J. Math. Soc. Japan
Vol. 37, No. 2, 1985

# Calculation of the class numbers and fundamental units of abelian extensions over imaginary quadratic fields from approximate values of elliptic units

By Ken NAKAMULA

(Received Dec. 28, 1981)
(Revised May 11, 1984)

## §0. Introduction.

**0.1.** Any number field we consider is a finite extension of the rational number field $\boldsymbol{Q}$ in the complex number field $\boldsymbol{C}$.

Let $L/F$ be an abelian extension of number fields. For $L$, denote its class number by $h$ and its group of units by $E$. We restrict our study to either of the following cases:

CASE 1. *$F=\boldsymbol{Q}$ and $L$ is contained in the real number field $\boldsymbol{R}$.*

CASE 2. *$F$ is an imaginary quadratic number field.*

In this paper, we give a general procedure to calculate $h$ and to find together fundamental units of $L$. We first connect $h$ to a finite index subgroup $\boldsymbol{E}$ of $E$ by an index formula of the form $h=c(E:\boldsymbol{E})$ (Theorem 2 below). Hence $c$ $(\in\boldsymbol{Q})$ is rather easy to know and $\boldsymbol{E}$ is generated by cyclotomic (Case 1) or so called *elliptic* (Case 2) units. The process to decide $(E:\boldsymbol{E})$ starts from the generators of $\boldsymbol{E}$, and ends at a free basis of $E$ (Algorithm 4 below). Thus $h$ and, at a time, fundamental units are obtained. To make the process effective, an upper bound of $(E:\boldsymbol{E})$ should be known beforehand. So we majorize $(E:\boldsymbol{E})$ by using the generators of $\boldsymbol{E}$ (Theorem 3).

Our method will be computer implementable, though we do not discuss it in detail. What we emphasize is that the classical (explicit) theory of cyclotomic fields or complex multiplication offers us a new general way of calculating $h$ and $E$ as above.

We are mainly interested in Case 2. Because, in Case 1, our formula for $h$ is that of Leopoldt [**14**] and the principle of calculation is the same as in Gras-Gras [**6**]. Investigating Case 1 together, we improve Gras-Gras's method itself. In Case 2, an analogy of Leopoldt's formula has been given by Schertz [**24**, I] or Gillard-Robert [**5**], which, however, has not taken Gras-Gras's method into account. This tempts us to prove a more appropriate analogy of Leopoldt's formula as in Theorem 2.

**0.2.** We state the main results, preparing the notation. The symbol $\sharp S$ denotes the number of elements of a finite set $S$.

For the abelian extension $L/F$, we let $A$ be the galois group with $n=\sharp A=[L:F]$ ($>1$) and $\Lambda$ be the set of $\boldsymbol{Q}$-irreducible characters of $A$. It is known that there is a canonical bijection $\lambda\mapsto F_\lambda$ from $\Lambda$ to the set of cyclic subextensions of $L/F$. Denote the torsion part of $E$ by $W$. For each $\lambda\in\Lambda$, we consider the group $H_\lambda$ of proper $\lambda$-relative units, which is an $A$-subgroup of $E_\lambda=E\cap F_\lambda$ containing $W_\lambda=W\cap F_\lambda$, see (17) in § 2. Put $\Lambda^*=\Lambda\setminus\{1\}$. Denoting by $H$ the product of $H_\lambda$ ($\lambda\in\Lambda^*$) and $W$, we shall see that the product is direct modulo $W$, that $E^n\subset H$ and that $(E:H)$ divides $Q_A w^{n-1}$. Here $w=\sharp W$ and $Q_A$ is the *Grenzindex* in [**14**]. For every $\lambda\in\Lambda^*$, a cyclotomic or an elliptic unit $\eta_\lambda\in H_\lambda$, $\eta_\lambda\notin W_\lambda$, will be defined explicitly so that a finite index subgroup $\boldsymbol{E}_\lambda$ of $H_\lambda$ will be generated by $\eta_\lambda{}^a$ ($a\in A$) and $W_\lambda$. So $(E:\boldsymbol{E})<\infty$, where $\boldsymbol{E}$ is the product of $\boldsymbol{E}_\lambda$ ($\lambda\in\Lambda^*$) and $W$. We can express this as $c_L Q_A h=h_1(E:\boldsymbol{E})$ with the class number $h_1$ of $F$ and a certain $c_L\in\boldsymbol{Q}$, $c_L>0$, or exactly state

THEOREM 2. *The notation being as above, one has*

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

We shall see that $c_L$ is a simple natural number, see Propositions 8, 9 (and Theorem 4). To decide $(E:\boldsymbol{E})$, putting $Y=\{\eta_\lambda{}^a\,|\,\lambda\in\Lambda^*,\ a\in A\}$, we use

ALGORITHM 4. (See § 3, as to an actual procedure.) *Assume that an upper bound of* $(E:\boldsymbol{E})$ *is given and that every unit in* $Y$ *is known approximately with precision good enough. Then the index* $(E:\boldsymbol{E})$ *can be decided, finding together a set* $Z$ *of fundamental units of* $L$. *Each* $\varepsilon\in Z$ *is obtained as a pair* $(P_\varepsilon, \varepsilon')$, *where* $P_\varepsilon$ *is the minimal polynomial of* $\varepsilon$ *over* $F$ *and* $\varepsilon'\in\boldsymbol{C}$ *is given closer to* $\varepsilon$ *than to other zeros of* $P_\varepsilon$ *as in* (31).

We shall majorize $(E:\boldsymbol{E})$ by an explicit function of the units in $Y$ and of other simpler invariants for $L/F$. Any unit in $Y$ is numerically known by arithmetic of $F$ and by evaluating certain well-known functions. So, the assumption in Algorithm 4 is satisfied. The essential technique utilized in Algorithm 4 is a simple application of the fundamental theorem on symmetric functions. The fact that the ring of integers of $F$ is discrete in $\boldsymbol{C}$ enables us to execute Algorithm 4 only using approximate values of the units in $Y$. Consequently, all that is needed is to compute exactly in $F$ and approximately in $\boldsymbol{C}$. No usual geometric method is employed to find $Z$. It is not necessary to know any integral basis of $L$.

For each $\lambda\in\Lambda^*$, we have another way to decide $(H_\lambda:\boldsymbol{E}_\lambda)$ and to find a free basis of $H_\lambda$, which further requires some arithmetic of a cyclotomic field, see Algorithm 3 in § 3. After that, we can apply Algorithm 4, to decide $(E:H)$.

This way seems to be more efficient, and the idea has been given in [**6**], although there was some ambiguity as an algorithm. Utilizing symmetric functions, we dissolve the ambiguity and also generalize the method to apply to non-galois extensions of $F$. A few examples of non-galois extensions of $\boldsymbol{Q}$ have been studied in [**17**], [**20**], based on the formulas of Schertz [**24**, II].

**0.3.** An interpretation of classical theorems on units as in Proposition 1 below is fundamental for our general discussion and will be often used without any specification.

The group ring $\boldsymbol{Z}[A]$ over the ring $\boldsymbol{Z}$ of rational intergers acts canonically on $E$, so $E$ is a (multiplicative) $\boldsymbol{Z}[A]$-module. Then we have the $\boldsymbol{Z}[A]$-homomorphism

$$l : E \longrightarrow \boldsymbol{R}[A]\,; \quad \varepsilon \longmapsto \sum_{a\in A} \log(\|\varepsilon^{a}\|)\cdot a^{-1}\,, \tag{1}$$

where $\|z\|=|z|$ in Case 1 and $\|z\|=|z|^2$ in Case 2. We regard $\boldsymbol{R}[A]$ as an euclidean space, introducing an inner product $\langle x, y\rangle$ ($x, y\in\boldsymbol{R}[A]$) so that $A$ is an ortho-normal basis of $\boldsymbol{R}[A]$. For an order $\mathfrak{o}'$ of $\boldsymbol{Q}[A]e'$ with an idempotent $e'$ of $\boldsymbol{Q}[A]$, by an *$\mathfrak{o}'$-lattice* (in $\boldsymbol{R}\mathfrak{o}'$) we mean a discrete $\mathfrak{o}'$-submodule of $\boldsymbol{R}[A]$ spanning $\boldsymbol{R}\mathfrak{o}'$ over $\boldsymbol{R}$. Let $e_1$ denote the primitive idempotent of $\boldsymbol{Q}[A]$ associated with the trivial character of $A$, and put

$$e=1-e_1\,, \qquad \mathfrak{o}_e=\boldsymbol{Z}[A]e\,, \qquad V=\boldsymbol{R}[A]e\,. \tag{2}$$

Dirichlet's theorem and Kronecker's theorem are now expressed as

PROPOSITION 1. *The image $l(E)$ is an $\mathfrak{o}_e$-lattice in $V$, and the kernel* Ker$(l)$ *is the torsion part $W$ of $E$.*

In § 1, we summarize some properties of $\mathfrak{o}_e$-lattices (in $V$). In § 2, we prove Theorem 2 and majorize $(E : \boldsymbol{E})$ under a formal condition. In § 3, we fully describe Algorithms 3, 4. We devote § 4-§ 5 to studying actual calculation in some detail, restricting ourselves to Case 2. In particular, in § 4, we give explicit elliptic units which satisfy the formal condition in § 2 and the assumption in Algorithm 4; in § 5, we give numerical examples. As to a summary of this paper, see the reports [**18**], [**19**].

## § 1. Preliminaries.

Let $A$, $\Lambda$, $\Lambda^*$ be as in § 0.2 with $n=\sharp A>1$, and $e$, $\mathfrak{o}_e$, $V$ be given by (2). Denote by $\Psi$ the group of $\boldsymbol{C}$-irreducible characters of $A$. We imply by $\psi|\lambda$ that $\lambda$ is the sum of the $\boldsymbol{Q}$-conjugates of $\psi$ with $\psi\in\Psi$, $\lambda\in\Lambda$. Any character of $A$ is extended linearly on $\boldsymbol{C}[A]$. If not specified, operations are considered in $\boldsymbol{C}[A]$.

**1.1.** With each $\lambda\in\Lambda$, we associate the primitive idempotent $e_\lambda$ of $\boldsymbol{Q}[A]$. If

$\mathfrak{o}$ is the maximal order of $\boldsymbol{Q}[A]e$, we have the next well-known direct sum decomposition

$$\mathfrak{o}=\bigoplus_{\lambda\in A^*}\mathfrak{o}_\lambda\,; \qquad \mathfrak{a}_\lambda:=\mathfrak{o}e_\lambda=\boldsymbol{Z}[A]e_\lambda \quad (\lambda\in A^*).$$

For every $\lambda\in A^*$, there are the $\lambda(1)$ (conjugate) isomorphisms

$$\phi\ :\ \boldsymbol{Q}[A]e_\lambda \xrightarrow{\cong} \boldsymbol{Q}^\lambda:=\boldsymbol{Q}(\phi) \qquad (\phi\,|\,\lambda), \tag{3}$$

which map $\mathfrak{o}_\lambda$ onto the ring of integers of the value field $\boldsymbol{Q}^\lambda$. We denote the absolute value of the discriminant of the cyclotomic field $\boldsymbol{Q}^\lambda$ by $d_\lambda$. The *Grenzindex* $Q_A$ of [14] is then expressed as

$$Q_A=(\mathfrak{o}:\mathfrak{o}_e)=\sqrt{n^{n-2}/\prod_{\lambda\in A^*}d_\lambda}\,. \tag{4}$$

We also mention the direct sum decompositions

$$\boldsymbol{R}[A]=V_1\oplus V\,, \qquad V=\bigoplus_{\lambda\in A^*}V_\lambda\,; \quad V_\lambda:=\boldsymbol{R}[A]e_\lambda \quad (\lambda\in A). \tag{5}$$

Let us take an $\mathfrak{o}_e$-lattice $M$ in $V$. We have the maximum $\mathfrak{o}$-module $\tilde{M}$ contained in $M$, and that is given by the direct sum

$$\tilde{M}=\bigoplus_{\lambda\in A^*}M^\lambda\,; \qquad M^\lambda:=M\cap V_\lambda=\{x\in M\,|\,e_\lambda x=x\} \quad (\lambda\in A^*). \tag{6}$$

Regarding the dual $M^*:=\mathrm{Hom}_{\boldsymbol{Z}}(M, \boldsymbol{Z})$ as an $\mathfrak{o}_e$-module by

$$(zg)(x)=g(zx) \qquad (z\in\mathfrak{o}_e,\ g\in M^*,\ x\in M),$$

Fröhlich [3], Theorem 4 and (7.2), has proved

PROPOSITION 2. *The index $(M:\tilde{M})$ divides $Q_A$; and $(M:\tilde{M})=Q_A$ holds if and only if $M^*$ is $\mathfrak{o}_e$-projective.*

REMARK 1. The sentence just below (9*) of [14], §5.3, requires a modification. Indeed, when $a^2=1$ for all $a\in A$, not $(M:\tilde{M})=Q_A$ but $2^{n-1}n^{-1}(M:\tilde{M})=Q_A$ holds if $M$ is $\boldsymbol{Z}[A]$-principal.

REMARK 2. Proposition 2 also says that $\tilde{M}$ is an $\mathfrak{o}$-lattice, so each direct summand $M^\lambda$ in (6) is an $\mathfrak{o}_\lambda$-lattice in $V_\lambda$.

For any $\lambda\in A^*$, let now $M_\lambda$ be an $\mathfrak{o}_\lambda$-lattice in $V_\lambda$. Via (3), $M_\lambda$ is operator isomorphic to a non-zero ideal of $\boldsymbol{Q}^\lambda$. If $N_\lambda$ is a non-zero $\boldsymbol{Z}[A]$-submodule of $M_\lambda$, then $N_\lambda$ is an $\mathfrak{o}_\lambda$-lattice, and we can define an ideal $\mathfrak{J}$ of the Dedekind domain $\mathfrak{o}_\lambda$ by its inverse

$$\mathfrak{J}^{-1}=\{x\in\boldsymbol{Q}[A]e_\lambda\,|\,xN_\lambda\subset M_\lambda\} \tag{7}$$

so that the index is its absolute norm:

$$(8) \qquad (M_\lambda : N_\lambda) = \mathrm{N}(\phi(\mathcal{J})) \quad (\phi|\lambda)\,.$$

For every prime number $p$, take a prime ideal $\mathfrak{p}$ of $\boldsymbol{Q}^\lambda$ above $p$, let $\mathrm{N}(\mathfrak{p}) = p^s$ with $s \in \boldsymbol{Z}$, $s > 0$, and choose an integer $\alpha \in p\mathfrak{p}^{-1}$ such that $\alpha p^{-1}\mathfrak{p}$ is an (integral) ideal prime to $\mathfrak{p}$. If $\phi|\lambda$, we decide an $x_\phi \in \mathfrak{o}_\lambda$ by $\phi(x_\phi) = \alpha$. Similar to Proposition IV.2 of [**6**], we have

PROPOSITION 3. *The notation being as above, the following conditions are equivalent with each other:*

(i) *$p$ divides $(M_\lambda : N_\lambda)$.*

(ii) *$p^s$ divides $(M_\lambda : N_\lambda)$.*

(iii) *$x_\phi N_\lambda \subset pM_\lambda$ for some $\phi|\lambda$.*

PROOF. By (8), each of (i), (ii) holds if and only if $\mathfrak{p} \supset \phi(\mathcal{J})$ for some $\phi|\lambda$. The inclusion $\mathfrak{p} \supset \phi(\mathcal{J})$ is equivalent to $p^{-1}x_\phi \in \mathcal{J}^{-1}$ by the choice of $\alpha$, so to $x_\phi N_\lambda \subset pM_\lambda$ by (7). Thus we complete the proof.

REMARK 3. When (iii) above holds, the $p$-parts of $p^{-s}(M_\lambda : N_\lambda)$ and $(M_\lambda : p^{-1}x_\phi N_\lambda)$ are the same. If we further define an ideal $\mathcal{P}_\phi$ of $\mathfrak{o}_\lambda$ by $\phi(\mathcal{P}_\phi) = \mathfrak{p}$, the $\mathfrak{o}_\lambda$-lattice $\mathcal{P}_\phi{}^{-1}N_\lambda$ is contained in $M_\lambda$ of index exactly $p^{-s}(M_\lambda : N_\lambda)$.

REMARK 4. In case $\mathfrak{p}$ is principal, if we assume $(\alpha) = p\mathfrak{p}^{-1}$, then $p^{-1}x_\phi N_\lambda = \mathcal{P}_\phi{}^{-1}N_\lambda$ in Remark 3.

**1.2.** Let $e_\phi \in \boldsymbol{C}[A]$ be the primitive idempotent associated with each $\phi \in \Psi$. Extend the inner product $\langle x, y\rangle$ in § 0.3 as a hermitian product on $\boldsymbol{C}[A]$. Then not only $A$ but the set $\{\sqrt{n}e_\phi | \phi \in \Psi\}$ is an ortho-normal basis, so the decompositions in (5) are orthogonal.

If $m(M)$ denotes the volume of a fundamental domain in $V$ for the $\mathfrak{o}_e$-lattice $M$ in § 1.1, it is easy to see that

$$(9) \qquad m(M) = \sqrt{n}\,|\det(\langle x_i, a\rangle)_{1 \leq i < n,\, 1 \neq a \in A}|$$

with any $\boldsymbol{Z}$-basis $\{x_i\}_{i=1}^{n-1}$ of $M$. When $M$ is an $\mathfrak{o}$-lattice, then $M = \tilde{M}$ in (6), so the orthogonality implies that

$$(10) \qquad m(M) = \prod_{\lambda \in A^*} m_\lambda(M^\lambda)\,,$$

where $m_\lambda(M^\lambda)$ is the volume of a fundamental domain in $V_\lambda$ for $M^\lambda$, see Remark 2. Relative to a $\boldsymbol{Z}$-basis $\{a-1 | a \in A\}$ of an $\mathfrak{o}_e$-lattice (the augmentation ideal of $\boldsymbol{Z}[A]$), the fundamental parallelotope $B$ is a convex body of $V$ symmetric with respect to the origin:

$$(11) \qquad B = \{x \in V \mid |\langle x, a\rangle| \leqq 1 \text{ for all } a \in A,\ a \neq 1\}\,.$$

LEMMA 1. *The volume of $B$ in $V$ is $2^{n-1}\sqrt{n}$.*

PROOF. Clear by (9), (11).

Till the end of this section, we fix any $\lambda \in \Lambda^*$. For the $\mathfrak{o}_\lambda$-lattices $M_\lambda$, $N_\lambda$ given in § 1.1, we have

$$(M_\lambda : N_\lambda) = m_\lambda(N_\lambda)/m_\lambda(M_\lambda)\,, \tag{12}$$

where $m_\lambda(M_\lambda)$ or $m_\lambda(N_\lambda)$ is the volume of a fundamental domain in $V_\lambda$ for $M_\lambda$ or $N_\lambda$, respectively. Let $v_\lambda$ $(>0)$ be the volume of a convex body $B^\lambda$ in $V_\lambda$ defined by

$$B^\lambda = B \cap V_\lambda\,, \tag{13}$$

and $d_\lambda$ be the absolute value of the discriminant of $\boldsymbol{Q}^\lambda$. Put

$$u(M_\lambda) = \inf\{\max_{a \in A}(\langle x,\ a\rangle) \mid x \in M_\lambda,\ x \neq 0\}\,. \tag{14}$$

Similar to Proposition II.1 of [**6**], we have

PROPOSITION 4. *Let the notation be as above. Then* $u(M_\lambda)>0$. *For every* $y \in N_\lambda$, $y \neq 0$, *one has*

$$(M_\lambda : N_\lambda) \leqq \frac{\sqrt{d_\lambda}}{v_\lambda} \prod_{\phi \mid \lambda} \frac{2|\phi(y)|}{u(M_\lambda)\sqrt{n}} \leqq \lambda(1)!\sqrt{d_\lambda} \prod_{\phi \mid \lambda} \frac{2|\phi(y)|}{u(M_\lambda)n\sqrt{\pi}}\,.$$

*If* $n=p$, *a prime number, then* $v_\lambda = 2^{p-1}\sqrt{p}$.

PPOOF. The last assertion is a consequence of Lemma 1. Let $x \in M_\lambda$. Then $\max_{a \in A}(\langle x,\ a\rangle) \geqq (n-1)^{-1}\max_{a \in A}(|\langle x,\ a\rangle|)$ since the sum of $\langle x,\ a\rangle$ $(a \in A)$ vanishes. Therefore $u(M_\lambda)>0$ because the discrete module $M_\lambda$ has an element with the smallest positive maximum norm. The inequalities follow from the lemmas below and from (12).

LEMMA 2. $m_\lambda(M_\lambda) \geqq v_\lambda(u(M_\lambda)/2)^{\lambda(1)}$.

LEMMA 3. *For every* $y \in N_\lambda$, $y \neq 0$, *one has*

$$m_\lambda(N_\lambda) \leqq \sqrt{d_\lambda} \prod_{\phi \mid \lambda} \frac{|\phi(y)|}{\sqrt{n}}\,;$$

*the equality holds if and only if* $N_\lambda = \boldsymbol{Z}[A]y$.

LEMMA 4. $v_\lambda \geqq (\sqrt{n\pi})^{\lambda(1)}/\lambda(1)!$.

PROOFS. Lemma 2: Let $t = 2 \cdot {}^{\lambda(1)}\sqrt{m_\lambda(M_\lambda)/v_\lambda} > 0$. Then the convex body $tB^\lambda$, which is symmetric with respect to the origin, has the volume $2^{\lambda(1)}m_\lambda(M_\lambda)$ in $V_\lambda$. By Minkowski's theorem, there exists an $x \in M_\lambda \cap tB^\lambda$, $x \neq 0$. We may suppose $\langle x,\ 1\rangle \leqq 0$, replacing $x$ by $-x$ if necessary. By (11), (13), (14), we see that

$$u(M_\lambda) \leqq \max_{1 \neq a \in A}(\langle x,\ a\rangle) \leqq \max_{1 \neq a \in A}(|\langle x,\ a\rangle|) \leqq t\,.$$

Taking the $\lambda(1)$-th power, we complete the proof.

Lemma 3: Since $\boldsymbol{Z}[A]y=\mathfrak{o}_\lambda y\subset N_\lambda$, it is sufficient to prove the equality for $N_\lambda=\mathfrak{o}_\lambda y$. The linear transformation $V_\lambda\ni x\mapsto yx\in V_\lambda$ has the eigenvalues $\phi(y)$ $(\phi|\lambda)$, so we may only prove

$$m_\lambda(\mathfrak{o}_\lambda)=\sqrt{d_\lambda n^{-\lambda(1)}}. \tag{15}$$

When $\lambda(1)=1$, (15) is clear. Let $\lambda(1)>1$ and put $r=(1/2)\lambda(1)$. Then $r\in\boldsymbol{Z}$. Among the conjugates in (3), we take distinct $\phi_1, \cdots, \phi_r$ which are not complex conjugate with each other. Then the map

$$V_\lambda \longrightarrow \boldsymbol{R}^{\lambda(1)}; \qquad x\longmapsto \sqrt{2/n}\,(\mathrm{Re}\,(\phi_i(x)),\ \mathrm{Im}\,(\phi_i(x)))_{1\leqq i\leqq r} \tag{16}$$

is an isometrical isomorphism from the euclidean space $V_\lambda$ to the real vector space $\boldsymbol{R}^{\lambda(1)}$. Hence we obtain (15) easily, see for example Lemma 2 in [**13**], V, §2. This completes the proof.

Lemma 4: The case $\lambda(1)=1$ is trivial. Let $\lambda(1)>1$. By (11), (13) and by the definition of the inner product, we get

$$B_\lambda:=\left\{x\in V_\lambda\,\middle|\,\sum_{\phi|\lambda}|\phi(x)|\leqq n\right\}\subset B^\lambda.$$

Via (16), the volume of $B_\lambda$ in $V_\lambda$ is $(\sqrt{n\pi})^{\lambda(1)}/\lambda(1)!$, see Lemma 3 in [**13**], V, §3, for example. Thus the inclusion proves Lemma 4.

Remark 5. A general arithmetic expression of $v_\lambda$ is not known yet for a composite $n$, see [**6**], II, 4, (c).

## §2. A decomposition and a majorization of $h$.

Let us now study the abelian extenison $L/F$ in §0. For the galois group $A$, we use the notation in §1. Let $n=[L:F]=\#A>1$. We do not distinguish Cases 1, 2.

**2.1.** We define a group $H$, a $\boldsymbol{Z}[A]$-submodule of the group $E$ of units of $L$ containing the torsion part $W$ of $E$.

For any $\lambda\in\Lambda$, let $\tilde{A}_\lambda=\{a\in A \mid \lambda(a)=\lambda(1)\}$ (a subgroup of $A$), denote the fixed field of $\tilde{A}_\lambda$ by $F_\lambda$ (a cyclic subextension of $L/F$) and put $E_\lambda=E\cap F_\lambda$, $W_\lambda=W\cap F_\lambda$. Define an order relation $\leq$ of $\Lambda$ by

$$\mu\leq\lambda \iff \tilde{A}_\mu\supset\tilde{A}_\lambda \iff F_\mu\subset F_\lambda;$$

and let $\mu<\lambda$ denote that $\mu\leq\lambda$, $\mu\neq\lambda$. For each $\lambda\in\Lambda$, we consider a $\boldsymbol{Z}[A]$-module $H_\lambda$, the group of *proper $\lambda$-relative units*, given by

$$H_\lambda=\{\varepsilon\in E_\lambda \mid \mathrm{N}^\lambda_\mu(\varepsilon)\in W_\mu \text{ for every } \mu<\lambda\}, \tag{17}$$

where $\mathrm{N}^\lambda_\mu$ is the norm from $F_\lambda$ to $F_\mu$. Note that $H_\lambda$ depends only on $F_\lambda/F$. Obviously $F=F_1$ and $E_1=H_1=W_1$. Taking the product for all non-trivial $\boldsymbol{Q}$-rational characters, we set

$$H=W\cdot\prod_{\lambda\in\Lambda^*}H_\lambda\,. \tag{18}$$

We also consider, for the image $M=l(E)$ via $l$ in (1), the inverse images $\tilde{E}$, $E^\lambda$ of $\tilde{M}$, $M^\lambda$ in (6):

$$\tilde{E}=\prod_{\lambda\in\Lambda^*}E^\lambda\,;\qquad E^\lambda=\{\varepsilon\in E\mid e_\lambda l(\varepsilon)=l(\varepsilon)\}\quad(\lambda\in\Lambda^*)\,. \tag{19}$$

The product in (19) is therefore direct modulo $W$.

To see the difference of $\tilde{E}$ and $H$, for any $\lambda\in\Lambda$, we let

$$x_\lambda=\sum_{a\in\tilde{A}_\lambda}a\quad\text{in }\boldsymbol{Z}[A]\,,\qquad \tilde{e}_\lambda=\sum_{\mu\leq\lambda}e_\mu\quad\text{in }\boldsymbol{Q}[A]\,,$$

put $n(\lambda)=(A:\tilde{A}_\lambda)=[F_\lambda:F]$ and prove

LEMMA 5. *Let $\mu$, $\lambda\in\Lambda$ and $x\in\boldsymbol{C}[A]$. Then*

$$ax=x\ \text{for all}\ a\in\tilde{A}_\lambda\iff\tilde{e}_\lambda x=x\,; \tag{20}$$

$$x_\lambda e_\mu=\begin{cases}\dfrac{n}{n(\lambda)}e_\mu & \text{if }\mu\leq\lambda\,,\\[2ex] 0 & \text{otherwise.}\end{cases} \tag{21}$$

PROOF. Obviously $\tilde{e}_\lambda x\neq x$ if and only if $e_\psi x\neq0$ for some $\psi\in\Psi$ with $\psi(A_\lambda)\neq1$. So (20) follows easily. Since $\tilde{e}_\lambda e_\mu=e_\mu$ $(\mu\leq\lambda)$ and $ax_\lambda=x_\lambda$ $(a\in\tilde{A}_\lambda)$, we obtain (21) on account of (20).

THEOREM 1. *Let $\lambda\in\Lambda^*$ and $w=\#W$. Then*

$$(E^\lambda)^w\subset E_\lambda\cap E^\lambda=H_\lambda\ (\subset E^\lambda)\,.$$

*Particularly, $l(H_\lambda)$ is an $\mathfrak{o}_\lambda$-lattice in $V_\lambda$.*

PROOF. Let $\varepsilon\in E^\lambda$. If $a\in\tilde{A}_\lambda$, then $al(\varepsilon)=l(\varepsilon)$ by (19), (20), therefore $\varepsilon^{a-1}\in W$, hence $(\varepsilon^w)^a=\varepsilon^w$. This proves $(E^\lambda)^w\subset F_\lambda$, so $(E^\lambda)^w\subset E_\lambda\cap E^\lambda$. Next let $\varepsilon\in E_\lambda$. For any $\mu<\lambda$, we see that $\mathrm{N}^\lambda_\mu(\varepsilon)\in W_\mu$ if and only if $l(\mathrm{N}^\lambda_\mu(\varepsilon))=(n(\lambda)/n)x_\mu l(\varepsilon)=0$, while (20), (21) show that

$$x_\mu l(\varepsilon)=x_\mu\tilde{e}_\lambda l(\varepsilon)=\frac{n}{n(\mu)}\tilde{e}_\mu l(\varepsilon)\,.$$

Therefore $\varepsilon\in H_\lambda$ if and only if $e_\mu l(\varepsilon)=0$ for all $\mu<\lambda$, or, by (20) again, if and only if $e_\lambda l(\varepsilon)=l(\varepsilon)$. This proves $H_\lambda=E_\lambda\cap E^\lambda$ on account of (19). The last assertion now follows from what we have studied in § 1.1 since $H_\lambda$ is a finite index $A$-subgroup of $E^\lambda$.

COROLLARY 1. *The product in* (18) *is direct modulo $W$. If $Q_A$ is as in* (4), *then $(E:H)$ divides $Q_A w^{n-1}$. Moreover $E^n \subset H$.*

PROOF. The first assertion is trivial as the product in (19) is direct modulo $W$. The second assertion directly follows from Proposition 2 and Theorem 1. If $\lambda \in \Lambda^*$, then $ne_\lambda \in \boldsymbol{Z}[A]$, therefore $\varepsilon^{(ne_\lambda)} \in E_\lambda \cap E^\lambda$ $(\varepsilon \in E)$ by (19), (20). So the product $E^n$ of $E^{(ne_\lambda)}$ $(\lambda \in \Lambda^*)$ is contained in $H$ by Theorem 1 and by (18).

REMARK 6. If $n=p$, a prime number, obviously $E=H$ and $Q_A=1$.

REMARK 7. In Case 1, we have $(E^\lambda : H_\lambda) \leqq 2$ $(\lambda \in \Lambda^*)$ by [**14**], §6.

**2.2.** We give an index formula for the class number $h$ of $L$ under a formal condition, which is always satisfied as will be seen in §4.

For each $\lambda \in \Lambda$, we put $A_\lambda = A/\tilde{A}_\lambda$, which we regard as the galois group of $F_\lambda/F$, then $E_\lambda$, $H_\lambda$, $W_\lambda$ are $\boldsymbol{Z}[A_\lambda]$-modules. If $\psi | \lambda$, we consider $\psi$ as a character of $A_\lambda$. Set $\boldsymbol{C}^\times = \boldsymbol{C} \setminus \{0\}$. For any $z \in \boldsymbol{C}$, we denote $\|z\| = |z|$ or $|z|^2$ respectively in Case 1 or 2.

Assume that, for each $\lambda \in \Lambda^*$, there is a map

$$\text{(C0)} \qquad \theta_\lambda :\ A_\lambda \longrightarrow \boldsymbol{C}^\times$$

satisfying (C1), (C2) below:

(C1) *If $a$, $b \in A_\lambda$, then* $\dfrac{\theta_\lambda(a)}{\theta_\lambda(1)} \in E_\lambda$ *and* $\left(\dfrac{\theta_\lambda(a)}{\theta_\lambda(1)}\right)^b = \dfrac{\theta_\lambda(ab)}{\theta_\lambda(b)}$.

(C2) *If $\psi | \lambda$, then $S(\psi) \neq 0$, where* $S(\psi) = \sum_{a \in A_\lambda} \psi(a^{-1}) \log(\|\theta_\lambda(a)\|)$.

Under the conditions (C0)-(C2), the image $\theta_\lambda(A_\lambda)$ generates a subgroup $\Theta_\lambda$ of the multiplicative group $\boldsymbol{C}^\times$. Via the actions

$$\theta_\lambda(a)^b = \theta_\lambda(ab) \qquad (a,\ b \in A_\lambda),$$

we consider $\Theta_\lambda$ as a $\boldsymbol{Z}[A_\lambda]$-module. By (C1), if $\mathcal{J}_\lambda$ denotes the augmentation ideal of $\boldsymbol{Z}[A]$, the subgroup $\Theta_\lambda{}^{\mathcal{J}_\lambda} = \theta_\lambda(1)^{\mathcal{J}_\lambda}$ of $E_\lambda$ is also a $\boldsymbol{Z}[A_\lambda]$-submodule of $E_\lambda$; the operations are compatible. Fixing a generator $a(\lambda)$ of the cyclic group $A_\lambda$, we put

$$T(\lambda) = \prod_{p | n(\lambda)} (a(\lambda)^{n(\lambda)p^{-1}} - 1) \quad (\in \mathcal{J}_\lambda),$$

where $p$ runs through the prime divisors of $n(\lambda) = \# A_\lambda = [F_\lambda : F]$ $(>1)$. Let us define a $\boldsymbol{Z}[A_\lambda]$-submodule $\boldsymbol{E}_\lambda$ of $E_\lambda$ by

$$\text{(22)} \qquad \boldsymbol{E}_\lambda = W_\lambda \cdot \eta_\lambda{}^{\boldsymbol{Z}[A_\lambda]}, \qquad \eta_\lambda = \theta_\lambda(1)^{T(\lambda)} \quad (\in E_\lambda).$$

On the other hand, by (C2), we define a number $c_L > 0$ satisfying

$$\text{(23)} \qquad c_L R h = h_1 \prod_{\lambda \in \Lambda^*} \prod_{\psi | \lambda} |S(\psi)| = h_1 \prod_{\psi \in \Psi^*} |S(\psi)|.$$

Here $R$ is the regulator of $L$, $h_1$ is the class number of $F$, and $\Psi^*=\Psi\setminus\{1\}$. From this formal analytic formula, we obtain

THEOREM 2. *The assumption and the notation being as above, one has $\eta_\lambda\in H_\lambda$, $\eta_\lambda\notin W_\lambda$ for every $\lambda\in\Lambda^*$. If $Q_A$ is as in* (4), *then*

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

*where $\boldsymbol{E}$ is the product of $\boldsymbol{E}_\lambda$ ($\lambda\in\Lambda^*$) and $W$* (*direct modulo $W$*).

PROOF. Let $\lambda\in\Lambda^*$ and suppose $L=F_\lambda$, or equivalently $A=A_\lambda$. As the first assertion is independent of $L$ containing $F_\lambda$, we may prove it under this supposition. From the definition, it is easily verified that

$$l(\eta_\lambda)=T(\lambda)\sum_{a\in A}\log(\|\theta_\lambda(a)\|)\cdot a^{-1}.$$

If $\mu<\lambda$, then $(a^{n(\mu)}-1)e_\mu=0$ by (20), hence $e_\mu T(\lambda)=0$. Therefore $0\neq T(\lambda)\in \boldsymbol{Q}[A]e_\lambda$, which proves $\eta_\lambda\in E^\lambda$ on account of (19), thus $\eta_\lambda\in H_\lambda$ by Theorem 1. Moreover, via (3), we have

$$\psi(l(\eta_\lambda))=\psi(T(\lambda))S(\psi)\qquad\text{with}\quad 0\neq\psi(T(\lambda))\in\boldsymbol{Q}^\lambda\quad(\psi|\lambda),$$

which proves $\eta_\lambda\notin W_\lambda$ on account of (C2). Note that the different of $\boldsymbol{Q}^\lambda$ is the principal ideal generated by $n/\psi(T(\lambda))$ for any $\psi|\lambda$. So, taking the product of the above equalities, we get

$$\prod_{\psi|\lambda}|\psi(l(\eta_\lambda))|=d_\lambda{}^{-1}\prod_{\psi|\lambda}n|S(\psi)|. \tag{24}$$

Removing the assumption $A=A_\lambda$, this remains true as we easily see. By the first assertion just obtained, we can apply the results in § 1 putting $M_\lambda=l(H_\lambda)$ and $N_\lambda=l(\boldsymbol{E}_\lambda)=\boldsymbol{Z}[A]l(\eta_\lambda)$, see also Theorem 1. Thus, by Lemma 3, we can express (24) as

$$(H_\lambda:\boldsymbol{E}_\lambda)=(m_\lambda(M_\lambda)\sqrt{d_\lambda})^{-1}\prod_{\psi|\lambda}\sqrt{n}\,|S(\psi)|, \tag{25}$$

see also (12). While, if we put $M=l(H)$ in § 1, then $m(M)=\sqrt{n}R(E:H)$ by (9), and $\tilde{M}=M$ in (6) with $M^\lambda=l(H_\lambda)=M_\lambda$ ($\lambda\in\Lambda^*$) by Theorem 1. Hence we obtain from (10) that

$$\sqrt{n}R(E:H)=\prod_{\lambda\in\Lambda^*}m_\lambda(M_\lambda).$$

Combining this with (23), (25), we complete the proof.

REMARK 8. Assume $A=A_\lambda$ with some $\lambda\in\Lambda^*$. By the proof above, $T(\lambda)$ is a non-zero element of $\mathfrak{o}_\lambda$ and $l(\boldsymbol{E}_\lambda)$ is an $\mathfrak{o}_\lambda$-lattice of the form $\mathfrak{o}_\lambda T(\lambda)y$. Since $\mathfrak{o}_\lambda T(\lambda)$ is stable under the isomorphisms of $\mathfrak{o}_\lambda$, the group $\boldsymbol{E}_\lambda$ is independent of the choice of $a(\lambda)$. By (21), $\mathrm{N}^\lambda_\mu(\eta_\lambda)=1$ if $\mu<\lambda$. These facts are true even in case $A\neq A_\lambda$.

REMARK 9. Theorems 1, 2 enable us to use the results in §1 for the $\mathfrak{o}_\lambda$-lattices $M_\lambda=l(H_\lambda)$, $N_\lambda=l(\boldsymbol{E}_\lambda)=\boldsymbol{Z}[A]l(\eta_\lambda)$ $(\lambda\in\Lambda^*)$.

**2.3.** Assuming (C0)-(C2), we majorize $(H_\lambda:\boldsymbol{E}_\lambda)$ in Theorem 2.

Let $\lambda\in\Lambda^*$. We define a real number $\kappa_\lambda\geqq 1$ by

$$\kappa_\lambda=\inf\{\max_{a\in A}(\|\varepsilon^a\|)\mid \varepsilon\in H_\lambda,\ \varepsilon\notin W_\lambda\}, \tag{26}$$

which depends only on $F_\lambda/F$. Then we have

THEOREM 3. *The strict inequality $\kappa_\lambda>1$ holds. Under the conditions* (C0)-(C2), *let $\boldsymbol{E}_\lambda$ be given by* (22). *Then*

$$(H_\lambda:\boldsymbol{E}_\lambda)\leqq\frac{1}{v_\lambda\sqrt{d_\lambda}}\prod_{\phi|\lambda}\frac{2\sqrt{n}\,|S(\phi)|}{\log(\kappa_\lambda)}\leqq\frac{\lambda(1)!}{\sqrt{d_\lambda}}\prod_{\phi|\lambda}\frac{2|S(\phi)|}{\sqrt{\pi}\log(\kappa_\lambda)}\,.$$

*Here $v_\lambda$ is as in Proposition 4. If $n(\lambda)=p$, a prime number, then*

$$(H_\lambda:\boldsymbol{E}_\lambda)\leqq\prod_{\phi|\lambda}\frac{|S(\phi)|}{\log(\kappa_\lambda)}\,.$$

PROOF. We may assume $L=F_\lambda$. Then $A=A_\lambda$ and $n=n(\lambda)$. From a property of the logarithmic function, follows

$$\log(\kappa_\lambda)=\inf\{\max_{a\in A}(\log(\|\varepsilon^a\|))\mid\varepsilon\in H_\lambda,\ \varepsilon\notin W_\lambda\}.$$

Let $M_\lambda$, $N_\lambda$ be as in Remark 9. Then $u(M_\lambda)=\log(\kappa_\lambda)$ in (14). Hence Proposition 4, together with (24), easily completes the proof.

COROLLARY 2. *The assumption and the notation being the same as in Theorem* 2, *one has*

$$h\leqq\frac{h_1}{c_L}\left(\frac{2w}{\sqrt{\pi}}\right)^{n-1}\prod_{\lambda\in\Lambda^*}\frac{\lambda(1)!}{\sqrt{d_\lambda}}\prod_{\phi|\lambda}\frac{|S(\phi)|}{\log(\kappa_\lambda)}\qquad(w=\sharp W)\,.$$

*If $a^p=1$ for all $a\in A$ with a prime number $p$, then*

$$h\leqq\frac{h_1w^{n-1}}{c_L}\prod_{\lambda\in\Lambda^*}\prod_{\phi|\lambda}\frac{|S(\phi)|}{\log(\kappa_\lambda)}\,.$$

PROOF. Clear from Corollary 1 and Theorems 2, 3.

We prove here a useful property of an $\varepsilon\in H$ of the form

$$\varepsilon=\prod_{\lambda\in\Lambda^*}\varepsilon_\lambda\,;\qquad \varepsilon_\lambda\in H_\lambda,\ \varepsilon_\lambda\notin W_\lambda\ \text{or}\ \varepsilon_\lambda=1\quad(\lambda\in\Lambda^*)\,. \tag{27}$$

For any $\Phi\subset\Lambda^*$, let $F_\Phi$ be the composite of $F_\lambda$ $(\lambda\in\Phi)$ and $F$. As a generalization of Proposition III.1 in [**6**], we can show

PROPOSITION 5. *Let $\varepsilon\in H$ be given by* (27). *Then $F(\varepsilon)=F_{\Phi_\varepsilon}$, where $\Phi_\varepsilon=$*

$\{\lambda \in \Lambda^* \mid \varepsilon_\lambda \neq 1\}$.

PROOF. Clearly $\varepsilon \in F_{\Phi_\varepsilon}$. Assume $F(\varepsilon) \neq F_{\Phi_\varepsilon}$. Then $\varepsilon^a = \varepsilon$ for some $a \in A$, $a \notin \tilde{A}_\lambda$, with some $\lambda \in \Phi_\varepsilon$. By (19), (27) and by Theorem 1, we see that $l(\varepsilon_\lambda{}^a) = e_\lambda l(\varepsilon^a) = e_\lambda l(\varepsilon) = l(\varepsilon_\lambda)$, hence $(\varepsilon_\lambda{}^w)^a = \varepsilon_\lambda{}^w$. Thus $F_\mu = F(\varepsilon_\lambda{}^w)$ for a certain $\mu < \lambda$, and then $\mathrm{N}_\mu^\lambda(\varepsilon_\lambda{}^w) = \varepsilon_\lambda{}^{wq} \in W_\mu \subset W_\lambda$ by (17), where $q = n(\lambda)/n(\mu)$. Consequently $\varepsilon_\lambda \in W_\lambda$, but $\varepsilon_\lambda \neq 1$ as $\lambda \in \Phi_\varepsilon$, which contradicts (27), and we complete the proof.

Let $\lambda \in \Lambda^*$ and $D_\lambda$ be the discriminant relative to $F_\lambda/F$. As an estimation of $\kappa_\lambda$ in (26), we have

PROPOSITION 6. *The absolute norm* $\mathrm{N}(D_\lambda)$ *does not exceed* $(\|n(\lambda)\| \kappa_\lambda{}^{n(\lambda)-1})^{n(\lambda)}$, *i.e.* $\kappa_\lambda \geqq \sqrt[n(\lambda)-1]{\sqrt[n(\lambda)]{\mathrm{N}(D_\lambda)}/\|n(\lambda)\|}$.

PROOF. We may suppose $L = F_\lambda$, $A = A_\lambda$, $n = n(\lambda)$. Let $\varepsilon \in H_\lambda$, $\varepsilon \notin W_\lambda$. Then, since $F(\varepsilon) = F_\lambda$ by Proposition 5, Hadamard's inequality shows

$$\mathrm{N}(D_\lambda) \leqq \|\det(\varepsilon^{ia})_{0 \leqq i < n,\, a \in A}\|^2 \leqq \|\prod_{i=0}^{n-1} \sum_{a \in A} |\varepsilon^a|^{2i}\|,$$

hence

$$\mathrm{N}(D_\lambda) \leqq \|n^n \max_{a \in A} (|\varepsilon^a|^{n(n-1)})\|.$$

Thus the assertion follows.

REMARK 10. When $\mathrm{N}(D_\lambda) > \|n(\lambda)\|$, Proposition 6 and Theorem 3 majorize $(H_\lambda : \boldsymbol{E}_\lambda)$ by a simple function of $\theta_\lambda(a)$ $(a \in A_\lambda)$, $n(\lambda)$ and $\mathrm{N}(D_\lambda)$. In Case 1, not assuming $\mathrm{N}(D_\lambda) > n(\lambda)^{n(\lambda)}$, [6] has given a better estimation. In Case 2, even if $\mathrm{N}(D_\lambda) \leqq n(\lambda)^{2n(\lambda)}$, we can consider as follows: Let $h_\lambda$ be the class number of $F_\lambda$. As is well-known, $h_\lambda$ does not exceed the number of integral ideals $\mathfrak{a}$ of $F_\lambda$ with $1 \leqq \mathrm{N}(\mathfrak{a}) \leqq x$, where $x = (2n(\lambda))!\,(\sqrt{d}/\pi n(\lambda)^2)^{n(\lambda)} \sqrt{\mathrm{N}(D_\lambda)}$ with the discriminant $-d$ of $F$. By Theorem 2, $(H_\lambda : \boldsymbol{E}_\lambda) \leqq c_{F_\lambda} Q_{A_\lambda} h_\lambda / h_1$. Thus $(H_\lambda : \boldsymbol{E}_\lambda)$ is majorized by a simple function of $h_1$, $d$, $c_{F_\lambda}$, $Q_{A_\lambda}$, $n(\lambda)$ and $\mathrm{N}(D_\lambda)$; roughly estimating, $(H_\lambda : \boldsymbol{E}_\lambda) \leqq c_{F_\lambda} Q_{A_\lambda} x^{2n(\lambda)} / h_1$.

## § 3. Calculation of $h$ and $E$.

We prepare general algorithms in § 3.1, give an outline of our method in § 3.2, and state the main algorithms in § 3.3.

**3.1.** Fix a number field $k$ as a base field. Let $q \in \boldsymbol{Z}$, $q > 0$, and $\alpha \in I$ be given, where $I$ is the ring of all algebraic integers in $\boldsymbol{C}$. For a given number field $K \supset k(\alpha)$, we show a way to decide $K \cap I_{q,\alpha}$ explicitly in a sense, where $I_{q,\alpha} = \{\beta \in I \mid \beta^q = \alpha\}$.

Let $I_k = I \cap k$ and $X$ be a complex variable. For any $\beta \in I$, let $P_\beta \in I_k[X]$ be its minimal polynomial over $k$. The set of conjugates of $\beta$ over $k$ is the inverse image $J^{-1}(P_\beta)$ via the map $J$ defined by

$$J: I \longrightarrow I_k[X]; \qquad \beta \longmapsto P_\beta .$$

The image $J(I)$ consists of all monic irreducible polynomials in $I_k[X]$. We first give two lemmas. It is easy to prove

LEMMA 6. *If $\beta \in I_{q,\alpha}$, then $k(\alpha) \subset k(\beta)$, $[k(\beta): k(\alpha)] \leqq q$ and the set of conjugates of $\beta$ over $k(\alpha)$ is given by $I_{q,\alpha} \cap J^{-1}(P_\beta)$.*

Let $f \in \boldsymbol{Z}$, $1 \leqq f \leqq q$, $N = f[k(\alpha): k]$ and let $P = P_\alpha{}^f \in M$, where

$$M = \{Q \in I_k[X] \mid Q \text{ is monic of degree } N\}.$$

Factor $P$ as $P = (X-\alpha_1) \cdots (X-\alpha_N)$ in $I[X]$. Among the $q^N$ elements $(X-\beta_1) \cdots (X-\beta_N)$ $(\beta_1 \in I_{q,\alpha_1}, \cdots, \beta_N \in I_{q,\alpha_N})$ of $I[X]$, let $M_f = M_{q,\alpha,f}$ consist of those belonging to $I_k[X]$:

$$M_f = M_{q,\alpha,f} = \{(X-\beta_1) \cdots (X-\beta_N) \in M \mid \beta_i \in I_{q,\alpha_i} \ (1 \leqq i \leqq N)\}. \tag{28}$$

LEMMA 7. *For any $Q \in M$ factoring as $Q = Q_1 \cdots Q_r$ with $Q_1, \cdots, Q_r \in J(I)$, one has $Q \in M_f$ if and only if $Q_1, \cdots, Q_r \in J(I_{q,\alpha})$; and then $Q_1 \in M_{f_1}, \cdots, Q_r \in M_{f_r}$ with certain $f_i \in \boldsymbol{Z}$, $f_i > 0$ $(1 \leqq i \leqq r)$ such that $f_1 + \cdots + f_r = f$.*

PROOF. The 'only if'-part follows from the definition. Let $Q_1, \cdots, Q_r \in J(I_{q,\alpha})$. For $i = 1, \cdots, r$, by Lemma 6, we have $Q_i \in M_{f_i}$ with $f_i \in \boldsymbol{Z}$, $f_i > 0$, such that $\deg(Q_i) = f_i[k(\alpha): k]$; thus $f = f_1 + \cdots + f_r$ and $Q \in M_f$, which proves the 'if'-part and completes the proof.

As $I_{q,\alpha} \cap k(\alpha) = \{\beta \in I_{q,\alpha} \mid k(\alpha) = k(\beta)\}$, similar to Lemma IV.1 of [**6**], from Lemmas 6, 7, we immediately obtain

PROPOSITION 7. *The map $J$ is injective on $I_{q,\alpha} \cap k(\alpha)$, and the image $J(I_{q,\alpha} \cap k(\alpha))$ coincides with $M_1 = M_{q,\alpha,1}$.*

We next express (28) in terms of the coefficients, using a bijection $c: M \to I_k{}^N := \{(u_1, \cdots, u_N) \in \boldsymbol{C}^N \mid u_1, \cdots, u_N \in I_k\}$ (in the complex vector space $\boldsymbol{C}^N$) defined by

$$c(Q) = (u_1, \cdots, u_N) \qquad (Q = X^N - u_1 X^{N-1} + \cdots + (-1)^N u_N \in M).$$

For the above $P$, we have another expression

$$c(P) = (s_1(\alpha_1, \cdots, \alpha_N), \cdots, s_N(\alpha_1, \cdots, \alpha_N)), \tag{29}$$

where $s_i = s_i(x_1, \cdots, x_N)$ $(1 \leqq i \leqq N)$ are the elementary symmetric functions of $N$ independent complex variables $x_1, \cdots, x_N$:

$$s_1 = \sum_{i=1}^{N} x_i, \quad s_2 = \sum_{1 \leq i < j \leq N} x_i x_j, \quad \cdots, \quad s_N = \prod_{i=1}^{N} x_i .$$

For $i=1, \cdots, N$, as is well-known, we can define a polynomial $\sigma_i=\sigma_i(s_1, \cdots, s_N) \in \boldsymbol{Z}[s_1, \cdots, s_N]$ by

$$\sigma_i(s_1(x_1, \cdots, x_N), \cdots, s_N(x_1, \cdots, x_N))=s_i(x_1^q, \cdots, x_N^q).$$

Denote $\sigma(u)=\{\sigma_1(u_1, \cdots, u_N), \cdots, \sigma_N(u_1, \cdots, u_N)\} \in I_k^N$ for every $u=(u_1, \cdots, u_N) \in I_k^N$. Obviously from the definition, follows

LEMMA 8.
$$c(M_f)=c(M_{q,\alpha,f})=\{u \in I_k^N \mid \sigma(u)=c(P)\}.$$

We proceed under an important assumption. Suppose that

(30) *$I_k$ is discrete in $\boldsymbol{C}$;*

i.e. $k=\boldsymbol{Q}$ or $k$ is imaginary quadratic. To know $P_\alpha$, we prepare

ALGORITHM 0. *Let $J^{-1}(P_\alpha)$ be known approximately with precision good enough. Then $P_\alpha$ can be decided.*

PROCEDURE. By (29), (30), if $z_1, \cdots, z_N \in \boldsymbol{C}$ is close enough to $\alpha_1, \cdots, \alpha_N$, then $c(P)$ is the nearest (relative to the maximum norm of $\boldsymbol{C}^N$) element of $I_k^N$ to $(s_1(z_1, \cdots, z_N), \cdots, s_N(z_1, \cdots, z_N))$.

Conversely, let $Q \in J(I)$ be given. Then $J^{-1}(Q)$ can be known approximately with any good precision by Lehmer's method in [**12**], § 2.7, for example. If some $\beta' \in \boldsymbol{C}$ is given close enough to one $\beta \in J^{-1}(Q)$, we can know $\beta$ approximately with any good precision (or can decide $\beta$); a sufficient condition of such a $\beta'$ is given by

(31) $$|\beta'-\beta|<|\beta'-\gamma| \qquad \text{for all } \gamma \in J^{-1}(Q), \quad \gamma \neq \beta.$$

Under a stronger condition, we may use other methods in [**12**], but we do not discuss them (or error estimate); and $\beta' \in \boldsymbol{C}$ only denotes a number close to $\beta \in I$; whenever $\beta'$, $P_\beta$ are both given, we assume $\beta'$ to be close enough to $\beta$ depending on circumstances. In this sense, we *express $\beta$ by $(P_\beta, \beta')$* (only approximately unless $\beta \in k$).

ALGORITHM 1. *Let $P_\alpha$ be known. Then $J(I_{q,\alpha} \cap k(\alpha))$ can be known. When $I_{q,\alpha} \cap k(\alpha) \neq \emptyset$, let $\alpha'$ be further given. Then all $(P_\beta, \beta')$ $(\beta \in I_{q,\alpha} \cap k(\alpha))$ can be obtained.*

PROCEDURE. By Proposition 7, we may know $M_1$ and $(Q, \beta')$ $(Q \in M_1, \beta \in I_{q,\alpha} \cap J^{-1}(Q))$. More generally, we have (I)-(II) below:

(I) Let $c(P)$ be given. Take a bounded set $B$ in $\boldsymbol{C}^N$ so that $c(M_f) \subset B$; e.g. put $B=\{(b_1, \cdots, b_N) \in \boldsymbol{C}^N \mid |b_i| \leqq \binom{N}{i} \sqrt[q]{m^i} \ (1 \leqq i \leqq N)\}$ with $m=1+\max_{1 \leq i \leq N}(|v_i|)$, where $c(P)=(v_1, \cdots, v_N)$. Then $B \cap I_k^N$ is a finite set by (30). Computing $\sigma(u)$

$(u \in B \cap I_k{}^N)$, we know $M_f$ by Lemma 8.

(II) Let $Q \in J(I) \cap M_f$ and $(P_\alpha, \alpha')$ be given. Eliminating the $q-f$ points in $I_{q,\alpha} \setminus J^{-1}(Q)$ (see Lemma 6) from $I_{q,\alpha}$ (approximately known using $\alpha'$), we obtain $(P_\beta, \beta')$ for each $\beta \in I_{q,\alpha} \cap J^{-1}(Q)$.

REMARK 11. If $B$ in (I) is close to $c(M_f)$, we can omit (II) since the zeros of $Q \in M$ are continuous functions of $c(Q)$.

ALGORITHM 2. *For a number field $K \supset k(\alpha)$, let $K = k(\delta)$ with $\delta = \alpha\gamma^q \neq 0$, $\gamma \in I \cap K$, and $P_\delta$ be known. Then $\sharp(I_{q,\alpha} \cap K)$ can be known. When $I_{q,\alpha} \cap K \neq \emptyset$, let $\gamma'$ (with precision good enough) and $(P_\alpha, \alpha')$ be further given. Then all $(P_\beta, \beta')$ $(\beta \in I_{q,\alpha} \cap K)$ can be obtained.*

PROCEDURE. Since the maps $I_{q,\alpha} \cap K \ni \beta \mapsto \beta\gamma \in I_{q,\delta} \cap K$ and $I_{q,\delta} \cap K \ni \varepsilon \mapsto P_\varepsilon \in M_{q,\delta,1}$ are bijective (see Proposition 7), we do:

(I) Let $P_\delta$ be given. Decide $M_{q,\delta,1}$ by (I) of Algorithm 1; then $\sharp(I_{q,\alpha} \cap K) = \sharp M_{q,\delta,1}$ is known. Let $\delta' = \alpha'\gamma'^q$ be also given. Then all $(P_\varepsilon, \varepsilon')$ $(\varepsilon \in I_{q,\delta} \cap K)$ are known by (II) of Algorithm 1.

(II) Let $(P_\alpha, \alpha')$ be given. Decide $M_f = M_{q,\alpha,f}$ $(1 \leqq f \leqq q)$ by (I) of Algorithm 1. Eliminating $Q \in M_f$ such that $r > 1$ and $f_i < f$, $Q_i \in M_{f_i}$ $(1 \leqq i \leqq r)$ in Lemma 7, we get $J(I) \cap M_f$ inductively for $f = 1, \cdots, q$. Since $J(I_{q,\alpha})$ is the union of $J(I) \cap M_f$ $(1 \leqq f \leqq q)$, we obtain all $(P_\beta, \beta')$ $(\beta \in I_{q,\alpha})$ by (II) of Algorithm 1.

(III) Let $(P_\beta, \beta')$ $(\beta \in I_{q,\alpha})$, $(P_\varepsilon, \varepsilon')$ $(\varepsilon \in I_{q,\delta} \cap K)$ be known by (I), (II). For every $\varepsilon \in I_{q,\delta} \cap K$, we find a unique $\beta \in I_{q,\alpha}$ such that $\beta'/\varepsilon'$ is close to $\gamma'$; thus we can decide all $(P_\beta, \beta')$ $(\beta \in I_{q,\alpha} \cap K)$.

REMARK 12. It will be possible to give another algorithm, using Lagrange's resolvent as in Proposition 1 of [**17**, III].

**3.2.** Coming back to the abelian extension $L/F$, we sketch how to decide the class number $h$ and the group $E$ of units of $L$. Putting $k = F$ in § 3.1, we keep the notation there.

Let $C(\mathfrak{f})$ be the ray class group of $F$ modulo an ideal $\mathfrak{f}$ $(\neq 0)$ of $I_F$. By arithmetic of $F$ as in Remark 14 below, we can obtain for $C(\mathfrak{f})$ a full set of representative ideals expressing its group operation and the conductor of each subgroup: When $\mathfrak{f} = I_F$, a method for deciding the class number $h_1$ of $F$ offers such a way, see [**1**], Chapter 2, § 7. When $\mathfrak{f} \neq I_F$, we may use the exact sequence

$$1 \longrightarrow W_1/W_1(\mathfrak{f}) \longrightarrow (I_F/\mathfrak{f})^\times \longrightarrow C(\mathfrak{f}) \longrightarrow C(I_F) \longrightarrow 1, \tag{32}$$

where $W_1(\mathfrak{f}) = W_1 \cap (1+\mathfrak{f})$ is the group of units of $F$ congruent to 1 modulo $\mathfrak{f}$ and $(I_F/\mathfrak{f})^\times$ is the group of units of the ring $I_F/\mathfrak{f}$; the conductor for a subgroup of $C(\mathfrak{f})$ is known by reduction (modulo divisors of $\mathfrak{f}$) of its inverse image via the map $(I_F/\mathfrak{f})^{\times}\to C(\mathfrak{f})$.

Take a subgroup $U$, expressed as a subset of a full set of representative ideals as above, of $C(\mathfrak{f})$ with conductor exactly $\mathfrak{f}$. Let $L/F$ be the class field corresponding to $U$; so $C(\mathfrak{f})/U\approx A$ via the Artin map; i.e. instead of $L$, we start from the class group $U$ corresponding to $L/F$. Then $Q_A$ is known by (4). As we shall do later, define $\theta_\lambda$ $(\lambda\in\Lambda^*)$ in (C0) by means of well-known class invariants so that (C1), (C2) hold. Then $c_L$ in (23) is easily known (cf. (36) below), and $\theta_\lambda(a)$ $(\lambda\in\Lambda^*,\ a\in A_\lambda)$ are approximately known with any good precision; see [**6**] (Case 1) and Proposition 8 in §4.1 (Case 2). For the units $\eta_\lambda\in\boldsymbol{E}_\lambda$ $(\lambda\in\Lambda^*)$ in (22), let

$$Y=\bigcup_{\lambda\in\Lambda^*}Y_\lambda;\qquad Y_\lambda=J^{-1}(P_{\eta_\lambda})=\{\eta_\lambda^a\,|\,a\in A_\lambda\}\quad(\lambda\in\Lambda^*).\tag{33}$$

Then $Y$ can be known approximately with any good precision. (See Examples 3, 4 in §5.2 as to this step.)

We accomplish our purpose by Theorem 2; starting from $Y$, we decide $(E:\boldsymbol{E})$ and find a free basis $Z$ of $E$; every fundamental unit $\varepsilon\in Z$ is obtained as a pair $(P_\varepsilon,\ \varepsilon')$ (cf. the context of (31)). We divide this in two steps: First, for each $\lambda\in\Lambda^*$, starting from $Y_\lambda$, we decide $(H_\lambda:\boldsymbol{E}_\lambda)$ and find a free basis $Z^\lambda$ of $H_\lambda$ by Algorithm 3. Next, starting from $Z^\lambda$ $(\lambda\in\Lambda^*)$, we decide $(E:H)$ and find $Z$ by Algorithm 4. (We can decide $(E:\boldsymbol{E})$ only by Algorithm 4, see §0.2.)

We add a few preparatory observations. As in Remark 10, by using the values of $\theta_\lambda(a)$ $(\lambda\in\Lambda^*,\ a\in A_\lambda)$ or by another method,

(34) *$r_\lambda\in\boldsymbol{Z}$ can be taken so that $(H_\lambda:\boldsymbol{E}_\lambda)\leqq r_\lambda$ $(\lambda\in\Lambda^*)$.*

(See also Example 2.) By Proposition 5, for an $\eta\in\boldsymbol{E}$ of the form

(27′) $\eta=\prod_{\lambda\in\Lambda^*}\eta_\lambda^{x(\lambda)}$ *with explicit* $x(\lambda)\in\boldsymbol{Z}[A_\lambda]$ $(\lambda\in\Lambda^*)$,

we can know $J^{-1}(P_\eta)$ approximately. Therefore, by Algorithm 0,

(35) *$P_\eta$ can be decided if $\eta\in\boldsymbol{E}$ is given as in (27′).*

(See Examples 3.(i), 5, 6.) Moreover, as an application of (35),

(36) *$w(:=\#W)$, $w_\lambda(:=\#W_\lambda)\in\boldsymbol{Z}$ $(\lambda\in\Lambda)$ can be decided.*

Indeed, we can do as follows: Decide $f\in\boldsymbol{Z}$, $f>0$, by $f\boldsymbol{Z}=\mathfrak{f}\cap\boldsymbol{Z}$. Let $x(\lambda)=12f$ $(\lambda\in\Lambda^*)$ in (27′). Then $L=F(\eta)$ by Proposition 5, so, by (35) and by Algorithm 2, we decide the number of $12f$-th roots of 1 in $L$, which is equal to $w$ since $w$ divides $12f$ by Lemme 7 of [**23**]. For each $\lambda\in\Lambda^*$, put $\eta=\eta_\lambda{}^{12f}$ in (27′) and get $w_\lambda$ similarly. As $w_1$ is known a priori, (36) holds. (See Example 5.(i).)

Remark 13. In Case 2, for a ring class field, we may start from a ring class subgroup, see Proposition 9 in §4.2. Instead of (32), we then use (4) in [**20**], where the case $n=3$ was studied.

REMARK 14. If a number field $K$ has the ring of integers of type $\boldsymbol{Z}[\omega]$ with an explicit $P=P(X)\in\boldsymbol{Z}[X]$ as the minimal polynomial of $\omega\in K$ over $\boldsymbol{Q}$, the following arithmetic of $K$ is possible, which we can apply to $K=\boldsymbol{Q}^{\lambda}$ ($\lambda\in\Lambda^*$) (the $n(\lambda)$-th cyclotomic fields) or to $K=F$: Every element of $K$ is written via the basis $\{\omega^i\}_{i=0}^{N-1}$, where $N=[K:\boldsymbol{Q}]$. The sum, the product of elements of $K$ or the inverse of a non-zero element of $K$ is computable as usual. Any (non-zero fractional) ideal of $K$ is expressed by its $\boldsymbol{Z}$-basis obtained from its finite generators by elementary matrix transformation. Hence the sum or the product of ideals of $K$ is also known. The inverse of an ideal of $K$ is the dual multiplied by the different $P'(\omega)$ so is known by elementary matrix transformation since the traces of $\omega^i$ ($1\leqq i\leqq 2N-2$) are given by Newton's formula, see [**13**], III, §1. The prime ideals of $K$ above a given prime number $p$ are decided by factoring $P$ modulo $p$, see Proposition 25 in [**13**], I, §8. Thus, we can explicitly factor a given ideal of $K$ into prime ideals of $K$. For given ideals $\mathfrak{a}$, $\mathfrak{f}$, $\mathfrak{f}\subset\boldsymbol{Z}[\omega]$, of $K$, an explicit $\beta\in\mathfrak{a}\mathfrak{f}^{-1}$ can be found so that $\beta\mathfrak{a}^{-1}\mathfrak{f}$ is prime to $\mathfrak{f}$; e.g. decide the distinct prime ideals $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ of $K$ dividing $\mathfrak{f}$, let $\mathfrak{b}=\mathfrak{a}^{-1}\mathfrak{f}\mathfrak{p}_1\cdots\mathfrak{p}_r$, take one $\beta_i\in\mathfrak{b}\mathfrak{p}_i^{-1}$, $\beta_i\notin\mathfrak{b}$, for each $i=1,\cdots,r$, and put $\beta=\beta_1+\cdots+\beta_r$.

**3.3.** Let us decide $(E:\boldsymbol{E})$ and find a free basis $Z$ of $E$ under the situation as in §3.2, esp. under (34), (36) executed in advance. Further $Y$ in (33) is assumed to be known approximately with precision good enough, so (35) is often utilized.

ALGORITHM 3. *Let $\lambda\in\Lambda^*$. The index $(H_\lambda:\boldsymbol{E}_\lambda)$ can be decided, finding a free basis $Z^\lambda$ of $H_\lambda$. Each $\varepsilon\in Z^\lambda$ is obtained as $(P_\varepsilon,\ \varepsilon')$.*

PROCEDURE. Let $M_\lambda$, $N_\lambda$ be as in Remark 9. Put $r=1$ and $\mathcal{J}=\mathfrak{o}_\lambda$. Note that $P_{\eta_\lambda}$ is known by (35). For every prime number $p$, we use the result and the notation in Proposition 3 and Remark 3. By ordinary arithmetic of $\boldsymbol{Q}^\lambda$ as in Remark 14, we can do (I)-(III):

(I) Take every prime number $p$ in increasing order of $p^s$. Put $\eta=\eta_\lambda$, $q=(p,\ w_\lambda)$ (the greatest common divisor) and go to (II).

(II) If $p^s>r_\lambda$, then $(H_\lambda:\boldsymbol{E}_\lambda)=r$ and $\mathcal{J}$ is that defined by (7); go to (III). If $p^s\leqq r_\lambda$, for each $\phi|\lambda$, put $\xi_\phi=\eta^{qx\phi}$, get $P_{\xi_\phi}$ from $P_\eta$ and decide $J(I_{qp,\xi_\phi}\cap F_\lambda)$ by Algorithm 1. When $I_{pq,\xi_\phi}\cap F_\lambda=\emptyset$ (i.e. $\eta^{x\phi}$ is not a $p$-th power in $F_\lambda$ modulo $W_\lambda$) for any $\phi|\lambda$, go to (I) to take the next $p$. Else, choose one $Q\in J(I_{pq,\xi_\phi}\cap F_\lambda)$ with some $\phi|\lambda$; then, as $Q=P_\varepsilon$ for an $\varepsilon\in H_\lambda$ with $\varepsilon^p=\zeta\eta^{x\phi}$, $\zeta\in W_\lambda$, replace $r$ by $p^s r$, $\mathcal{J}$ by $\mathcal{P}_\phi\mathcal{J}$, $r_\lambda$ by $p^{-s}r_\lambda$, $\eta$ by $\varepsilon$ and repeat (II) for the same $p$.

(III) Let $\{z_i\}_{i=1}^{\lambda(1)}$ be a $\boldsymbol{Z}$-basis of $r\mathcal{J}^{-1}\subset\mathfrak{o}_\lambda$. Note that $M_\lambda=r^{-1}(r\mathcal{J}^{-1})N_\lambda$. Put

$q=(r, w_\lambda)$. For $i=1, \cdots, \lambda(1)$, put $\xi_i=\eta_\lambda{}^{qz_i}$, decide $P_{\xi_i}$ by (35). We obtain $(P_{\varepsilon_i}, \varepsilon_i')$ for an $\varepsilon_i\in I_{rq,\xi_i}\cap F_\lambda$ by Algorithm 1, then $\varepsilon_i\in H_\lambda$ such that $\varepsilon_i{}^r=\zeta\eta_\lambda{}^{z_i}$ with some $\zeta\in W_\lambda$. Thus we may put $Z^\lambda=\{\varepsilon_i\}_{i=1}^{\lambda(1)}$.

Remark 15. If the class number of $\boldsymbol{Q}^\lambda$ is one, we obtain $Z^\lambda$ only by (I)-(II) above, provided $\alpha$ is chosen as in Remark 4, but such an $\alpha$ is not obtained by arithmetic as in Remark 14 alone.

Let $\{\xi_i\}_{i=1}^{n-1}$ be the union of $Z^\lambda$ $(\lambda\in\Lambda^*)$. Put $q=(w, n)$. Since $E^n\subset H$ by Corollary 1, we can define, inductively for $i=1, \cdots, n-1$, the smallest divisor $k_i\in\boldsymbol{Z}$, $k_i>0$, of $n$ such that

$$(37)\qquad (\xi_1{}^{j_1}\cdots\xi_{i-1}{}^{j_{i-1}}\xi_i{}^{k_i})^q=\varepsilon_i{}^{nq}\qquad\text{with an}\quad \varepsilon_i\in E$$

for some $j_1\in\{0, \cdots, k_1-1\}, \cdots, j_{i-1}\in\{0, \cdots, k_{i-1}-1\}$ (i.e. the unit in the parentheses in (37) is an $n$-th power in $L$ modulo $W$); then $(E:H)=n^{n-1}/k_1\cdots k_{n-1}$ and $Z=\{\varepsilon_i\}_{i=1}^{n-1}$ is a free basis of $E$.

Algorithm 4. *Let $Z^\lambda$ $(\lambda\in\Lambda^*)$ be given by Algorithm 3. Then $(E:H)$ can be decided, finding a set $Z$ of fundamental units of $L$. Every $\varepsilon\in Z$ is obtained as $(P_\varepsilon, \varepsilon')$.*

Procedure. Inductively for $i=1, \cdots, n-1$, we decide the $k_i$ above by (I) and obtain $(P_{\varepsilon_i}, \varepsilon_i')$ for an $\varepsilon_i$ as in (37) by (II):

(I) Take every divisor $k_i\in\boldsymbol{Z}$, $k_i>0$, of $n$ in increasing order. Let $\xi=\xi(j_1, \cdots, j_{i-1}, k_i)$ be any unit as in the left side of (37). Then $\xi$ is of the form in (27). We may assume that $\xi'$ is given with precision good enough. Let $\eta$ be the product of all $\eta_\lambda$ $(\lambda\in\Lambda^*, \lambda\notin\Phi_\xi)$, where $\Phi_\xi$ is as in Proposition 5. Then $L=F(\varepsilon)$, where $\varepsilon=\xi\eta^{qn}$. Take a small $t\in\boldsymbol{Z}$, $t>0$, such as $\xi^t\in\boldsymbol{E}$. Then $\varepsilon^t$ is of the form in (27′). Decide $P_{\varepsilon^t}$ by (35). Since $\varepsilon'$ is known, we can decide $P_\varepsilon$ in $J(I_{t,\varepsilon^t}\cap L)$ obtained by Algorithm 1. So we test by Algorithm 2 whether $I_{nq,\xi}\cap L$ is empty or not. If $I_{nq,\xi}\cap L=\emptyset$ for all $j_1\in\{0, \cdots, k_1-1\}, \cdots, j_{i-1}\in\{0, \cdots, k_{i-1}\}$, we repeat (I) for the next divisor $k_i$ of $n$. If $I_{nq,\xi}\cap L\neq\emptyset$ for some $\xi$, then $k_i$ is that defined above; fix such a $\xi$ and go to (II).

(II) We keep the notation in (I). Since $\xi^t$ is also of the form in (27′), we decide $P_{\xi^t}$ by (35), and obtain $(P_\xi, \xi')$ by using Algorithm 1 similarly. As $\eta'$ is given, we obtain $(P_{\varepsilon_i}, \varepsilon_i')$ for an $\varepsilon_i\in I_{nq,\xi}\cap L$ which satisfies (37) by using Algorithm 2.

Remark 16. In the procedures above, for simplicity, we have not taken into account of efficiency of algorithms. As to actual calculation, see Examples 5, 6 in §5.3 and [**17**], [**20**].

## § 4. Explicit elliptic units.

In Case 1, Leopoldt [14] and Gras-Gras [6] used cyclotomic units $\eta_\lambda \in H_\lambda$ as in (22), giving $\theta_\lambda$ in (C0) explicitly by means of the sine function. Then $c_L=1$ in (23). Numerical tables of $h$ and $E$ have been given in [7], [8], [9], [15].

In the rest of this paper, we only study Case 2.

We explicitly define $\theta_\lambda$ $(\lambda \in \Lambda^*)$ in (C0) so that (C1), (C2) hold, quoting Siegel [25], Ramachandra [22], Robert [23] in § 4.1, and Hasse [11], Deuring [2], Meyer [16], Schertz [24] in § 4.2. Considering as in Stark [26], we show another formula in § 4.3 like that in Theorem 2 with a smaller $c_L$ but with elliptic units not so explicit. As to details, see the above literatures.

**4.1.** For each $\lambda \in \Lambda^*$, let $\mathfrak{f}_\lambda$ $(\subset I_F)$ be the conductor of $F_\lambda/F$, and decide $f_\lambda \in \boldsymbol{Z}$, $f_\lambda > 0$, by $f_\lambda \boldsymbol{Z} = \mathfrak{f}_\lambda \cap \boldsymbol{Z}$. From the ray class group $C(\mathfrak{f}_\lambda)$ onto the galois group $A_\lambda$, there is a canonical homomorphism denoted by $\sigma_\lambda : C(\mathfrak{f}_\lambda) \to A_\lambda$, the Artin map. For every $a \in A_\lambda$, let

$$\theta_\lambda(a) = \theta_\lambda^{\mathfrak{f}}(a) = \begin{cases} \prod\limits_{k \in (\sigma_\lambda)^{-1}(a)} \delta(k) & \text{if } f_\lambda = 1, \\ \prod\limits_{k \in (\sigma_\lambda)^{-1}(a)} \varphi_{\mathfrak{f}_\lambda}(k) & \text{otherwise.} \end{cases} \tag{38}$$

Here the class invariants $\delta(k)$ and $\varphi_{\mathfrak{f}_\lambda}(k)$ are defined as follows: For complex variables $t$, $z$, $\mathrm{Im}(z)>0$, put $\hat{e}(t) = \exp(2\pi\sqrt{-1}\,t)$ and set

$$\eta(z) = \hat{e}\left(\frac{z}{24}\right) \prod_{j=1}^{\infty} (1-\hat{e}(jz)),$$

$$\varphi(t, z) = 2\hat{e}\left(\frac{z}{12} + \frac{t\,\mathrm{Im}(t)}{2\,\mathrm{Im}(z)}\right) \sin(\pi t) \prod_{j=1}^{\infty} (1-\hat{e}(jz+t))(1-\hat{e}(jz-t)).$$

If $\mathcal{L} = z_1\boldsymbol{Z} + z_2\boldsymbol{Z}$ with $z_1, z_2 \in \boldsymbol{C}^\times$, $\mathrm{Im}(z_1/z_2)>0$, we can define $\Delta(\mathcal{L})$ by

$$(2\pi)^{-12}\Delta(\mathcal{L}) = (z_2^{-1}\eta(z_1/z_2)^2)^{12}.$$

When $f_\lambda = 1$, for any $k \in C(I_F)$, let $\mathfrak{a} \in k^{-1}$, $\alpha \in F$, $\alpha I_F = \mathfrak{a}^{h_1}$, and put

$$\delta(k) = \alpha^{12}((2\pi)^{-12}\Delta(\mathfrak{a}))^{h_1}. \tag{39}$$

When $f_\lambda \neq 1$, for any $k \in C(\mathfrak{f}_\lambda)$, take an ideal $\mathfrak{a}$, one $\beta \in \mathfrak{a}\mathfrak{f}_\lambda^{-1}$ so that $\beta\mathfrak{a}^{-1}\mathfrak{f}_\lambda \in k$, choose a $\boldsymbol{Z}$-basis $\{\alpha_1, \alpha_2\}$, $\mathrm{Im}(\alpha_1/\alpha_2)>0$, of $\mathfrak{a}$, and put

$$\varphi_{\mathfrak{f}_\lambda}(k) = \varphi(\beta/\alpha_2, \alpha_1/\alpha_2)^{12 f_\lambda}. \tag{40}$$

Let $w = \# W$, $w_\lambda = \# W_\lambda$ $(\lambda \in \Lambda)$, put $w(\mathfrak{f}_\lambda) = \#(W_1 \cap (1+\mathfrak{f}_\lambda))$, and set

$$c_\lambda = \begin{cases} 24h_1 & \text{if } f_\lambda = 1, \\ 12 f_\lambda w(\mathfrak{f}_\lambda) & \text{otherwise.} \end{cases} \tag{41}$$

PROPOSITION 8. *For each $\lambda\in\Lambda^*$, let the map $\theta_\lambda$ in* (C0) *be given by* (38). *Then* (C1), (C2) *are satisfied, and $c_L$ in* (23) *is a natural number expressed explicitly by $c_\lambda$ ($\lambda\in\Lambda^*$) in* (41) *as*

$$c_L=w^{-1}w_1\prod_{\lambda\in\Lambda^*}c_\lambda{}^{\lambda(1)}. \tag{42}$$

*One can compute $\theta_\lambda(a)$ ($\lambda\in\Lambda^*$, $a\in A_\lambda$) with any good precision.*

PROOF. The conditions (C1), (C2) are verified easily by Propositions 4, 15 and Théorème 3.(ii) of [23]. The expression of $c_L$ is obtained together. To compute $\theta_\lambda(a)$ ($\lambda\in\Lambda^*$, $a\in A_\lambda$), we can utilize the explicit Fourier expansions in Propositions 5, 6 of [25], I, §4, for $\eta(z)$ and $\hat{\mathrm{e}}((t\,\mathrm{Im}(\bar{t}))/(2\,\mathrm{Im}(z)))\eta(z)\varphi(t,z)$. The fact that $c_L\in\boldsymbol{Z}$ follows from Lemme 7 of [23] and from Lemma 9 below.

LEMMA 9. *Let $p$ be a prime number. For any $q\in\boldsymbol{Z}$, define $v(q)\in\boldsymbol{Z}$, $v(q)\geqq 0$, by $q\in p^{v(q)}\boldsymbol{Z}$, $q\notin p^{v(q)+1}\boldsymbol{Z}$. If $v(w)>v(w_1)$, then $v(w)=v(w_\lambda)$ with some $\lambda\in\Lambda^*$ such that $f_\lambda>1$ or $n(\lambda)=2$, except the case where $p=2$, $F\neq\boldsymbol{Q}(\sqrt{-1})$, $F\neq\boldsymbol{Q}(\sqrt{-2})$, $v(w)\geqq 3$. In the exceptional case, $v(w)-v(w_1)\leqq\sum_{\lambda\in\Lambda^*}\min(v(w_\lambda), v(n(\lambda)))$.*

PROOF. The assertions are verified without any difficulty.

REMARK 17. In (41), $w(\mathfrak{f}_\lambda)>1$ only when $F\neq\boldsymbol{Q}(\sqrt{-1})$, $F\neq\boldsymbol{Q}(\sqrt{-3})$, $\mathfrak{f}_\lambda=2I_F$ and 2 does not split in $F/\boldsymbol{Q}$. Then $w(\mathfrak{f}_\lambda)=2$, and $\sharp C(\mathfrak{f}_\lambda)=2h_1$ or $3h_1$ respectively if 2 ramifies or inerts in $F/\boldsymbol{Q}$.

**4.2.** Let now $\Lambda_R^*$ ($\subset\Lambda^*$) be the set of (rational) ring class characters of $L/F$; namely $\Lambda_R^*$ consists of $\lambda\in\Lambda^*$ such that $F_\lambda/F$ is a ring class field. For each $\lambda\in\Lambda_R^*$, we have $\mathfrak{f}_\lambda=f_\lambda I_F$. Denote by $I_{f_\lambda}$ the order of $F$ with conductor $f_\lambda$, by $R(f_\lambda)$ the group of classes of proper $I_{f_\lambda}$-ideals of $F$, and let $\tau_\lambda: R(f_\lambda)\to A_\lambda$ be the canonical onto homomorphism such that the composite $C(\mathfrak{f}_\lambda)\to R(f_\lambda)\xrightarrow{\tau_\lambda}A_\lambda$ is the Artin map $\sigma_\lambda$. For any ideal $\mathfrak{a}$ in $I_1=I_F$ prime to $f_\lambda$, put $\tilde{\mathfrak{a}}=\mathfrak{a}\cap I_{f_\lambda}$. Define natural numbers $g(\lambda)$, $m(\lambda)$ by

$$g(\lambda)=\frac{q}{(q,\,n(\lambda))},\quad m(\lambda)=\frac{n(\lambda)}{(q,\,n(\lambda))}\qquad\text{with}\quad q=\sharp R(f_\lambda)/h_1\,.$$

For any $k\in\mathrm{Ker}(\tau_\lambda)$, take and fix one $\tilde{\mathfrak{b}}_k\in k$. For each $a\in A_\lambda$, take an ideal $\mathfrak{a}$ of $I_1$ prime to $f_\lambda$ so that $\tilde{\mathfrak{a}}\in k_0{}^{-1}$ with some $k_0\in(\tau_\lambda)^{-1}(a)$, choose an $\alpha\in F$ such that $\mathfrak{a}^{h_1}=\alpha I_1$, and let

$$\theta_\lambda(a)=\theta_\lambda^R(a)=\alpha^{12g(\lambda)}\prod_{k\in\mathrm{Ker}(\tau_\lambda)}\left(\frac{\Delta(\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}_k)}{\Delta(\tilde{\mathfrak{b}}_k)}\right)^{m(\lambda)}. \tag{43}$$

For each $\lambda\in\Lambda^*$, we further put

$$c_\lambda=\begin{cases}24m(\lambda) & \text{if } \lambda\in\Lambda_R^*\,,\\ 12f_\lambda & \text{otherwise.}\end{cases} \tag{44}$$

PROPOSITION 9. *For each* $\lambda\in\Lambda^*$, *let the map* $\theta_\lambda$ *in* (C0) *be given by* (43) $(\theta_\lambda=\theta_\lambda^R)$ *if* $\lambda\in\Lambda_R^*$, *and by* (38) $(\theta_\lambda=\theta_\lambda^S)$ *otherwise. Then* (C1), (C2) *are satisfied, and* $c_L$ *in* (23) *is a natural number expressed explicitly by* $c_\lambda$ $(\lambda\in\Lambda^*)$ *in* (44) *as in* (42). *One can compute* $\theta_\lambda(a)$ $(\lambda\in\Lambda^*,\ a\in A_\lambda)$ *with any good precision.*

PROOF. If we observe that

$$\sum_{a\in A_\lambda}\psi(a)=0 \qquad \text{whenever } \psi|\lambda,\ \lambda\in\Lambda^*,$$

and that $w(\mathfrak{f}_\lambda)=1$ $(\lambda\in\Lambda^*,\ \lambda\notin\Lambda_R^*)$ by Remark 17, the conditions (C1), (C2) are verified easily by (3.12), Satz (3.2) (and its proof) in [**24**, I], and by Propositions 5, 6 in [**25**]. The expression of $c_L$ is obtained together. To compute $\theta_\lambda(a)$ $(\lambda\in\Lambda^*,\ a\in A_\lambda)$, we can do similarly as in the proof of Proposition 8. If $\lambda\in\Lambda_R^*$, then $F(W_\lambda)$ is a cyclic ring class field over $F$ abelian over $\boldsymbol{Q}$, so $w_\lambda$ divides 12 by Satz 1, b) of [**10**]. Hence $c_L\in\boldsymbol{Z}$ follows from Lemme 7 in [**23**] and from Lemma 9 above by the same way.

REMARK 18. If $f_\lambda=1$, we have $\theta_\lambda^S(a)/\theta_\lambda^S(1)=\theta_\lambda^R(a)^q$, $q=h_1/n(\lambda)$.

**4.3.** In this subsection, we assume that $\theta_\lambda=\theta_\lambda^S$, $c_\lambda$ and $\eta_\lambda$ $(\lambda\in\Lambda^*)$ are respectively given by (38), (41) and (22).

Let $f_\lambda=1$. For any $k\in C(I_F)^2$, take a prime ideal $\mathfrak{p}$, $\mathfrak{p}^{-2}\in k$, $6\notin\mathfrak{p}$, splitting in $F/\boldsymbol{Q}$, then choose $\alpha$, $\beta\in F$, $\mathrm{Im}(\beta)>0$, such that $\alpha I_F=\mathfrak{p}^{h_1}$ and that $\{\beta, 1\}$ (resp. $\{\beta, p^2\}$) is a $\boldsymbol{Z}$-basis of $I_F$ (resp. $\mathfrak{p}^2$), where $p=\mathrm{N}(\mathfrak{p})$. Then $\eta(p^{-2}\beta)/p\eta(\beta)$ belongs to the absolute class field $F^{(1)}$ of $F$ by [**2**], C.21, therefore, by the expression $\delta(k)/\delta(1)=\alpha^{24}(\eta(p^{-2}\beta)/p\eta(\beta))^{24h_1}$, the norm $\theta_\lambda(\sigma_\lambda(k))/\theta_\lambda(1)=\mathrm{N}_{F_\lambda}^{F^{(1)}}(\delta(k)/\delta(1))$ is a $(24h_1/n(\lambda))$-th power in $F_\lambda$, thus $\eta_\lambda$ is also so by the definition (of $T(\lambda)$) unless $n(\lambda)=2$. Consequently, putting

$$(45) \qquad \tilde{c}_\lambda=n(\lambda) \qquad \text{if } n(\lambda)>2,\ f_\lambda=1\,,$$

the following assertion is obtained:

$$(46) \qquad \eta_\lambda^{\tilde{c}_\lambda}\in H_\lambda^{c_\lambda} \qquad \text{and} \qquad \tilde{c}_\lambda\in\boldsymbol{Z},\ \tilde{c}_\lambda>0,\ \text{divides } c_\lambda\,.$$

By Corollary 3 in § 2.3 of [**23**] and by Remark 17 above, putting

$$(45') \qquad \tilde{c}_\lambda=6n(\lambda)=12 \qquad \text{if } n(\lambda)=2,\ f_\lambda=1\,,$$

we also obtain (46). Let next $f_\lambda>1$. For any $k\in C(\mathfrak{f}_\lambda)$, take $\beta$, $\alpha_1$, $\alpha_2$ as in (40). Then $\varphi(\beta/\alpha_2, \alpha_1/\alpha_2)$ belongs to the ray class field modulo $12f_\lambda^2$ over $F$ by Theorem 3 of [**26**], so $\theta_\lambda(a)$ $(a\in A_\lambda)$ are $c_\lambda$-th powers in the ray class field modulo $12f_\lambda{}^2w(\mathfrak{f}_\lambda)$ over $F$ by Lemme A-4 of [**6**], hence Lemma 6 of [**26**] and Lemme 7 of [**23**] prove (46) by putting

$$(45'') \qquad \tilde{c}_\lambda=w_\lambda \qquad \text{if } f_\lambda>1\,.$$

Theorem 2 and Proposition 8, together with Lemme 7 of [**23**] and Lemma 9, now enable us to state

THEOREM 4. *There are certain units $\tilde{\eta}_\lambda \in H_\lambda$ $(\lambda \in \Lambda^*)$ such that*

$$\tilde{c}_L Q_A h = h_1(E:H) \prod_{\lambda \in \Lambda^*} (H_\lambda : W_\lambda \cdot \tilde{\eta}_\lambda^{\boldsymbol{Z}[A]}) .$$

*Here $\tilde{c}_L$ is a natural number given by $\tilde{c}_\lambda$ in* (45), (45′), (45″) *as*

$$\tilde{c}_L = w^{-1} w_1 \prod_{\lambda \in \Lambda^*} \tilde{c}_\lambda^{\lambda(1)} .$$

REMARK 19. Though we cannot compute $\tilde{\eta}_\lambda$ approximately, Theorem 4 is useful to find divisors of $(H_\lambda : \boldsymbol{E}_\lambda)$ in Theorem 2. The process described above is also efficient for $\theta_\lambda = \theta_\lambda^R$ in (43), but is omitted here.

## § 5. Examples.

We study only Case 2. Let $-d$ be the discriminant of $F$, $\mathfrak{f}$ be the conductor for $L/F$ and decide $f \in \boldsymbol{Z}$, $f>0$, by $f\boldsymbol{Z} = \mathfrak{f} \cap \boldsymbol{Z}$.

**5.1.** Let us study some special cases.

EXAMPLE 1. Let $n=p$ be a prime number and $\Lambda^* = \{\lambda\}$. Fix a generator $b$ of $A$ and a primitive $p$-th root $\zeta \in \boldsymbol{C}$ of 1. Put

$$c = \begin{cases} 24h_1 \\ 24h_1 \\ 12fw(\mathfrak{f}) \end{cases} \quad s = \begin{cases} c/p & \text{if } f=1,\ p>2\,, \\ 2h_1 & \text{if } f=1,\ p=2\,, \\ c/w & \text{otherwise}\,. \end{cases}$$

Then, by Theorems 2, 3 and by Proposition 8, we have

$$w^{-1} w_1 c^{p-1} h = h_1(E:\boldsymbol{E}), \quad \boldsymbol{E} = W \cdot \eta_\lambda^{\boldsymbol{Z}[b]}, \quad \eta_\lambda = \theta_\lambda(b)/\theta_\lambda(1),$$

$$(E:\boldsymbol{E}) \leqq \prod_{i=1}^{p-1} \frac{2}{\log(\kappa)} \left| \prod_{j=0}^{p-1} \zeta^{ij} \log(|\theta_\lambda(b^j)|) \right| .$$

Here $\theta_\lambda = \theta_\lambda^S$ in (38), so $\boldsymbol{E} \subset E^s$ by Theorem 4, and $\kappa = \kappa_\lambda$ in (26), so

$$\kappa = \inf\left\{ \max_{1 \leqq i \leqq p} (|\varepsilon|^{2b^i}) \,\middle|\, \varepsilon \in E,\ \varepsilon \notin W \right\} \geqq p^t \cdot \sqrt[p]{\mathrm{N}(\mathfrak{f})} \qquad \left(t = \frac{2}{1-p}\right)$$

by Proposition 6. (See also Remarks 6, 10.)

EXAMPLE 2. Fix one $\lambda \in \Lambda^*$, assume $L=F_\lambda$ and let $\kappa = \kappa_\lambda$ be given by (26). Then $\kappa = \inf\{|\varepsilon|^2 \mid \varepsilon \in H^\circ\}$, where

$$H^\circ = \{\varepsilon \in H_\lambda \mid \varepsilon \notin W_\lambda,\ |\varepsilon| \geqq |\varepsilon^a|\ (a \in A)\}.$$

Assume that $L/\boldsymbol{Q}$ is galois, put $K = L \cap \boldsymbol{R}$ and $\kappa^\circ = \inf\{|\varepsilon| \mid \varepsilon \in K \cap H^\circ\}$. The galois group of $L/\boldsymbol{Q}$ is the semi-direct product of the normal subgroup $A$ and the galois group of $L/K$ generated by the complex conjugation. So, if $\varepsilon\in H^{\circ}$, then $\bar{\varepsilon}\in H^{\circ}$ and $|\varepsilon|^{2}\in K\cap H^{\circ}$. Hence $\kappa\geqq\kappa^{\circ}$. In some cases, we can estimate $\kappa^{\circ}$ using the discriminant $D^{\circ}$ of $K$:

(i) When $n=2$, clearly $\kappa^{\circ}\geqq\varepsilon^{\circ}\geqq(\sqrt{|D^{\circ}|}+\sqrt{|D^{\circ}|+4s})/2$, where $\varepsilon^{\circ}(>1)$ is the fundamental unit of $K$ and $s=\pm1=\mathrm{N}(\varepsilon^{\circ})$ is its norm.

(ii) When $n=3$ and $D^{\circ}\neq-23$, it is known by Artin's lemma that $\kappa^{\circ}>\sqrt[3]{|D^{\circ}|/4-6}$, see [**20**].

(iii) When $n=4$ and $A$ is cyclic, we can show similarly as Artin's lemma that $\kappa^{\circ}>\sqrt{\sqrt[3]{|D^{\circ}|/4+512}-7}$, see [**17**, II].

**5.2.** Let $I_1=\omega\boldsymbol{Z}+\boldsymbol{Z}$ be the ring of integers of $F$, where

$$\omega=\begin{cases}\sqrt{-d}/2 & \text{if } 4\,|\,d\,,\\ (-1+\sqrt{-d})/2 & \text{otherwise.}\end{cases}$$

We show how we get elliptic units. Recall Remark 8 again.

EXAMPLE 3. Let $L$ be the absolute class field of $F$. Then $\mathfrak{f}=\mathrm{I}_1$ and $n=h_1$. Let $\theta_{\lambda}(a)$ ($\lambda\in\Lambda^{*}$, $a\in A_{\lambda}$) be given by (38), (39).

(i) Let $d=20$. Then $h_1=2$, $L=\boldsymbol{Q}(\sqrt{5},\sqrt{-1})$. The absolute ideal class group $C(I_1)$ is represented by $I_1$ and $\mathfrak{p}=(\omega-2)\boldsymbol{Z}+2\boldsymbol{Z}$. Let $\Lambda^{*}=\{\lambda\}$ and $A=\{1, b\}$. Then, since $\mathfrak{p}^{2}=2I_1$, we have

$$\theta_{\lambda}(1)=\eta(\omega)^{48}, \qquad \theta_{\lambda}(b)=2^{12}\Bigl(\frac{1}{2}\eta\Bigl(\frac{\omega-1}{2}\Bigr)^{2}\Bigr)^{24}.$$

As in the proof of Proposition 8, we can compute by (22) that

$$\eta_{\lambda}=\theta_{\lambda}(b)/\theta_{\lambda}(1)=\eta_{\lambda}{}^{-b}\sim 321.99689438-4.1150486124\cdot10^{-13}\cdot\omega.$$

As we get $\eta_{\lambda}+\eta_{\lambda}{}^{b}\sim322.00000000-4.1150089233\cdot10^{-13}\cdot\omega$, the minimal polynomial $P_{\eta_{\lambda}}$ of $\eta_{\lambda}$ over $F=\boldsymbol{Q}(\sqrt{-5})$ is decided by Algorithm 0:

$$P_{\eta_{\lambda}}=X^{2}-322X+1 \qquad (\eta_{\lambda}=161+72\sqrt{5}).$$

(ii) Let $d=84$. Then $h_1=4$ and $L=\boldsymbol{Q}(\sqrt{-1},\sqrt{-3},\sqrt{-7})$. Let $\Lambda^{*}=\{\lambda_1,\lambda_2,\lambda_3\}$. Then $\{F_{\lambda_1}, F_{\lambda_2}, F_{\lambda_3}\}=\{F(\sqrt{-1}), F(\sqrt{-3}), F(\sqrt{-7})\}$. For $i=1, 2, 3$, the $\lambda_i$-relative elliptic units in (22) are as follows:

$$\eta_{\lambda_i}=\delta_0\delta_i/\delta_j\delta_k\in H_{\lambda_i}=E_{\lambda_i} \qquad (\{i, j, k\}=\{1, 2, 3\}).$$

Here the class invariants $\delta_i$ ($i=0, 1, 2, 3$) are given by

$$\delta_0=\eta(\omega)^{96}, \qquad \delta_1=3^{24}\Bigl(\eta\Bigl(\frac{\omega}{3}\Bigr)^{2}\Big/3\Bigr)^{48},$$

$$\delta_2=2^{24}\Big(\frac{1}{2}\eta\Big(\frac{\omega+1}{2}\Big)^2\Big)^{48},\qquad \delta_3=(\omega+2)^{24}\Big(\eta\Big(\frac{\omega+2}{5}\Big)^2\Big/5\Big)^{48}.$$

(iii) Let $d=104$. Then $h_1=6$ and $L/F$ has just three cyclic subextensions $F_2=\boldsymbol{Q}(\sqrt{-1}, \sqrt{13})$, $F_3$ and $F_6=L$ of degrees respectively 2, 3 and 6. The elliptic units in (22) are as follows:

$$\eta_2=\delta_3\delta_1^+\delta_1^-/\delta_0\delta_2^+\delta_2^- \qquad \text{belongs to } F_2$$

$$\eta_3=\delta_2^+\delta_1^-/\delta_0\delta_3,\qquad \eta_3^{b^2}=\delta_1^+\delta_2^-/\delta_2^+\delta_1^- \qquad \text{belong to } F_3.$$

$$\eta_6=\delta_0\delta_1^-/\delta_2^+\delta_3,\qquad \eta_6^b=\delta_0\delta_1^+/\delta_3\delta_2^-,\qquad \eta_6^{1+b^2+b^4}=\eta_6^{1+b^3}=1.$$

Here $b$ is a generator of the cyclic group $A$, and

$$\delta_0=\eta(\omega)^{144},\qquad \delta_1^{\pm}=(12\omega\pm109)^{12}\Big(\eta\Big(\frac{\omega\pm2}{5}\Big)^2\Big/5\Big)^{72},$$

$$\delta_2^{\mp}=(\omega\pm1)^{24}\Big(\eta\Big(\frac{\omega\pm1}{3}\Big)^2\Big/3\Big)^{72},\quad \delta_3=2^{36}\Big(\frac{1}{2}\eta\Big(\frac{\omega}{2}\Big)^2\Big)^{72}.$$

The signs correspond respectively.

EXAMPLE 4. Now we consider ramifying cases.

(i) Let $d=7$ and $L$ be the ray class field modulo $3I_1$ over $F$. Then $\mathfrak{f}=3I_1$, and $C(\mathfrak{f})$ is cyclic of order $n=4$ represented by $I_1$, $\mathfrak{p}=(\omega+1)I_1$, $\mathfrak{p}^2=(\omega-1)I_1$, $\bar{\mathfrak{p}}=\omega I_1=2\mathfrak{p}^{-1}$. Let $A^*=\{\lambda_2, \lambda_4\}$ with $n(\lambda_i)=i$ $(i=2, 4)$. Then, by (22), we have

$$\eta_{\lambda_2}=\varphi_1\varphi_3/\varphi_0\varphi_2,\qquad \eta_{\lambda_4}=\varphi_2/\varphi_0,$$

where $\varphi_i$ $(i=0, 1, 2, 3)$ are defined by (40) as follows:

$$\varphi_0=\varphi\Big(\frac{1}{3}, \omega\Big)^{36},\qquad \varphi_1=\varphi\Big(\frac{\omega+1}{3}, \omega\Big)^{36},$$

$$\varphi_2=\varphi\Big(\frac{\omega-1}{3}, \omega\Big)^{36},\qquad \varphi_3=\varphi\Big(\frac{\omega}{3}, \omega\Big)^{36}.$$

We observe that $C(\mathfrak{f})\cong R(3)$, the group of classes of proper $I_3$-ideals, so we can take other elliptic units defined by $\theta_\lambda=\theta_\lambda^R$ in (43). Fix a generator $b$ of $A$ and put

$$\delta_0=(\eta(3\omega)^2/\omega(\omega-1))^{12},\qquad \delta_1=\Big(\eta\Big(\frac{3\omega}{2}\Big)^2\Big/2(\omega-1)\Big)^{12},$$

$$\delta_2=\Big(\eta\Big(\frac{3\omega+1}{4}\Big)^2\Big/4\omega\Big)^{12},\qquad \delta_3=\Big(\eta\Big(\frac{3\omega+1}{2}\Big)^2\Big/4\Big)^{12}.$$

Further let $E_2=E_{\lambda_2}=H_{\lambda_2}$, $H_4=H_{\lambda_4}$. Then we have

$$\eta_2=\delta_1\delta_3/\delta_0\delta_2\in E_2 \qquad \text{with } \eta_2^{1+b}=1;$$

$$\eta_4=\delta_2/\delta_0, \quad \eta_4{}^b=\delta_3/\delta_1\in H_4 \qquad \text{with } \eta_4{}^{1+b^2}=1\,.$$

(ii) Let $d=3$, $n=6$ and $\mathfrak{f}=7I_1=(2\omega+3)(2\omega-1)I_1$ be given first. Then, since $C(\mathfrak{f})$ is cyclic of order 6 and the conductor of the subgroup $U=1$ is exactly $\mathfrak{f}$, a corresponding $L$ actually exists and is uniquely decided as the ray class field modulo $\mathfrak{f}$ over $F$. The elliptic units in (22) can be explicitly written similarly as in Example 3.(iii), utilizing (40) instead of (39).

(iii) Let $d=8$, $n=2$ and $\mathfrak{f}=6I_1=\omega^2(\omega+1)(\omega-1)I_1$ be given first. Then $C(\mathfrak{f})$ is of type (2, 2), so there are three subgroups $U_1$, $U_2$, $U_3$ of index 2. It is easy to see that the conductors of $U_1$, $U_2$, $U_3$ are $2I_1$, $3I_1$, $6I_1$. Therefore only one subgroup, say $U_1$, can correspond to an abelian extension $L/F$ of degree $n=2$ with conductor $\mathfrak{f}=6I_1$. The group $U_1$ is represented by $I_1$, $(2\omega+3)I_1$, and the non-trivial coset of $C(\mathfrak{f})/U_1$ is represented by $(3\omega+1)I_1$, $(\omega+3)I_1$. We also see that $L=\boldsymbol{Q}(\sqrt{-2}, \sqrt{-6})$ by [**10**].

**5.3.** Though the moduli of elliptic units are exceedingly large in general, we can do as in Example 5.(ii) then.

Example 5. The assumption and the notation being the same as in Example 3.(i), Theorems 2, 3 show that

$$48w^{-1}h=(E:W\times\langle\eta_\lambda\rangle)\leqq 2|\log(|\eta_\lambda|)|/\log(\kappa) \qquad \text{with } \kappa=\kappa_\lambda\,,$$

see also Example 1. We compute $h$ and $E$ in two different ways:

(i) The first one is to follow our general way faithfully. Let us decide $w$ by (36). Recall that $w$ divides 12. From $P_{\eta_\lambda}$, we obtain $P_\xi=X^2-33385282X+1$ for $\xi=\eta_\lambda{}^3$. Consider the equation

$$\alpha^3-3\alpha\beta=33385282, \qquad \beta^3=1 \qquad (\alpha,\ \beta\in I_1=\boldsymbol{Z}[\omega])\,.$$

Obviously $\beta=1$, and $\alpha$ is close to $\rho u+(\rho u)^{-1}$ for some $\rho\in\boldsymbol{C}$, $\rho^3=1$, where $u=321.99689438-4.1150486124\cdot10^{-13}\cdot\omega$. The equation has only one solution $(\alpha, \beta)=(322, 1)$, so $w$ is prime to 3. For $\xi=\eta_\lambda{}^4$, we get $P_\xi=X^2-10749957122X+1$. Similarly, we see that the equation

$$\alpha^4-4\alpha^2\beta+2\beta^2=10749957122, \qquad \beta^4=1 \qquad (\alpha,\ \beta\in I_1)$$

has just 4 solutions $(\alpha, \beta)=(\pm 322, 1)$, $(\pm 144\omega, 1)$. Thus $w=4$ and

$$12h=(E:\langle\sqrt{-1}\rangle\times\langle\eta_\lambda\rangle)\leqq 2|\log(|\eta_\lambda|)|/\log(\kappa)\,. \tag{47}$$

This identity also implies that $\eta_\lambda{}^4\in E^{48}$; i.e. the equation

$$((((\alpha^3-3\alpha\beta)^2-2\beta^3)^2-2\beta^6)^2-2\beta^{12})^2-2\beta^{24}=10749957122, \qquad \beta^{48}=1$$

is soluble in $I_1$. By the same method as above, we find the 4 solutions $(\alpha, \beta)=$

$(\pm 1, -1)$, $(\pm\omega, -1)$. Therefore $h=(E:\langle\sqrt{-1}\rangle\times\langle\varepsilon^{\circ}\rangle)$ with $\varepsilon^{\circ}\in E$, $P_{\varepsilon^{\circ}}=X^2-X-1$. By virtue of Remark 10, we have $h\leqq 1+4+4=9$ since $x<4$ by the notation there. While, for $p=2, 3, 5, 7$, we see that $\varepsilon^{\circ q}$ is not a $pq$-th power in $L$, where $q=(p, w)=(p, 4)$; this is the simplest case of Algorithm 3. Consequently, we get

$$h=1 \quad \text{and} \quad E=\langle\sqrt{-1}\rangle\times\langle\varepsilon^{\circ}\rangle \quad \text{with } P_{\varepsilon^{\circ}}=X^2-X-1 \quad (\varepsilon^{\circ}=(1+\sqrt{5})/2).$$

(ii) The second way is to use a smaller unit. Practically, $w=4$ is clear, so we start from (47). Since $\kappa\geqq(1+\sqrt{5})/2$ by Example 2.(i), we have $(E:\langle\sqrt{-1}\rangle\times\langle\eta_\lambda\rangle)\leqq 24$. We can show $\eta_\lambda=\varepsilon^{12}$, where

$$\varepsilon=\frac{3\omega+2}{49}g\Big(\frac{\omega+10}{7}\Big) \qquad \text{with } g(z)=(\eta(z)/\eta(7z))^4,$$

and $g(z)$ is a modular function with respect to the group

$$\Gamma_0(7)=\left\{\begin{pmatrix} s & t \\ u & v\end{pmatrix}\in SL_2(\boldsymbol{Z}) \;\middle|\; u\in 7\boldsymbol{Z}\right\}.$$

The Fourier expansion of $g(z)$ at every cusp has coefficients in $\boldsymbol{Q}$. Therefore, since $\{\omega+10, 7\}$, $\{\omega+10, 1\}$ are bases of ideals, the value $g((\omega+10)/7)$ belongs to the absolute class field $L$ of $F$, hence $\varepsilon\in E$. By a similar treatment as the example of Theorem 3 in [**26**] on pp. 217-218, it can be shown that

$$g\Big(\frac{\omega+10}{7}\Big)^b=g\Big(\frac{\omega+10}{21}\Big)=-\Big(\frac{49}{3\omega+2}\Big)^2\Big/g\Big(\frac{\omega+10}{7}\Big).$$

Thus $h=(E:\langle\sqrt{-1}\rangle\times\langle\varepsilon\rangle)\leqq 2$ with $\varepsilon^{1+b}=-1$. Computing approximately,

$$\varepsilon \sim 1.294382\cdot 10^{-9}-1.617977601\sqrt{-1}$$

follows. Applying Algorithm 0, we get

$$\varepsilon+\varepsilon^b=\varepsilon-\varepsilon^{-1} \sim 0.000000001-0.999984415\omega,$$

so $P_\varepsilon=X^2+\omega X-1$. If $\varepsilon=\xi^2$ or $\xi^2\sqrt{-1}$ with $\xi\in E$, then $-1$ is a square in $F=\boldsymbol{Q}(\sqrt{-5})$, which is a contradiction. Thus the same result holds;

$$h=1, \qquad E=\langle\sqrt{-1}\rangle\times\langle\varepsilon\rangle \qquad \text{with } P_\varepsilon=X^2+\omega X-1 \quad (\varepsilon=-\varepsilon^{\circ}\sqrt{-1}).$$

EXAMPLE 6. Let the assumption and the notation be the same as in Example 4.(i). Then $w=w_{\lambda_4}=w_{\lambda_2}=6$, $w_1=2$. Let $\boldsymbol{E}_i=W\cdot\eta_i^{\boldsymbol{Z}[b]}$ $(i=2, 4)$, $F_2=F_{\lambda_2}$ and $h_2$ be the class number of $F_2$. By Theorem 2,

$$9216h=(E:H)(E_2:\boldsymbol{E}_2)(H_4:\boldsymbol{E}_4) \qquad \text{and} \qquad 8h_2=(E_2:\boldsymbol{E}_2)$$

hold, see also Proposition 9 and (4). The complex conjugate of $\eta_4^b$ is $\eta_4^{b^3}$. Hence Theorem 3 claims

$$(H_4:\boldsymbol{E}_4)\leqq\frac{32}{v_4}\Bigl(\frac{\log(|\eta_4|)}{\log(\kappa_4)}\Bigr)^2 \quad\text{and}\quad (E_2:\boldsymbol{E}_2)\leqq\frac{2\log(|\eta_2|)}{\log(\kappa_2)}\,.$$

Here $v_4=v_{\lambda_4}=8$ by (11), (13), and

$$\kappa_4=\kappa_{\lambda_4}>\sqrt{\sqrt[3]{842.75}-7},\qquad \kappa_2=\kappa_{\lambda_2}\geqq(5+\sqrt{21})/2$$

by Examples 2.(i), (iii). The values of the elliptic units are

$$\eta_2\sim 526.99810246+1.5774048734\cdot10^{-12}\cdot\sqrt{-1}\,,$$

$$\eta_4\sim 31277.539527+3.4516838278\cdot10^{-10}\cdot\sqrt{-1}\,,$$

$$\eta_4^b\sim 0.73022048160+0.68321156918\sqrt{-1}\,.$$

Therefore, together with Algorithm 0, we obtain

$$P_{\eta_2}=X^2-527X+1\,,\qquad (E_2:\boldsymbol{E}_2)\leqq 8\,;$$

$$P_{\eta_4}=X^4-31279X^3+45681X^2-31279X+1,\qquad (H_4:\boldsymbol{E}_4)\leqq 2143\,.$$

Immediately $8h_2=(E_2:\boldsymbol{E}_2)=8$, $h_2=1$, so $\tilde\varepsilon_2{}^8=\eta_2$ or $-\eta_2$ with an $\tilde\varepsilon_2\in E_2$, and $E_2=\langle-1\rangle\times\langle\tilde\varepsilon_2\rangle$. We find $\tilde\varepsilon_2$ by Algorithm 1, testing whether

$$((\rho^2\pm1)^2-2)^2-2=527 \quad\text{or}\quad -527\,,\qquad |\rho|\leqq\sqrt{7}\,,$$

with some $\rho\in I_1$ similarly as in Example 5.(i);

(48) $$E_2=\langle-1\rangle\times\langle\tilde\varepsilon_2\rangle,\quad P_{\tilde\varepsilon_2}=X^2-(2\omega+1)X-1,\quad |\tilde\varepsilon_2|>1,\quad h_2=1.$$

Before we apply Algorithm 3, we reduce $\eta_4$ to a smaller unit. As is mentioned in Remark 19, we can find that $\eta_4\in H_4{}^{24}$. Put $K=L\cap\boldsymbol{R}$ and $H_4^\circ=H_4\cap K$. Since $\eta_4\in H_4^\circ$, $\eta_4>1$, and $w=6$, we have $\eta_4\in H_4^{\circ 6}$. By Algorithm 1 (cf. [**17**, II]), we see that $\eta_4=\xi_1{}^6$ with $\xi_1\in H_4^\circ$, $\xi_1>1$, $P_{\xi_1}=X^4-7X^3+9X^2-7X+1$. Similarly, we see that $\xi_1=\xi_2{}^2$ with $\xi_2\in H_4^\circ$, $\xi_2>1$, $P_{\xi_2}=X^4-X^3-3X^2-X+1$, and that $\xi_2\notin H_4^{\circ 2}$, hence $\xi_2\notin H_4{}^2$, so $-\xi_2\in H_4{}^2$. Therefore, for $\alpha$, $\beta$, $\gamma\in I_1$, checking the conditions

$$\alpha^2-2\beta=\gamma^2-2\beta=-1,\quad \beta^2+2\alpha\gamma+2=-3,\quad |\alpha|,|\gamma|\leqq\sqrt{17},\quad |\beta|\leqq\sqrt{40},$$

we see by Algorithm 1 again that $-\xi_2=\varepsilon_4{}^2$ with $\varepsilon_4\in H_4$,

(49) $$P_{\varepsilon_4}=X^4-(2\omega+1)X^3-3X^2+(2\omega+1)X+1,\quad |\varepsilon_4|>1,\quad \varepsilon_4{}^{1+b^2}=-1\,.$$

Put $\tilde{\boldsymbol{E}}_4=W\varepsilon_4{}^{\boldsymbol{Z}[b]}$. Then $(H_4:\tilde{\boldsymbol{E}}_4)=24^{-2}(H_4:\boldsymbol{E}_4)\leqq3$. We use Algorithm 3 here. No prime ideal $\mathfrak{p}$ of $\boldsymbol{Q}^{\lambda_4}=\boldsymbol{Q}(\sqrt{-1})$ except $\mathfrak{p}=(1-\sqrt{-1})\boldsymbol{Z}[\sqrt{-1}]$ has the norm $\mathrm{N}(\mathfrak{p})\leqq3$. Since $w=6$, testing whether $\varepsilon_4{}^{2(1-b)}$ or $\varepsilon_4{}^{2(1+b)}$ belongs to $H_4{}^4$ in a similar manner, we get $(H_4:\tilde{\boldsymbol{E}}_4)=1$;

(50) $$H_4=W\times\langle\varepsilon_4\rangle\times\langle\varepsilon_4{}^b\rangle\,,\qquad (H_4:\tilde{\boldsymbol{E}}_4)=24^2\,.$$

Corollary 1 shows that $(E:H)$ divides $2\cdot 6^3$. In the present case, from Proposition 1 of [**21**] (and 1.2.A there), follows that $(E:H)$ divides 2, while $2h=(E:H)$ by (48), (50). Therefore

$$(E:H)=2\,,\qquad h=1\,. \tag{51}$$

Since $\tilde{\varepsilon}_2$, $\varepsilon_4$, $\varepsilon_4^b$ form a free basis of $H$ and since $w=6$, one of the units $\pm\varepsilon_4$, $\pm\varepsilon_4^b$, $\pm\varepsilon_4^{1-b}$, $\pm\tilde{\varepsilon}_2$, $\pm\tilde{\varepsilon}_2\varepsilon_4$, $\pm\tilde{\varepsilon}_2\varepsilon_4^b$, $\pm\tilde{\varepsilon}_2\varepsilon_4^{1-b}$ is a square in $L$, and we actually find by Algorithms 1, 2 that

$$E=W\times\langle\varepsilon_4\rangle\times\langle\varepsilon_4^b\rangle\times\langle\varepsilon_2\rangle,\qquad P_{\varepsilon_2}=X^4-\omega X^3+(\omega+1)X-1 \tag{52}$$

with $\varepsilon_2\in E$ such that $\varepsilon_2^2=-\tilde{\varepsilon}_2\varepsilon_4^{1-b}$; this is a simple case of Algorithm 4. In (52), it is easy to see that we may take as $\varepsilon_2$ any one of the 4 conjugates. The units $\tilde{\varepsilon}_2$, $\varepsilon_4$ are uniquely decided by (48), (49). Thus the following has been computed:

*For the ray class field $L$ modulo* 3 *over $\boldsymbol{Q}(\sqrt{-7})$, the class numbers and the groups of units of the subfield $F_2=\boldsymbol{Q}(\sqrt{-7},\sqrt{-3})$ and $L$ are given by* (48)-(52).

Starting from $\eta_{\lambda_2}$, $\eta_{\lambda_4}$ in Example 4.(i) ($P_{\eta_{\lambda_2}}=X^2-12098X+1$, $P_{\eta_{\lambda_4}}=X^4-5531575X^3-4737927X^2-5531575X+1$, $\eta_{\lambda_2}{}^2=\eta_2{}^3$, $\eta_{\lambda_4}^2=\eta_4{}^3$), we can attain to the same result.

## References

[1] Z. R. Borevich and I. R. Shafarevich, Number theory, Academic Press, New York, 1966.

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

[3] A. Fröhlich, Invariants for modules over commutative separable orders, Quart. J. Math. Oxford Ser. (2), **16** (1965), 193-232.

[4] R. Gillard, Remarques sur les unités cyclotomiques et les unités elliptiques, J. Number Theory, **11** (1979), 21-48.

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

[6] G. Gras and M.-N. Gras, Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\boldsymbol{Q}$, Bull. Sci. Math. 2$^e$ série, **101** (1977), 97-129.

[7] M.-N. Gras, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cycliques cubiques de $\boldsymbol{Q}$, J. Reine Angew. Math., **277** (1975), 89-116.

[8] M.-N. Gras, Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\boldsymbol{Q}$, Publ. Math. Univ. Besançon, 1977/78, fasc. 2.

[9] M.-N. Gras, Classes et unités des extensions cycliques réelles de degré 4 de $\boldsymbol{Q}$, Ann. Inst. Fourier, **29** (1979), 107-124.

[10] F. Halter-Koch, Geschlechtertheorie der Ringklassenkörper, J. Reine Angew. Math., **250** (1971), 107-108.

[11] H. Hasse, Das Zerlegungsgesetz für die Teiler des Moduls in den Ringklassenkörpern

der komplexen Multiplikation, Monatsh. Math., **38** (1931), 331-334.

[12] A. S. Householder, The numerical treatment of a single nonlinear equation, McGraw-Hill, 1970.

[13] S. Lang, Algebraic number theory, Addison-Wesley, 1970.

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

[15] S. Mäki, The determination of units in real cyclic sextic fields, Lecture Notes in Math., **797**, Springer, 1980.

[16] C. Meyer, Die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern, Berlin, 1957.

[17] K. Nakamula, Class number calculation and elliptic unit, I. Cubic case, II. Quartic case, III. Sextic case, Proc. Japan Acad. Ser. A, **57** (1981), 56-59, 117-120, 363-366.

[18] K. Nakamula, Elliptic unit and class number calculation, RIMS Kôkyûroku, **411** (1981), 88-98.

[19] K. Nakamula, On elliptic units and a class number decomposition, RIMS Kôkyûroku, **440** (1981), 167-178.

[20] K. Nakamula, Class number calculation of a cubic field from the elliptic unit, J. Reine Angew. Math., **331** (1982), 114-123.

[21] K. Nakamula, A construction of the groups of units of some number fields from certain subgroups, Tokyo J. Math., **5** (1982), 85-106.

[22] K. Ramachandra, Some applications of Kronecker's limit formulas, Ann. of Math., **80** (1964), 104-148.

[23] G. Robert, Unitės elliptiques, Bull. Soc. Math. France, mémoire **36**, 1973.

[24] R. Schertz, Die Klassenzahl der Teilkörpern abelscher Erweiterungen imaginär-quadratischer Zahlkörper, I, II, J. Reine Angew. Math., **295** (1977), 151-168, **296** (1977), 58-79.

[25] C. L. Siegel, Lectures on advanced analytic number theory, Tata Inst. Fund. Research, Bombay, 1961.

[26] H. M. Stark, $L$-functions at $s=1$, IV, Advances in Math., **35** (1980), 197-235.

(Full editions of [**17**, II, III] will appear in Acta Arith., **45**, n°3.)

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