ACTA ARITHMETICA
XLV (1985)

Class number calculation of a quartic field from the elliptic unit

by

KEN NAKAMULA (Tokyo)

Introduction. Let K be a quartic number field with negative discriminant and having a quadratic subfield K_2. The object of this paper is to give an effective way of calculating the class number and fundamental units of K at a time. It is a generalization of our previous paper [6] which treats a cubic number field with negative discriminant. As in cubic case, the method depends on the formula of R. Schertz [11] between the class number and the elliptic unit. The only change is that we consider the relative class number and relative units with respect to K/K_2. A summary of the results has been given in the note [5, II], see also the errata at the end of this paper.

A similar method introduced in [5, III] is explained fully in a different paper [8]. The method in [5] is an analogy of G. Gras and M.-N. Gras [1] which calculates the class number and fundamental units of an absolutely abelian real number field. Another generalization of their method is given in [9] for abelian extensions over imaginary quadratic fields. It is remarkable that all these algorithms go on by some arithmetic of integers of the ground fields and by computing special values of certain well-known functions approximately. This fact stems from the explicitness of the classical theory developped by Kronecker–Weber and their successors.

In § 1, we quote some necessary results in [7] and show preliminary lemmas, introducing notations. Theorems 1 and 2, which assure the effectiveness of the algorithm, are proved in § 2. In § 3, § 4 and § 5, the actual computation is described. § 6 treats another non-galois quartic subfield in the galois closure of K/Q. Pure quartic fields $Q(\sqrt[4]{n})$ and $Q(\sqrt[4]{-4n})$ are contained in those types of fields we study. Numerical examples are given in § 7.

1. Notations and preliminaries. All number fields we consider are finite extensions of Q in C. The symbol $\langle \alpha_1, \ldots, \alpha_n \rangle$ implies a subgroup of the multiplicative group of C generated by its elements $\alpha_1, \ldots, \alpha_n$. The nth root $\sqrt[n]{\alpha}$ is taken to be positive whenever α is positive real.

Let K be a quartic number field with discriminant $D<0$ and K_2 be its quadratic subfield with discriminant $d_2>0$. We consider K in $\boldsymbol{R}$. According to [7], we choose the fundamental units of K as follows. Let H be the subgroup of relative units in the group E of positive units of K, and take the generator $\varepsilon_1>1$ of the infinite cyclic group H for the first fundamental unit. Namely, let

$$\langle\varepsilon_1\rangle = H = \{\varepsilon\in E \mid N_{K/K_2}(\varepsilon)=1\}, \quad \varepsilon_1>1. \tag{1}$$

As the second fundamental unit, let $\eta_2>1$ be the fundamental unit of K_2, and take

$$\varepsilon_2\in\{\varepsilon_1\eta_2, \sqrt{\varepsilon_1\eta_2}, \sqrt{\eta_2}\}, \quad \varepsilon_2>1. \tag{2}$$

Then ε_1, ε_2 are decided uniquely and generate E, see [7], (4)–(7) and Remark 1. Let h, h_2 respectively be the class numbers of K, K_2. Then, by Satz (2.3) and Satz (3.2) of [11],

$$h/h_2 = (E:\langle\eta,\eta_2\rangle)/2.$$

Here $\eta>1$ is the elliptic unit of K which will be defined by (12) in § 4. Since $\eta\in H$, we have

$$\eta=\varepsilon_1^{h'} \quad \text{with} \quad h'=(H:\langle\eta\rangle). \tag{3}$$

Therefore it is obtained by (1), (2) that

$$h/h_2 = h'h_0/2 \quad \text{with} \quad h_0=(E:\langle\varepsilon_1,\eta_2\rangle)=1 \text{ or } 2. \tag{4}$$

We assume h_2, η_2 are known, as they are given in a usual manner, and shall decide h', h_0 via the calculation of ε_1, ε_2, which will be obtained in the form of their minimal polynomials over $\boldsymbol{Q}$. The main part of the computation is that of h', see § 4. An additional investigation is necessary to decide h_0, see § 5.

Relative units have a good feature as follows. Let $\varepsilon\in H$, $\varepsilon>1$, then its conjugates are given by $\varepsilon^{\pm1}$, $\exp(\pm\sqrt{-1}\,\theta)$ with $0<\theta<\pi$. Therefore $K=\boldsymbol{Q}(\varepsilon)$ and the minimal polynomial of ε has the form

$$X^4-sX^3+tX^2-sX+1 \quad \text{with} \quad s,\ t\in\boldsymbol{Z}. \tag{5}$$

Moreover we have

$$\alpha:=\mathrm{Tr}_{K/K_2}(\varepsilon)=\varepsilon+\varepsilon^{-1}>2>T:=2\cos(\theta)>-2. \tag{6}$$

LEMMA 1. *The coefficient s in (5) is completely decided by the conditions*

$$|s-\alpha|<2, \quad \alpha(s-\alpha)\in\boldsymbol{Z}.$$

And then t in (5) is given by $t=2+\alpha(s-\alpha)$.

Proof. Since $s=\alpha+T$, $t=2+\alpha T$, the lemma immediately follows from (6).

Further let $D(\varepsilon)$ be the discriminant of ε with respect to $K/\boldsymbol{Q}$, then it is a non-zero multiple of D.

LEMMA 2. *The estimation $|D|\leqslant|D(\varepsilon)|<4\big((\varepsilon^2+7)^3-8^3\big)$ holds.*

Proof. Only the second inequality is non-trivial. Define the polynomial function on $\boldsymbol{R}$ by $g(X)=(\alpha-X)^4(4-X^2)$, then, by (6), we have

$$|D(\varepsilon)|=(\alpha^2-4)\,g(T).$$

In the interval $(-2,2)$, we see $g(X)$ attains its maximum at $X=M$, where M is the unique zero of $g'(X)$ in $(-2,2)$. It is easily seen that

$$\alpha M=3M^2-8, \quad -4/3<M<-8/3\alpha.$$

Therefore we obtain

$$g(M)=4\cdot3^{-6}\big(633\alpha^4+4536\alpha^2+1728-3\alpha M(4\alpha^4+393\alpha^2+864)\big),$$

and then

$$g(M)<4\cdot3^{-6}\big(633\alpha^4+4536\alpha^2+1728+(24-64\alpha^{-2})(4\alpha^4+393\alpha^2+864)\big).$$

Multiplying this by α^2-4, we get

$$|D(\varepsilon)|<4\cdot3^{-6}(729\alpha^6+10796\alpha^4-57536\alpha^2-44544+221184\alpha^{-2}).$$

From this, the lemma follows after an easy calculation.

For any $\xi\in E$ such that $K=\boldsymbol{Q}(\xi)$, let

$$X^4-s(\xi)X^3+t(\xi)X^2-u(\xi)X+v(\xi) \tag{7}$$

be its minimal polynomial over $\boldsymbol{Q}$. In particular, we denote

$$s=s(\varepsilon_1), \quad t=t(\varepsilon_1); \quad s'=s(\varepsilon_2), \quad t'=t(\varepsilon_2), \quad u'=u(\varepsilon_2), \quad v'=v(\varepsilon_2). \tag{8}$$

Let the minimal polynomial of η_2 over $\boldsymbol{Q}$ be given by

$$X^2-lX+c. \tag{9}$$

To compute h_0, we need the following two lemmas.

LEMMA 3. *Put $d_2'=\sqrt{(l^2-4c)(s^2-4t+8)}$, then $d_2'\in\boldsymbol{N}$ and $d_2\,|\,d_2'$. For $\xi=\varepsilon_1\eta_2$, we have*

$$u(\xi)=c\big(ls-s(\xi)\big), \quad v(\xi)=1$$

and

$$s(\xi)=(ls+d_2')/2, \quad t(\xi)=l^2+c(t-4).$$

Proof. Put $\varepsilon=\varepsilon_1$ and use the same notation as in (6). Then $K_2=\boldsymbol{Q}(\eta_2)=\boldsymbol{Q}(\alpha)$ holds, and α, T are the conjugate roots of the irreducible equation $X^2-sX+t-2=0$. Therefore the first statement immediately follows. It is easily seen that $s(\xi)+cu(\xi)=ls$, $t(\xi)=l^2+c(t-4)$, $v(\xi)=1$ and

that $s(\xi) = \mathrm{Tr}_{K_2/Q}(\alpha\eta_2)$. Since each α, η_2 is the larger one among its conjugates, we can compute $s(\xi)$ directly and obtain the second assertion.

Assume $c = -1$ in (9), let $\beta = \eta_2(\varepsilon_1 - \varepsilon_1^{-1})$ and put

$$a = 4s^2 - (t+2)^2, \quad b = \beta + a\beta^{-1}. \tag{10}$$

LEMMA 4. *The assumption being as above, we have* $a, b \in N$ *and* $K_2 = Q(\beta)$.

Proof. Put $\varepsilon = \varepsilon_1$ and use the notation in (6). Then $\beta = \eta_2(\alpha^2 - 4)$, and so $N_{K_2/Q}(\beta) = (\alpha^2-4)(4-T^2) = a \in N$, hence $b = \mathrm{Tr}_{K_2/Q}(\beta) \in N$. Suppose $\beta \in Z$, then $0 < \beta = (4-T^2)/\eta_2 < 4$ and $a = \beta^2 \equiv 0$ or $1 \pmod 4$, while $a \equiv -t^2 \pmod 4$. Therefore $\beta = 2$, $a = 4$, so $s = 1$, $t = -2$, thus $2 = \eta_2\alpha > 2$, which is a contradiction. This proves the lemma.

2. An upper bound of h' and a recursive sequence

2.1. Let $\varepsilon \in H$, $\varepsilon > 1$, then $\varepsilon = \varepsilon_1^n$ with $n \in N$. The next theorem gives an easily computable upper bound of n from ε and the discriminant D.

THEOREM 1. *The assumption being as above, we have*

$$n < B(\varepsilon) := 2\log(\varepsilon)/\log\left(\sqrt[3]{(|D|/4)+512} - 7\right).$$

Proof. By Lemma 2 above, the result is similarly shown as Theorem 1 of [6].

This theorem enables us to know a finite number of possible values of n from an approximate value of ε. Especially, for the elliptic unit η given by (12) in § 4, the index h' in (3) is smaller than $B(\eta)$. Therefore the following is obvious from (4).

COROLLARY 1. *The relative class number* h/h_2 *is smaller than* $B(\eta)$.

2.2. For $j, k \in Z$, define a recursive sequence $r_n = r_n(j, k)$ $(n = 1, 2, 3, \ldots)$ by the following:

$$r_1 = j, \quad r_2 = jr_1 - 2k, \quad r_3 = jr_2 - kr_1 + 3j, \quad r_4 = jr_3 - kr_2 + jr_1 - 4,$$
$$r_n = jr_{n-1} - kr_{n-2} + jr_{n-3} - r_{n-4} \quad (n = 5, 6, \ldots).$$

Let $\xi \in H$, $\xi > 1$, and $n \in N$. Put $\varepsilon = \sqrt[n]{\xi}$ and $\alpha = \varepsilon + \varepsilon^{-1}$. For every $j \in Z$, denote by $j' \in Z$ the nearest one to $2 + \alpha(j - \alpha)$. Recall the notation in (7). We may consider only $s(\cdot)$, $t(\cdot)$ for units in H on account of (5).

THEOREM 2. *The notation being as above, the real number* ε *belongs to* H *if and only if there is* $j \in Z$ *such that*

$$|j - \alpha| < 2, \quad r_n(j, j') = s(\xi), \quad r_n(j'-2, j^2 - 2j' + 2) + 2 = t(\xi). \tag{11}$$

Moreover $s(\varepsilon) = j$, $t(\varepsilon) = j'$ *if* (11) *holds with* $j \in Z$.

Proof. Assume $\varepsilon \in H$ and put $j = s(\varepsilon)$. Then $|j - \alpha| < 2$ and $j' = t(\varepsilon)$ by Lemma 1. Writing $s(\xi)$, $t(\xi)$ as polynomials of j, j', we obtain the equalities in (11). Conversely, suppose (11) is satisfied by $j \in Z$. Let the roots of the equation $X^4 - jX^3 + j'X^2 - jX + 1 = 0$ be $\lambda^{\pm 1}$, $\mu^{\pm 1}$. Then $\lambda^{\pm n}$, $\mu^{\pm n}$ are the conjugates of ξ by the equalities in (11). So we assume $\lambda^n = \xi$, and then $K = Q(\xi)$ is contained in $Q(\lambda)$. Since λ is of degree at most 4 over Q, we have $K = Q(\lambda)$, therefore $\lambda \in R$ and $\varepsilon = \pm\lambda$, hence $\varepsilon \in H$. If $\varepsilon = -\lambda$, it is derived from (6), (11) that $2 > |j - \alpha| = |s(\varepsilon) + \alpha| > 2\alpha - 2 > 2$, a contradiction. This implies that $\varepsilon = \lambda$, $s(\varepsilon) = j$, $t(\varepsilon) = j'$, thus the proof is complete.

This theorem gives an effective way to judge whether ε belongs to H or not when $s(\xi)$, $t(\xi)$ are known. During the test we obtain $s(\varepsilon)$, $t(\varepsilon)$ together if $\varepsilon \in H$.

3. Calculation of a ring class group. To obtain the elliptic unit of K, we should calculate a ring class subgroup of the imaginary quadratic field $F = Q(\sqrt{d_2 D})$. The results of this section owe very much to F. Halter-Koch [2], the method is the same as in H. Hasse [3], and the computation goes similarly as in § 3 of [6], so consult them in detail.

Every K we consider is characterized as the maximal real subfield of its galois closure $L = K \cdot F$, which is a cyclic quartic ring class field extension over F with conductor $f \in N$, and then $D = -dd_2 f^2$ holds, where $-d$ is the discriminant of F. We compute every subgroup U^* of the ring class group $R^*(f)$ modulo f in F such that $R^*(f)/U^*$ is cyclic of order 4 and that the conductor of U^* is exactly f, assuming that d and f are given. We also compute a class r^* such that $r^* U^*$ is of order 2 in $R^*(f)/U^*$. Note that the quadratic subextension $L_2 = K_2 \cdot F$ has the conductor $f_2 \in N$, $f_2 | f$, over F.

Let I_1 be the ring of integers of F. To avoid the complexity, we treat only when I_1 is principal and f is odd. Then we have

$$d = 3, 4, 7, 8, 11, 19, 43, 67 \text{ or } 163,$$
$$f = p_1 \ldots p_{m'}, \quad f_2 = p_1 \ldots p_m, \quad m' \geqslant m > 0.$$

Here $p_1, \ldots, p_{m'}$ are distinct prime numbers such that

$$p_i \equiv \left(\frac{-d}{p_i}\right) \pmod 4 \quad \text{for} \quad i = 1, \ldots, m,$$

where $\left(\frac{-d}{\cdot}\right)$ is the Kronecker symbol. In case $d = 4$, we have $f_2 \equiv \pm 1 \pmod 8$. For $i = 1, \ldots, m'$, let z_i be a *primitive ring root* modulo p_i, see Remark 2 of [6], which satisfies $z_i \equiv n \pmod{f/p_i}$ with $n \in Z$, $(n, f/p_i) = 1$, and put

$$k_i = \tfrac{1}{2}\left(p_i - \left(\frac{-d}{p_i}\right)\right).$$

PROPOSITION 1. *The notation being as above, we take* $x_i = 1$ *or* 3 *for* $i = 1, \ldots, m-1$. *Then a subgroup* U^* *of* $R^*(f)$, *corresponding to a cyclic*

quartic ring class field extension L/F with conductor f such that f_2 is the conductor of the quadratic subextension L_2/F, is represented by the following principal ideals of F:

$$\prod_{i=1}^{m-1}(z_i^{x_i}z_{i+1})^{X_i}\prod_{i=m+1}^{m'}(z_1^2z_i)^{X_i}\prod_{i=1}^{m'}z_i^{4Y_i}I_1,$$

where, for $i=1,\ldots,m'$,

$$0\leqslant X_i<4\ (i\neq m),\quad 0\leqslant Y_i<\tfrac{1}{2}k_i\quad \text{if}\quad k_i\quad \text{even},$$
$$0\leqslant X_i<2\ (i\neq m),\quad 0\leqslant Y_i<k_i\quad \text{if}\quad k_i\quad \text{odd},$$
$$0\leqslant Y_m<\tfrac{1}{6}k_m\quad \text{if}\quad d=3,\quad 0\leqslant X_{m-1}+4Y_m<k_m\quad \text{if}\quad d=4.$$

The class r^* represented by $z_1^2I_1$ is of order 2 modulo U^*.

Proof. Similarly shown to Proposition 2 of [3].

The field K in question is realized as the maximal real subfield of L and K_2 is that of L_2. The galois closure of K/Q is L. The discriminant d_2 of K_2 is decided as below. Consider the decomposition $df_2^2=d_2\tilde{d}_2$ such that $d_2>0$ and $-\tilde{d}_2<0$ are the discriminants of quadratic number fields and that $f_2|d_2|df_2$. The character χ which corresponds to the quadratic extension $Q(\sqrt{d_2},\sqrt{-\tilde{d}_2})/F$ is given by (4.4) of [10]. There is a unique decomposition as above which satisfies $\chi(z_1I_1)=\ldots=\chi(z_mI_1)=-1$, and this determines the d_2. If K_2 is fixed, in other words, if f_2 is fixed in addition to d, f, there are 2^{m-1} distinct K with the same discriminant $D=-dd_2f^2$, each corresponding to the choice of $x_1,\ldots,x_{m-1}$ in Proposition 1.

4. Calculation of η, ε_1 and h'. We keep the notation in § 3. The representatives of U^*, r^*U^* being given as in Proposition 1, we compute Z_k, Z_{rk} ($k\in U$), where the notation is the same as in § 3 of [6]. By the *elliptic unit* of K, we mean the unit $\eta>1$ defined by

$$\eta=\prod_{k\in U}\frac{\sqrt{\mathrm{Im}(Z_{rk})}\,|\eta(Z_{rk})|^2}{\sqrt{\mathrm{Im}(Z_k)}\,|\eta(Z_k)|^2},\tag{12}$$

where $\eta(\cdot)$ is the Dedekind eta function. Then the formula (4) in § 1 holds as we have already seen. Computing a good approximate value of η by Lemma 3 of [5, I] for example, we can decide $s(\eta)$, $t(\eta)$ by Lemma 1, recall (5) and the notation in (7). Such a procedure is actually effective as is explained in §4 of [6].

The calculation of ε_1 in (1), s, t in (8) and h' in (3), from $s(\eta)$, $t(\eta)$ and an approximate value of η, goes completely by the same manner as in § 5 of [6]. Instead of Theorems 1, 2 there, we now utilize Theorems 1, 2 of this paper for the effectiveness of our computation. Numerical examples in § 7 will

explain how this algorithm goes. It only uses some arithmetic in Z and can be translated into a program of electric computers.

As is seen from Lemma 2, the magnitude of η becomes exceedingly large unless $|D|$ is small. If the integer part of η has N decimal digits, at least $2N+2$ digits precision is required to decide the coefficients of the minimal polynomial of η. After we have obtained $s(\eta)$, $t(\eta)$, less accuracy for approximate values of units is enough, however. So, it is important to find any other method, algebraic or else, to decide the minimal polynomial of the elliptic unit η.

5. Calculation of ε_2 and h_0. The remaining problem is to decide ε_2 in (2) and h_0 in (4). We suppose that the minimal polynomial (9) of η_2 is known. Using the notation in (7), (8), we compute s', t', u', v' from s, t, l, c.

To test whether $\xi=\varepsilon_1\eta_2$ is a square in K, we need the following proposition. Put $\varepsilon=\sqrt{\xi}$, $\gamma=\sqrt{\eta_2}$ and $\alpha=\sqrt{\varepsilon_1}+c\sqrt{\varepsilon_1^{-1}}$.

PROPOSITION 2. *The notation being as above, the real number ε is a unit in E if and only if certain rational integers i, j, k satisfy*

$$|i-\alpha\gamma|<2\gamma^{-1},\quad s(\xi)=i^2-2j,\quad t(\xi)=j^2-2ik+2c,\quad u(\xi)=k^2-2cj.\tag{13}$$

Moreover, if (13) holds for i, j, $k\in Z$, we have $s'=i$, $t'=j$, $u'=k$, $v'=c$ and $h_0=2$.

Proof. Assume $\varepsilon\in E$, then ε, $c\varepsilon^{-1}\eta_2$, $\gamma^{-1}\exp(\pm\sqrt{-1}\,\theta)$ are its conjugates over Q with $0<\theta<\pi$. Therefore (13) is shown as in the proof of Theorem 2. Now take i, j, $k\in Z$ which satisfy (13). Then, in the same way as before, the polynomial $g(X)=X^4-iX^3+jX^2-kX+c$ has a root λ such that $K=Q(\xi)=Q(\lambda)$ and $\varepsilon=\pm\lambda$. Therefore $\varepsilon\in E$ is obtained. We also note that $|s(\varepsilon)-\alpha\gamma|<2\gamma^{-1}$ holds. Suppose $\varepsilon=-\lambda$, then $i=-s(\varepsilon)$, so $|\alpha\gamma\pm i|<2\gamma^{-1}$, hence $c=-1$. While, the integer $\alpha\gamma=\mathrm{Tr}_{K/K_2}(\varepsilon)$ is represented as $\alpha\gamma=\frac{1}{2}(n\sqrt{d_2}-i)$ with $n\in Z$, therefore

$$|n\sqrt{d_2}+i|<4\gamma^{-1},\quad |n\sqrt{d_2}-3i|<4\gamma^{-1}.$$

If $n=0$, we obtain $\alpha\gamma=-i/2=0$, a contradiction. Otherwise, since $|n\sqrt{d_2}|<4\gamma^{-1}$, we have $d_2=5$, $n=\pm1$, $i=0$, namely $\alpha\gamma=\pm\frac{1}{2}\sqrt{5}$, which is also a contradiction. Thus $\varepsilon=\lambda$ and the proof ends.

To test whether η_2 is a square in K, we restrict ourselves to the case $c=-1$ on account of Remark 1 of [7].

PROPOSITION 3. *Assume $c=-1$ and let a, b be given by (10). For $\sqrt{\eta_2}\in E$, it is necessary and sufficient that $a=a'^2$, $b=b'^2-2a'$ with a', $b'\in Z$. And then $s'=u'=0$, $t'=-l$, $v'=-1$ and $h_0=2$.*

Proof. Let β be as in Lemma 4. Since $K=K_2(\varepsilon_1-\varepsilon_1^{-1})$, the condition $K=K_2(\sqrt{\eta_2})$ is equivalent to the condition that β is a square in K_2. By

Lemma 4, we can prove that the latter occurs if and only if $a = a'^2$, $b = b'^2 - 2a'$ by the same method as Theorem 2 or Proposition 2. Other assertions are trivial.

Remark 1. Proposition 2 is a little simpler than Proposition 3 in [5, II]. The latter, however, indicates a general procedure as in Algorithm 1 of [9] which can be applied to a number field of higher degree. Proposition 3, together with its proof, is a special case of a more general method which utilizes the Lagrange resolvent. For another example of this method, see Proposition 4 of [8].

Remark 2. Since K/K_2 is ramified, either h_0 or h' is even by (4), so we get $\varepsilon_2 \neq \varepsilon_1 \eta_2$ if we know h' is odd during the computation of ε_1. We also see that $\varepsilon_2 = \sqrt{\eta_2}$ may occur only when $Q(\sqrt{D}) = Q(\sqrt{-1})$, and then $a = a'^2$ in Proposition 3 is always true. Therefore, by the results of [2], we can restrict ourselves only in case $d = 4d_2 \equiv 4 \pmod{16}$, $f \mid 8$, $f_2 = 1$ and in case $d = d_2 \equiv 8 \pmod{16}$, $f = 4$, $f_2 = 2$, where the notation is the same as in § 3. These facts are useful in the actual calculation.

All necessary constants in Propositions 2, 3 to decide ε_2 in (2) are computable by (10) and Lemma 3 after we have obtained s, t in (7), l, c in (9) and approximate values of ε_1, η_2. Thus s', t', u', v' and h_0 are computed in a finite number of steps, and the calculation of the class number h ends completely by (4).

6. Another quartic subfield $\tilde{K}$. The galois closure L of K/Q contains a totally imaginary non-galois quartic subfield $\tilde{K}$. Let $\tilde{h}$ and $\tilde{\varepsilon}_0$ be its class number and a fundamental unit. Further let $\tilde{h}_2$ and $-\tilde{d}_2$ respectively be the class number and the discriminant of its quadratic subfield $\tilde{K}_2 = Q(\sqrt{D})$. Then it easily follows, by the Brauer–Kuroda theorem, from a character relation of the galois group of L/Q that

$$\frac{h \log(|N_{K/K_2}(\varepsilon_2)|)}{h_2 \log(\eta_2)} = \frac{\tilde{h} |\log(|\tilde{\varepsilon}_0|^2)|}{\tilde{h}_2 \log(\varepsilon_1)}.$$

Since $|\tilde{\varepsilon}_0|^2 = N_{L/K}(\tilde{\varepsilon}_0) \in H$ by (1), this implies

$$h' = 2h/h_0 h_2 = \tilde{h}(H : \langle |\tilde{\varepsilon}_0|^2 \rangle)/\tilde{h}_2$$

by (2), (4). Applying Proposition 5 of [7] to this, we obtain

$$(H : \langle |\tilde{\varepsilon}_0|^2 \rangle) = 2/\tilde{h}_0$$

with

$$\tilde{h}_0 = (\langle \varrho, \tilde{\varepsilon}_0 \rangle : \langle \varrho, \tilde{\varepsilon}_1 \rangle) = 1 \text{ or } 2, \quad \tilde{\varepsilon}_1 = N_{L/\tilde{K}}(\varepsilon_1), \tag{14}$$

where ϱ is a generator of the group of 2-nd power roots of 1 in $\tilde{K}_2$. So it follows that

$$\tilde{h}/\tilde{h}_2 = h' \tilde{h}_0/2 = h\tilde{h}_0/h_2 h_0, \tag{15}$$

and thus the computation of $\tilde{h}$ is reduced to that of $\tilde{h}_2$, $\tilde{h}_0$. We assume $\tilde{h}_2$ is known by a usual manner. To decide $\tilde{h}_0$, it is enough to see whether $\tilde{\varepsilon}_1$ or $\varrho\tilde{\varepsilon}_1$ is a square in $\tilde{K}$, and that is accomplished by the same technique as in § 4, § 5.

Let s, t be as in (7), then $\tilde{\varepsilon}_1$ has its minimal polynomial

$$X^4 - (t-2)X^3 + (s^2 - 2t + 2)X^2 - (t-2)X + 1. \tag{16}$$

When $\tilde{d}_2 = 4$, taking $\varrho = \pm\sqrt{-1}$ suitably, we have

$$X^4 - \sqrt{a}X^3 + (s^2 - 2t - 2)X^2 + \sqrt{a}X + 1$$

as the minimal polynomial of $\varrho\tilde{\varepsilon}_1$. Here a is given by (10) and $\sqrt{a} \in N$ holds as in Remark 2. Assume $\tilde{\varepsilon}_1 = \varepsilon^2$ with $\varepsilon \in \tilde{K}$, and let the minimal polynomial of ε be

$$X^4 - iX^3 + jX^2 - kX + 1 \tag{17}$$

with i, j, $k \in Z$. Then $\sqrt{\varepsilon_1^{\pm 1}} \exp(\pm\sqrt{-1}\theta)$ are the conjugates of ε with $0 < \theta < \pi$, so we easily see that

$$i^2 = 2s + t + 2, \quad j = s + 2, \quad k = i. \tag{18}$$

Conversely, if (18) holds with i, j, $k \in Z$, a zero, say ε, of (17) satisfies $\varepsilon^2 = \tilde{\varepsilon}_1$, therefore $\tilde{K} = Q(\tilde{\varepsilon}_1) = Q(\varepsilon)$ as before. We can show that $-\tilde{\varepsilon}_1$ is a square in $\tilde{K}$ if and only if

$$i^2 = 2s - t - 2, \quad j = s - 2, \quad k = -i, \tag{19}$$

hold with i, j, $k \in Z$, and then (17) gives the minimal polynomial of a fundamental unit of $\tilde{K}$. In case $\tilde{d}_2 = 4$, we consider

$$i^2 = 2s + \sqrt{a}, \quad k^2 = 2s - \sqrt{a}, \quad ik = t + 2, \quad j = s, \tag{19'}$$

in place of (19), in order to test whether $\varrho\tilde{\varepsilon}_1$ is a square in $\tilde{K}$ or not. On account of (14), we can state as follows.

Proposition 4. *The notation being as above, the index $\tilde{h}_0 = 2$ holds if and only if certain i, j, $k \in Z$ satisfy* (18) *or* (19) (*satisfy* (18) *or* (19′) *in case $\tilde{d}_2 = 4$*), *and then* (17) *is the minimal polynomial over Q of a fundamental unit of $\tilde{K}$. Otherwise $\tilde{h}_0 = 1$ and* (16) *is the minimal polynomial over Q of a fundamental unit of $\tilde{K}$.*

Thus we complete the computation of $\tilde{h}$ by (15). We add a relation between h and $\tilde{h}$ derived from Proposition 5 of [7] and (15) above, in the end.

Corollary 2. *If $\varepsilon_2 = \sqrt{\varepsilon_1 \eta_2}$ in* (2), *we have $h_0 = \tilde{h}_0 = 2$, and consequently $h/h_2 = \tilde{h}/\tilde{h}_2$.*

Remark 3. Since $\tilde{K}/\tilde{K}_2$ is abelian and $\tilde{K}_2/Q$ is quadratic, we see that $\tilde{K}/\tilde{K}_2$ is a ramified extension by the fact that $\tilde{K}$ is not galois over Q. So we

get $\tilde{h}_0 = 2$ if h' is odd by using (15) similarly as in Remark 2, and then the conclusion in Corollary 2 is also valid. In such a case, the integer $h/h_2 = \tilde{h}/\tilde{h}_2$ is odd.

7. Examples

7.1. We use the notation in § 3 and § 6. The fields K and $\tilde{K}$ are pure if and only if $d = 4$. Then $K = Q(\sqrt[4]{n})$, $\tilde{K} = Q(\sqrt[4]{-4n})$, where $n = AB^2C^3$ with pairwise relatively prime A, B, $C \in \boldsymbol{N}$, which is decided by computing the quartic power residue symbol $\left(\frac{\cdot}{\cdot}\right)_4$ in Hasse [4]. When the conductor f of L/F is odd, we give them exactly. Let $y_1, \ldots, y_m \in \boldsymbol{Z}$ so that

$$\left(\frac{z_i}{p_i}\right)_4 = \sqrt{-1}^{y_i} \quad (i = 1, \ldots, m),$$

and put

$$S = \{i \mid 1 \leqslant i \leqslant m,\ (-1)^{i-1} x_1 \ldots x_{i-1} y_i \equiv y_1 \pmod 4\}.$$

Then we have

$$A = \prod_{i \in S} p_i, \quad C = f_2/A, \quad B = \begin{cases} f/f_2 & \text{if} \quad f_2 \equiv 1 \pmod 8, \\ 2f/f_2 & \text{if} \quad f_2 \equiv -1 \pmod 8. \end{cases}$$

Of course A and C may be replaced with each other.

7.2. Recall the notation in (7), (8), (9). We mean by

$$X^4 - \tilde{s}X^3 + \tilde{t}X^2 - \tilde{u}X + 1$$

the minimal polynomial of a certain fundamental unit of $\tilde{K}$ in § 6. The symbols h, h_2, h_0, $\tilde{h}$, $\tilde{h}_2$, $\tilde{h}_0$ and h' are as in § 1 and § 6.

(i) Let $d = 3$ in § 3. We first give an example when L/F has an even conductor. Assume $f = 16$, $f_2 = 8$, then $d_2 = 24$, $D = -2^{11}3^2$. There is a unique K with the discriminant D and the elliptic unit is given by

$$\eta = \left| \eta\left(\frac{8\omega}{3}\right) \eta\left(\frac{-1+4\omega}{2}\right) \Big/ \eta(8\omega)\, \eta\left(\frac{3+4\omega}{6}\right) \right|^2, \quad \omega = \sqrt{-3}.$$

Compute it approximately, and we see $\eta \sim 37.569300442$. We use Lemma 1 now. Then $36 \leqslant s(\eta) \leqslant 39$ follows. Next put $\alpha = \eta + \eta^{-1}$, then $2 + \alpha(36-\alpha) \sim -57.99999909$, $2 + \alpha(37-\alpha) \sim -20.40408117$, $2 + \alpha(38-\alpha) \sim 17.19183675$, $2 + \alpha(39-\alpha) \sim 54.78775467$, therefore $s(\eta) = 36$ and $t(\eta) = -58$. By Theorem 1, we get $h' < B(\eta) \sim 3.1$, so $h' \leqslant 3$. Let $n = 2$, $\xi = \eta$ in Theorem 2. Then $(j, j') = (5, -6)$, $(6, 0)$, $(7, 6)$ or $(8, 13)$. Calculating the recursive sequences in (11), we see that $\sqrt{\eta} \notin H$, so h' is odd. Similarly we obtain that h' is not divisible by 3. Hence

$$\varepsilon_1 = \eta, \quad s = 36, \quad t = -58, \quad h' = 1.$$

We mention that $h_2 = 1$, $l = 10$, $c = 1$ and $\eta_2 = 5 + 2\sqrt{6}$. Therefore

$$h_0 = 2, \quad h = 1, \quad \varepsilon_2 = \sqrt{\varepsilon_1 \eta_2},$$

by Remark 2, and $s(\xi) = 372$, $t(\xi) = 38$, $u(\xi) = -12$ ($\xi = \varepsilon_1 \eta_2$) by Lemma 3. By the inequality and the first two equalities in (13), we should have $s' = 20$, $t' = (20^2 - 372)/2 = 14$, $u' = (14^2 + 2 - 38)/40 = 4$, on account of Proposition 2. Indeed the last equality in (13) is satisfied, too, i.e. $4^2 - 28 = -12$. Thus

$$s' = 20, \quad t' = 14, \quad u' = 4, \quad v' = 1.$$

Either Corollary 2 or Remark 3 says that

$$\tilde{h}_0 = 2, \quad \tilde{h} = 1,$$

since $\tilde{d}_2 = 8$, $\tilde{h}_2 = 1$. We actually see $2s + t + 2 = 16 = 4^2$, so

$$\tilde{s} = 4, \quad \tilde{t} = 38, \quad \tilde{u} = 4$$

by Proposition 4.

(ii) As an example of Proposition 1, let $d = 7$, $f = f_2 = 3$. Then $d_2 = 21$, $D = 3^3 7^2$, and K is uniquely decided. In this case, we see $\eta \sim 2.3692054048$ and obtain

$$\varepsilon_1 = \eta, \quad h' = 1, \quad s = 1, \quad t = -3,$$

only by Lemma 1 and Theorem 1. As in (i), we get

$$h_0 = 2, \quad h = 1, \quad \varepsilon_2 = \sqrt{\varepsilon_1 \eta_2}$$

since $h_2 = 1$. As $l = 5$, $c = 1$ and $\eta_2 = \frac{1}{2}(5 + \sqrt{21})$, we have $X^4 - 13X^3 + 18X^2 + 8X - 1$ as the minimal polynomial of $\varepsilon_1 \eta_2$ by Lemma 3. In Proposition 2, we may test only for $i = 4, 5$. In the same way as above, we obtain

$$s' = 5, \quad t' = 6, \quad u' = 2, \quad v' = 1.$$

Since $\tilde{d}_2 = 3$, $\tilde{h}_2 = 1$, Proposition 4 shows easily that

$$\tilde{h}_0 = 2, \quad \tilde{h} = 1, \quad (\tilde{s}, \tilde{t}, \tilde{u}) = (1, 3, 1).$$

(iii) We treat the case as in Remark 2. Let $d = 8$, $f = 4$, $f_2 = 2$. Then $d_2 = 8$, $D = -2$, and K is unique. We know $h_2 = 1$, $\eta_2 = 1 + \sqrt{2}$, $l = 2$, $c = -1$, $\tilde{d}_2 = 4$ and $\tilde{h}_2 = 1$. Utilizing the approximate value $\eta \sim 4.611581784$, it is shown that

$$h' = 1, \quad (s, t) = (4, -2), \quad h_0 = 2, \quad h = 1.$$

By (10), we have $a = 64 = 8^2$, $b \sim 47.99999988$, hence $b = 50$. Putting $a' = b' = 8$ in Proposition 3, we find

$$\varepsilon_2 = \sqrt{\eta_2}, \quad (s', t', u', v') = (0, -2, 0, -1),$$

which again proves $h_0 = 2$. For K, considering (19′) now, we get

$$\tilde{s} = \tilde{t} = \tilde{u} = 4, \quad \tilde{h}_0 = 2, \quad \tilde{h} = 1.$$

(iv) In case the class number of $F = Q(\sqrt{d_2 D})$ is not 1, we have the following example. Let $d = 39$, $f = 1$. Namely, let K be the maximal real subfield of the absolute class field of $Q(\sqrt{-39})$. Then $\eta \sim 1.722083804$. So we see that

$$h' = 1, \quad h_0 = 2, \quad h = 1, \quad \tilde{h}_0 = 2, \quad \tilde{h} - 1,$$

and that

$$(s, t) = (1, -1), \quad (s', t', u', v') = (2, -2, -3, -1), \quad (\tilde{s}, \tilde{t}, \tilde{u}) = (1, -1, -1).$$

7.3. For pure quartic fields $K = Q(\sqrt[4]{n})$ and $K = Q(\sqrt[4]{-4n})$, $n \in N$, a few numerical results are given in the table below. We mention that $\varepsilon_2 \neq \sqrt{\eta_2}$ in (2) as in Remark 2 and that s', t', u', v' are obtained by Lemma 3 when $\varepsilon_2 = \varepsilon_1 \eta_2$, $h_0 = 1$. The method in 7.1 is applied to decide n for $f = 15$.

Table 1

f	n	h'	s,	t	h_0	s',	t',	u',	v'	h	$\tilde{h}_0$	$\tilde{s}$,	$\tilde{t}$,	$\tilde{u}$	$\tilde{h}$
6	12	2	2,	0	1	10,	12,	−2,	1	1	1	−2,	6,	−2	1
7	28	1	4,	−1	2	10,	13,	−4,	1	1	2	3,	6,	3	1
8	2	1	12,	6	2	4,	−6,	4,	−1	1	2	4,	10,	−4	1
10	5	2	6,	6	1	8,	−1,	2,	1	1	2	2,	4,	−2	1
12	3	2	14,	24	1	46,	36,	10,	1	1	1	22,	150,	22	1
15	540	2	4,	−9	2	8,	9,	2,	1	4	2	1,	6,	1	4
15	60	2	64,	66	1	496,	126,	16,	1	2	2	14,	66,	14	4

An approximate value of η utilized in each case above is listed in the following table. The integer part of the upper bound $B(\eta)$ of h', the coefficients $s(\eta)$, $t(\eta)$ and an approximate value of $2+\alpha(s(\eta)-\alpha)$, where $\alpha = \eta + \eta^{-1}$, are also contained there.

Table 2

f	n	η	$[B(\eta)]$	$s(\eta)$	$t(\eta)$	$2+\alpha(s(\eta)-\alpha)$
6	12	5.274510563	3	4	−6	−5.999999990
7	28	4.419480363	3	4	−1	−0.999999985
8	2	11.57042700	4	12	6	6.000000187
10	5	25.37700210	2	24	−34	−33.99999979
12	3	146.7393188	5	148	186	186.0000463
15	540	32.46112731	2	34	51	50.99999993
15	60	3964.967221	5	3964	−3834	−3833.999769

Errata for [5, II]

page	line	for	read
117	15	positive units	positive relative units
118	38	$2+\alpha(\alpha-s)$	$2+\alpha(s-\alpha)$
120	5	generates	is of order 2 in
	22	$\sqrt{\eta_e}$	$\sqrt{\eta_2}$

References

[1] G. Gras and M.-N. Gras, *Calcul du nombre de classes et des unités des extensions abéliennes réelles de Q*, Bull. Soc. Math. France 2e série 101 (1977), pp. 97–129.

[2] F. Halter-Koch, *Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe*, J. Number Theory 3 (1971), pp. 412–443.

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

[4] — *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Würzburg, Wien, 1970.

[5] K. Nakamula, *Class number calculation and elliptic unit, I, II, III*, Proc. Japan Acad. 57A (1981), pp. 77–81, 117–120, 363–366.

[6] — *Class number calculation of a cubic field from the elliptic unit*, J. Reine Angew. Math. 331 (1982), pp. 114–123.

[7] — *A construction of the groups of units of some number fields from certain subgroups*, Tokyo J. Math. 5 (1982), pp. 85–106.

[8] — *Class number calculation of a sextic field from the elliptic unit*, Acta Arith., this volume, pp. 229–247.

[9] — *Calculation of the class numbers and fundamental units of abelian extensions over imaginary quadratic fields from approximate values of elliptic units*, to appear in J. Math. Soc. Japan 37 (2) (1985).

[10] R. Schertz, *L-Reien in Imaginär-quadratischen Zahlkörpern und ihre Anwendung auf Klassenzahlprobleme bei biquadratischen Zahlkörpern II*, J. Reine Angew. Math. 270 (1975), pp. 195 212.

[11] — *Die Klassenzahl der Teilkörper abelscher Erweiterungen imaginär-quadratischer Zahlkörper II*, ibid. 296 (1977), pp. 58–79.

DEPARTMENT OF MATHEMATICS, TOKYO METROPOLITAN UNIVERSITY
2-1-1 Fukazawa, Setagaya, Tokyo, 158 Japan

Received on 6.12.1983 (1386)