ACTA ARITHMETICA
XLV (1985)

Note on an index formula of elliptic units in a ring class field

by

HEIMA HAYASHI (Kumamoto, Japan)

1. Introduction. Let $\boldsymbol{Q}$ be the field of rational numbers, $\boldsymbol{Z}$ the ring of rational integers and $\Sigma = \boldsymbol{Q}(\sqrt{D})$ an imaginary quadratic number field with discriminant D. For a natural number f, we denote by K_f the ring class field over Σ with conductor f, by O_f the order in Σ with conductor f (O_1 means the maximal order in Σ) and by $\mathrm{Cl}(K_f/\Sigma)$ the ring ideal class group modulo f in Σ, i.e. the group of the equivalent classes of proper O_f-ideals in Σ by the usual equivalence relation. We denote by $\sigma\colon \mathrm{Cl}(K_f/\Sigma) \to \mathrm{Gal}(K_f/\Sigma)$ the isomorphism from $\mathrm{Cl}(K_f/\Sigma)$ to the galois group of K_f over Σ via Artin's reciprocity law. For any intermediate field K of K_f/Σ with conductor f, we define $\mathrm{Cl}(K_f/K)$ to be the subgroup of $\mathrm{Cl}(K_f/\Sigma)$ whose image by σ is equal to the galois group of K_f over K, and $\mathrm{Cl}(K/\Sigma)$ to be the factor group of $\mathrm{Cl}(K_f/\Sigma)$ by $\mathrm{Cl}(K_f/K)$.

Let C be a class in $\mathrm{Cl}(K_f/\Sigma)$ and let $\mathfrak{a}_f$ be an O_f-ideal in C^{-1}. Let α be an element in Σ such that $(\mathfrak{a}_f O_1)^h = (\alpha)$ as an O_1-ideal, where h is the class number of Σ. We define $\delta_{K_f}(C)$ by

$$\delta_{K_f}(C) = \alpha^{12}\left(\frac{\Delta(\mathfrak{a}_f)}{\Delta(O_f)}\right)^h.$$

Herein $\Delta(\ )$ means the usual lattice function expressed by using the Dedekind eta-function as follows:

$$\Delta(\mathfrak{m}) = \left(\frac{2\pi}{\omega_2}\right)^{12}\eta\left(\frac{\omega_1}{\omega_2}\right)^{24}$$

where $\mathfrak{m} = [\omega_1, \omega_2]$ is a 2-dimensional complex lattice with $\boldsymbol{Z}$-basis $\{\omega_1, \omega_2\}$, $\mathrm{Im}(\omega_1/\omega_2) > 0$. $\delta_{K_f}(C)$ depends only on the class C, not on the choice of $\mathfrak{a}_f$, and is a unit in K_f. As is well known,

$$\delta_{K_f}(C)^{\sigma(C_1)} = \delta_{K_f}(CC_1)/\delta_{K_f}(C_1) \quad \text{for any } C, C_1 \text{ in } \mathrm{Cl}(K_f/\Sigma).$$

For each c in $\mathrm{Cl}(K/\Sigma)$ we define $\delta_K(c)$ as the relative norm of $\delta_{K_f}(C)$ w.r.t.

K_f/K, where C is a class in $\mathrm{Cl}(K_f/\Sigma)$ contained in c. Of course $\delta_K(c)$ depends only on c and is a unit in K.

For typographical reasons, we shall sometimes write

$$\delta_K(C) = \delta_f(C),$$

if $K = K_f$.

For each K, we denote by h_K, E_K, μ_K and w_K respectively the class number of K, the group of all units in K, the torsion part of E_K and the number of elements in μ_K. (When $K = \Sigma$, the subscript K is omitted from these notations.) Let $\varDelta_K$ be the subgroup of E_K generated by μ_K and the $\delta_K(c)$'s. Then the following index formula holds (cf. [7]):

$$(E_K;\ \varDelta_K) = (12wh)^{[K;\Sigma]-1}\frac{w}{w_K}\Big({\prod_{\chi}}' a(\chi)\Big)\frac{h_K}{h},$$

where χ ranges over all non-principal characters associated with the extension K/Σ, and for each χ, $a(\chi)$ is given by

$$a(\chi) = \frac{f}{f_\chi}\sum_{\substack{f_1 \\ f = f_1 t_1}} \frac{[K_f;\ K_{f_1}]}{t_1^2}\prod_{\substack{\mathfrak{p} \\ \mathfrak{p}|f_1}}\left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}}\right)$$

Herein f_χ means the conductor of χ, f_1 ranges over all positive divisors of f such that $f_\chi | f_1$, $\mathfrak{p}$ ranges over all prime ideals (O_1-ideals) in Σ containing f_1 and $N\mathfrak{p}$ denotes the absolute norm of $\mathfrak{p}$. We note here that $a(\chi)$ is another expression of $\prod_p G(p^{n_p(\chi)}, \chi)$ in the paper of Schertz [6], and $a(\chi) = 1$ for any χ if $f = 1$.

Recently Kersey proved a refined index formula for the unramified case as follows ([2]; we referred it to [3], ch. 9):

Theorem 1. *In the case where $f = 1$, there exists a subgroup $\mathscr{E}_K$ of E_K such that $\mathscr{E}_K^{12wh} \subset \varDelta_K$, for which the following index formula holds*:

$$(E_K;\ \mathscr{E}_K) = [K;\ \Sigma]\,\frac{h_K}{h}.$$

The most important part of Kersey's proof is the proof of Proposition 1 (§ 3) in the case where $f = 1$. He proved it by making use of the distribution of the Siegel function and many complicated tools including the quadratic relation of Klein forms ([3], ch. 12).

Our main purpose in this note is to give another simple proof for Proposition 1. Our proof is based only on the classical facts in the theory of complex multiplication, and can be accomplished also in the case where $f \neq 1$. Moreover by following the same procedures as those of Kersey, we have the following:

Theorem 2. *There exists a subgroup $\mathscr{E}_K$ of E_K such that $\mathscr{E}_K^{24h} \subset \varDelta_K$, for which the following index formula holds*:

$$(E_K;\ \mathscr{E}_K) = \frac{1}{e}[K;\ \Sigma]\left({\prod_{\chi}}'\left(a(\chi)\frac{w}{2}\right)\right)\frac{h_K}{h},$$

where $e = 2$ or 1 according to whether w_K is divisible by 8 or not.

Remark 1. In the cases where $D = -3$, -4 the assertion of Theorem 1 is trivial, and hence Theorem 2 is a generalization of Theorem 1.

2. Lemmas and terminologies. In this section we shall provide several lemmas. Lemmas 1 and 2 are classical facts in the theory of modular functions, and Lemmas 3 and 4 are fundamental results in the theory of complex multiplication.

Let the notations be the same as in Section 1. Let $\eta(\tau)$ and $j(\tau)$ respectively be the Dedekind eta-function and j-function in the theory of modular functions as usual. We denote by $\boldsymbol{Q}(X, Y)$ the field of rational functions on X and Y with $\boldsymbol{Q}$-coefficients.

Lemma 1 (Weber [8]). *Let s be a natural number prime to 6. Then*

$$\left(\frac{\eta(s\tau)}{\eta(\tau)}\right)^{2n} \in \boldsymbol{Q}(j(\tau),\ j(s\tau)) \quad \textit{with} \quad n = \begin{cases} 2 & \textit{for } s \equiv 1 \pmod 3, \\ 3 & \textit{for } s \equiv 1 \pmod 4, \\ 6 & \textit{otherwise}. \end{cases}$$

Lemma 2 (Newman [4]). *Let s be a natural number and $\{r_n\}$ a family of rational integers, whose indices n are positive divisors of s, satisfying the following conditions*:

(1) $r_1 = 0$,

(2) $\sum_n (n-1)r_n \equiv 0 \pmod{24}$,

(3) $\sum_n \left(\frac{s}{n} - s\right) r_n \equiv 0 \pmod{24}$ *and*

(4) $\prod_n n^{r_n}$ *is a square of a rational integer.*

Then $g(\tau) = \prod_n \left(\frac{\eta(n\tau)}{\eta(\tau)}\right)^{r_n}$ is contained in $\boldsymbol{Q}(j(\tau), j(s\tau))$.

By Satz (3,4) in [5], the statement in Lemma 1 can be translated into the statement on the special value $(\eta(s\omega)/\eta(\omega))$, where ω is a number in Σ such that $\mathrm{Im}(\omega) > 0$. In order to translate the function-theoretic result such as in Lemma 2 into the result on the special value of the same function, we need the following consideration:

Let the primitive matrix of determinant s mean the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that

$$a, b, c, d \in \boldsymbol{Z}, \quad (a, b, c, d) = 1 \quad \text{and} \quad ad - bc = s.$$

For a primitive matrix $S = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ we denote $\dfrac{a\tau+b}{c\tau+d}$ by $S(\tau)$. Two primitive matrices S_1 and S_2 of the same determinant will be called *equivalent* if and only if there exists a unimodular matrix M such that $S_1 = MS_2$. As is well known, $j(s\tau)$ is algebraic over $Q(j(\tau))$ and its irreducible polynomial over $Q(j(\tau))$ is given by

$$I_s(X, j(\tau)) = \prod_S \bigl(X - j(S(\tau))\bigr),$$

where S ranges over a complete representative system of the inequivalent primitive matrices of determinant s. Now for any complex number ω such that $\mathrm{Im}(\omega) > 0$ and for any function $g(\tau)$ in $Q(j(\tau), j(s\tau))$, the value $g(\omega)$ is contained in $Q(j(\omega), j(s\omega))$ whenever $I'_s(j(s\omega), j(\omega)) \neq 0$, where $I'_s(j(s\tau), j(\tau))$ means the differential quotient of $I_s(X, j(\tau))$ at $X = j(s\tau)$ ([1]). A necessary and sufficient condition for $I'_s(j(s\omega), j(\omega)) \neq 0$ is that $s\omega$ is not modular equivalent to $S(\omega)$ for any primitive matrix S of determinant s such that S is not equivalent to $\begin{bmatrix} s & 0 \\ 0 & 1 \end{bmatrix}$.

LEMMA 3. *Let C be a class in $\mathrm{Cl}(K_f/\Sigma)$, and let $f \neq 1$ when $D = -3$ or -4. Then for any prime number q,*

(1) $\delta_f(C)^{q+1} = \delta_f(C)^{\sigma(C_{\mathfrak{q}})+\sigma(C_{\bar{\mathfrak{q}}})} N_{qf/f}(\delta_{qf}(\tilde{C}))$ *if* $q \sim \mathfrak{q}\bar{\mathfrak{q}}$ *in* Σ *and* $q \nmid f$.

(2) $\delta_f(C)^{q+1} = \delta_f(C)^{\sigma(C_{\mathfrak{q}})} N_{qf/f}(\delta_{qf}(\tilde{C}))$ *if* $q \sim \mathfrak{q}^2$ *in* Σ *and* $q \nmid f$.

(3) $\delta_f(C)^{q+1} = N_{qf/f}(\delta_{qf}(\tilde{C}))$ *if* $q \sim \mathfrak{q}$ *in* Σ *and* $q \nmid f$.

(4) $\delta_f(C)^{q+1} = \delta_{fq^{-1}}(\tilde{\tilde{C}}) N_{qf/f}(\delta_{qf}(\tilde{C}))$ *if* $q \mid f$.

Herein $C_{\mathfrak{q}}$ (resp. $C_{\bar{\mathfrak{q}}}$) is the class in $\mathrm{Cl}(K_f/\Sigma)$ which contains the O_f-ideal $\mathfrak{q} \cap O_f$ (resp. $\bar{\mathfrak{q}} \cap O_f$), $\tilde{C}$ is any one class in $\mathrm{Cl}(K_{qf}/\Sigma)$ such that $\sigma(\tilde{C})$ is an extension of $\sigma(C)$ to $\mathrm{Gal}(K_{qf}/\Sigma)$, $\tilde{\tilde{C}}$ is the class in $\mathrm{Cl}(K_{fq^{-1}}/\Sigma)$ such that $\sigma(\tilde{\tilde{C}})$ is the restriction of $\sigma(C)$ to $\mathrm{Gal}(K_{fq^{-1}}/\Sigma)$, and $N_{qf/f}$ means the norm map from K_{qf} to K_f.

Proof. A proof can be accomplished, using the following identity:

$$q^{12} = \prod_S q^{12} \frac{\Delta\left(S\begin{bmatrix}\alpha_1 \\ \alpha_2\end{bmatrix}\right)}{\Delta\left(\begin{bmatrix}\alpha_1 \\ \alpha_2\end{bmatrix}\right)},$$

where $\{\alpha_1, \alpha_2\}$ is a $\boldsymbol{Z}$-basis of a complex lattice, and S ranges a complete representative system of the inequivalent primitive matrices of determinant q.

LEMMA 4. *For any C, C_1 in $\mathrm{Cl}(K_f/\Sigma)$, $\delta_f(C_1^2)^{1-\sigma(C)}$ is in E_K^{24h}.*

Proof. From the definition, we have

$$\delta_f(C_1^2) = \alpha^{24}\left(\frac{\Delta(\mathfrak{a}_f^2)}{\Delta(O_f)}\right)^h,$$

where $\mathfrak{a}_f$ is an O_f-ideal in C_1^{-1} and α is an element in Σ such that $(\mathfrak{a}_f O_1)^h = (\alpha)$ as a principal O_1-ideal. By a result of Deuring ([1], p. 41), $\Delta(\mathfrak{a}_f^2)/\Delta(O_f)$ is contained in K_f^{24}.

Let $\mathfrak{A}_f$ be the multiplicative group of the fractional ideals in Σ relatively prime to f. (Hereinafter ideal means O_1-ideal.) Let $\mathfrak{U}$ be the subgroup of $\mathfrak{A}_f$ associated with the extension K/Σ and $\mathrm{Cl}(K/\Sigma)^*$ the factor group of $\mathfrak{A}_f$ by $\mathfrak{U}$. Of course $\mathrm{Cl}(K/\Sigma) \simeq \mathrm{Cl}(K/\Sigma)^*$ and an explicit correspondence between $\mathrm{Cl}(K/\Sigma)$ and $\mathrm{Cl}(K/\Sigma)^*$ has been given in [1]. For each class c in $\mathrm{Cl}(K/\Sigma)$, we denote by c^* the class in $\mathrm{Cl}(K/\Sigma)^*$ which corresponds to c. Now since $\Sigma(\mu_K)$ is an abelian extension over Q, $\Sigma(\mu_K)/Q$ is an extension of type $(2, 2, \ldots)$ (cf. [1]), and hence w_K must be at most a divisor of 24. Moreover for any ideal $\mathfrak{a}$ in Σ prime to wf, the value of the absolute norm $N\mathfrak{a} \pmod{w_K}$ depends only on the class c^* to which $\mathfrak{a}$ belongs.

DEFINITION. An ideal $\mathfrak{a}$ in Σ will be said to be *K-admissible* if it is prime to wf and satisfies the following conditions:

If $w_K = 2$, then $N\mathfrak{a} \equiv 1 \pmod{24}$.
If $w_K = 4$, then

$$N\mathfrak{a} \equiv \begin{cases} 1 \pmod{24} & \text{for } \Sigma = Q(\sqrt{-4}), \\ 1 \text{ or } 7 \pmod{24} & \text{otherwise.} \end{cases}$$

If $w_K = 6$, then

$$N\mathfrak{a} \equiv \begin{cases} 1 \pmod{24} & \text{for } \Sigma = Q(\sqrt{-3}), \\ 1 \text{ or } 17 \pmod{24} & \text{otherwise.} \end{cases}$$

If $w_K = 8$, then

$$N\mathfrak{a} \equiv \begin{cases} 1 \text{ or } 13 \pmod{24} & \text{for } \Sigma = Q(\sqrt{-4}), \\ 1, 7, 13 \text{ or } 19 \pmod{24} & \text{otherwise.} \end{cases}$$

If $w_K = 12$, then

$$N\mathfrak{a} \equiv \begin{cases} 1 \text{ or } 17 \pmod{24} & \text{for } \Sigma = Q(\sqrt{-4}), \\ 1 \text{ or } 7 \pmod{24} & \text{for } \Sigma = Q(\sqrt{-3}), \\ 1, 7, 17 \text{ or } 23 \pmod{24} & \text{otherwise.} \end{cases}$$

If $w_K = 24$, then

$$N\mathfrak{a} = \begin{cases} 1, 5, 13 \text{ or } 17 \pmod{24} & \text{for } \Sigma = Q(\sqrt{-4}), \\ 1, 7, 13 \text{ or } 19 \pmod{24} & \text{for } \Sigma = Q(\sqrt{-3}), \\ 1, 5, 7, 11, 13, 17, 19 \text{ or } 23 \pmod{24} & \text{otherwise.} \end{cases}$$

For any K-admissible ideal $\mathfrak{a}$ the value of $N\mathfrak{a} \pmod{24}$ depends only on the class c^* to which $\mathfrak{a}$ belongs. In each class of $\mathrm{Cl}(K/\Sigma)^*$ there are infinitely many K-admissible prime ideals of degree 1. We define a homomorphism $l\colon \mathrm{Cl}(K/\Sigma) \to (Z/24Z)^\times$ by $l(c) = N\mathfrak{a} \bmod 24$, where $\mathfrak{a}$ is a K-admissible ideal in the associated class c^*. Plainly the kernel of l contains $\mathrm{Cl}(K/\Sigma)^2$.

Remark 2. Our definition of K-admissibility is essentially equal to that of Kersey, but has been slightly modified.

3. Proof of main result. Let the notations be the same as in Sections 1 and 2. In this section we shall prove the following:

PROPOSITION 1. *Let c_1 and c_2 be any two classes in $\mathrm{Cl}(K/\Sigma)$ and n the least positive rational integer such that*

$$n\big(l(c_1)-1\big)\big(l(c_2)-1\big) \equiv 0 \pmod{24}.$$

Then

$$\left(\frac{\delta_K(c_1 c_2)}{\delta_K(c_1)\,\delta_K(c_2)}\right)^n \in E_K^{24h}.$$

Proof. It suffices to prove this only for the case where $K = K_f$. Since in the cases where $(D, f) = (-3, 1), (-3, 2), (-3, 3), (-4, 1)$ or $(-4, 2)$ the assertion is trivial, we shall exclude these cases throughout this proof.

Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be K_f-admissible prime ideals of degree 1 in C_1^{*-1} and C_2^{*-1} respectively, and let $p_i = N\mathfrak{p}_i$ $(i = 1, 2)$. Then n is determined by the congruence $n(p_1-1)(p_2-1) \equiv 0 \pmod{24}$. Let v be a rational integer such that $\left[p_1, \dfrac{\sqrt{D}+v}{2}\right] = \mathfrak{p}_1$ and $\left[p_2, \dfrac{\sqrt{D}+v}{2}\right] = \mathfrak{p}_2$. Indeed v is determined by the congruence $v^2 \equiv D \pmod{4p_1 p_2}$. For our later arguments, we will choose v as $v^2 \equiv D \pmod{4p_1^2 p_2^2}$. Plainly $\left[1, f\dfrac{\sqrt{D}+v}{2}\right] = O_f$, and the following three O_f-ideals

$$\left[p_1, f\frac{\sqrt{D}+v}{2}\right], \quad \left[p_2, f\frac{\sqrt{D}+v}{2}\right] \quad \text{and} \quad \left[p_1 p_2, f\frac{\sqrt{D}+v}{2}\right]$$

represent the classes C_1^{-1}, C_2^{-1} and $(C_1 C_2)^{-1}$ respectively ([1]). From the definition we have

$$\frac{\delta_f(C_1 C_2)}{\delta_f(C_1)\,\delta_f(C_2)} = \left(\frac{\eta\left(\dfrac{f(\sqrt{D}+v)}{2p_1 p_2}\right)\eta\left(\dfrac{f(\sqrt{D}+v)}{2}\right)}{\eta\left(\dfrac{f(\sqrt{D}+v)}{2p_1}\right)\eta\left(\dfrac{f(\sqrt{D}+v)}{2p_2}\right)}\right)^{24h} = \left(\frac{\eta(p_1 p_2\omega)\,\eta(\omega)}{\eta(p_1\omega)\,\eta(p_2\omega)}\right)^{24h}$$

where $\omega = f\dfrac{\sqrt{D}+v}{2p_1 p_2}$. Let $\eta(\mathfrak{p}_1, \mathfrak{p}_2, v) = \eta(p_1 p_2\omega)\,\eta(\omega)/\eta(p_1\omega)\,\eta(p_2\omega)$. By using Lemma 1, it can be easily confirmed that

$$\eta(\mathfrak{p}_1, \mathfrak{p}_2, v)^{2n} \in K_f. \tag{3.1}$$

We shall show in three steps that $\eta(\mathfrak{p}_1, \mathfrak{p}_2, v)^n$ is in K_f.

Step 1: First we assume that $I'_{p_1 p_2}\big(j(p_1 p_2\omega), j(\omega)\big) \neq 0$. (This assumption will be considered in the next step.)

(i) If $n = 1$, i.e. $(p_1-1)(p_2-1) \equiv 0 \pmod{24}$, by Lemma 2 and the assumption that $I'_{p_1 p_2}\big(j(p_1 p_2\omega), j(\omega)\big) \neq 0$, we have

$$\frac{\eta(p_1 p_2\omega)}{\eta(\omega)}\left(\frac{\eta(p_1\omega)}{\eta(\omega)}\right)^{-1}\left(\frac{\eta(p_2\omega)}{\eta(\omega)}\right)^{-1} \in Q\big(j(\omega), j(p_1 p_2\omega)\big).$$

Since ω and $p_1 p_2\omega$ are basis quotients of $\left[p_1 p_1, f\dfrac{\sqrt{D}+v}{2}\right]$ and $\left[1, f\dfrac{\sqrt{D}+v}{2}\right]$ respectively, each of the values $j(\omega)$ and $j(p_1 p_2\omega)$ generates the ring class field K_f over Σ. Hence $\eta(\mathfrak{p}_1, \mathfrak{p}_2, v)$ is in K_f.

(ii) In the cases where $(p_1, p_2) \equiv (11, 17)$ or $(11, 19) \pmod{24}$, using the same method as in (i) we have

$$\frac{\eta(p_1 p_2\omega)}{\eta(\omega)}\left(\frac{\eta(p_1\omega)}{\eta(\omega)}\right)^{-1}\frac{\eta(p_2\omega)}{\eta(\omega)} \in Q\big(j(\omega), j(p_1 p_2\omega)\big).$$

Since

$$\eta(\mathfrak{p}_1, \mathfrak{p}_2, v) = \left(\frac{\eta(p_2\omega)}{\eta(\omega)}\right)^{-2}\frac{\eta(p_1 p_2\omega)}{\eta(\omega)}\left(\frac{\eta(p_1\omega)}{\eta(\omega)}\right)^{-1}\frac{\eta(p_2\omega)}{\eta(\omega)},$$

$\eta(\mathfrak{p}_1, \mathfrak{p}_2, v)^n$ is contained in K_f (by Lemma 1).

(iii) In the remaining cases, using the same method as in (i) we have

$$\frac{\eta(p_1 p_2\omega)}{\eta(\omega)}\,\frac{\eta(p_1\omega)}{\eta(\omega)}\left(\frac{\eta(p_2\omega)}{\eta(\omega)}\right)^{-1} \in Q\big(j(\omega), j(p_1 p_2\omega)\big).$$

Thus for the similar reason to one in (ii), $\eta(\mathfrak{p}_1, \mathfrak{p}_2, v)^n$ is in K_f.

Step 2: A complete system of the inequivalent primitive matrices of determinant $p_1 p_2$ can be taken as follows:

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : ad = p_1 p_2, \ 0 \leqslant b < d \text{ and } (a, b, d) = 1.$$

It is at least necessary for $j(p_1 p_2\omega) = j(S(\omega))$ that $S(\omega)$ is a basis quotient of a proper O_f-ideal. Now there are the following three possibilities that $S(\omega)$ is a basis quotient of a proper O_f-ideal:

$$S_1 = \begin{bmatrix} p_1 & 0 \\ 0 & p_2 \end{bmatrix}, \quad S_2 = \begin{bmatrix} p_2 & 0 \\ 0 & p_1 \end{bmatrix} \quad \text{and} \quad S_3 = \begin{bmatrix} 1 & 0 \\ 0 & p_1 p_2 \end{bmatrix}.$$

(Note that v has been chosen as $v^2 \equiv D \pmod{4p_1^2 p_2^2}$.) Indeed $S_1(\omega)$, $S_2(\omega)$ and $S_3(\omega)$ are basis quotients of $\left[p_1, f\dfrac{\sqrt{D}+v}{2}\right]^2$, $\left[p_2, f\dfrac{\sqrt{D}+v}{2}\right]^2$ and

$\left[p_1 p_2, f\dfrac{\sqrt{D}+v}{2}\right]^2$ respectively. Therefore in the cases where none of the three classes C_1^2, C_2^2 or $C_1^2 C_2^2$ are equal to the unit class C_0 in $\mathrm{Cl}(K_f/\Sigma)$, it always holds that $I'_{p_1 p_2}(j(p_1 p_2 \omega), j(\omega)) \neq 0$ and hence $\{\delta_f(C_1 C_2)/\delta_f(C_1)\delta_f(C_2)\}^n$ is contained in K_f^{24h}.

Also in the cases where at least one of C_1^2, C_2^2 nad $C_1^2 C_2^2$ is equal to C_0, *whenever there exists a class B in $\mathrm{Cl}(K_f/\Sigma)$ whose order is equal to an odd prime number or to*

$$\begin{cases} 8 & \textit{for} \quad w_K = w, \\ 16 & \textit{for} \quad w_K \neq w, \end{cases}$$

the same consideration as above can be applied, and it can be shown that $\{\delta_f(C_1 C_2)/\delta_f(C_1)\delta_f(C_2)\}^n$ is contained in K_f^{24h}. Indeed for any i ($i = 1, 2, \ldots$) we have

$$(3.2) \qquad \left(\frac{\delta_f(C_1 C_2)}{\delta_f(C_1)\delta_f(C_2)}\right)^{\sigma(B^i)} = \frac{\delta_f(C_1 C_2 B^{2i})}{\delta_f(C_1 B^i)\delta_f(C_2 B^i)} \, \frac{\delta_f(C_1 C_2 B^i)\delta_f(B^i)}{\delta_f(C_1 C_2 B^{2i})},$$

and when the order of B is equal to an odd prime number q such that $q \geqslant 5$, it is always possible to choose a suitable i so that none of the following $(C_1 B^i)^2$, $(C_2 B^i)^2$, $(C_1 C_2 B^i)^2$, $(C_1 C_2 B^{2i})^2$ are equal to C_0, and $l(B^i) = 1$. Hence $\{\delta_f(C_1 C_2)/\delta_f(C_1)\delta_f(C_2)\}^{n\sigma(B^i)}$ and also $\{\delta_f(C_1 C_2)/\delta_f(C_1)\delta_f(C_2)\}^n$ are contained in K_f^{24h}. When the order of B is equal to 3, 8 or 16, if $C_1^2 = C_2^2 = C_0$, then the same consideration as above can be applied, and even if $C_1^2 \neq C_0$ or $C_2^2 \neq C_0$, we are able to obtain the same conclusion by tedious checking of all possible cases where at least one of $(C_1 B^i)^2$, $(C_2 B^i)^2$, $(C_1 C_2 B^i)^2$ and $(C_1 C_2 B^{2i})^2$ is equal to C_0. Therein if C_1 is a class of order 6 or of order 8, and if $C_2^2 = C_0$ or $C_1^2 C_2^2 = C_0$, we should use the identity

$$\left(\frac{\delta_f(C_1 C_2)}{\delta_f(C_1)\delta_f(C_2)}\right)^{\sigma(C_1^2)} = \frac{\delta_f(C_1^3 C_2)}{\delta_f(C_1)\delta_f(C_1^2 C_2)} \delta_f(C_1^2)^{1-\sigma(C_1)},$$

and Lemma 4.

Step 3: If there no longer exists a class B in $\mathrm{Cl}(K_f/\Sigma)$ such as in Step 2, we may use the norm relation (Lemma 3). Indeed if $D \neq -4$ and -8, D is divisible by an odd prime number q. Here f is not divisible by q, because $\mathrm{Cl}(K_f/\Sigma)$ does not contain any class of odd prime order. We let $q \sim \mathfrak{q}^2$ in Σ. Then by (2) of Lemma 3, we have

$$(3.3) \qquad \left(\frac{\delta_f(C_1 C_2)}{\delta_f(C_1)\delta_f(C_2)}\right)^{n(q+1)} = \left(\frac{\delta_f(C_1 C_2)}{\delta_f(C_1)\delta_f(C_2)}\right)^{n\sigma(C_\mathfrak{q})} N_{\mathfrak{q}f/f}\left(\frac{\delta_{\mathfrak{q}f}(\tilde{C}_1 \tilde{C}_2)}{\delta_{\mathfrak{q}f}(\tilde{C}_1)\delta_{\mathfrak{q}f}(\tilde{C}_2)}\right)^n.$$

Herein $C_\mathfrak{q}$, $\tilde{C}_1$ and $\tilde{C}_2$ are the same as in Lemma 3. By the formula (3.1) the left-hand side of the equation (3.3) is contained in K_f^{24h}. Since there exists a class $\tilde{B}$ of order q in $\mathrm{Cl}(K_{\mathfrak{q}f}/\Sigma)$, $\{\delta_{\mathfrak{q}f}(\tilde{C}_1 \tilde{C}_2)/\delta_{\mathfrak{q}f}(\tilde{C}_1)\delta_{\mathfrak{q}f}(\tilde{C}_2)\}^n$ is contained in $K_{\mathfrak{q}f}^{24h}$, and hence $\{\delta_f(C_1 C_2)/\delta_f(C_1)\delta_f(C_2)\}^n$ is also contained in K_f^{24h}.

Now we know the following facts:

(I) *When $D = -4$ and f is divisible by an odd prime number other than $\{3, 7, 17, 31\}$ or by 32, then there exists a class B in $\mathrm{Cl}(K_f/\Sigma)$ whose order is divisible by an odd prime number or by 16. Especially when $(D, f) = (-4, 17)$ or $(-4, 31)$, then $w_K = w = 4$, and there exists a class B of order 8 in $\mathrm{Cl}(K_f/\Sigma)$.*

(II) *When $D = -8$ and f is divisible by an odd prime number other than $\{3, 7\}$ or by 16, then there exists a class B in $\mathrm{Cl}(K_f/\Sigma)$ whose order is divisible by an odd prime number or by 16. Especially when $(D, f) = (-8, 7)$, then $w_K = w = 2$ and $\mathrm{Cl}(K_f/\Sigma)$ is a cyclic group of order 8.*

Therefore for the complete proof of Proposition 1 we have only to check the finite number of cases listed up in Table I. In Table I, TYPE indicates the type of abelian group $\mathrm{Cl}(K_f/\Sigma)$. It is not so difficult to verify that the assertion of Proposition 1 is true for all cases in Table I, but this is very tedious. We shall here omit the precise verification and point out only a few essential facts.

Verification for all cases except for the three cases where $(D, f) = (-4, 12)$, $(-8, 6)$ and $(-8, 12)$ can be carried out only by using the tools employed in Steps 1 and 2. Verification for the cases where $(D, f) = (-4, 12)$ and $(-8, 12)$ can be done by using (3) of Lemma 3. Verification for the case where $(D, f) = (-8, 6)$ can be done by numerical computations. Therein we may use the following representative O_6-ideals:

$$[1, 6\sqrt{-2}], \quad [2, 3\sqrt{-2}+1], \quad [3, 2\sqrt{-2}] \quad \text{and} \quad [6, \sqrt{-2}+1].$$

Table I

(D, f)	TYPE	w_K	w
$(-4, 4)$	(2)	8	4
$(-4, 8)$	(4)	8	4
$(-4, 16)$	(8)	8	4
$(-4, 3)$	(2)	12	4
$(-4, 6)$	(4)	12	4
$(-4, 12)$	(4, 2)	24	4
$(-4, 24)$	(4, 4)	24	4
$(-4, 48)$	(4, 8)	24	4
$(-4, 7)$	(4)	4	4
$(-4, 14)$	(8)	4	4
$(-4, 28)$	(8, 2)	8	4
$(-4, 56)$	(8, 4)	8	4
$(-4, 112)$	(8, 8)	8	4
$(-8, 2)$	(2)	8	2
$(-8, 4)$	(4)	8	2
$(-8, 8)$	(8)	8	2
$(-8, 3)$	(2)	6	2
$(-8, 6)$	(2, 2)	24	2
$(-8, 12)$	(2, 4)	24	2
$(-8, 24)$	(2, 8)	24	2

Remark 3. In the unramified case, w_K is at most a divisor of 12, and $w_K > 2$ if and only if $D = -3$ or -4. Hence for any pair (c_1, c_2) of the

classes in $\mathrm{Cl}(K/\Sigma)$, $n\big(l(c_1)-1\big)\big(l(c_2)-1\big)$ is divisible by 24 if and only if it is divisible by ww_K, and hence Proposition 1 is a generalization of Kersey's result ([3], ch. 11).

Let $\Delta_K(c_0)$ be the subgroup of Δ_K generated by μ_K and all units of the following form:

$$\left(\frac{\delta_K(c_1c_2)}{\delta_K(c_1)\,\delta_K(c_2)}\right)^n,$$

with a rational integer n such that $n\big(l(c_1)-1\big)\big(l(c_2)-1\big) \equiv 0 \pmod{24}$. Then by Proposition 1, $\Delta_K(c_0)$ is contained in $\mu_K E_K^{24h}$. Let n_0 be the least positive rational integer such that $n_0\big(l(c_1)-1\big)\big(l(c_2)-1\big) \equiv 0 \pmod{24}$ for any pair (c_1, c_2) of the classes in $\mathrm{Cl}(K/\Sigma)$. As can be easily confirmed, $n_0 = 1, 2, 3$ or 6, and $n_0 = \frac{1}{2}(w_K/w)$ or (w_K/w) according to whether w_K is divisible by 8 or not. Moreover by following a procedure similar to one of Kersey ([3], ch. 9, 5), we have $\big(\Delta_K;\ \Delta_K(c_0)\big) = n_0[K;\ \Sigma]$, and hence Theorem 2.

References

[1] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzykl. math., Wiss. 1–2, 2. Aufl., Heft 10, Stuttgart 1958.

[2] D. Kersey, *The index of modular units in complex multiplication*, to appear.

[3] D. Kubert and S. Lang, *Modular Units*, Springer, Berlin–Heidelberg–New York 1981.

[4] M. Newman, *Construction and application of a class of modular functions*, Proc. London Math. Soc. 7 (1957), pp. 334–350.

[5] R. Schertz, *L-Reihen in imaginär-quadratischen Zahlkörpern und ihre Anwendung auf Klassenzahlprobleme bei quadratischen und biquadratischen Zahlkörpern I, II*, J. Reine Angew. Math. 262/263 (1973), pp. 120–133; 270 (1974), pp. 195–212.

[6] – *Zur Theorie der Ringklassenkörper über imaginärquadratischen Zahlkörpern*, J. Number Theory 10 (1978), pp. 70–82.

[7] C. L. Siegel, *Lectures on advanced analytic number theory*, Tata Institute Lecture Notes, 1961.

[8] H. Weber, *Lehrbuch der Algebra*, Vol. III, 3-rd Ed., Chelsea, New York 1962.

DEPARTMENT OF MATHEMATICS
KYUSHU-TOUKAI UNIVERSITY
223 Toroku, Ohe-cho, Kumamoto 862
Japan

Received on 14.10.1983 (1377)

ACTA ARITHMETICA
XLV (1985)

Über eine Vermutung von Choi, Erdös und Nathanson

von

JOACHIM ZÖLLNER (Mainz)

Sei N die Menge der natürlichen Zahlen und $N_0 = N \cup \{0\}$. Seien h und $N \in N$. Eine Menge $A \subseteq N_0$ mit $0 \in A$ heißt *Abschnittsbasis* der Ordnung h für N, falls jedes $n \in [1, N] \cap N$ darstellbar ist als Summe von h Elementen aus A.

Nach einem bekannten Satz von Lagrange ist jede natürliche Zahl darstellbar als Summe von vier Quadraten ganzer Zahlen. Daher ist für jedes $N \in N$ die Menge $A = \{a^2 \mid a \in N_0,\ a^2 \leqslant N\}$ Abschnittsbasis der Ordnung 4 für N und es gilt $|A| \leqslant N^{1/2}+1$.

Choi, Erdös und Nathanson [1] haben Abschnittsbasen A der Ordnung 4 für jedes $N \in N$ konstruiert, die ebenfalls nur aus Quadraten bestehen und für die gilt $|A| < (2/\log 2)\,N^{1/3}\log N$. Andererseits folgt aus kombinatorischen Gründen für eine Abschnittsbasis der Ordnung 4, daß $|A| \geqslant N^{1/4}$. Eine in [1] formulierte Vermutung lautet nun:

Zu jedem $\varepsilon > 0$ und $N \geqslant N(\varepsilon)$ existiert eine Abschnittsbasis A der Ordnung 4 für N, die nur aus Quadraten besteht und für die gilt $|A| \leqslant N^{(1/4)+\varepsilon}$.

Diese Aussage ist offensichtlich äquivalent mit

SATZ 1. *Zu jedem $\varepsilon > 0$ und jedem $N \in N$ existiert eine Abschnittsbasis A der Ordnung 4 für N, die nur aus Quadraten besteht und für die gilt $|A| \leqslant c_1 N^{(1/4)+\varepsilon}$ mit einem $c_1 = c_1(\varepsilon) > 0$.*

Dieser Satz soll im folgenden bewiesen werden. Im Beweis, der in weiten Teilen dem in [1] folgt, wird an entscheidender Stelle folgendes Ergebnis von Erdös und Nathanson [2] verwendet:

Zu jedem $\varepsilon > 0$ existiert eine Menge B_ε von Quadraten, so daß jede natürliche Zahl $n \neq 4^s(8t+7)$; $s, t \in N_0$ darstellbar ist als Summe von höchstens drei Quadraten aus B_ε und daß gilt

$$B_\varepsilon(x) \leqslant Cx^{(1/3)+\varepsilon} \quad \text{für ein } C = C(\varepsilon) > 0.\,(^1)$$

Mit einer kleinen Ergänzung versehen, übernehmen wir dies als

[1] Für eine Menge $M \subseteq N_0$ und $x \in R$ bedeutet $M(x) = |M \cap [1, x]|$.