数理解析研究所講究録
440巻 1981年 168-178

On elliptic units and a class number decomposition

By Ken NAKAMULA

Department of Mathematics, Tokyo Metropolitan University

In this note, we study Problems 1 and 3 of our preceding note [4]. Namely, for any abelian extension over an imaginary quadratic field, a decomposition of the class number related to elliptic units is given (Problem 3), and a procedure of calculation of the class number and fundamental units is explained (Problem 1). The full exposition of the results will appear elsewhere with some examples.

Introduction

Let A be a finite abelian group, F be the rational number field $\mathbb{Q}$ or an imaginary quadratic number field, and L be an abelian extension over F with the galois group A. We assume L is real in case $F = \mathbb{Q}$. Further let h be the class number of L.

In case $F = \mathbb{Q}$, H. W. Leopoldt [3] has given a decomposition of h related to cyclotomic units. Based on Leopoldt's decomposition, G. Gras and M.-N. Gras [2] has introduced a method to compute the class number h and fundamental units of L together.

In case F is imaginary quadratic, there are several formulas for h related to elliptic units, see G. Robert [5], R. Schertz [6], R. Gillard and G. Robert [1], and their references. Those formulas, however, are not suitable to apply Gras' algorithm to compute h. This tempts us to seek for a new decomposition of h so that it is more appropriate for Gras' algorithm.

In §1, we give a general decomposition of h, Theorem 1, which includes Leopoldt's decomposition and the formula (3) in [4] as special cases. In §2, we give more explicit formulas in case F is imaginary quadratic. In §3, we explain about Gras' method. In §4, we give the rested problems for the actual calculation of h in case F is imaginary quadratic.

As to the general results, there is no need to distinguish the cases $F = \mathbb{Q}$ and $F \neq \mathbb{Q}$, because they treat about the structure of the group of units of L as a space of integral representation of A, i.e. as a (multiplicative) $\mathbb{Z}[A]$-module, cf. Proposition 2.

Notations

By a number field, we mean a subfield of $\mathbb{C}$ finite degree over $\mathbb{Q}$. For any finite set S, the number of its elements is denoted by #S. The symbol $\phi(\cdot)$ is Euler's function.

Let A be an abelian group of finite order n.

Ψ: the group of ($\mathbb{C}$-irreducible) characters of A.

Λ: the set of $\mathbb{Q}$-irreducible characters of A.

$\Psi^* = \Psi \setminus \{1\}$, $\Lambda^* = \Lambda \setminus \{1\}$.

Let $\lambda \in \Lambda$ and $\psi \in \Psi$. Denote $\psi \in \lambda$ when ψ is a $\mathbb{C}$-irreducible component of λ, i.e. $\lambda = \mathrm{Tr}_{\mathbb{Q}(\psi)/\mathbb{Q}}(\psi)$.

$\tilde{A}_\lambda = \{ a \in A \mid \lambda(a) = \lambda(1) \}$, $A_\lambda = A/\tilde{A}_\lambda$, $n_\lambda = \#A_\lambda$.

$\mathbb{Q}^\lambda$: the n_λ-th cyclotomic field.

d_λ: the absolute discriminant of $\mathbb{Q}^\lambda$.

Let L/F be an abelian extension of number fields with the galois group A.

F_λ: the fixed field of $\tilde{A}_\lambda$.

E (resp. E_λ): the group of units of L (resp. F_λ).

W (resp. W_λ): the torsion part of E (resp. E_λ).

$w = \#W$, $w_\lambda = \#W_\lambda$.

The group ring $\mathbb{Z}[A]$ acts on E as usual and E is regarded as a (multiplicative) $\mathbb{Z}[A]$-module. In particular, E_λ is regarded as a $\mathbb{Z}[A_\lambda]$-module.

§1. General decomposition.

In this section, we assume $F = \mathbb{Q}$, $L \subsetneqq \mathbb{R}$ or F is imaginary quadratic.

Let $\lambda \in \Lambda^*$. We define the group H_λ of proper λ-relative units by

$$H_\lambda = \{ \varepsilon \in E_\lambda \mid N_{F_\lambda/F_{\lambda'}}(\varepsilon) \in W_{\lambda'}, \quad \text{if} \quad \lambda' \in \Lambda,\ F_{\lambda'} \subsetneqq F_\lambda \}.$$

Then H_λ is a $\mathbb{Z}[A_\lambda]$-submodule of E_λ and contains W_λ. Let H be a $\mathbb{Z}[A]$-submodule of E given by

$$(1) \qquad H = W \cdot \prod_{\lambda \in \Lambda^*} H_\lambda$$

and put

$$(2) \qquad Q_A = \sqrt{n^{n-2} / \prod_{\lambda \in \Lambda^*} d_\lambda} \in \mathbb{N} \quad (\text{cf. } [3]).$$

PROPOSITION 1. *The product in (1) is direct modulo W. The quotient H_λ/W_λ is a free abelian group of rank $\phi(n_\lambda)$ for $\lambda \in \Lambda^*$ The index $(E:H)$ is finite and is a divisor of $Q_A w^{n-1}$. The index of any $\mathbb{Z}[A_\lambda]$-submodule, which contains W_λ, of H_λ is given by the absolute norm of an integral ideal of $\mathbb{Q}^\lambda$ for $\lambda \in \Lambda^*$.*

Let R be the regulator of L and h (resp. h_1) be the class number of L (resp. F). We set the following somewhat formal assumption.

ASSUMPTION 1. *For* $\lambda \in \Lambda^*$, *there is a map* $\theta_\lambda : A \longrightarrow \mathbb{C} \setminus \{0\}$ *such that*

$$\theta_\lambda(a)/\theta_\lambda(1) \in E_\lambda, \quad (\theta_\lambda(a)/\theta_\lambda(1))^b = \theta_\lambda(ab)/\theta_\lambda(b)$$

if $a, b \in A_\lambda$. *Further the class number formula*

$$c_L hR = h_1 \prod_{\psi \in \Psi^*} R(\psi)$$

holds with $c_L > 0$, *where*

$$R(\psi) = \left| \sum_{a \in A_\lambda} \psi(a) \log \|\theta_\lambda(a)\| \right| \qquad (\lambda \in \Lambda^*, \ \lambda \ni \psi).$$

The symbol $\|\cdot\| = |\cdot|$ *or* $|\cdot|^2$ *respectively when* $F = \mathbb{Q}$ *or not.*

Define the action of A_λ on $\theta_\lambda(1)$ by

$$\theta_\lambda(1)^a = \theta_\lambda(a) \quad (a \in A_\lambda)$$

and consider the (multiplicative) $\mathbb{Z}[A_\lambda]$-module $\theta_\lambda(1)^{\mathbb{Z}[A_\lambda]}$. Then, for the ideal I_λ of augumentation of $\mathbb{Z}[A_\lambda]$, the image $\theta_\lambda(1)^{I_\lambda}$ is not only a subset but also a $\mathbb{Z}[A_\lambda]$-submodule of E_λ by Assumption 1. Fix a generator $a(\lambda)$ of the cyclic group A_λ and put

$$T_\lambda = \prod_{p | n_\lambda} (a(\lambda)^{n_\lambda/p} - 1) \quad (\in I_\lambda),$$

where p runs through the prime divisors of n_λ. Let the unit

$$\eta_\lambda = \theta_\lambda(1)^{T_\lambda} \quad (\in E_\lambda)$$

and the group

$$\mathbb{E}_\lambda = W_\lambda \cdot \eta_\lambda^{\mathbb{Z}[A_\lambda]}.$$

THEOREM 1. *The assumption and the notation being as above, the group* $\mathbb{E}_\lambda$ *is a finite index* $\mathbb{Z}[A_\lambda]$-*submodule of* H_λ *and is independent of the choice of* $a(\lambda)$ *for each* $\lambda \in \Lambda^*$. *It holds that*

$$c_L Q_A h = h_1 (E:H) \prod_{\lambda \in \Lambda^*} (H_\lambda : \mathbb{E}_\lambda).$$

The proofs of Proposition 1 and Theorem 1 mostly depend on the property of the $\mathbb{Z}[A]$-module E as in Proposition 2 below. For $\lambda \in \Lambda$, let e_λ be the primitive idempotent

$$e_\lambda = n^{-1} \sum_{a \in A} \lambda(a^{-1}) a$$

of the group ring $\mathbb{Q}[A]$. Let ℓ be the $\mathbb{Z}[A]$-homomorphism

$$\ell : E \longrightarrow \mathbb{R}[A] : \varepsilon \longmapsto \sum_{a \in A} (\log \|\varepsilon^a\|) a^{-1},$$

and M be its image, $M = \ell(E)$.

PROPOSITION 2. <u>The kernel of</u> ℓ <u>is the torsion part</u> W <u>of</u> E, <u>and the image</u> M <u>is free with rank</u> $n-1$ <u>over</u> $\mathbb{Z}$ <u>and is annihilated by the idempotent</u> e_1.

When $F = \mathbb{Q}$, for $\lambda \in \Lambda^*$, let f_λ $(\in \mathbb{N})$ be the conductor for the cyclic extension $\mathbb{Q}_\lambda/\mathbb{Q}$, and put

$$\theta_\lambda(a) = \prod_{x \in S_a} |\sin(\pi x/f_\lambda)| \quad (a \in A_\lambda).$$

Here $S_a = \{ x \in \mathbb{Z} \mid 0 < x < f_\lambda/2,\ (x, f_\lambda) = 1,\ \left(\frac{\mathbb{Q}^{(f_\lambda)}/\mathbb{Q}}{x}\right)\Big|_{\mathbb{Q}_\lambda} = a \}$ for $a \in A_\lambda$, and $\left(\frac{\mathbb{Q}^{(m)}/\mathbb{Q}}{\cdot}\right)$ is Artin's symbol for the m-th cyclotomic field $\mathbb{Q}^{(m)}$. Then Assumption 1 is verified and Satz 21 in Leopoldt [3] is obtained as a corollary of Theorem 1 ($c_L = h_1 = 1$).

§2. Explicit decomposition.

In this section, we assume F is imaginary quadratic.

To obtain an explicit decomposition of the class number h of L, it is enough to find the maps θ_λ $(\lambda \in \Lambda^*)$ which satisfy Assumption 1.

For $\lambda \in \Lambda^*$, let $\mathfrak{f}_\lambda$ be the conductor (an integral ideal of F) for the extension F_λ/F, f_λ be the smallest positive integer in $\mathfrak{f}_\lambda$, and C_λ be the ray class group modulo $\mathfrak{f}_\lambda$ in F. Then there exists a canonical surjection $\sigma_\lambda : C_\lambda \longrightarrow A_\lambda$, Artin's map. We define the map θ_λ by

$$\theta_\lambda(a) = \begin{cases} \prod_{c \in \sigma_\lambda^{-1}(a)} \phi_{\mathfrak{f}_\lambda}(c) & \text{if } f_\lambda \neq 1 \\ \prod_{c \in \sigma_\lambda^{-1}(a)} \delta(c) & \text{if } f_\lambda = 1 \end{cases} \qquad (a \in A_\lambda).$$

Here $\phi_{\mathfrak{f}_\lambda}(c)$ is the Ramachandra-Robert class invariant and $\delta(c)$ is the Siegel class invariant defined as follows, see [5]. Let t and z be complex variables with $\mathrm{Im}(z) > 0$, and let $\hat{e}(t) = \exp(2\pi\sqrt{-1}t)$. Put

$$\phi(t,z) = 2\hat{e}\left(\frac{z}{12}+\frac{t(t-\bar{t})}{2(z-\bar{z})}\right)\sin(\pi t)\prod_{k=1}^{\infty}(1-2\cos(\pi t)\hat{e}(kt)+\hat{e}(2kt)),$$

$$\eta(z) = \hat{e}(z/24)\prod_{k=1}^{\infty}(1-\hat{e}(kz)).$$

For $c \in C_\lambda$, take an ideal $\mathfrak{a}$ of F such that $\mathfrak{a}^{-1}\mathfrak{f}_\lambda$ is an integral ideal which belongs to c, and choose a $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2\}$ of $\mathfrak{a}$ so that $\mathrm{Im}(\alpha_1/\alpha_2) > 0$. When $f_\lambda \neq 1$, the invariant is given by

$$\phi_{\mathfrak{f}_\lambda}(c) = \phi(1/\alpha_2, \alpha_1/\alpha_2)^{12f_\lambda}.$$

When $f_\lambda = 1$, further choose an element α of F such that $\mathfrak{a}^{h_1} = (\alpha)$. Then the invariant is given by

$$\delta(c) = \alpha^{12}(\alpha_2^{-1}\eta(\alpha_1/\alpha_2)^2)^{12h_1}.$$

THEOREM 2 (Siegel-Ramachandra-Robert). <u>The above defined</u> θ_λ $(\lambda \in \Lambda^*)$ <u>satisfy</u> Assumption 1 <u>with</u>

$$c_L = w^{-1}w_1 \prod_{\lambda \in \Lambda^*} k_\lambda^{\phi(n_\lambda)},$$

$$k_\lambda = \begin{cases} 12f_\lambda \#(W_1 \cap (1+\mathfrak{f}_\lambda)) & \underline{\text{if}}\ f_\lambda \neq 1, \\ 12h_1w_1 & \underline{\text{otherwise}}. \end{cases}$$

By Theorems 1 and 2, an explicit decomposition of h is given.

This decomposition enables us to compute h by Gras' method, because the generating elliptic units η_λ $(\lambda \in \Lambda^*)$ are numerically known, see §3.

We keep the assumption that θ_λ $(\lambda \in \Lambda^*)$ are given as above. If we do not require the explicitness of generating elliptic units, we have a better formula for h than is obtained from Theorems 1 and 2. Indeed, the w_λ-th power of the $\theta_\lambda(a)$ is the $12f_\lambda \#(W_1 \cap (1+\mathfrak{f}_\lambda))$-th power of an integer of F_λ by Stark [7] when $f_\lambda \neq 1$, and $\theta_\lambda(a)/\theta_\lambda(1)$ is the $2(h_1/n_\lambda)$-th power of a unit of F_λ by Robert [5] when $f_\lambda = 1$. Therefore we have the following theorem.

THEOREM 3. <u>For</u> $\lambda \in \Lambda^*$, <u>there exists a</u> λ-<u>relative unit</u> η'_λ, <u>which is expressed by the values of ellptic modular functions, such that the principally generated</u> $\mathbb{Z}[A_\lambda]$-<u>module</u> $\mathbb{E}'_\lambda = W_\lambda \cdot \eta'^{\,\mathbb{Z}[A_\lambda]}_\lambda$ <u>is finite index in</u> H_λ. <u>If we put</u>

$$c'_L = w^{-1} w_1 \prod_{\lambda \in \Lambda^*} k'^{\,\phi(n_\lambda)}_\lambda,$$

$$k'_\lambda = \begin{cases} w_\lambda & \text{if } f_\lambda \neq 1, \\ 12n_\lambda & \text{if } f_\lambda = 1, \end{cases}$$

<u>we have the decomposition</u>

$$c'_L Q_A h = (E:H) \prod_{\lambda \in \Lambda^*} (H_\lambda : \mathbb{E}'_\lambda)$$

<u>of the class number</u> h.

We assume now that L/F is a <u>ring class field</u> extension. Then we have another explicit formula, though we do not give it here. Namely, we have another $\{ \theta_\lambda \mid \lambda \in \Lambda^* \}$ which satisfy Assumption 1 by Schertz [6]. As a special case, we obtain the following formula.

PROPOSITION 3 (Schertz). Assume $L/\mathbb{Q}$ is a dihedral extension of degree $2p$ with an odd prime number p. Then

$$h = h_1(E:\pm\eta^{\mathbb{Z}[A]})$$

with a unit η which is given explicitly by the values of the Dedekind eta-function $\eta(z)$.

§3. General method of calculation of h.

We assume here $F = \mathbb{Q}$, $L \subsetneqq \mathbb{R}$ or F is imaginary quadratic. We let θ_λ $(\lambda \in \Lambda^*)$ to satisfy Assumption 1, and use the same notation as in §1.

General procedure of calculation of h and fundamental units of L are as follows (Gras' method):

I. Calculate approximate values of the units η_λ^a $(\lambda \in \Lambda^*,\ a \in A_\lambda)$.

II. Decide the minimal polynomials of η_λ^a $(\lambda \in \Lambda^*,\ a \in A_\lambda)$ over F from their approximate values.

III. Determine a set of generators of H_λ in the form of their minimal polynomials over F. At the same time, calculate the index $(H_\lambda : \mathbb{E}_\lambda)$.

IV. Determine a set of fundamental units of L in the form of their minimal polynomials over F. At the same time, calculate the index $(E:H)$.

In the step III, we can calculate an upper bound of $(H_\lambda : \mathbb{E}_\lambda)$ from approximate values of η_λ^a $(a \in A_\lambda)$, and so the algorithm is effective. In the step IV, we know an upper bound $Q_A w^{n-1}$ of $(E:H)$, so it is also effective, see Proposition 1. Therefore, if we can calculate the values η_λ^a $(\lambda \in \Lambda^*,\ a \in A_\lambda)$ as exact as is desired, there is an effective way of calculation of h and E at a time.

The above explained procedure is mostly the same as in Gras-Gras [2] even in case F is imaginary quadratic, so see it more in detail. We have an improvement of Gras' method itself due to the fundamental theorem of symmetric polynomials, so we need less exactness of approximate values of the units η_λ^a than before. It is remarkable that the algorithm goes only by arithmetic of the integers in the ground field F. We also note that H_λ is ismorphic to a fractional ideal of the cyclotomic field $\mathbb{Q}^\lambda$ and the property is utilized in the step III, see Proposition 1. Moreover the property that $F_\lambda = F(\varepsilon)$ if $\varepsilon \in H_\lambda$, $\varepsilon \notin H_\lambda$, enables the step III. Of course the step IV is possible by the reason that H is decomposed in the direct product modulo W as in (1), see Proposition 1.

§4. Actual calculation.

We assume here F is imaginary quadratic.

In this case, the actual calculation of h is more complicated than absolutely abelian case. The most difficult problem exists in the step I of §3.

We start the calculation assuming that the ground field F, the galois group A and the conductor $\mathfrak{f}$ of L/F, are given. Then h_1 can be computed as usual and Q_A in (2) is easily known. Further let θ_λ $(\lambda \in \Lambda^*)$ be given as in §2. Then the constant c_L is not so difficult to compute. Therefore, the crucial problem is to obtain very good approximate values of the elliptic units η_λ^a $(\lambda \in \Lambda^*, a \in A_\lambda)$. If we use $\theta_\lambda (\lambda \in \Lambda^*)$ as in §2, the problem is formulated as in the following.

By class field theory, we may consider in stead of L the corresponding subgroup U of the ray class group modulo $\mathfrak{f}$ in F.

There are a finite number of such U for a given triple $(F, A, \mathfrak{f})$.

PROBLEM 4. Find an effective way of calculation of explicit representatives of every such U and its factor group so that $\theta_\lambda(a)$ in §2 are represented explicitly by using them.

After we have solved Problem 4, we should solve

PROBLEM 5. Find good estimations of the functions which appear in the definition of $\theta_\lambda(a)$ in §2 so that the elliptic units η_λ^a are computable as exact as is desired.

These two problems can be solved at least "theoretically". But the solutions are not sufficiently good yet in order to carry out efficient calculation of h and E, for example to make tables of them. The rested problem is, therefore, to do a systematical treatment of making tables by ellectric computers, or to solve Problems 4 and 5 in case the degree n is small so that Gras' algorithm becomes "effective" and "efficient".

We mention that, if all these problems are solved, Problem 2 in [4] is partly solved, because Problem 1 and Problem 2 are closely connected with each other.

References

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

[2] G. Gras & M.-N. Gras, Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\mathbb{Q}$, Bull. Sc.

Math. 2e série, 101 (1977), 97-129.

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

4 K. Nakamula, Elliptic unit and class number calculation, RIMS Kokyuroku 411(1981), 88-98.

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

6 R. Schertz, Die Klassenzahl der Teilkörper abelscher Erweitelungen imaginärquadratischer Zahlkörper, I, J. reine angew. Math. 295 (1977), 151-168.

7 H. M. Stark, L-functions at s = 1, IV, Advances in Math. 35 (1980), 197-235.

Ken NAKAMULA
Department of Mathematics
Tokyo Metropolitan University
2-1-1 Fukazawa, Setagaya
Tokyo, 158 JAPAN