12. *Class Number Calculation and Elliptic Unit. I*

Cubic Case

By Ken NAKAMULA
Department of Mathematics, Tokyo Metropolitan University

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

Let K be a real cubic number field with the discriminant $D<0$. In the following, an effective algorithm will be given, to calculate the class number h and the fundamental unit ε_1 (>1) of K at a time.

Angell [1] has given a table of h and ε_1 of K for $D>-20000$. In the special case when $K=\boldsymbol{Q}(\sqrt[3]{m})$, a pure cubic number field, Dedekind [5] has given an analytic method to calculate h. In such a pure cubic case, Dedekind's method has been improved by several authors, see [3] and [13]. In all these algorithms, however, it is necessary to compute ε_1 by Voronoi's algorithm, see [6, pp. 232–290], before the calculation of h.

Our method does not need Voronoi's algorithm, and h and ε_1 are calculated at a time. The starting point of the method is the index formula on elliptic units given by Schertz, see [11] and [12], and the idea of the algorithm is learned from G. Gras and M.-N. Gras [8]. There is a similar algorithm to compute the class number and fundamental units of a real quartic number field which is not totally real and contains a quadratic subfield, see the author's [10]. The author expects that such an algorithm will be generalized to calculate the class number of a non-galois number field whose galois closure is an abelian extension over an imaginary quadratic number field.

§ 1. **Illustration of algorithm.** The class number h of K is given by the index of the subgroup generated by the so called "elliptic unit" η_e (>1) of K, of which the definition will be given in § 4, in the group of positive units of K, see [11]:

(1) $$\eta_e=\varepsilon_1^h, \qquad \text{i.e. } h=(\langle\varepsilon_1\rangle : \langle\eta_e\rangle).$$

Our method consists of the following steps:

(i) to compute an approximate value of η_e (§ 4),

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

(iii) for any unit $\xi(>1)$ of K, to give an explicit upper bound $B(\xi)$ of $(\langle\varepsilon_1\rangle : \langle\xi\rangle)$ (Proposition 1),

(iv) for any unit $\xi(>1)$ of K and for a natural number μ, to judge whether a real number $\sqrt[\mu]{\xi}\,(>1)$ is an element to K or not, and to compute the minimal polynomial of $\sqrt[\mu]{\xi}$ over $\boldsymbol{Q}$ if it is an element of K

(Proposition 2).

Now, the computation of h and ε_1 goes as follows. Determine the minimal polynomial of η_e over $\boldsymbol{Q}$ by (i) and (ii). Put $h(\eta_e)=1$ and compute $B(\eta_e)$ by (iii). Put $\xi=\eta_e$, and test whether the set

$$S(\xi):=\{p \mid p: \text{prime number}, \ p \leqq B(\xi), \ \sqrt[p]{\xi} \in K\}$$

is empty or not by (iv). If $S(\xi)$ is empty, then $\varepsilon_1=\xi$ and $h=h(\xi)$. If $S(\xi)$ is not empty, take the smallest prime p in $S(\xi)$, and let $\varepsilon=\sqrt[p]{\xi}$, $B(\varepsilon)=B(\xi)/p$ and $h(\varepsilon)=ph(\xi)$. The minimal polynomial of ε over $\boldsymbol{Q}$ can be calculated by (iv). Next, put $\xi=\varepsilon$ and repeat the above procedure for ξ by using (iv). Then $S(\xi)$ becomes an empty set in a finite number of steps.

§ 2. Upper bound of *h*. The following Artin's lemma essentially gives an upper bound of the index of a subgroup of the group of units of K.

Lemma 1 (Artin [2]). *Let $\varepsilon(>1)$ be a unit of K. Then the absolute value of the discriminant $D(\varepsilon)$ of ε is smaller than* $4\varepsilon^3+24$, i.e. $|D(\varepsilon)|<4\varepsilon^3+24$.

Note that $D(\varepsilon)$ is a non-zero multiple of the discriminant D of K since ε is irrational. It is easy to see that $(|D|-24)/4>1$. Then we have

Proposition 1. *Let $\xi(>1)$ be a unit of K. Then*

$$(\langle\varepsilon_1\rangle : \langle\xi\rangle)<3 \log(\xi)/\log((|D|-24)/4).$$

On account of (1), we have

Corollary. *Let η_e be the elliptic unit of K. Then the class number h of K satisfies*

$$h<3 \log(\eta_e)/\log((|D|-24)/4).$$

§ 3. μ-th root of units. For any positive unit ξ of K, we denote by $s(\xi)$ and $t(\xi)$ the absolute trace of ξ and $1/\xi$ respectively. The following lemma enables us to calculate the minimal polynomial of a unit of K over $\boldsymbol{Q}$ from an approximate value of the unit.

Lemma 2. *Let $\xi(>1)$ be a unit of K. Then $s(\xi)$ is a rational integer such that $|s(\xi)-\xi|<2\sqrt{1/\xi}(<2)$ and that $1/\xi+\xi(s(\xi)-\xi)$ is a rational integer, and $t(\xi)$ is given by $t(\xi)=1/\xi+\xi(s(\xi)-\xi)$.*

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

$$r_1=s, \quad r_2=s^2-2t, \quad r_3=s^3-3st+3,$$
$$r_\mu=sr_{\mu-1}-tr_{\mu-2}+r_{\mu-3} \qquad \text{if } \mu \geqq 4.$$

Then we have

Proposition 2. *Let $\xi(>1)$ be a unit of K and μ be a natural number. Put $\varepsilon=\sqrt[\mu]{\xi}(>1)$. The real number ε belongs to K if and only if there exists a rational integer u such that*

$$|u-\varepsilon|<2\sqrt{1/\varepsilon}(<2),$$
$$r_\mu(u, v)=s(\xi) \quad \textit{and} \quad r_\mu(v, u)=t(\xi),$$

where v is the nearest rational integer to $1/\varepsilon+\varepsilon(u-\varepsilon)$. *If* ε *belongs to* K, *then*

$$s(\varepsilon)=u \quad and \quad t(\varepsilon)=v.$$

This proposition gives us an effective method to judge whether the μ-th root of a unit $\xi(>1)$ of K is an element of K or not. It only uses $s(\xi)$, $t(\xi)$ and an approximate value of ξ.

§ 4. **Elliptic unit.** In order to define the elliptic unit η_e of K, let us prepare some notations. Let the imaginary quadratic number field $\Sigma:=\boldsymbol{Q}(\sqrt{D})$ 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 6 over $\boldsymbol{Q}$ and cyclic cubic over Σ. The abelian extension L/Σ has a rational conductor (f) with a natural number f, and $D=-f^2d$. Moreover, L is contained in the ring class field Σ_f modulo f over Σ. All these facts are known in Hasse [9]. Let $\mathfrak{R}(f)$ be the ring class group of Σ modulo f. By the classical theory of complex multiplication, see Deuring [7], the ring class field $\Sigma_f=\Sigma(j(\mathfrak{k}))$ for $\mathfrak{k}\in\mathfrak{R}(f)$, where $j(\mathfrak{k})$ is the ring class invariant as usual, and there is the canonical isomorphism

$$\lambda:\mathfrak{R}(f)\cong\mathrm{Gal}\,(\Sigma_f/\Sigma)\,;\ j(\mathfrak{k}')^{\lambda(\mathfrak{k})}=j(\mathfrak{k}'\mathfrak{k}^{-1}) \qquad \text{for } \mathfrak{k},\ \mathfrak{k}'\in\mathfrak{R}(f).$$

Let $\mathfrak{U}:=\lambda^{-1}(\mathrm{Gal}\,(\Sigma_f/L))$, take and fix a class $\mathfrak{h}$ of $\mathfrak{R}(f)$ which does not belong to $\mathfrak{U}$. For $\mathfrak{k}\in\mathfrak{R}(f)$, denote by $\gamma_\mathfrak{k}$ a complex number with its imaginary part positive such that $\boldsymbol{Z}\gamma_\mathfrak{k}+\boldsymbol{Z}\in\mathfrak{k}$. Then the elliptic unit η_e of K is defined, independent of the choice of $\mathfrak{h}$ and $\gamma_\mathfrak{k}$, by the following:

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

Here $\eta(z)$ is the Dedekind eta-function:

$$\eta(z)=\exp\,(\pi iz/12)\prod_{\nu=1}^{\infty}(1-\exp\,(2\pi i\nu z)).$$

Now we should see how an approximate value of η_e is computed. Suppose that $\mathfrak{R}(f)$ and $\mathfrak{U}$ have been given already. Then, since we can take $\gamma_\mathfrak{k}$ so that $\mathrm{Im}\,(\gamma_\mathfrak{k})\geqq\sqrt{3}/2$ as in [4], we can compute η_e by (2), using the following lemma for example.

Lemma 3. *Let $z=x+iy$ be a complex number with the imaginary part $y>0$, and put*

$$R_N(z):=-\pi y/6+\sum_{\nu=1}^{N-1}\log|1-\exp\,(2\pi i\nu z)|^2.$$

Then

$$|\log|\eta(z)|^2-R_N(z)|<\frac{(2-\exp\,(-2\pi Ny))\exp\,(-2\pi Ny)}{(1-\exp\,(-2\pi Ny))(1-\exp\,(-2\pi y))}.$$

If the discriminant D of K is given, it is easy to compute f. Then we can count out explicitly every subgroup $\mathfrak{U}$ of $\mathfrak{R}(f)$ which may correspond to K as in Hasse [9]. Thus *the class numbers and the fundamental units of all cubic number fields with the same discriminant*

D can be computed as described above. In pure cubic case, i.e. $K = \boldsymbol{Q}(\sqrt[3]{m})$ with a cube free natural number m, the corresponding subgroup $\mathfrak{U}$ of $\mathfrak{R}(f)$ is perfectly determined from the value m, see [5].

References

[1] I. O. Angell: A table of complex cubic fields. Bull. London Math. Soc., **5**, 37–38 (1973).

[2] E. Artin: Theory of Algebraic Numbers. Lecture note, Göttingen (1959).

[3] P. Barrucand, H. C. Williams, and L. Baniuk: A computational technique for determining the class number of a pure cubic field. Math. Comp., **30**, 312–323 (1976).

[4] Z. I. Borevich and I. R. Shafarevich: Number Theory. Academic Press, New York-London (1966).

[5] R. Dedekind: Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern. J. reine angew. Math., **121**, 40–123 (1900).

[6] B. N. Delone and D. K. Faddeev: The Theory of Irrationalities of the Third Degree. Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R.I. (1964).

[7] M. Deuring: Die Klassenkörper der komplexen Multiplikation. Enzycl. der Math. Wiss. I/2, 2 Aufl., Heft 10, Stuttgart (1958).

[8] G. Gras and M.-N. Gras: Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\boldsymbol{Q}$. Publ. Math. Univ., Besançon (1974–1975).

[9] H. Hasse: Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. Math. Z., **31**, 565–582 (1930).

[10] K. Nakamula: Class number calculation and elliptic unit II (preprint).

[11] R. Schertz: Arithmetische Ausdeutung der Klassenzahlformel für einfach reelle kubische Zahlkörper. Abh. Math. Sem. Universität Hamburg, **41**, 211–223 (1974).

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

[13] H. C. Williams: G. Cormack & E. Seah, Calculation of the regulator of a pure cubic field. Math. Comp., **34**, 567–611 (1980).