88

ELLIPTIC UNIT AND CLASS NUMBER CALCULATION

(惰円単数と類数の計算について)

By   Ken NAKAMULA

Department of Mathematics, Tokyo Metropolitan University

In this note, an effective method will be introduced to calcu-
late the class numbers and fundamental units of certain non-galois
number fields, utilizing so called "elliptic units".

Introduction

For a real abelian number field, G. Gras and M.-N. Gras [3] has
introduced an effective method to calculate its class number and fun-
damental units together, utilizing cyclotomic units. Their method is
based on an index formula for the class number, related to cyclotomic
units, given by H.W. Leopoldt [5]. For a finite abelian extension over
an imaginary quadratic number field, a similar index formula for the
relative class number, related to elliptic units, has been given by R.
Schertz [11, I]. Moreover, for a non-galois number field of which the
galois closure over $\mathbb{Q}$ is an abelian extension over an imaginary quad-
ratic number field, Schertz [11, II] has given a similar index formula.
So we consider the following problems:

PROBLEM 1. Let L be a finite abelian extension over an imag-
inary quadratic number field Σ, and denote respectively by $\bar{h}$ and h'

the class numbers of L and Σ . Find an effective method to calculate
h̄/h' and fundamental units together, utilizing elliptic units of L.

PROBLEM 2. Let K be a non-galois number field of which the
galois closure over ℚ is an abelian extension over an imaginary quad-
ratic number field, and denote respectively by h and h_0 the class
numbers of K and the maximal absolutely abelian subfield of K. Find
an effective method to calculate h/h_0 and fundamental units of K to-
gether, utilizing elliptic units of K.

The fomulas in [11] are too complicated to deal with these prob-
lems in general. So we set the following problem:

PROBLEM 3. Notations being as above, simplify the index for-
mulas for h̄/h', Satz(3.5) of [11, I], and h/h_0, Satz(2.3) of [11, II],
so as to be more appropriate for Gras' method to apply to Problems 1
and 2.

As to Problem 3, during the preparation of this manuscript after
the talk, the author obtained a simplification of the formula in Satz
(3.5) of [11, I] by a similar manner as in [5]. The simplified formula,
which will be stated in §1, makes it possible to use Gras' method for
Problem 1, though it is not sufficiently effective yet, see [8]. R. Gillard
and G. Robert have given in [2] several index formulas analogous to Satz
(3.3) of [11, I], however their view-point is different from ours.

A solution of Problem 2 in case K is cubic or quartic over ℚ
will be given in §2. In such a case, the index formula is simple and the
problem is reduced to a calculation, starting from an approximate value
of an elliptic unit, of a generator of an infinite cyclic group. The cal-

culation is done by some arithmetic and requires no geometrical algo-
rithm. We shall give some numerical examples in §3.

Notations

For a number field k, we denote respectively by E_k, W_k, w_k
and D_k the group of units of k, the torsion part of E_k, the number
of elements of W_k and the discriminant of k.

§1. Leopoldt's decomposition

Let L be an abelian extension of degree n over a number field
Σ with the galois group A of L/Σ. Denote by Ψ and Λ the group
of characters of A and the set of $\mathbb{Q}$-irreducible characters of A
respectively. Every $\lambda \in \Lambda$ is the sum of the $\mathbb{Q}$-conjugates of a charac-
ter $\psi \in \Psi$, so we denote $\lambda = \bar{\psi}$. For $\psi \in \Psi$, the intermidiate field of L/Σ
fixed by $\mathrm{Ker}(\psi)$ depends only on $\bar{\psi}$, so the field is denoted by $\Sigma_{\bar{\psi}}$.

In case $\Sigma = \mathbb{Q}$ and L is totally real, Leopoldt [5] has given
a decomposition of the class number $\bar{h}$ of L as follows:

$$(1) \qquad Q_A \bar{h} = (E_L : \prod_{1 \neq \lambda \in \Lambda} H_\lambda) \prod_{1 \neq \lambda \in \Lambda} (H_\lambda : C_\lambda) .$$

Here Q_A is a natural number given by

$$(2) \qquad Q_A = \sqrt{n^{n-2} / \prod_{\lambda \in \Lambda} d_\lambda}, \quad d_\lambda = |D_{\mathbb{Q}(\psi)}| \quad \text{with} \quad \psi \in \Psi, \; \bar{\psi} = \lambda,$$

and H_λ consists of $\varepsilon \in E_{\Sigma_\lambda}$ such that $N_{\Sigma_\lambda/k}(\varepsilon) = \pm 1$ for all proper sub-
fields k of Σ_λ, the group of proper λ-relative units in [5], and
the subgroup C_λ of H_λ is generated by a unit η_λ, the generating
λ-relative cyclotomic unit in [5], and its conjugates together with
± 1. The product $\prod_{1 \neq \lambda \in \Lambda} H_\lambda$ is the direct product modulo ± 1. In (1),

- 3 -

th factor Q_A is easily calculated by (2), and $(E_L : \prod_{1 \neq \lambda \in \Lambda} H_\lambda)$ is

a divisor of $2^{a-1} Q_A$, where a is the number of elements of Λ. For

every $\lambda \in \Lambda$, $\lambda \neq 1$, the generating λ-relative cyclotomic unit η_λ is known

numerically explicitly. Therefore we can calculate $\bar{h}$ by Gras' method-

od in [3], which consists of the following steps:

   (i) to give an upper bound $B(\eta_\lambda)$ of $(H_\lambda : C_\lambda)$, $B(\eta_\lambda)$ can be

   calculated from η_λ, $\lambda \in \Lambda$, $\lambda \neq 1$;

   (ii) for $\xi \in H_\lambda$ and for each $\nu \in \mathbb{N}$, to look for $\varepsilon \in H_\lambda$ such

   that $\varepsilon^\nu = \xi$, $\lambda \in \Lambda$, $\lambda \neq 1$;

   (iii) for $\xi \in \prod_{1 \neq \lambda \in \Lambda} H_\lambda$ and for each $\nu \in \mathbb{N}$, to look for $\varepsilon \in E_L$

   such that $\varepsilon^\nu = \xi$,

By (i) and by $(E_L : \prod_{1 \neq \lambda \in \Lambda} H_\lambda) \leq 2^{a-1} Q_A$, the calculation completes in

a finite number of steps and an upper bound of the number of steps is

also known. By (ii) and (iii), fundamental units of L are obtained

explicitly in the form of their minimal polynomials over $\mathbb{Q}$, and $Q_A \bar{h}$

is calculated at the same time.

   In case Σ is an imaginary quadratic number field, let $\bar{h}$ and

h' respectively be the class numbers of L and Σ. For $\lambda \in \Lambda$, $\lambda \neq 1$, put

$$n_\lambda = [\Sigma_\lambda : \Sigma], \qquad w_\lambda = w_{\Sigma_\lambda},$$

and let f_λ be the smallest natural number contained in the conductor

of Σ_λ / Σ, $\bar{w}_\lambda$ be the number of elements of W_Σ congruent to 1 modulo

the conductor of Σ_λ / Σ, and set

$$c_L = (w/w_L) \prod_{1 \neq \lambda \in \Lambda, \; f_\lambda = 1} (12 n_\lambda)^{\varphi(n_\lambda)} \prod_{\lambda \in \Lambda, \; f_\lambda \neq 1} (w_\lambda \bar{w}_\lambda)^{\varphi(n_\lambda)},$$

where $\varphi(\cdot)$ is Euler's function. Further let Q_A be given by (2) and

H_λ be the group of units $\varepsilon \in E_{\Sigma_\lambda}$ such that $N_{\Sigma_\lambda / k}(\varepsilon) \in W_k$ for all proper

intermidiate fields k of Σ_λ / Σ. Then, using the results of [9] and

[12], we can find a unit $\eta_\lambda \epsilon H_\lambda$ related to elliptic modular functions in an explicit form. Moreover, denoting by E_λ the subgroup of H_λ generated by η_λ and its conjugates together with W_{Σ_λ}, we obtain the following decomposition of the relative class number $\bar{h}/h'$:

$$(3) \qquad c_L Q_A(\bar{h}/h') = (E_L : \prod_{1 \neq \lambda \epsilon \Lambda} H_\lambda) \prod_{1 \neq \lambda \epsilon \Lambda} (H_\lambda : E_\lambda).$$

Precise definition of η_λ is ommitted here, see [8]. In (3), the product $\prod_{1 \neq \lambda \epsilon \Lambda} H_\lambda$ is the direct product modulo W_L and the index $(E_L : \prod_{1 \neq \lambda \epsilon \Lambda} H_\lambda)$ is a divisor of $w_L^{n-1} Q_A$. We can use Gras' method to (3) <u>almost</u> <u>similarly</u> as in case $\Sigma = \mathbb{Q}$ and L is real, though it is not sufficiently effective yet only because the ground field Σ and the elliptic units η_λ are more complicated.

§2. Certain non-galois cases

In this section, we give an answer to Problem 2 in certain cases, introducing an effective algorithm to calculate the class number and fundamental units together.

<u>Cubic</u> <u>Case</u> (see [6]). Let K be a real cubic number field with

$$D := D_K < 0 \qquad \text{and} \qquad E_K = <-1, \epsilon_1> \quad \text{with} \quad \epsilon_1 > 1.$$

Then the galois closure of $K/\mathbb{Q}$ is a cyclic cubic extension over the imaginary quadratic number field $\Sigma = \mathbb{Q}(\sqrt{D})$, and the condition of Problem 2 is satisfied. Indeed we have the following formula for the class number h of K, see [10]:

$$(4) \qquad h = (<\epsilon_1> : <\eta_e>), \qquad \eta_e > 1,$$

where η_e is given explicitly as in (2) of [6] or (1.15) of [10]. We illustrate the process of the calculation of h and ϵ_1 from an approximate value of η_e.

For every positive unit $\xi \neq 1$ of K, let

$$X^3 - s(\xi)X^2 + t(\xi)X - 1$$

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

LEMMA. If $\xi \in E_K$ and $\xi > 1$, we have

$$|s(\xi) - \xi| < 2\sqrt{1/\xi} \quad \text{and} \quad t(\xi) = (1/\xi) + \xi(s(\xi) - \xi).$$

This lemma enables us to calculate the minimal polynomial of η_e over $\mathbb{Q}$ from an approximate value of η_e since $s(\eta_e)$ and $t(\eta_e)$ are in $\mathbb{Z}$. From Artin's lemma in [1], we see the following:

PROPOSITION 1. Let $\xi \in E_K$ and $\xi > 1$, then

$$(<\varepsilon_1> : <\xi>) < B(\xi) := 3\log(\xi)/\log((|D| - 24)/4).$$

REMARK. It is always true that $(|D| - 24)/4 > 1$.

Proposition 1 gives an upper bound $B(\eta_e)$ of h, which can be calculated from the value of η_e, on account of (4). Therefore we can calculate h and the minimal polynomial of ε_1 together, if we have a way to check whether $\sqrt[\nu]{\eta_e} \in K$ or $\notin K$ and to decide the minimal polynomial of $\sqrt[\nu]{\eta_e}$ when $\sqrt[\nu]{\eta_e} \in K$, for each $\nu \in \mathbb{N}$, $\nu < B(\eta_e)$. The following proposition gives such a way.

For $s, t \in \mathbb{Z}$, define a recursive sequence $r_\nu = r_\nu(s,t)$ $(\nu \in \mathbb{N})$ by

$$r_1 = s, \quad r_2 = sr_1 - 2t, \quad r_3 = sr_2 - tr_1 + 3,$$
$$r_\nu = sr_{\nu-1} - tr_{\nu-2} + r_{\nu-3} \quad \text{if} \quad \nu > 3.$$

PROPOSITION 2. For $\xi \in E_K$, $\xi > 1$, and for $\nu \in \mathbb{N}$, let ε be the positive real ν-th root of ξ. Then $\varepsilon \in K$ holds if and only if there exists $s \in \mathbb{Z}$ such that $|s - \varepsilon| < 2\sqrt{1/\varepsilon}$, $r_\nu(s,t) = s(\xi)$ and $r_\nu(t,s) = t(\xi)$, where $t \in \mathbb{Z}$ is the nearest to $(1/\varepsilon) + \varepsilon(s - \varepsilon)$. Further, if $\varepsilon \in K$, then the above s and t are unique so that $s = s(\varepsilon)$ and $t = t(\varepsilon)$.

94

Quartic Case (see [7]). Let K be a real, not totally real, quadratic extension over a real quadratic number field K_2 with

$$D:=D_K<0, \quad d_2:=D_{K_2}>0 \quad \text{and} \quad E_{K_2}=<-1,\ \eta_2> \quad \text{with} \quad \eta_2>1.$$

Further let H be the group of $\varepsilon\in E_K$, $\varepsilon>0$ such that $N_{K/K_2}(\varepsilon)=1$. Then we see

$$H=<-1,\ \varepsilon_1> \quad \text{with} \quad \varepsilon_1>1$$

and

$$E_K=H\times<\varepsilon_2> \quad \text{(direct product)} \quad \text{with} \quad \varepsilon_2=\eta_2,\sqrt{\eta_2} \quad \text{or} \quad \sqrt{\varepsilon_1\eta_2}.$$

In this case, the galois closure of $K/\mathbb{Q}$ is a cyclic quartic extension over the imaginary quadratic number field $\Sigma=\mathbb{Q}(\sqrt{Dd_2})$, and K_2 is the maximal absolutely abelian subfield of K. Let h and h_0 be the class numbers of K and K_2 respectively. Then we have the following formula, see [7]:

$$(5) \qquad h/h_0=(1/2)(E_K:H\times<\eta_2>)(H:<\eta_e>), \qquad \eta_e>1,$$

where η_e is given explicitly as in (4) of [7]. Therefore h/h_0 is calculated as a result of the determination of ε_1 and ε_2 from η_2 and η_e. The most important point of our algorithm is the determination of ε_1 from an approximate value of η_e. It is done similarly as in Cubic Case utilizing the fact that the minimal polynomial of every $\varepsilon\in H$, $\varepsilon>1$, has the form

$$X^4-s(\varepsilon)X^3+t(\varepsilon)X^2-s(\varepsilon)X+1, \qquad |s(\varepsilon)-\varepsilon-(1/\varepsilon)|<2,$$

and that the absolute value of its discriminant is smaller than

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

We do not explain the algorithm more, see [7] in detail.

REMARK. In Problem 2, we may assume (h_0 and) fundamental units of the maximal absolutely abelian subfield of K is known, because they are obtained by Gras' algorithm . In Quartic Case, we have assumed

that η_2 is given in the form of its minimal polynomial over $\mathbb{Q}$.

§3. Examples

Notations being the same as in §2, we give some numerical examples in <u>Cubic Case</u>. Assume that the discriminant D of K is given. Then we can compute approximate values of the elliptic units η_e of cubic fields with the same discriminant D, using the results of [4], as described in [6]. In particular, if $\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{-3})$, then $K=\mathbb{Q}(\sqrt[3]{m})$, a pure cubic field, and we can determine m in the course of the computation of η_e.

(i) $D=-3\cdot6^2$, $K=\mathbb{Q}(\sqrt[3]{2})$;

$$\eta_e \sim 3.8473.$$

By Lemma,

$$s(\eta_e)=\begin{cases} 3, \\ 4, \end{cases} \text{ resp. } t(\eta_e)\sim\begin{cases} -2.9999, \\ 0.8474, \end{cases}$$

hence $s(\eta_e)=3$ and $t(\eta_e)=-3$. By Proposition 1,

$$B(\eta_e)\sim1.3277,$$

thus

$$h=1, \quad \varepsilon_1=\eta_e : X^3-3X^2-3X-1.$$

(ii) $D=-3\cdot9^2$, $K=\mathbb{Q}(\sqrt[3]{3})$;

$$\eta_e \sim 12.4920.$$

By Lemma,

$$s(\eta_e)=12, \qquad t(\eta_e)\sim-6.0660,$$

hence $t(\eta_e)=-6$. By Proposition 1,

$$B(\eta_e)\sim1.8925,$$

thus

$$h=1, \quad \varepsilon_1=\eta_e : X^3-12X^2-6X-1.$$

(iii) $D=-3 \cdot 10^2$, $K=\mathbb{Q}(\sqrt[3]{10})$;

$$\eta_e \sim 23.30224706, \quad s(\eta_e)=23, \quad t(\eta_e)=-7, \quad B(\eta_e) \sim 2.23084832,$$

are obtained similarly as above. Let $\xi=\eta_e$ and $\nu=2$, and use Proposition 2, then

$$\varepsilon \sim 4.827240107, \quad s=\begin{cases} 4, \\ 5, \end{cases} \quad \text{resp.} \quad t=\begin{cases} -4, \\ 1, \end{cases}$$

and $r_2(4,-4)=24$, $r_2(5,1)=23$ and $r_2(1,5)=-9$. Hence $\sqrt{\eta_e} \notin K$, and thus

$$h=1, \quad \varepsilon_1=\eta_e:X^3-23X^2-7X-1.$$

(iv) $D=-3 \cdot 14^2$, $K=\mathbb{Q}(\sqrt[3]{28})$;

$$\eta_e \sim 142.8810688, \quad s(\eta_e)=143, \quad t(\eta_e)=17, \quad B(\eta_e) \sim 3.008033956.$$

Similarly as in (iii), we see that $\sqrt{\eta_e} \notin K$. Let $\xi=\eta_e$ and $\nu=3$ in Proposition 2, then

$$\varepsilon \sim 5.22767141, \quad s=\begin{cases} 5, \\ 6, \end{cases} \quad \text{resp.} \quad t=\begin{cases} -1, \\ 4, \end{cases}$$

and $r_3(5,-1)=143$, $r_3(-1,5)=17$. Therefore $\sqrt[3]{\eta_e} \in K$, and thus

$$h=3, \quad \varepsilon_1^3=\eta_e, \quad \varepsilon_1:X^3-5X^2-X-1.$$

(v) $D=-3 \cdot 18^2$, then we similarly obtain

(a) $K=\mathbb{Q}(\sqrt[3]{6})$; $h=1$, $\varepsilon_1=\eta_e \sim 326.9908343:X^3-327X^2-3X-1$.

(b) $K=\mathbb{Q}(\sqrt[3]{12})$; $h=1$, $\varepsilon_1=\eta_e \sim 164.9818529:X^3-165X^2-3X-1$.

(vi) $D=-4 \cdot 9^2$, then there is only one cubic field with the discriminant $-4 \cdot 9^2$;

$$\eta_e \sim 57.26225761, \quad B(\eta_e) \sim 2.812497649,$$

$$h=1, \quad \varepsilon_1=\eta_e:X^3-57X^2-15X-1.$$

(vii) $D=-4 \cdot 13^2$, then there is only one field;

$$\eta_e \sim 705.0326250, \quad B(\eta_e) \sim 3.862523967,$$

$$h=3, \quad \varepsilon_1^3=\eta_e:X^3-705X^2-23X-1, \quad \varepsilon_1:X^3-9X^2+X-1.$$

And the discriminant of ε_1 is $-4D$.

References

[1]   E. Artin, Theory of Algebraic Numbers, Lecture Note, Göttingen,
      1959.

[2]   R. Gillard & G. Robert, Groupes d'unités elliptiques, Bull. Soc.
      Math. France, 107 (1979), 305-317.

[3]   G. Gras & M.-N. Gras, Calcul du nombre de classes et des unités
      des extension abéliennes réelles de $\mathbb{Q}$, Bull. Sc. Math. 2e série,
      101 (1977), 97-129.

[4]   H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf
      klassenkörpertheoretischer Grundlage, Math. Zeitschrift, 31
      (1930), 565-582.

[5]   H. W. Leopoldt, Über Einheitengruppe und Klassenzahl reeler
      abelscher Zahlkörper, Abh. Deutsche Akad. Wiss. Berlin, Math.-
      Nat. Kl. 1953 Nr. 2, 48 pp., 1954.

[6]   K. Nakamula, Class number calculation and elliptic unit ——
      I. Cubic case, to appear in Proc. Japan Acad.

[7]   K. Nakamula, Class number calculation and elliptic unit ——
      II. Quartic case, submitted.

[8]   K. Nakamula, On elliptic units and a class number decomposition,
      in preparation.

[9]   G. Robert, Unités élliptiques, Bull. Soc. Math. France, mémoire
      36 (1973), 77 pp.

[10] R. Schertz, Arithmetische Ausdeutung der Klassenzahlformel für
      einfach reelle Kubische Zahlkörper, Abh. Math. Sem. Universität
      Hamburg 41 (1974), 211-223.

[11] R. Schertz, Die Klassenzahl der Teilkörper abelscher Erweitlungen

88

imaginärquadratischer Zahlkörper, I, J.reine angew. Math. 295
(1977), 151-168, II, ibid. 296 (1977), 58-79.

[12] H. M. Stark, Class fields and modular forms of weight one,
"Modular functions of one variable" V (1976, Bonn), 277-288 —
Berlin Heidelberg New York, Springer-Verlag, Lecture Notes in
Mathematics, 601.

Ken NAKAMULA

Department of Mathematics

Tokyo Metropolitan University

2-1-1 Fukazawa, Setagaya

Tokyo, 158 JAPAN