25. *Class Number Calculation and Elliptic Unit. II*

Quartic Case

By Ken NAKAMULA
Department of Mathematics, Tokyo Metropolitan University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 12, 1981)

Let K be a real quartic number field which is not totally real and contains a (real) quadratic subfield K_2. Let $D(<0)$, h and E_+ respectively be the discriminant, the class number and the group of positive units of K. In the following, an effective algorithm will be given to calculate h and E_+ at a time.

Our method is the same as in our preceding note [3] except for a slight change. We shall show a method to compute the relative class number with respect to K/K_2, assuming that the class number of K_2 is known.

§ 1. Illustration of algorithm. Let d_2, h' and $\eta_2\,(>1)$ respectively be the discriminant, the class number and the fundamental unit of K_2. We can compute h' and η_2 in a usual manner if d_2 is given. So we assume that h' and η_2 are explicitly given. The group E_+ of positive units of K is a free abelian group of rank 2. Let H_+ be the group of positive units of K/K_2, and $\varepsilon_1\,(>1)$ be the generator of H_+, i.e.

$$H_+ :=\{\varepsilon \in E_+ \mid N_{K/K_2}(\varepsilon)=1\}=\langle \varepsilon_1\rangle.$$

Then, as in [2], the relative unit ε_1 generates E_+ together with another unit $\varepsilon_2(>1)$, i.e. $E_+=\langle \varepsilon_1, \varepsilon_2\rangle$, where

$$(1) \qquad \varepsilon_2=\sqrt{\varepsilon_1\eta_2},\quad \sqrt{\eta_2}\quad \text{or}\quad \eta_2.$$

Let η_e be the so-called "elliptic unit" of K, of which the definition will be given in § 5. Then, applying the results of Schertz [4], we see that $\eta_e>1$ and $\eta_e \in H_+$, and obtain the following relation between η_e and the class number h of K:

$$(2) \qquad h/h'=(E_+ : \langle \varepsilon_1, \eta_2\rangle)(H_+ : \langle \eta_e\rangle)/2.$$

Therefore, the calculation of the relative class number h/h' is reduced to the determination of the group index $(H_+ : \langle \eta_e\rangle)$ and the unit ε_2. Our method consists of the following steps:

(i) to compute an approximate value of η_e (§ 5),

(ii) to compute the minimal polynomial of η_e over $\boldsymbol{Q}$ (Lemma 2),

(iii) for $\xi \in H_+$ $(\xi>1)$, to give an explicit upper bound $B(\xi)$ of $(H_+ : \langle \xi\rangle)$ (Proposition 1),

(iv) for $\xi \in H_+$ $(\xi\neq 1)$, and for a natural number μ, to judge whether a real number $\sqrt[\mu]{\xi}$ belongs to K or not, and to compute the minimal polynomial of $\sqrt[\mu]{\xi}$ over $\boldsymbol{Q}$ if it belongs to K (Proposition 2),

(v) to determine ε_2 and to compute the minimal polynomial of ε_2 over $\boldsymbol{Q}$ (§ 4).

Now, the computation of $(H_+ : \langle \eta_e \rangle)$ and ε_1 goes similarly as described in § 1 of [3] by using (i) to (iv), and then h/h' and ε_2 are decided by (v) on account of (2).

§ 2. Upper bound of h/h'. The following lemma essentially gives an upper bound of the index of a subgroup of H_+.

Lemma 1. *Let $\varepsilon \in H_+$ ($\varepsilon > 1$). Then the absolute value of the discriminant $D(\varepsilon)$ of ε is smaller than* $4((\varepsilon^2+7)^3-8^3)$, i.e.

$$|D(\varepsilon)| < 4((\varepsilon^2+7)^3-8^3).$$

Note that $D(\varepsilon)$ is a non-zero multiple of the discriminant D of K, since ε does not belong to K_2. Then we have

Proposition 1. *Let $\xi \in H_+$ ($\xi > 1$), then*

$$(H_+ : \langle \xi \rangle) < 2 \log(\xi) / \log(\sqrt[3]{|D|/4+8^3}-7).$$

On account of (1) and (2), we have

Corollary. *Let η_e be the elliptic unit of K. Then*

$$h/h' < 2 \log(\eta_e) / \log(\sqrt[3]{|D|/4+8^3}-7).$$

§ 3. μ-th root of relative unit. For any element ξ of K, which does not belong to K_2, let

$$X^4 - s(\xi)X^3 + t(\xi)X^2 - u(\xi)X + v(\xi)$$

be the minimal polynomial of ξ over $\boldsymbol{Q}$.

If $\xi \in H_+$ ($\xi \neq 1$), then $u(\xi) = s(\xi)$ and $v(\xi) = 1$. The following lemma enables us to compute the minimal polynomial of ξ from an approximate value of ξ.

Lemma 2. *Let $\xi \in H_+$ ($\xi \neq 1$). Then $s(\xi)$ is a rational integer such that $|s(\xi) - \alpha| < 2$ and that $2 + \alpha(s(\xi) - \alpha)$ is a rational integer, and $t(\xi)$ is given by $t(\xi) = 2 + \alpha(s(\xi) - \alpha)$, where $\alpha = \xi + \xi^{-1}$.*

For any rational integers s and t, define $r_\mu = r_\mu(s, t)$ ($\mu = 1, 2, 3, \cdots$) as follows:

$$r_1 = s,\ r_2 = sr_1 - 2t,\ r_3 = sr_2 - tr_1 + 3s,\ r_4 = sr_3 - tr_2 + sr_1 - 4,$$
$$r_\mu = sr_{\mu-1} - tr_{\mu-2} + sr_{\mu-3} - r_{\mu-4} \quad \text{if } \mu \geqq 5.$$

Then we have

Proposition 2. *Let $\xi \in H_+$ ($\xi \neq 1$), and μ be a natural number. Put $\varepsilon = \sqrt[\mu]{\xi}$ (>0) and $\alpha = \varepsilon + \varepsilon^{-1}$. The real number ε belongs to K if and only if there exists a rational integer s such that*

$$|s - \alpha| < 2, \quad r_\mu(s, t) = s(\xi) \quad \text{and} \quad r_\mu(t-2, s^2-2t+2) = t(\xi) - 2,$$

where t is the nearest rational integer to $2 + \alpha(\alpha - s)$. If ε belongs to K, then

$$s(\varepsilon) = s \quad \text{and} \quad t(\varepsilon) = t.$$

This proposition gives us an effective method of judge whether the μ-th root of $\xi \in H_+$ ($\xi \neq 1$) is an element of H_+ or not. It only uses

$s(\xi)$, $t(\xi)$ and an approximate value of ξ.

§4. Determination of ε_2. Let the polynomial

$$X^2-lX+c; \quad l\in \boldsymbol{Z}, \quad c=\pm 1$$

be the minimal polynomial of the fundamental unit $\eta_2(>1)$ of K_2 over $\boldsymbol{Q}$.

We observe that $v(\varepsilon_1\eta_2)=1$. The following lemma enables us to calculate $s(\varepsilon_1\eta_2)$, $t(\varepsilon_1\eta_2)$ and $u(\varepsilon_1\eta_2)$ from ε_1 and η_2.

Lemma 2′. *Put $\alpha=\varepsilon_1+\varepsilon_1^{-1}$. Then $s(\varepsilon_1\eta_2)$ is a rational integer such that $|s(\varepsilon_1\eta_2)-\alpha\eta_2|<2\eta_2^{-1}(<2)$ and that $l^2-2c+\alpha\eta_2(s(\varepsilon_1\eta_2)-\alpha\eta_2)$ and $\alpha\eta_2^{-1}+\eta_2^2(s(\varepsilon_1\eta_2)-\alpha\eta_2)$ are rational integers, and $t(\varepsilon_1\eta_2)$ and $u(\varepsilon_1\eta_2)$ are given by $t(\varepsilon_1\eta_2)=l^2-2c+\alpha\eta_2(s(\varepsilon_1\eta_2)-\alpha\eta_2)$ and $u(\varepsilon_1\eta_2)=\alpha\eta_2^{-1}+\eta_2^2(s(\varepsilon_1\eta_2)-\alpha\eta_2)$.*

We can judge whether $\varepsilon_2=\sqrt{\varepsilon_1\eta_2}$ or not by the following proposition, using $s(\varepsilon_1\eta_2)$, $t(\varepsilon_1\eta_2)$, $u(\varepsilon_1\eta_2)$ and an approximate value of ε_1.

Proposition 3. *Put $\alpha=\sqrt{\varepsilon_1}+c\sqrt{1/\varepsilon_1}$. The real number $\sqrt{\varepsilon_1\eta_2}$ belongs to K if and only if there exists a rational integer s such that*

$$|s-\alpha\sqrt{\eta_2}|<2\sqrt{1/\eta_2}(<2),$$

$$s(\varepsilon_1\eta_2)=s^2-2t, \quad t(\varepsilon_1\eta_2)=t^2-2su+2c \quad \text{and} \quad u(\varepsilon_1\eta_2)=u^2-2ct,$$

where t and u are the nearest rational integers respectively to

$$cl+\alpha\sqrt{\eta_2}(s-\alpha\sqrt{\eta_2}) \quad \text{and} \quad \alpha\sqrt{1/\eta_2}+c\eta_2(s-\alpha\sqrt{\eta_2}).$$

If $\varepsilon_2=\sqrt{\varepsilon_1\eta_2}\in K$, then

$$s(\varepsilon_2)=s, \quad t(\varepsilon_2)=t, \quad u(\varepsilon_2)=u \quad \text{and} \quad v(\varepsilon_2)=c.$$

It is easy to see

Lemma 3. *If $\varepsilon_2=\sqrt{\eta_2}\in K$, then $c=-1$.*

We can judge whether $\varepsilon_2=\sqrt{\eta_2}$ or not by the following proposition, using ε_1 and η_2.

Proposition 4. *Assume $c=-1$, and let $\delta=\eta_2(\varepsilon_1-\varepsilon_1^{-1})^2$. Put*

$$b=(2s(\varepsilon_1))^2-(t(\varepsilon_1)+2)^2 \quad \text{and} \quad a=\delta+b/\delta.$$

Then a and b are natural numbers. The real number $\sqrt{\eta_2}$ belongs to K if and only if there exist rational integers a' and b' such that

$$b'^2=b \quad \text{and} \quad a'^2-2b'=a.$$

If $\varepsilon_2=\sqrt{\eta_2}\in K$, then

$$s(\varepsilon_2)=u(\varepsilon_2)=0, \quad t(\varepsilon_2)=-l \quad \text{and} \quad v(\varepsilon_2)=-1.$$

On account of (1), Propositions 3 and 4 give an effective method to determine ε_2. It only uses ε_1 and η_2.

§5. Elliptic unit. In order to define the elliptic unit η_e of K, let us prepare some notations. Denote by d_2 the discriminant of K_2. Let the imaginary quadratic number field $\Sigma:=\boldsymbol{Q}(\sqrt{Dd_2})$ and the discriminant of Σ be $-d$. Then the galois closure of $K/\boldsymbol{Q}$ is the composite field $L:=K\Sigma$, which is dihedral of degree 8 over $\boldsymbol{Q}$ and cyclic quartic over Σ. The abelian extension L/Σ has a rational conductor (f) with a natural number f, and $D=-f^2dd_2$. Moreover, L is contained in the ring class field Σ_f modulo f over Σ. All these facts are known by

Halter-Koch [1]. Let $\mathfrak{R}(f)$ be the ring class group of Σ modulo f, and λ be the canonical isomorphism

$$\lambda : \mathfrak{R}(f) \overset{\sim}{\rightarrow} \mathrm{Gal}(\Sigma_f/\Sigma)$$

as in § 4 of [3]. Let $\mathfrak{U} := \lambda^{-1}(\mathrm{Gal}(\Sigma_f/L))$, take and fix a class $\mathfrak{h}$ of $\mathfrak{R}(f)$ such that $\mathfrak{h}\mathfrak{U}$ generates the cyclic quotient group $\mathfrak{R}(f)/\mathfrak{U}$. For $\mathfrak{k} \in \mathfrak{R}(f)$, denote by $\gamma_{\mathfrak{k}}$ a complex number with positive imaginary part such that the module $Z\gamma_{\mathfrak{k}} + Z$ belongs to the class $\mathfrak{k}$. Then the elliptic unit η_e of K is defined, independent of the choice of $\mathfrak{h}$ and $\gamma_{\mathfrak{k}}$, by the following:

$$(4) \qquad \eta_e := \prod_{\mathfrak{k} \in \mathfrak{U}} \sqrt{\mathrm{Im}(\gamma_{\mathfrak{k}\mathfrak{h}})/\mathrm{Im}(\gamma_{\mathfrak{k}})}\,|\eta(\gamma_{\mathfrak{k}\mathfrak{h}})/\eta(\gamma_{\mathfrak{k}})|^2.$$

Here $\eta(z)$ is the Dedekind eta-function, of which an estimate as in Lemma 3 of [3] holds. Thus, when $\mathfrak{R}(f)$ and $\mathfrak{U}$ are explicitly given, an approximate value of η_e can be computed.

If the discriminant D of K is given, there are finite possible pairs $\{d, d_2\}$, and it is easy to compute f. Therefore, we can count out explicitly every subgroup $\mathfrak{U}$ of $\mathfrak{R}(f)$ which may correspond to K similarly as in the cubic case, using the results in [1]. Thus *the class numbers and the fundamental units of all quartic fields K with the same discriminant D can be computed* as described above.

§ 6. Appendix. (i) The following propositions help to determine ε_2.

Proposition 5. *If $\sqrt{\eta_e}$ does not belong to K, then $\varepsilon_2 \neq \eta_2$.*

Proposition 6. *If $\sqrt{\eta_e}$ belongs to K, then*

$$d = d_2 \equiv 8 \pmod{16},\ f = 4;$$

or

$$d = 4d_2 \equiv 4 \pmod{16},\ f = 1, 2, 4 \text{ or } 8.$$

The former follows from (2) and the fact that h' divides h, and the latter is proved by the results in [1].

(ii) The galois closure L of K/Q contains a totally complex quartic subfield F not conjugate to K. Further algorithm to compute the class number and the group of units of F exists. It uses the results in [2].

References

[1] F. Halter-Koch: Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe. J. Number Theory, **3**, 412–443 (1971).

[2] K. Nakamula: On the group of units of a non-galois quartic or sextic number field. Proc. Japan Acad., **56**A, 77–81 (1980).

[3] ——: Class number calculation and elliptic unit. I. ibid., **57**A, 56–59 (1981).

[4] R. Schertz: Die Klassenzahl der Teilkörper abelscher Erweitlungen imaginärquadratischer Zahlkörper. I. J. reine angew. Math., **295**, 151–168 (1977); ditto. II. ibid., **296**, 58–79 (1977).