark 3.8.** Notice that \( D' \) is the subgroup of all units in \( C \) satisfying the conditions (C1)–(C4) of Proposition 2.6.

**Lemma 3.9.** Let \( 2^l = [k : \mathbb{Q}] \). Then
\[
[D : D'] = 2^b,
\]
where \( b \leq \left( \frac{l}{2} \right) \) if \( \sqrt{-1} \in k \) and \( b \leq \left( \frac{l+1}{2} \right) \) otherwise.
Proof. If the restrictions of \( \sigma, \tau \in G \) to \( k(i) \) coincide then \( s_{\sigma, \rho}(\varepsilon) = s_{\tau, \rho}(\varepsilon) \) for any \( \rho \in G \) and \( \varepsilon \in D \). Let \( \tau_1, \ldots, \tau_m \in G \) be such that their restrictions to \( k(i) \) form a basis of \( \Gal(k(i)/Q) \). Lemma 3.6 implies that \( D' \) is the intersection of the kernels of \( s_{\tau_i, \tau_j}(\cdot) \) for \( 1 \leq i < j \leq m \). The lemma follows. \( \square \)

Lemma 3.10. Let us denote \( t_{\sigma}(\varepsilon) = \delta(\sigma, \varepsilon)^{\sigma+1} \delta(\sigma, \psi(\sigma, \varepsilon))^2 \). Then

\[
t_{\sigma}(\varepsilon \eta) = t_{\sigma}(\varepsilon) t_{\sigma}(\eta),
\]

\[
t_{\sigma \tau}(\varepsilon) = t_{\sigma}(\varepsilon) t_{\tau}(\varepsilon)
\]

for all \( \varepsilon, \eta \in D' \) and for all \( \sigma, \tau \in G \).

Proof. It follows easily that

\[
\delta(\sigma, \varepsilon)^{1+\sigma} = \begin{cases} 
\delta(\sigma, \varepsilon)^2 & \text{if } i^{\sigma} = i, \\
1 & \text{otherwise}.
\end{cases}
\]

The relation \((\varepsilon \eta)^{1-\sigma} = \varepsilon^{1-\sigma} \eta^{1-\sigma}\) gives that \( \Delta(\sigma, \cdot) \delta(\sigma, \cdot)^2 \) is a homomorphism for all \( \varepsilon, \eta \in C \). Therefore using the definition of \( D \) (namely the condition (C1) of Proposition 2.6) we have \( \delta(\sigma, \cdot)^2 : D \to \{-1, 1\} \) is a homomorphism for any \( \sigma \in G \). Similarly, the identity \( \psi(\sigma, \varepsilon \eta)^{1-\sigma} = \psi(\sigma, \varepsilon)^{1-\sigma} \psi(\sigma, \eta)^{1-\sigma} \) (see Lemma 2.1) states that \( \Delta(\sigma, \psi(\sigma, \cdot))^2 : C \to \{-1, 1\} \) is a homomorphism for any \( \sigma \in G \). Hence, the definition of \( D \) (namely the condition (C2) of Proposition 2.6) gives that \( \delta(\sigma, \psi(\sigma, \cdot))^2 : D \to \{-1, 1\} \) is a homomorphism for any \( \sigma \in G \). The first identity follows.

Since \( \sigma \tau + 1 = (\sigma + 1) \tau + (\tau + 1)(-1) + 2 \) then

\[
\delta(\sigma \tau, \varepsilon)^{\sigma \tau+1} = \delta(\sigma, \varepsilon)^{\sigma+1} \cdot \delta(\sigma, \varepsilon)^{\tau+1} \cdot \delta(\sigma \tau, \varepsilon)^2. \tag{12}
\]

Moreover, for \( \rho = \sigma \) or \( \rho = \tau \) independently whether \( i^\rho = -i \) or \( i^\rho = i \), the identity \( \delta(\sigma \tau, \varepsilon)^2 = \delta(\sigma, \varepsilon)^2 \delta(\tau, \varepsilon)^2 \Delta(\sigma, \psi(\tau, \varepsilon))^2 \) obtained in the proof of Lemma 3.6 (see the identity (9)), gives that

\[
\delta(\sigma \tau, \varepsilon)^{\rho+1} = \delta(\sigma, \varepsilon)^{\rho+1} \delta(\tau, \varepsilon)^{\rho+1} \Delta(\sigma, \psi(\tau, \varepsilon))^\rho+1. \tag{13}
\]

Therefore, putting (12) and (13) together we obtain

\[
\delta(\sigma \tau, \varepsilon)^{\sigma \tau+1} = \delta(\sigma, \varepsilon)^{\sigma+1} \cdot \delta(\tau, \varepsilon)^{\tau+1} \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^\sigma+1 \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^\tau+1 \cdot \delta(\tau, \varepsilon)^2 \cdot \delta(\sigma, \varepsilon)^2 \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^2. \tag{14}
\]

Since \( \Delta(\sigma, \psi(\tau, \varepsilon))^2 = \Delta(\sigma, \psi(\tau, \varepsilon))^{-2} \) and since \( \delta(\sigma, \varepsilon)^2 = \delta(\sigma, \varepsilon)^{-2} \) we have

\[
\delta(\sigma \tau, \varepsilon)^{\sigma \tau+1} = \delta(\sigma, \varepsilon)^{\sigma+1} \cdot \delta(\tau, \varepsilon)^{\tau+1} \cdot \delta(\sigma, \varepsilon)^{-1} \cdot \delta(\tau, \varepsilon)^{-1} \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^{\sigma-1} \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^{\tau+1}. \tag{15}
\]

Now we use the identity (iv) obtained in the proof of Lemma 3.6. Hence, changing \( \rho \) to \( \tau \) and \( \tau \) to \( \sigma \tau \) we obtain
\[ \delta(\sigma \tau, \psi(\sigma \tau, \varepsilon))^2 = \delta(\sigma, \psi(\sigma, \varepsilon))^2 \cdot \delta(\tau, \psi(\tau, \varepsilon))^2 \cdot \Delta(\sigma \tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 \]
\[ \cdot \frac{\Delta(\sigma \tau, \psi(\sigma, \varepsilon)) \Delta(\sigma \tau, \psi(\tau, \varepsilon))}{\Delta(\sigma \tau, \psi(\sigma \tau, \varepsilon))}. \] \quad (16)\]

Further, we substitute \( \delta(\sigma \tau, \psi(\sigma, \varepsilon))^2 \) and \( \delta(\sigma \tau, \psi(\tau, \varepsilon))^2 \) in this relation by the identity (iii) obtained in the proof of Lemma 3.6 where we change \( \rho \) to \( \tau \) (and eventually \( \tau \) to \( \sigma \)). Then the condition (C2) of Proposition 2.6 gives
\[ \delta(\sigma \tau, \psi(\sigma \tau, \varepsilon))^2 = \delta(\sigma, \psi(\sigma, \psi(\tau, \varepsilon)))^2 \cdot \delta(\tau, \psi(\tau, \varepsilon))^2 \cdot \Delta(\sigma \tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 \cdot \Delta(\sigma \tau, \psi(\sigma \tau, \varepsilon))^2 \cdot \Delta(\sigma, \psi(\tau, \psi(\sigma, \varepsilon)))^2 \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^2. \] \quad (17)\]

If we use the condition (C3) of Proposition 2.6 and the identity
\[ s_{\sigma, \tau}(\varepsilon) = \delta(\tau, \varepsilon)^{\sigma-1} \cdot \delta(\sigma, \psi(\tau, \varepsilon))^2 \cdot \delta(\varepsilon, \sigma)^{\tau-1} \cdot \delta(\tau, \psi(\sigma, \varepsilon))^2 = 1, \]
resulting from the definition of \( D' \), then multiplying (15) and (17) we obtain
\[ t_{\sigma \tau}(\varepsilon) = t_{\sigma}(\varepsilon) \cdot t_{\tau}(\varepsilon) \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^{\sigma-1} \cdot \Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1} \cdot \Delta(\sigma, \psi(\tau, \psi(\sigma, \varepsilon)))^2 \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^2. \] \quad (18)\]

It follows from Lemma 2.2 that
\[ \Delta(\sigma \tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = \Delta(\sigma, \psi(\sigma, \psi(\tau, \varepsilon)))^2 \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2. \]

Hence, we have to show that
\[ \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^{\sigma-1} \cdot \Delta(\sigma, \psi(\tau, \psi(\sigma, \varepsilon)))^{\tau-1} \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^2 \cdot \Delta(\sigma, \psi(\tau, \psi(\sigma, \varepsilon)))^2 = 1. \]

Similarly as in the proof of Lemma 3.6 we deduce easily from the relation \( \varepsilon^{(1-\sigma)(1-\tau)} = \varepsilon^{(1-\tau)(1-\sigma)} \) that
\[ \psi(\tau, \psi(\sigma, \varepsilon)) = \psi(\sigma, \psi(\tau, \varepsilon)) \]
and so we have
\[ \Delta(\sigma, \psi(\tau, \psi(\sigma, \varepsilon)))^2 \cdot \Delta(\sigma, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1. \]
Further, it is easy to see that $\Delta(\sigma, \psi(\tau, \varepsilon))^{\tau-1} \cdot \Delta(\sigma, \psi(\tau, \varepsilon))^{-2} \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1$ and we only need to show that

$$\Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1} \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^{-2} \cdot \Delta(\sigma, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1.$$ 

The relation $\psi(\tau, \varepsilon)(1-\tau)(1-\sigma) = \psi(\tau, \varepsilon)(1-\sigma)(1-\tau)$ implies that

$$\Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1} \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^{-2} \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1.$$ 

At first, we express

$$\psi(\tau, \psi(\tau, \varepsilon))^{2(1-\sigma)} = \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^2 \cdot \varphi(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^4 \cdot \psi(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^4.$$ 

Similarly we have

$$\psi(\sigma, \psi(\tau, \varepsilon))^{2(1-\tau)} = \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 \cdot \varphi(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^4 \cdot \psi(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^4.$$ 

Putting things together and using that $\varphi(\cdot, \cdot)$ is a third root of unity and $\psi(\cdot, \cdot)$ belongs to the non-torsion group generated by $B$ we obtain

$$\frac{\Delta(\tau, \psi(\tau, \varepsilon))^{1-\sigma} \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^2}{\Delta(\sigma, \psi(\tau, \varepsilon))^{1-\tau} \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2} = 1.$$ 

Recall that $\Delta(\tau, \psi(\tau, \varepsilon)) = 1$. Hence, the identity $\Delta(\sigma, \psi(\tau, \varepsilon))^{1-\tau} = \Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1}$ gives

$$\Delta(\tau, \psi(\sigma, \varepsilon))^{\tau-1} \cdot \Delta(\sigma, \psi(\tau, \psi(\tau, \varepsilon)))^{-2} \cdot \Delta(\tau, \psi(\sigma, \psi(\tau, \varepsilon)))^2 = 1.$$ 

The lemma follows immediately. \(\square\)

Now we define another subgroup of $C$. Recall that Lemma 3.10 states that $t_{\sigma}(\cdot)$ is a homomorphism $D' \to \{-1, 1\}$ for every $\sigma \in G$.

**Definition 3.11.** Let $D''$ be the intersection of the kernels of the homomorphisms $t_{\sigma}(\cdot): D' \to \{-1, 1\}$ for all $\sigma \in G$.

**Remark 3.12.** Notice that $D''$ is the subgroup of all units in $C$ satisfying all conditions of Proposition 2.6, in other words $D'' = C \cap (K_J^2 \cup 2K_J^2)$.

**Lemma 3.13.** Let $2^l = [k : \mathbb{Q}]$. Then

$$[D' : D''] = 2^c,$$

where $c \leq l - 1$ if $\sqrt{-1} \in k$, $c \leq l$ if $\sqrt{-1} \notin k$ and $k$ is imaginary, and $c \leq l + 1$ if $k$ is real.
Proof. This follows from Lemma 3.10 similarly as Lemmas 3.5 and 3.9 using the observation that if \( k \) is imaginary and \( \tau_1 \) is the complex conjugation then \( t_{\tau_1}(\varepsilon) = 1 \) for all \( \varepsilon \in C \). \( \square \)

4. The divisibility of \([E : C]\) by a power of 2

In this section we introduce the main results of this text.

Lemma 4.1. Let \( \varepsilon \in C \). If there is \( \gamma \in K_J \) such that \( \varepsilon = \gamma^2 \) or \( \varepsilon = 2\gamma^2 \), then \( \xi_{\varepsilon} \) defined by \( \xi_{\varepsilon}(\sigma) = \gamma^{1-\sigma} \) is a character on \( \text{Gal}(K_J / k) \), i.e., \( \xi_{\varepsilon}: \text{Gal}(K_J / k) \to \{ -1, 1 \} \) is a homomorphism, and \( \gamma \in k \) if and only if \( \xi_{\varepsilon} \) is the principal character. Moreover,

\[
\tilde{\xi}: C \cap (K_J^2 \cup 2K_J^2) \to \hat{\text{Gal}}(K_J / k),
\]

where \( \tilde{\xi}(\varepsilon) = \xi_{\varepsilon} \), is a homomorphism, i.e., \( \xi_{\varepsilon\eta}(\sigma) = \xi_{\varepsilon}(\sigma)\xi_{\eta}(\sigma) \) for all \( \varepsilon, \eta \in C \cap (K_J^2 \cup 2K_J^2) \) and for any \( \sigma \in G \).

Proof. The lemma follows immediately from \( 1 - \sigma \tau = (1 - \sigma) + (1 - \tau)\sigma \). \( \square \)

Theorem 4.2. Let \( n = \#J \) and \( 2^l = [k : \mathbb{Q}] \).

(i) If \( k \) is real then

\[
2^{2l-n-l^2-l-3} \mid [E : C].
\]

(ii) If \( k \) is imaginary and \( \sqrt{-1} \notin k \) then

\[
2^{2l-1-n-l^2-l-1} \mid [E : C].
\]

(iii) If \( \sqrt{-1} \in k \) then

\[
2^{2l-1-n-l^2-l} \mid [E : C].
\]

Proof. Let \( D''' = C \cap (k^2 \cup 2k^2) \), i.e. \( D''' \) consists of all \( \varepsilon \in C \) of the form \( \varepsilon = \eta^2 \) or \( \varepsilon = 2\eta^2 \) for a suitable \( \eta \in k \). Recall that from Lemma 4.1 and the definitions of \( D'' \) and \( D''' \) it follows that \( [D'' : D'''] = 2^d \), where \( d \leq n - l \). Moreover, using Lemmas 3.5, 3.9 and 3.13 we know that \( [C : D'''] = [C : D] \cdot [D : D'] \cdot [D' : D''] \cdot [D'' : D'''] = 2^{a+b+c+d} \), where

\[
a + b + c + d \leq \begin{cases} 
l^2 + n + l + 1 & \text{if } k \text{ is real}, \\
l^2 + n + l - 1 & \text{if } k \text{ is imaginary and } \sqrt{-1} \notin k, \\
l^2 + n + l - 2 & \text{if } \sqrt{-1} \in k.
\end{cases}
\]

From the definition of \( E \) and \( D''' \) we know that rank \( E = \text{rank } D''' \). Each unit in \( D''' \) is of the form \( \eta^2 \) or \( 2\eta^2 \) for a suitable \( \eta \in k \). Since \( (2\eta^2) \cdot (2\theta^2) = (2\eta\theta)^2 \) is again a square, there is a basis of \( D''' \) where all elements but at most one are squares. Therefore we have \( 2^{2l-2} \mid [E : D'''] \) if \( k \) is real and \( 2^{2l-1-2} \mid [E : D'''] \) if \( k \) is imaginary. The theorem follows using \( [E : C] = \frac{[E : D''']}{[C : D''']} \). \( \square \)
Putting together Proposition 1.4 and Theorem 4.2 we obtain a lower bound for the divisibility of the class number $h^+$ by a power of 2. A very explicit special case of this result is given by the following example.

**Example 4.3.** Let us denote $n = \# J$. Let us suppose $k = K, J$ and $\# \{ p \in J; \ p < 0 \} > 1$. Then

$$[E : C] = 2^{2n-2} - n \cdot Q h^+, $$
which can be obtained in the same way as in [1] (see Theorem 1 and Remark below its proof). Then Theorem 4.2 gives

$$2^{2n-1} - 2n - n^2 \mid [E : C]$$
and consequently

$$2^{2n-2} - n^2 - 1 \mid h^+ $$
because $Q \mid 2$.

**Acknowledgment**

The author would like to thank Radan Kučera for useful discussions and many remarks which improved this text.

**References**
