Journal of Number Theory 131 (2011) 1824–1826

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Remark on Polický's paper on circular units of a compositum of quadratic number fields

Akira Endô

Department of Mathematics, Kumamoto University, Kumamoto 860-8555, Japan

ARTICLE INFO

Article history:
Received 4 October 2010
Revised 25 December 2010
Accepted 15 March 2011
Available online 19 May 2011
Communicated by David Goss

MSC:
11R20
11R27

Keywords:
Compositum of quadratic number fields
Circular units

ABSTRACT

Remark on Polický's paper on circular units of a compositum of quadratic number fields is given.

Let k be a compositum of a finite number of quadratic number fields and K the genus field of k in the narrow sense, and assume that $i \in K$ and $\sqrt{2} \notin K$. Polický [1] defined a group C of circular units of k and computed a lower bound for the divisibility of the index of C in the full unit group E of k by a power of 2.

In this short note we show that in Proposition 2.6 of Polický [1], which gives a necessary and sufficient condition for that ϵ or 2ϵ is a square in K for $\epsilon \in C$, the condition $(C1)$ implies the conditions $(C2)$ and $(C3)$.

Denoting $G = Gal(K/Q)$, Q the field of rational numbers, for $\epsilon \in C$ and $\sigma \in G$ we have

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

E-mail address: endou@sci.kumamoto-u.ac.jp.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.03.009

where $\Delta(\sigma,\epsilon), \delta(\sigma,\epsilon) \in \{1, i\}$, $\varphi(\sigma,\epsilon) \in \{1, \zeta_3, \zeta_3^2\}$, $\zeta_3 = e^{2\pi i/3}$, $\Delta(\sigma,\epsilon)$, $\varphi(\sigma,\epsilon) \in k$ and $\psi(\sigma,\epsilon)$ belongs to a non-torsion subgroup of C. The condition $(C1)$ says that $\Delta(\sigma,\epsilon)^2 = \Delta(\sigma,\epsilon) = 1$ for all $\sigma \in G$.

Under the condition $(C1)$ we have

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

for all $\sigma \in G$. Since $\epsilon^{2(1-\sigma)} = \epsilon^{(1-\sigma)^2}$, it follows that

$$\begin{aligned}\varphi(\sigma,\epsilon)^4\psi(\sigma,\epsilon)^4 &= \delta(\sigma,\epsilon)^{2(1-\sigma)}\varphi(\sigma,\epsilon)^{2(1-\sigma)}\psi(\sigma,\epsilon)^{2(1-\sigma)}\\ &= \varphi(\sigma,\epsilon)^{2(1-\sigma)}\Delta\bigl(\sigma,\psi(\sigma,\epsilon)\bigr)^2\bigl(\delta\bigl(\sigma,\psi(\sigma,\epsilon)\bigr)\varphi\bigl(\sigma,\psi(\sigma,\epsilon)\bigr)\psi\bigl(\sigma,\psi(\sigma,\epsilon)\bigr)\bigr)^4\\ &= \Delta\bigl(\sigma,\psi(\sigma,\epsilon)\bigr)^2\varphi(\sigma,\epsilon)^{2(1-\sigma)}\varphi\bigl(\sigma,\psi(\sigma,\epsilon)\bigr)^4\psi\bigl(\sigma,\psi(\sigma,\epsilon)\bigr)^4,\end{aligned}$$

which implies

$$\Delta\bigl(\sigma,\psi(\sigma,\epsilon)\bigr)^2 = 1,$$

because $\Delta(\sigma,\psi(\sigma,\epsilon))^2$ is a forth power of an element of K and $\sqrt[4]{-1} \notin K$; thus the condition $(C2)$ holds. Similarly, for all $\sigma,\tau \in G$, it also follows from the identity $\epsilon^{(1-\sigma)(1-\tau)} = \epsilon^{(1-\tau)(1-\sigma)}$ that

$$\begin{aligned}&\frac{\delta(\sigma,\epsilon)^{2(1-\tau)}\varphi(\sigma,\epsilon)^{2(1-\tau)}\psi(\sigma,\epsilon)^{2(1-\tau)}}{\delta(\tau,\epsilon)^{2(1-\sigma)}\varphi(\tau,\epsilon)^{2(1-\sigma)}\psi(\tau,\epsilon)^{2(1-\sigma)}}\\ &\quad= \frac{\varphi(\sigma,\epsilon)^{2(1-\tau)}\Delta(\tau,\psi(\sigma,\epsilon))^2(\delta(\tau,\psi(\sigma,\epsilon))\varphi(\tau,\psi(\sigma,\epsilon))\psi(\tau,\psi(\sigma,\epsilon)))^4}{\varphi(\tau,\epsilon)^{2(1-\sigma)}\Delta(\sigma,\psi(\tau,\epsilon))^2(\delta(\sigma,\psi(\tau,\epsilon))\varphi(\sigma,\psi(\tau,\epsilon))\psi(\sigma,\psi(\tau,\epsilon)))^4}\\ &\quad= \frac{\Delta(\tau,\psi(\sigma,\epsilon))^2\varphi(\sigma,\epsilon)^{2(1-\tau)}\varphi(\tau,\psi(\sigma,\epsilon))^4\psi(\tau,\psi(\sigma,\epsilon))^4}{\Delta(\sigma,\psi(\tau,\epsilon))^2\varphi(\tau,\epsilon)^{2(1-\sigma)}\varphi(\sigma,\psi(\tau,\epsilon))^4\psi(\sigma,\psi(\tau,\epsilon))^4}\\ &\quad= 1,\end{aligned}$$

which implies

$$\Delta\bigl(\tau,\psi(\sigma,\epsilon)\bigr)^2 = \Delta\bigl(\sigma,\psi(\tau,\epsilon)\bigr)^2,$$

namely the condition $(C3)$ holds.

Let D be a subgroup of C consisting of $\epsilon \in C$ which satisfies $\Delta(\sigma,\epsilon)^2 = 1$ for all $\sigma \in G$. Let $[k:Q] = 2^l$. The Lemma 3.5 of [1] is rewritten as follows:

$$(C:D) = 2^a,$$

where $a \leqslant l$ if $i \in k$, and $a = 0$ if $i \notin k$.

Let D' be a subgroup of D consisting of $\epsilon \in D$ which satisfies $\delta(\sigma,\epsilon)^{1-\tau}\delta(\tau,\psi(\sigma,\epsilon))^2 = \delta(\tau,\epsilon)^{1-\sigma}\delta(\sigma,\psi(\tau,\epsilon))^2$ for all $\sigma,\tau \in G$. Lemma 3.9 of [1] asserts that

$$\bigl(D:D'\bigr) = 2^b,$$

where $b \leqslant \binom{l}{2}$ if $i \in k$, and $b \leqslant \binom{l+1}{2}$ if $i \notin k$.

Further, let D'' be a subgroup of D' consisting of $\epsilon \in D'$ which satisfies $\delta(\sigma,\epsilon)^{1+\sigma}\delta(\sigma,\psi(\sigma,\epsilon))^2 = 1$ for all $\sigma \in G$. We see $[k(i):Q] = 2^m$ with $m = l$ if $i \in k$, and $m = l+1$ if $i \notin k$. If $\tau_1 \in G$ denotes the complex conjugation, then $\delta(\tau_1,\epsilon)^{1+\tau_1}=1$, $\psi(\tau_1,\epsilon)=1$ and so $\delta(\tau_1,\epsilon)^{1+\tau_1}\delta(\tau_1,\psi(\tau_1,\epsilon))^2=1$ for all $\epsilon\in D'$. Accordingly, Lemma 3.13 of [1] is rewritten as follows:

$$\bigl(D':D''\bigr)=2^c,$$

where $c\leqslant l-1$ if $i\in k$, and $c\leqslant l$ if $i\notin k$.

Let D''' be a subgroup of D'' consisting of $\epsilon\in D''$ such that ϵ or 2ϵ is a square in k. Let $[K:Q]=2^n$. Then Lemma 4.1 of [1] asserts that

$$\bigl(D'':D'''\bigr)=2^d,$$

where $d\leqslant n-l$.

Therefore we have

$$\bigl(C:D'''\bigr)=(C:D)\bigl(D:D'\bigr)\bigl(D':D''\bigr)\bigl(D'':D'''\bigr)=2^{a+b+c+d},$$

where

$$a+b+c+d\leqslant\begin{cases}\frac{l^2+l}{2}+n-1 & \text{if } i\in k,\\ \frac{l^2+l}{2}+n & \text{if } \notin k.\end{cases}$$

Since $2^{2^{l-1}-2}|(E:D''')$ if k is imaginary, $2^{2^l-2}|(E:D''')$ if k is real, and $(E:C)=\frac{(E:D''')}{(C:D''')}$, Theorem 4.2 of [1] can be rewritten as follows:

Theorem. *If $i\in k$, then*

$$2^{2^{l-1}-\frac{l^2+l}{2}-n-1}\bigm|(E:C),$$

if k is imaginary and $i\notin k$, then

$$2^{2^{l-1}-\frac{l^2+l}{2}-n-2}\bigm|(E:C),$$

and if k is real, then

$$2^{2^{l}-\frac{l^2+l}{2}-n-2}\bigm|(E:C).$$

References

[1] Z. Polický, On the index of circular units in the full group of units of a compositum of quadratic fields, J. Number Theory 128 (2008) 1074–1090.