85. *Class Number Calculation and Elliptic Unit. III*

Sextic Case

By Ken NAKAMULA
Department of Mathematics, Tokyo Metropolitan University

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

In our preceding notes [2] and [3], we have introduced an effective method to calculate the class number of a certain cubic or quartic field utilizing its elliptic unit. In the following, we shall treat the same problem for a sextic field.

Let K be a real sextic number field which is not totally real and which contains a (real) quadratic subfield K_2 and a cubic subfield K_3. Let $D\,(>0)$, h and E_+ respectively be the discriminant, the class number and the group of positive units of K. Further, let h_2 and h_3 be the class numbers of K_2 and K_3 respectively. We shall give a way to compute h/h_2h_3 and E_+ at a time by using the "elliptic unit" of K.

§ 1. **Illustration of algorithm.** Let η_2 and η_3 be the fundamental units (>1) of K_2 and K_3 respectively, and let H_+ be the group of positive units of K, i.e.

$$H_+ := \{\varepsilon \in E_+ \mid N_{K/K_2}(\varepsilon) = N_{K/K_3}(\varepsilon) = 1\}.$$

Then, as in [1], there is the relative fundamental unit ε_1 (>1) in H_+, i.e. $H_+ = \langle \varepsilon_1 \rangle$, and ε_1 generates E_+ together with two other independent units. More precisely,

$$E_+ = \langle \varepsilon_1 \rangle \times \langle \varepsilon_2 \rangle \times \langle \varepsilon_3 \rangle$$

with

(1) $$\varepsilon_2 = \sqrt[3]{\eta_2}, \quad \sqrt[3]{\eta_2^{\pm 1}\varepsilon_1} \quad \text{or } \eta_2,$$

(2) $$\varepsilon_3 = \sqrt{\eta_3 \varepsilon_1} \qquad \text{or } \eta_3.$$

Let η be the elliptic unit of K, of which the definition will be given in § 5. Then, applying the results in Schertz [5], we see that $\eta > 1$ and $\eta \in H_+$, and obtain the following formula:

(3) $$h/h_2h_3 = (E_+ : \langle \varepsilon_1, \eta_2, \eta_3 \rangle)(H_+ : \langle \eta \rangle)/6.$$

Therefore, the calculation of h/h_2h_3 is reduced to the determination of the group index $(H_+ : \langle \eta \rangle)$ and that of the units ε_2, ε_3. The index $(H_+ : \langle \eta \rangle)$ is determined similarly as in [2] or [3] by using Theorems 1 and 2 below. The computation of ε_2 and ε_3 is explained in § 4.

§ 2. **Upper bound of h/h_2h_3.** The following lemma gives an upper bound of the index of a subgroup of H_+.

Lemma 1. *Let $1 < \varepsilon \in H_+$ and $D(\varepsilon)$ be the discriminant of ε. Then*

$$(0<)D(\varepsilon)<16\left(\left(\varepsilon+\frac{9}{7}\right)^7-290\right)^2.$$

It is easily seen that $D>144^2$, hence we have

Theorem 1. *Let $1<\varepsilon\in H_+$, then*

$$(H_+:\langle\varepsilon\rangle)<\log(\varepsilon)/\log\left(\sqrt[7]{(\sqrt{D}/4)+290}-\frac{9}{7}\right).$$

This theorem assures that our algorithm ends in a finite number of steps. Especially, we obtain an explicit upper bound of h/h_2h_3 on account of (1), (2) and (3).

Corollary. *Let η be the elliptic unit of K, then*

$$h/h_2h_3<\log(\eta)/\log\left(\sqrt[7]{(\sqrt{D}/4)+290}-\frac{9}{7}\right).$$

§ 3. n-th root of relative unit. For any element ξ of K such that $K=\boldsymbol{Q}(\xi)$, let

$$X^6-s(\xi)X^5+t(\xi)X^4-u(\xi)X^3+v(\xi)X^2-w(\xi)X+x(\xi)$$

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

Let $1\neq\varepsilon\in H_+$, then $K=\boldsymbol{Q}(\varepsilon)$ and we have

$$u(\varepsilon)=s(\varepsilon)^2+2(s(\varepsilon)-t(\varepsilon)+1),\quad v(\varepsilon)=t(\varepsilon),\quad w(\varepsilon)=s(\varepsilon),\quad x(\varepsilon)=1.$$

The following lemma enables us to compute the minimal polynomial of ε from its approximate value.

Lemma 2. *Notations being as above, let $\beta=\varepsilon+\varepsilon^{-1}$. Then $s(\varepsilon)$ is a rational integer such that $|s(\varepsilon)-\beta|<2\sqrt{\beta+2}$ and that $(s(\varepsilon)^2+\beta^2s(\varepsilon)-\beta^3+3\beta+2)/(\beta+2)\in\boldsymbol{Z}$, and $t(\varepsilon)$ is given by $t(\varepsilon)=(s(\varepsilon)^2+\beta^2s(\varepsilon)-\beta^3+3\beta+2)/(\beta+2)$.*

For any rational integers s and t, put $u=s^2+2(s-t+2)$ and define a recursive sequence $r_n=r_n(s,t)(n=1,2,\cdots)$ as follows:

$$r_1=s,\quad r_2=sr_1-2t,\quad r_3=sr_2-tr_1+3u,\quad r_4=sr_3-tr_2+ur_1-4t,$$
$$r_5=sr_4-tr_3+ur_2-tr_1+5s,\quad r_6=sr_5-tr_4+ur_3-tr_2+sr_1-6,$$
$$r_n=sr_{n-1}-tr_{n-2}+ur_{n-3}-tr_{n-4}+sr_{n-5}-r_{n-6}\qquad \text{if } n\geqq 7.$$

Then we have

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

$$|s-\beta|<2\sqrt{\beta+2},\quad r_n(s,t)=s(\xi),\quad r_n(s_0,t_0)=t(\xi).$$

Here t is the nearest rational integer to $(s^2+\beta^2s-\beta^3+3\beta+2)/(\beta+2)$,

$$s_0=t-s-3,\qquad t_0=r_3(s,t)+t_0-3.$$

If s satisfies the above condition, then

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

This theorem gives us an effective method to judge whether the n-th root of ξ is also an element of H_+ or not. It only requires $s(\xi)$, $t(\xi)$ and an approximate value of ξ.

§ 4. Determination of ε_2 and ε_3. The fundamental unit η_2 of K_2

is obtained explicitly as usual. The fundamental unit η_3 of K_3 is calculated by the method as in [2]. So we may assume that the minimal polynomials and approximate values of η_2 and η_3 are known. Then, after ε_1 is determined by the results in the preceding two sections, we can calculate the minimal polynomials of $\eta_2^{\pm 1}\varepsilon_1$ and $\eta_3\varepsilon_1$ by a lemma similar to Lemma 2′ of [3].

Put $\xi=\eta_3\varepsilon_1$ and $\varepsilon=\sqrt{\xi}$. Then we can judge whether the real number ε belongs to K or not, using approximate values of η_3 and ε_1 together with $s(\xi)$, $t(\xi)$, $u(\xi)$, $v(\xi)$, $w(\xi)$, $x(\xi)$. Namely, a proposition similar to Proposition 3 of [3] holds, because $s(\xi)$, $t(\xi)$, $u(\xi)$, $v(\xi)$, $w(\xi)$, $x(\xi)$ can be written explicitly as polynomials of $s(\varepsilon)$, $t(\varepsilon)$, $u(\varepsilon)$, $v(\varepsilon)$, $w(\varepsilon)$, $x(\varepsilon)$ if ε belongs to K, and because the possible values of $s(\varepsilon)$ and $w(\varepsilon)$ are bounded explicitly by elementary functions of η_3 and ε_1. Moreover $s(\varepsilon)$, $t(\varepsilon)$, $u(\varepsilon)$, $v(\varepsilon)$, $w(\varepsilon)$, $x(\varepsilon)$ are given during the test if ε belongs to K. Therefore an effective method for the determination of ε_3 is given.

Similarly we can judge whether $\sqrt[3]{\eta_2^{\pm 1}\varepsilon_1}$ belongs to K or not, using the minimal polynomial of $\eta_2^{\pm 1}\varepsilon_1$ and approximate values of η_2, ε_1. For the determination of ε_2, we have the following proposition in addition.

Proposition 1. *Let D_3 be the discriminant of K_3, and let*

$$X^3-yX^2+zX-1$$

be the minimal polynomial of η_3 over $\boldsymbol{Q}$. Put $\varepsilon=\sqrt[3]{\eta_2}\,(>0)$,

(i) *If ε belongs to K, the quadratic field $\boldsymbol{Q}(\sqrt{D_3D})$ contains a primitive cubic root of unity,* i.e. $\boldsymbol{Q}(\sqrt{D_3D})=\boldsymbol{Q}(\sqrt{-3})$.

(ii) *Assume $\boldsymbol{Q}(\sqrt{D_3D})=\boldsymbol{Q}(\sqrt{-3})$. Then*

$$X^2-(2y^3-9yz+27)X+(y^2-3z)^3=0$$

has an irrational real root γ in K_2. Furthermore, the real number ε belongs to K if and only if $\gamma\eta_2^2$ is a perfect cube in K_2.

Hence we have an effective way to decide ε_2.

§5. **Elliptic unit.** Every sextic field K in question is given in the following way. Let F be an imaginary quadratic number field with the discriminant $-d$. Let f be a natural number and $\mathfrak{R}(f)$ be the ring class group of F modulo f. Assume $\mathfrak{R}(f)$ contains a subgroup $\mathfrak{U}$ of index 6 such that the conductor of $\mathfrak{U}$ is exactly f. Let L be the class field of degree 6 over F corresponding to the ring class subgroup $\mathfrak{U}$. Then L is a dihedral extension of degree 12 over $\boldsymbol{Q}$. Let K be the maximal real subfield of L, then our assumption for K is satisfied. Conversely, when K is given, the galois closure L of $K/\boldsymbol{Q}$ is a dihedral extension of degree 12 over $\boldsymbol{Q}$ and is cyclic sextic over the imaginary quadratic subfield $F=\boldsymbol{Q}(\sqrt{D_3})$, where D_3 is the discriminant of K_3. Therefore L corresponds to a subgroup $\mathfrak{U}$ of index 6 in $\mathfrak{R}(f)$ with a natural number f. This correspondence between K and $\mathfrak{U}$ is one to one. We observe that $F=\boldsymbol{Q}(\sqrt{-3})$ if and only if K is pure sextic.

Let $\mathfrak{U}$ be the subgroup of $\mathfrak{R}(f)$ which corresponds to K. Then the elliptic unit η of K is defined by the following:

$$\eta=\prod_{\mathfrak{k}\in\mathfrak{U}}\sqrt{\operatorname{Im}(\gamma_{\mathfrak{r}\mathfrak{k}})\operatorname{Im}(\gamma_{\mathfrak{r}^3\mathfrak{k}})/\operatorname{Im}(\gamma_{\mathfrak{k}})\operatorname{Im}(\gamma_{\mathfrak{r}^2\mathfrak{k}})}\,|\eta(\gamma_{\mathfrak{r}\mathfrak{k}})\eta(\gamma_{\mathfrak{r}^3\mathfrak{k}})/\eta(\gamma_{\mathfrak{k}})\eta(\gamma_{\mathfrak{r}^2\mathfrak{k}})|^2.$$

Here $\eta(z)$ is the Dedekind eta function, and $\gamma_{\mathfrak{k}}$ is a complex number with positive imaginary part such that $Z\gamma_{\mathfrak{k}}+Z$ belongs to the class $\mathfrak{k}\in\mathfrak{R}(f)$. The class $\mathfrak{r}\in\mathfrak{R}(f)$ is chosen so that $\mathfrak{r}\mathfrak{U}$ generates the cyclic quotient group $\mathfrak{R}(f)/\mathfrak{U}$. The definition of η is independent of the choice of $\gamma_{\mathfrak{k}}$ and $\mathfrak{r}$. Therefore, if $\mathfrak{R}(f)$ and $\mathfrak{U}$ are explicitly given, we can calculate an approximate value of η using Lemma 3 of [2].

It is possible to obtain $\mathfrak{R}(f)$ and $\mathfrak{U}$ explicitly, although it seems to be very complicated in the actual calculation.

§6. Appendix. (i) The following propositions help to determine ε_2 and ε_3.

Proposition 2. (i) *Assume h_2 or h_3 is odd. Then $\varepsilon_3\neq\eta_3$ if $\sqrt{\eta}$ does not belong to K.* (ii) *Assume h_2 or h_3 is prime to 3. Then $\varepsilon_2\neq\eta_2$ if $\sqrt[3]{\eta}$ does not belong to K.*

Proposition 3. *Let f and d be as in §5, and let d_2 be the discriminant of K_2. Assume $\sqrt[3]{\eta_2}$ belongs to K. Then $d=3d_2$ or $3d_2=d$; and f is a power of 3.*

(ii) The galois closure L of $K/\boldsymbol{Q}$ contains a totally imaginary sextic subfield K' not conjugate to K. Further algorithm to compute the class number and fundamental units of K' exists. It uses the results in [1].

Corrections to References [2] and [3]. In [2], we add the assumption that "$D\neq-23$" throughout the note. See also [4] in detail. In Proposition 6 of [3], for '$\sqrt{\eta_e}$' read "$\sqrt{\eta_2}$". In the definition of H_+ in [3], line 6 of §1, for 'positive units' read "positive relative units".

References

[1] K. Nakamula: A construction of the groups of units of some number fields from certain subgroups (preprint).

[2] ——: Class number calculation and elliptic unit. I. Proc. Japan Acad., **57**A, 56–59 (1981).

[3] ——: Class number calculation and elliptic unit. II. ibid., **57**A, 117–120 (1981).

[4] ——: Class number calculation of a cubic field from the elliptic unit (to appear in J. reine angew. Math.).

[5] R. Schertz: Über die Klassenzahl gewisser nicht galoisscher Körper 6-ten Grades. Abh. Math. Sem. Hamburg., **42**, 217–224 (1974).