T. Ibukiyama
Nagoya Math. J.
Vol. 88 (1982), 181-195

ON MAXIMAL ORDERS OF DIVISION QUATERNION ALGEBRAS OVER THE RATIONAL NUMBER FIELD WITH CERTAIN OPTIMAL EMBEDDINGS

TOMOYOSHI IBUKIYAMA

In this paper, we shall give explicit Z-basis of certain maximal orders of definite quaternion algebras over the rational number field Q (See Theorems below). We shall also give some remarks on symmetric maximal orders in Ponomarev [9] and Hashimoto [6] (Proposition 4.3). More precise contents are as follows. Let D be a division quaternion algebra over $\boldsymbol{Q}$. Let T be the type number of D, that is, the number of the isomorphism classes, or equivalently, the number of conjugacy classes by $D^{\times}$, of maximal orders of D. The explicit formula for T is well known (Eichler [5]), and $T=1$ if D is indefinite, but $T>1$ in general if D is definite. Let $m=p_1\cdots p_t$ be the product of all finite ramified primes p_i for $D/\boldsymbol{Q}$. We shall give explicit $\boldsymbol{Z}$-basis of any maximal orders (up to isomorphism) which contain an element with the minimal polynomial x^2+m. We shall also give the number of the isomorphism classes of such maximal orders (Corollary 2.12). When m is a prime, this number has been given by Deuring [3]. Now, we shall state our Theorems. Choose a prime integer q such that

(1) $\quad (-q/p_i)=-1$ for $p_i \mid m$ such that $p_i \neq 2$, and

(2) $\quad q \equiv 3 \bmod 8$.

(Such q exists by virtue of Dirichlet's theorem of primes in arithmetic progression.) Then, D can be written explicitly as $D=\boldsymbol{Q}+\boldsymbol{Q}\alpha+\boldsymbol{Q}\beta+\boldsymbol{Q}\alpha\beta$, where $\alpha^2=-m$, $\beta^2=-q$, and $\alpha\beta=-\beta\alpha$. By (1) and (2) we have $(-m/q)=1$. Choose a rational integer r such that

(3) $$r^2+m \equiv 0 \bmod q .$$

Put

Received January 5, 1981.

$$O(q, r) = Z + Z\frac{1+\beta}{2} + Z\frac{\alpha(1+\beta)}{2} + Z\frac{(r+\alpha)\beta}{q}.$$

Then, this is a maximal order of D, which is essentially the same maximal order given in Albert [1] (See also [8]). Besides, when $m \equiv 3 \bmod 4$, we choose a rational integer r' such that

$$r'^2 + m \equiv 0 \bmod 4q. \tag{4}$$

Put

$$O'(q, r') = Z + Z\frac{1+\alpha}{2} + Z\beta + Z\frac{(r'+\alpha)\beta}{2q}.$$

Then, this is also a maximal order of D. Note that the isomorphism class of $O(q, r)$ or $O'(q, r')$ depends on q, but does not depend on r or r'. We fix r or r', once and for all, for each q satisfying (1) and (2), and denote these orders briefly by $O(q)$ or $O'(q)$, respectively. We also assume that $m \equiv 3 \bmod 4$ when we write $O'(q)$.

THEOREM 3. *Assume that a maximal order O of D has an element with the minimal polynomial $x^2 + m$. Then, there exists a prime integer q satisfying* (1) *and* (2) *such that either $O \cong O(q)$ or $O \cong O'(q)$.*

This is an easy corollary to the more precise theorems below. To explain Theorems 1, 2 below, we introduce a notion of optimal embeddings, following Eichler. Let K be a quadratic subfield of D, and o be an order of K. Let O be a maximal order of D. We say that o is an optimal subring of O when $O \cap K = o$. For example, $Z + Z\alpha$ (resp. $Z + Z(1+\alpha)/2$) is an optimal subring of $O(q)$ (resp. $O'(q)$). Conversely, we have

THEOREM 1. *Assume that a maximal order O of D has an optimal subring isomorphic to $Z + Z\sqrt{-m}$. Then, O is isomorphic to $O(q)$ for some integer q satisfying* (1) *and* (2).

When $m = 3 \bmod 4$, we also have

THEOREM 2. *Assume that a maximal order O of D has an optimal subring isomorphic to $Z + Z(1+\sqrt{-m})/2$. Then, O is isomorphic to $O'(q)$ for some prime integer q satisfying* (1) *and* (2).

Now, when m is a prime $p \equiv 1 \bmod 4$, certain maximal orders of $D \otimes_Q Q(\sqrt{p})$ which are called symmetric maximal orders have been defined,

related to the theory of quadratic forms (cf. Ponomarev [9], Hashimoto [6]). Some numerical examples of such orders have been given in Hashimoto [7]. In this paper, we shall also give explicit basis of any symmetric maximal orders (up to isomorphism) which contain a fourth root of unity (Proposition 4.3), as a corollary to above Theorems.

Remark. Assume that m is a prime integer p. Then, by combining the results by Deuring [2] with Theorem 3 above, one obtains an explicit basis of the endomorphism ring of any super singular elliptic curve whose j-invariant belongs to the finite prime field $\boldsymbol{F}_p$.

Remark. Shimizu [11] has constructed some examples of new forms with respect to $GL(2)$ by using certain maximal orders of definite quaternion algebras. In Theorem 2 of his paper, he assumed that such maximal orders (with prime discriminant p) are of the form $O(q)$, or of some analogous form. By virtue of our Theorem 3, we can replace the condition by more intrinsic assumption that the maximal orders in question have an element whose minimal polynomial is $x^2 + p$.

Now, we outline the content of each section. After some preliminaries in § 1, we count up the isomorphism classes of maximal orders of the form $O(q)$ or $O'(q)$ (for various q and fixed m) in § 2. The dependence of the isomorphism classes of $O(q)$ or $O'(q)$ on q will be also given ideal-theoretically there. In § 3, by using some arithmetic of quaternion algebra by Eichler [5], we show that $O(q)$ or $O'(q)$ exhaust all the isomorphism classes of the maximal orders in question, and complete the proofs of the theorems. In § 4, we see the relation between the above formulation and the Chevalley-Hasse-Noether parametrization, and also give a result on symmetric maximal orders.

§ 1. Preliminaries

Let D be a definite quaternion algebra over $\boldsymbol{Q}$ with discriminant m. Let q be a prime integer satisfying (1) and (2) in the introduction. Take α and β as in the introduction. Sometimes, we denote them by α_q and β_q to clarify their dependence on q. Though we have assumed that D is definite, the following Lemmas 1.1 and 1.2 are also valid even when D is indefinite if we replace g or m by $-q$ or $-m$, respectively, in the statements. First we have;

LEMMA 1.1. *D is isomorphic to* $D(q) = \boldsymbol{Q} + \boldsymbol{Q}\alpha_q + \boldsymbol{Q}\beta_q + \boldsymbol{Q}\alpha_q\beta_q$.

Proof. This is easily shown by classfield theory, and the proof will be omitted here. q.e.d.

Let q and q' be different primes satisfying (1) and (2). By Skolem-Noether's theorem, there exists an isomorphism of $D(q)$ to $D(q')$ which sends α_q to $\alpha_{q'}$. We fix such an isomorphism throughout the paper and identify α_q with $\alpha_{q'}$, which will be denoted briefly by α.

LEMMA 1.2. *$O(q)$ is a maximal order of D. If $m \equiv 3 \bmod 4$, $O'(q)$ is also a maximal order of D.*

Proof. It is easy to see that $O(q)$ and $O'(q)$ contain $\boldsymbol{Z} + \boldsymbol{Z}\alpha + \boldsymbol{Z}\beta_q + \boldsymbol{Z}\alpha\beta_q$. So $O(q)$ and $O'(q)$ contains a basis of D. So we have only to show that $O(q)$ and $O'(q)$ are subrings of D and that the discriminant of them are equal to $m^2\boldsymbol{Z}$. This can be shown by routine calculation, which we omit here. q.e.d.

Let O be any maximal order of D. Denote by e the half of the cardinality of the group $O^\times$ of the units of O. In the remainder of this section, we gather some easy arithmetics on $O(q)$ and $O'(q)$ with $e > 1$. which will be used in § 2. When $m = 2$ or 3, we have $T = 1$ (Eichler [4]), and Theorem 1 to 3 are obvious. From now on, we assume that $m \geqq 5$. Then $e = 1, 2$, or 3, and $O^\times$ is isomorphic to $\{\pm 1\}$, $\{\pm 1, \pm\sqrt{-1}\}$, or $\{\pm 1, \pm(-1 \pm \sqrt{-3})/2\}$, respectively (Eichler, loc. cit.,). As well known, $\boldsymbol{Q}(\sqrt{-1})$ can be embedded in D if and only if $p_i \equiv 3 \bmod 4$ or $p_i = 2$ for all $p_i \mid m$. $\boldsymbol{Q}(\sqrt{-3})$ can be embedded in D if and only if $p_i \equiv 2 \bmod 3$ or $p_i = 3$ for all $p_i \mid m$.

(1.3) The isomorphism class of O with $e = 2$ is at most unique. This is also true for maximal orders with $e = 3$. (Eichler, loc. cit.)

LEMMA 1.4. *Assume that $m \geqq 5$. Then, $e = 2$ for $O(q)$ (resp. $O'(q)$) if and only if there exist $x, y \in \boldsymbol{Z}$ such that $x^2 + my^2 = q$ (resp. $x^2 + my^2 = 4q$).*

Proof. First, assume that there exists an element $\gamma \in O(q)$ such that $n(\gamma) = 1$ and $\mathrm{tr}(\gamma) = 0$, where $n(\gamma)$ or $\mathrm{tr}(\gamma)$ means reduced norm or trace of γ, respectively. Put $\gamma = a + b(1 + \beta)/2 + c\alpha(1 + \beta)/2 + d(r + \alpha)\beta/q$, where $a, b, c, d \in \boldsymbol{Z}$. Then we have $c^2 \leqq 4/m \leqq 4/5$, so we have $c = 0$. Then $\mathrm{n}(\gamma) = 1$ and $\mathrm{tr}(\gamma) = 0$ imply that $(-aq + dr)^2 + d^2m = q$. The converse is obvious. As for $O'(q)$, the proof is virtually the same, and will be omitted here. q.e.d.

LEMMA 1.5. *Assume that* $m \geqq 5$. *Then,* $e = 3$ *for* $O(q)$ *if and only if there exist integers* x, y *such that* $x^2 + 4my^2 = 3q$. *We have* $e \neq 3$ *for any* $O'(q)$.

Proof. The proof is virtually the same as in Lemma 1.4, and will be omitted here. q.e.d.

We shall interpret Lemmas 1.4 and 1.5 ideal-theoretically. Let $I(2)$ be the group of fractional ideals of $\boldsymbol{Q}(\sqrt{-m})$ which is prime to 2, $P(2)$ be the group of principal ideals in $I(2)$. Put $P_Z(2) = \{\kappa \in I(2);\ \kappa \in \boldsymbol{Q}(\sqrt{-m}),\ \kappa \equiv a \bmod 2 \text{ for some } a \in \boldsymbol{Z}\}$, where mod means the multiplicative congruence. Let q be a prime which satisfies (1) and (2) as before. Then q unramifies and splits for $\boldsymbol{Q}(\sqrt{-m})/\boldsymbol{Q}$ because $(-m/q) = 1$. So we write the prime ideal decomposition of $q\boldsymbol{Z}$ as $(q) = \mathfrak{q}\bar{\mathfrak{q}}$, where $\mathfrak{q} \neq \bar{\mathfrak{q}}$ and $^-$ denotes the complex conjugation. By Lemma 1.4, we easily have;

COROLLARY 1.6. *We have* $e = 2$ *for* $O(q)$ (*resp.* $O'(q)$) *if and only if* $\mathfrak{q} \in P_Z(2)$ *if* $m \equiv 3 \bmod 4$, $\mathfrak{q} \in P(2)$ *if* $m \equiv 2 \bmod 4$ (*resp.* $\mathfrak{q} \in P(2)$).

Next, we assume that $\boldsymbol{Q}(\sqrt{-3})$ can be embedded in D. Then we can write a prime ideal decomposition of $3Z$ in $\boldsymbol{Q}(\sqrt{-m})/\boldsymbol{Q}$ as $\mathfrak{p}\bar{\mathfrak{p}}$, though it may be that $\mathfrak{p} = \bar{\mathfrak{p}}$. Then by Lemma 1.5, we easily have;

COROLLARY 1.7. *We have* $e = 3$ *for* $O(q)$ *if and only if* $\mathfrak{p}\mathfrak{q}$ *or* $\mathfrak{p}\bar{\mathfrak{q}}$ *belongs to* $P_Z(2)$.

Next, we have;

LEMMA 1.8. *Assume that* $m \equiv 3 \bmod 4$. *Then* $O(q)$ *is isomorphic to* $O'(q')$ *if and only if* $e = 2$ *for both* $O(q)$ *and* $O'(q')$.

Proof. If $O(q)$ is isomorphic to $O'(q')$, $O(q)$ must have an element γ such that $\mathrm{tr}(\gamma) = 1$ and $\mathrm{n}(\gamma) = (1 + m)/4$. Put $\gamma = a + b(1 + \beta)/2 + c\alpha(1 + \beta)/2 + d(r + \alpha)\beta/q$, where $a, b, c, d \in \boldsymbol{Z}$. We have $c^2 \leqq 1$. If $c = 0$, we have $(bq + 2dr)^2 + d^2m = mq$. We can put $bq + 2dr = my$, where $y \in \boldsymbol{Z}$. Then by Lemma 1.4, $e = 2$ for $O(q)$. If $c^2 = 1$, we have $bq + 2dr = 0$. Then $b \in 2\boldsymbol{Z}$, which contradicts the assumption that $\mathrm{tr}(\gamma) = 1$. Therefore the condition is necessary. The sufficiency is obvious by (1.3). q.e.d.

§ 2. The isomorphism classes of the maximal orders $O(q)$ and $O'(q)$

From now on, we assume that $m \geqq 5$, till the end of this paper. Let q and q' be different primes which satisfy (1) and (2). In this section, we establish the conditions for $O(q) \cong O(q')$ or $O'(q) \cong O'(q')$. Then we count up the isomorphism classes of such maximal orders. As before, we put $(q) = \mathfrak{q}\bar{\mathfrak{q}}$ and $(q') = \mathfrak{q}'\bar{\mathfrak{q}}'$.

PROPOSITION 2.1. *Notations being as above, $O(q)$ (resp. $O'(q)$) is isomorphic to $O(q')$ (resp. $O'(q')$) if and only if $\mathfrak{q}\mathfrak{q}' \in P_Z(2)$ (resp. $\mathfrak{q}\mathfrak{q}' \in P(2)$) for a suitable choice of q.*

Remark 2.2. We note that $\mathfrak{q}\mathfrak{q}'$ belongs to $P_Z(2)$ (resp. $P(2)$) if and only if we have $x^2 + 4my^2 = qq'$ (resp. $x^2 + my^2 = 4qq'$) for some $x, y \in \boldsymbol{Z}$.

Proof of Proposition 2.1. We divide the proof into three cases.

Case I. Assume that $e = 2$ for $O(q)$ (resp. $O'(q)$). Then by virtue of (1.3) and Corollary 1.6, the assertion is obvious.

Case II. Assume that $e = 3$ for $O(q)$. Then $O(q) \cong O(q')$ if and only if $e = 3$ also for $O(q')$. Notations being as in Corollary 1.7, choose $\mathfrak{q}$ so that $\bar{\mathfrak{p}}\mathfrak{q} \in P_Z(2)$. Then $\mathfrak{p}\mathfrak{q}' \in P_Z(2)$ if and only if $\mathfrak{q}\mathfrak{q}' \in P_Z(2)$. By virtue of Corollary 1.7, the assertion is obvious.

Case III. Assume that $e = 1$ for $O(q)$. First, assume that $O(q)$ is isomorphic to $O(q')$.

Let ϕ be an isomorphism of $O(q')$ to $O(q)$. Since $n(\alpha) = m$, $\alpha O(q)$ is the unique ideal of $O(q)$ whose reduced norm is equal to m. Then $\pm\alpha$ are the only elements of $O(q)$ with reduced norm m, and we have $\phi(\alpha) = \pm\alpha$. Now put $\phi((1 + \beta_{q'})/2) = a + b(1 + \beta_q)/2 + c\alpha(1 + \beta_q)/2 + d(r + \alpha)\beta_q/q$, where $a, b, c, d \in \boldsymbol{Z}$. We have $\phi(\alpha)\phi(\beta_{q'}) = -\phi(\beta_{q'})\phi(\alpha)$, so we have $c = 0$. As $\mathrm{tr}((1 + \beta_{q'})/2) = 1$ and $\mathrm{n}((1 + \beta_{q'})/2) = (1 + q')/4$, we have $2a + b = 1$ and $1/4 + (b/2 + dr/q)^2 q + d^2 m/q = (1 + q')/4$. Then we have $(bq + 2dr)^2 + 4d^2 m = qq'$, which is the condition we want by virtue of Remark 2.2. Conversely, assume that $x^2 + 4y^2 m = qq'$ for some $x, y \in \boldsymbol{Z}$. We have $x^2 + 4my^2 \equiv x^2 - 4r^2 y^2 = (x - 2ry)(x + 2ry) \bmod q$. Changing the sign of y if necessary, we get $x \equiv 2ry \bmod q$. Put $d = y$ and $b = (x - 2ry)/q$. Then b is an odd integer, because x is odd. Now, denote by ψ the $\boldsymbol{Q}$ linear map of D to D such that

$$
\begin{aligned}
\psi(1) &= 1 \\
\psi(\alpha) &= \varepsilon\alpha \\
\psi(\beta_{q'}) &= b\beta_q + 2d(r+\alpha)\beta_q/q \\
\psi(\alpha\beta_{q'}) &= \phi(\alpha)\phi(\beta_{q'}) \ ,
\end{aligned} \tag{2.3}
$$

where $\varepsilon = 1$ or -1. It is easy to see that ψ is an algebra automorphism of D. We shall show that ψ induces an isomorphism of $O(q')$ to $O(q)$, if we choose ε suitably. We have only to show that $\psi(O(q')) \subset O(q)$ for a suitable choice of ε. Put $\omega_1 = 1$, $\omega_2 = (1+\beta_q)/2$, $\omega_3 = \alpha(1+\beta_q)/2$, $\omega_4 = (r+\alpha)\beta_q/q$. By direct calculations, we have;

$$
\begin{aligned}
\psi(1) = 1 \ , \qquad & \psi((1+\beta_{q'})/2) = (1-b)/2 + b\omega_2 + d\omega_4 \ , \\
\psi(\alpha(1+\beta_{q'})/2) &= \varepsilon(qr(b-1) + 2d(r^2+m))/2q \\
&\quad - \varepsilon(qr(b-1) + 2d(r^2+m))\omega_2/q + \varepsilon\omega_3 \\
&\quad + \varepsilon((b-1)q + 2rd)\omega_4/2 \ , \\
\psi((r'+\alpha)\beta_{q'}/q) &= -(bq(r'-\varepsilon r) - 2d\varepsilon(m+r^2))/qq' \\
&\quad + (2bq(r'-\varepsilon r) - 4d\varepsilon(m+r^2))\omega_2/qq' \\
&\quad + (2r'd + \varepsilon(bq+2rd))\omega_4/q' \ .
\end{aligned} \tag{2.4}
$$

We show that we can choose ε so that the coefficients of $\omega_1, \cdots, \omega_4$ of the right hand side of the above equalities are integral. As b is odd, so $(1-b)/2 \in Z$. By (3) in the introduction, we have $(r^2+m)/q \in Z$. So we have $bq(r'-\varepsilon r) - 2d\varepsilon(m+r^2) \equiv 0 \bmod q$. By the definition of b and d, we have $(bq+2dr)^2 + 4md^2 = qq'$. Then $bq + 2dr \equiv 2dr$ or $-2dr \bmod q'$. We put $\varepsilon = 1$ or $\varepsilon = -1$ respectively. Then we have $bq(r'-\varepsilon r) - 2d\varepsilon(m+r^2) \equiv bq(r'-\varepsilon r) + 2d\varepsilon(r'+\varepsilon r)(r'+\varepsilon r) = (r'-\varepsilon r)(bq+2dr+2dr'\varepsilon) \equiv 0 \bmod q'$. Then we have proved the assertion for $O(q)$. As for $O'(q)$ with $e=1$, the proof is virtually the same, which will be omitted here.

q.e.d.

We note that the assumption $q \neq q'$ was used only to show that the coefficients of the right hand side of (2.4) are integers. Let A be the cardinarity of the automorphism group of $O(q)$ or $O'(q)$. We can obtain A for $O(q)$ or $O'(q)$ when $e=1$ by modifying the proof of Proposition 2.1 for $q = q'$. That is, we have;

PROPOSITION 2.5. *Assume that $e=1$ for $O(q)$ (resp. $O'(q)$). Then $A = 4$ if $\mathfrak{q}^2 \in P_Z(2)$ (resp. $\mathfrak{q}^2 \in P(2)$), and $A = 2$ otherwise.*

Proof. Here we give the proof only for $O(q)$, because the proof for

$O'(q)$ is virtually the same. As we have shown in the proof of Proposition 2.1, we can correspond an automorphism of $O(q)$ to integers x, y such that $x^2 + 4my^2 = q^2$. If $\mathfrak{q}^2 \notin P_Z(2)$, all solutions of this equation are $(\pm q, 0)$. Then we have $(b, d) = (\pm 1, 0)$ in (2.3). We have $bq(r - \varepsilon r) - 2d\varepsilon(m + r^2) = \pm q(r - \varepsilon r) \equiv 0 \bmod q^2$ if and only if $\varepsilon = 1$. So there are only two automorphisms of $O(q)$. If $\mathfrak{q}^2 \in P_Z(2)$, we can put $\mathfrak{q}^2 = (x + 2y\sqrt{-m})$ by virtue of Remark 2.2. Then, the solutions of the diophantine equation $x^2 + 4my^2 = q^2$ are $(\pm x, \pm y)$ and $(\pm q, 0)$. By the condition $x \equiv 2ry \bmod q$, only two of $(\pm x, \pm y)$, say (x, y) and $(-x, -y)$, are appropriate. Then we have $(b, d) = \pm((x - 2ry)/q, y)$ in (2.3). Then, we have $\varepsilon(bq + 2dr) + 2dr = \pm(x\varepsilon + 2ry) \equiv 0 \bmod q$ if and only if $\varepsilon = -1$. If $\varepsilon = -1$, $bq(r - \varepsilon r) - 2d\varepsilon(m + r^2) = 2bqr + 2d(m + r^2) = ((bq + 2dr)^2 + 4md^2 - b^2q^2)/2d = (1 - b^2)q^2/2d \equiv 0 \bmod q^2$, because $q \nmid d$. Then $A = 4$ in this case. q.e.d.

Next, we count up the isomorphism classes of $O(q)$ and $O'(q)$. Let F be the genus field of $\boldsymbol{Q}(\sqrt{-m})$, that is, the maximal unramified abelian extension of $\boldsymbol{Q}(\sqrt{-m})$ which is abelian over $\boldsymbol{Q}$. Put $\varepsilon_i = (-1)^{(p_i-1)/2}$ if $p_i \mid m$, $p_i \neq 2$, and put $\varepsilon_i = (-1)^{(m-2)/4}$ if $p_i = 2$, $2 \mid m$. It is well known that $F = \boldsymbol{Q}(\sqrt{\varepsilon_1 p_1}, \cdots, \sqrt{\varepsilon_t p_t})$ if $m \equiv 2, 3 \bmod 4$, and $F = \boldsymbol{Q}(\sqrt{\varepsilon_1 p_1}, \cdots, \sqrt{\varepsilon_t p_t}, \sqrt{-1})$ if $m \equiv 1 \bmod 4$. Let L_0 (resp. L) be the classifield over $\boldsymbol{Q}(\sqrt{-m})$ which corresponds with $P(2)$ (resp. $P_Z(2)$). As $P(2) \supset P_Z(2)$, we have $L \supset L_0 \supset F$. We also note that L and L_0 are Galois extensions of $\boldsymbol{Q}$. The Galois group $\mathrm{Gal}(L_0/\boldsymbol{Q})$ (resp. $\mathrm{Gal}(L/\boldsymbol{Q})$) is generated by $\mathrm{Gal}(L_0/\boldsymbol{Q}(\sqrt{-m}))$ (resp. $\mathrm{Gal}(L/\boldsymbol{Q}(\sqrt{-m}))$) and the complex conjugation ρ. For an element σ of $\mathrm{Gal}(L_0/\boldsymbol{Q}(\sqrt{-m}))$ or $\mathrm{Gal}(L/\boldsymbol{Q}(\sqrt{-m}))$, we have $\rho\sigma\rho = \sigma^{-1}$. Especially, the conjugacy class in $\mathrm{Gal}(L_0/\boldsymbol{Q}(\sqrt{-m}))$ (resp. $\mathrm{Gal}(L/\boldsymbol{Q}(\sqrt{-m}))$) which contains an element $\sigma \in \mathrm{Gal}(L_0/\boldsymbol{Q}(\sqrt{-m}))$ (resp. $\mathrm{Gal}(L/\boldsymbol{Q}(\sqrt{-m}))$) is $\{\sigma, \sigma^{-1}\}$, though it may be that $\sigma = \sigma^{-1}$. Let q be a prime which satisfies (1) and (2). Let ζ_8 be a primitive eighth root of unity. Then, any $\tau \in \mathrm{Gal}(L(\zeta_8)/\boldsymbol{Q})$ (resp. $\mathrm{Gal}(L_0(\zeta_8)/\boldsymbol{Q})$) in the Frobenius conjugacy class of q in $L(\zeta_8)$ (resp. $L_0(\zeta_8)$) satisfies,

$$\begin{aligned} \tau|_{\boldsymbol{Q}(\sqrt{\varepsilon_i p_i})} &\neq \mathrm{id} \quad \text{if } p_i \mid m,\ p_i \neq 2 \text{ and } \varepsilon_i = 1 \\ &= \mathrm{id} \quad \text{if } p_i \mid m,\ p_i \neq 2 \text{ and } \varepsilon_i = -1\,, \end{aligned} \tag{2.6}$$

$$\tau|_{\boldsymbol{Q}(\zeta_8)} = \tau_0\,, \qquad \text{where } \zeta_8^{\tau_0} = \zeta_8^3\,. \tag{2.7}$$

(Here $\tau|_*$ means the restriction of τ to *.) In fact, (2.6) is equivalent to (1) and (2.7) to (2). Let q' be a prime different from q which satisfies (1)

and (2). Denote the Frobenius conjugacy classes of q (resp. q') in $\mathrm{Gal}(L_0/\boldsymbol{Q})$ or $\mathrm{Gal}(L/\boldsymbol{Q})$ by $\{\sigma, \sigma^{-1}\}$ (resp. $\{\sigma', \sigma'^{-1}\}$). Then the condition in Proposition 2.1 is equivalent to say that $\{\sigma, \sigma^{-1}\} = \{\sigma', \sigma'^{-1}\}$. In other words, the Frobenius conjugacy class of q in $L/\boldsymbol{Q}$ (resp. $L_0/\boldsymbol{Q}$) determines the isomorphism class of $O(q)$ (resp. $O'(q)$). Conversely, let c be a conjugacy class in $\mathrm{Gal}(L/\boldsymbol{Q})$ (resp. $\mathrm{Gal}(L_0/\boldsymbol{Q})$) such that every element $\sigma \in c$ satisfies (2.6) and

$$\sigma|_{L\cap\boldsymbol{Q}(\zeta_8)} = \tau_0|_{L\cap\boldsymbol{Q}(\zeta_8)} \qquad \text{(resp.} \tag{2.8}$$

$$\sigma|_{L_0\cap\boldsymbol{Q}(\zeta_8)} = \tau_0|_{L_0\cap\boldsymbol{Q}(\zeta_8)}\text{)} . \tag{2.9}$$

Then every element of c can be uniquely lifted up to an element τ of $\mathrm{Gal}(L(\zeta_8)/\boldsymbol{Q})$ (resp. $\mathrm{Gal}(L_0(\zeta_8)/\boldsymbol{Q})$ so that τ satisfies (2.6) and (2.7). These lifted elements also form a conjugacy class c' in $\mathrm{Gal}(L(\zeta_8)/\boldsymbol{Q})$ (resp. $\mathrm{Gal}(L_0(\zeta_8)/\boldsymbol{Q})$). By virtue of Chebotarev's density theorem, there exists a prime integer $q \neq 2$, $q\nmid m$, such that the Frobenius conjugacy class of q in $L(\zeta_8)$ (resp. $L_0(\zeta_8)$) is c'. Summing up, we have;

COROLLARY 2.10. *The isomorphism classes of* $O(q)$ *(resp.* $O'(q)$*) correspond bijectively with the pairs* $\{\sigma, \sigma^{-1}\}$ *of elements of* $\mathrm{Gal}(L/\boldsymbol{Q})$ *(resp.* $\mathrm{Gal}(L_0/\boldsymbol{Q})$*) which satisfy* (2.6) *and* (2.8) *(resp.* (2.6) *and* (2.9)).

To count up the isomorphism classes of $O(q)$ or $O'(q)$ more precisely, we need next

LEMMA 2.11. *We have* $L \cap \boldsymbol{Q}(\zeta_8) = \boldsymbol{Q}$ *and* $L_0 \cap \boldsymbol{Q}(\zeta_8) = \boldsymbol{Q}$ *if* $m \equiv 3 \bmod 4$, $L \cap \boldsymbol{Q}(\zeta_8) = \boldsymbol{Q}(\sqrt{-1})$ *if* $m \equiv 1 \bmod 4$, *and* $L \cap \boldsymbol{Q}(\zeta_8) = \boldsymbol{Q}(\zeta_8)$ *if* $m \equiv 2 \bmod 4$.

Proof. This is an easy exercise of the classfield theory, and the proof will be omitted here. q.e.d.

Now let δ (resp. δ_0) be the number of elements σ of $\mathrm{Gal}(L/\boldsymbol{Q}(\sqrt{-m}))$ (resp. $\mathrm{Gal}(L_0/\boldsymbol{Q}(\sqrt{-m}))$) such that $\sigma^2 = 1$ and that σ satisfies (2.6) and (2.8) (resp. (2.6) and (2.9)). For any integer d such that $d \equiv 0$ or $1 \bmod 4$, we denote by $h(d)$ the class number of the quadratic order whose discriminant is d. Then we have;

COROLLARY 2.12. *The number of isomorphism classes of* $O(q)$ *(resp.* $O'(q)$*) is equal to* $h(-4m)/2^t + \delta/2$ *(resp.* $h(-m)/2^t + \delta_0/2$*), where* t *is the number of the prime divisors of* m.

Proof. Let σ be an element of $\mathrm{Gal}(L/\boldsymbol{Q})$ (resp. $\mathrm{Gal}(L_0/\boldsymbol{Q})$) which satisfies (2.6) and (2.8) (resp. (2.9)). By Corollary 2.10 and Lemma 2.11, the isomorphism classes of $O(q)$ (resp. $O'(q)$) correspond bijectively with the conjugacy classes in $\sigma\,\mathrm{Gal}(L/F)$ (resp. $\sigma\,\mathrm{Gal}(L_0/F)$) if $m \equiv 1$ or $3 \bmod 4$ (resp. $m \equiv 3 \bmod 4$) and those in $\sigma\,\mathrm{Gal}(L/F(\sqrt{-1}))$ if $m \equiv 2 \bmod 4$. We have $[F;\ \boldsymbol{Q}(\sqrt{-m})] = 2^{t-1}$ if $m \equiv 3 \bmod 4$, $= 2^t$ if $m \equiv 1 \bmod 4$, and $[F(\sqrt{-1});\ \boldsymbol{Q}(\sqrt{-m})] = 2^t$ if $m \equiv 2 \bmod 4$. As well known, $h(-16m) = 2h(-4m)$. Then the assertion is easily shown by direct calculation. q.e.d.

Remark 2.13. If we take m to be a prime $p \geqq 5$, we can show that $\delta = \delta_0 = 1$ if $p \equiv 3 \bmod 4$ and $\delta = 0$ if $p \equiv 1 \bmod 4$ by direct calculation. If $p \equiv 1 \bmod 4$, $O(q)$ is never isomorphic to $O'(q')$. If $p \equiv 3 \bmod 4$, $e = 2$ for $O(q)$ (resp. $O'(q)$) if and only if q fully decomposes in L (resp. L_0) over $\boldsymbol{Q}$. Then by Lemma 1.8 and Corollary 2.12, we have $(h(-p) + h(-4p))/2$ isomorphism classes of maximal orders which contains an element whose reduced norm is p. (Here we put $h(-p) = 0$ if $p \equiv 1 \bmod 4$.) As Deuring has shown in his paper [3], this is equal to the number of isomorphism classes of such maximal orders. Then, in this case, Theorems 1, 2, and 3 are obvious. To obtain Theorems 1, 2, and 3 in general without his results, we need some arithmetic of quaternion algebra which is due to Eichler, which will be reviewed in the next section.

Remark 2.14. It is not hard to show that F (resp. $F(\sqrt{-1})$) is the maximal $(2, \cdots, 2)$ extension of $\boldsymbol{Q}(\sqrt{-m})$ in L if $m \not\equiv 2 \bmod 4$ (resp. $m \equiv 2 \bmod 4$).

§ 3. Completion of the proofs of Theorems

First, we review some results which is due to Eichler [5], and then, apply them to complete the proofs of Theorems 1, 2, and 3. Here, we mainly follow the formulation of Shimizu [10] p. 178–179. Let O be a maximal order of D, K be a quadratic subfield of D, and o be an order of K. Let $\{o/p\}$ be the Eichler symbol:

$$\{o/p\} = 1, \text{ if } p \text{ divides the conductor of } o\,,$$
$$= (K/p) \text{ (Legendre symbol), otherwise}\,.$$

Put $1(o) = \prod_{p|m}(1 - \{o/p\})$. Then, there exists a maximal order of D which contains o optimally, if and only if $l(o) \neq 0$. Let ψ be an embedding of K into D. We say that ψ is an optimal embedding of o to O when $\psi(o)$

is an optimal subring of O. Two optimal embeddings ψ_1 and ψ_2 of o to O are said to be equivalent if there exists a unit $\gamma \in O^\times$ such that $\psi_1(\kappa) = \gamma\psi_2(\kappa)\gamma^{-1}$ for all $\kappa \in K$. Let $O_1, \cdots, O_T$ be a complete set of representatives of the isomorphism classes of maximal orders of D. Let g_i be the number of the equivalence classes of optimal embeddings of o to O_i, and H_i be the number of the two sided ideal classes of O_i. Then, the following equality has been known:

$$\sum_{i=1}^{T} g_i H_i = l(o)h(o) , \tag{3.1}$$

where $h(o)$ is the class number of o (Eichler and Shimizu, loc. cit.). Now, we apply the above equality to our case. Put $o = \boldsymbol{Z} + \boldsymbol{Z}\alpha$ and $o' = \boldsymbol{Z} + \boldsymbol{Z}(1 + \alpha)/2$. Let $H(q)$ (resp. $H'(q)$) be the number of the two sided ideal classes of $O(q)$ (resp. $O'(q)$), $g(q)$ (resp. $g'(q)$) be the number of the equivalence classes of optimal embeddings of o (resp. o') to $O(q)$ (resp. $O'(q)$), $A(q)$ (resp. $A'(q)$) be the cardinality of the group of ring automorphisms of $O(q)$ (resp. $O'(q)$), and $e(q)$ (resp. $e'(q)$) be the one half of the cardinality of the unit group $O(q)^\times$ (resp. $O'(q)^\times$). Then, we have

LEMMA 3.2. *The numbers $g(q)$, $g'(q)$, $A(q)$, $A'(q)$, $H(q)$, and $H'(q)$ are given as follows:*

$g(q)$	$A(q)$	$H(q)$	
2	2	2^{t-1}	*if* $e(q) = 1$ *and* $\mathfrak{q}^2 \notin P_{\boldsymbol{Z}}(2)$
2	4	2^{t-2}	*if* $e(q) = 1$ *and* $\mathfrak{q}^2 \in P_{\boldsymbol{Z}}(2)$
1	4	2^{t-1}	*if* $e(q) = 2$ *and* $2 \nmid m$
2	8	2^{t-2}	*if* $e(q) = 2$ *and* $2 \mid m$
2	6	2^{t-1}	*if* $e(q) = 3$ *and* $3 \nmid m$
2	12	2^{t-2}	*if* $e(q) = 3$ *and* $3 \mid m$

$g'(q)$	$A'(q)$	$H'(q)$	
2	2	2^{t-1}	*if* $e'(q) = 1$ *and* $\mathfrak{q}^2 \notin P(2)$
2	4	2^{t-1}	*if* $e'(q) = 1$ *and* $\mathfrak{q}^2 \in P(2)$
1	4	2^{t-1}	*if* $e'(q) = 2$ (*and* $2 \nmid m$)

where t is the number of the finite prime divisors of the discriminant of D, and $\mathfrak{q}$ is any prime ideal of $\boldsymbol{Q}(\sqrt{-m})$ which divides q.

Proof. When $e(q)$ or $e'(q)$ is equal to one, the value $A(q)$ or $A'(q)$ is

given in Proposition 2.7. It is also easy to see that there are only two optimal embeddings ψ_1 and ψ_2 of o to $O(q)$, or o' to $O'(q)$, where $\psi_1(\alpha) = \alpha$ and $\psi_2(\alpha) = -\alpha$. So, $g(q)$ or $g'(q) = 2$, since ψ_1 is not equivalent to ψ_2. Then, $H(q)$ or $H'(q)$ is given by the well known equality $H(q) = 2^t e(q)/A(q)$, or $H'(q) = 2^t e'(q)/A'(q)$ (Eichler [5]). The assertions for the other cases has been well known (Eichler [4], [5]) and is easy to see. q.e.d.

COROLLARY 3.3. *We have the following equalities*:

$$\begin{aligned} g(q)H(q) &= 2^t && \text{if } \mathfrak{q}^2 \notin P_Z(2)\,, \\ &= 2^{t-1} && \text{if } \mathfrak{q}^2 \in P_Z(2)\,, \\ g'(q)H'(q) &= 2^t && \text{if } \mathfrak{q}^2 \notin P(2)\,, \\ &= 2^{t-1} && \text{if } \mathfrak{q}^2 \in P(2)\,. \end{aligned}$$

Proof. When $e(q) = 1$ or $e'(q) = 1$, this is obvious. When $e(q)$ or $e'(q) = 2$, we have always $\mathfrak{q}^2 \in P_Z(2)$ by Corollary 1.6, since $[P(2): P_Z(2)] = 2$ if $m \equiv 2 \bmod 4$. When $e(q) = 3$, we have $\mathfrak{q}^2 \in P_Z(2)$ if and only if $3 \mid m$ by virtue of Corollary 1.7 (Note that we have assumed that $m \geqq 5$). q.e.d.

Proof of Theorems 1, 2, *and* 3. It is easy to see that $l(o) = 1$, $l(o') = 1$, $h(o) = h(-4m)$, and $h(o') = h(-m)$. Let $\{O(q_1), \cdots, O(q_n)\}$ (resp. $\{O'(q'_1), \cdots, O'(q'_s)\}$) be a complete set of representatives of the isomorphism classes of maximal orders of the form $O(q)$ (resp. $O'(q)$) for some primes q satisfying (1) and (2). Then, to prove the theorems, we have only to show that

$$\sum_{i=1}^{n} g(q_i)H(q_i) = h(-4m)\,, \quad \text{and} \quad \sum_{i=1}^{s} g'(q'_i)H'(q'_i) = h(-m)\,,$$

by virtue of the equality (3.1). But as we have seen in Corollary 2.12, there are δ (resp. δ_0) isomorphism classes of $O(q)$ (resp. $O'(q')$) such that $\mathfrak{q}^2 \in P_Z(2)$ (resp. $P(2)$), and $(h(-4m) - 2^{t-1}\delta)/2^t$ (resp. $(h(-m) - 2^{t-1}\delta_0)/2^t$) isomorphism classes of $O(q)$ (resp. $O'(q)$) such that $\mathfrak{q}^2 \notin P_Z(2)$ (resp. $P(2)$). So, the assertions are obvious. q.e.d.

Remark 3.4. We can calculate the trace of the Brandt matrix $B_0(m)$ with weight 0 by using Lemma 3.2, that is, $\operatorname{tr} B_0(m) = (h(-m) + h(-4m))/2$, where we put $h(-m) = 0$ if $m \not\equiv 3 \bmod 4$. Of course, this conicides with the special case of the trace formula by Eichler [5].

§ 4. Relation to Chevalley-Hasse-Noether parametrization and further remarks

Let K be a quadratic subfield of D, and o be an order of K. Let O be a maximal order of D which contains o optimally. By Chevalley, Hasse, and Noether, any maximal order of D which contains o optimally is isomorphic to $\mathfrak{a}O\mathfrak{a}^{-1}$ for some o ideal $\mathfrak{a}$. In this section, we show

PROPOSITION 4.1. *Notations being as before, Let* $\mathfrak{a}$ *be an integral ideal of* $o = \boldsymbol{Z} + \boldsymbol{Z}\alpha$ *which is prime to two. Put* $\mathfrak{q} = \boldsymbol{Z}q + \boldsymbol{Z}(r + \alpha)$. *Then, we have an isomorphism*: $\mathfrak{a}O(q, r)\mathfrak{a}^{-1} \cong O(q', r')$, *for any* q' *satisfying* (1) *and* (2) *which is the norm of some prime ideal* $\mathfrak{q}' \in \bar{\mathfrak{q}}\bar{\mathfrak{a}}^2P_{\boldsymbol{Z}}(2)$ (*resp.* $\mathfrak{q}' \in \bar{\mathfrak{q}}\bar{\mathfrak{a}}^2P(o)$), *if* $m \not\equiv 3 \bmod 4$ (*resp.* $m \equiv 3 \bmod 4$). *Here,* $P(o)$ *is the principal ideal group of* o.

PROPOSITION 4.2. *Assume that* $m \equiv 3 \bmod 4$. *Put* $\mathfrak{q} = \boldsymbol{Z}q + \boldsymbol{Z}(r + \alpha)/2$. *Let* $\mathfrak{a}$ *be an integral ideal of* $o = \boldsymbol{Z} + \boldsymbol{Z}(1 + \alpha)/2$. *Then, we have an isomorphism*: $\mathfrak{a}O'(q, r)\mathfrak{a}^{-1} \cong O'(q', r')$ *for any* q' *satisfying* (1) *and* (2) *which is the norm of a prime ideal* $\mathfrak{q}' \in \bar{\mathfrak{q}}\bar{\mathfrak{a}}^2P(o)$.

Proof of Proposition 4.2. *By definition,* $O'(q, r) = o + \mathfrak{q}\beta/q$. Then, we have $\mathfrak{a}O'(q, r)\mathfrak{a}^{-1} = o + \mathfrak{a}\bar{\mathfrak{a}}^{-1}\mathfrak{q}\beta/q = o + \mathfrak{a}^2\mathfrak{q}\beta/qa$, where $a = N(\mathfrak{a})$. By virtue of Theorem 2, there are q' and r' such that $\mathfrak{a}O'(q, r)\mathfrak{a}^{-1} \cong O'(q', r')$. Denote by β' the image of $\beta_{q'}$ in $\mathfrak{a}O'(q, r)\mathfrak{a}^{-1}$ by this isomorphism. Then, we have $\alpha\beta' = -\beta'\alpha$, since $\boldsymbol{Z} + \boldsymbol{Z}(1 + \alpha)/2$ is the unique optimal subring of $\mathfrak{a}O'(q, r)\mathfrak{a}^{-1}$ which is isomorphic to $\boldsymbol{Z} + \boldsymbol{Z}(1 + \alpha)/2$. So, β' belongs to $\mathfrak{a}^2\beta\mathfrak{q}/aq$. Put $\beta' = \kappa\beta$, where $\kappa \in \mathfrak{a}^2\mathfrak{q}/aq$. As $N(\beta') = q'$, we have $N(\kappa) = q'/q$ and $N(aq\kappa) = a^2qq'$. But $aq\kappa \in \mathfrak{a}^2\mathfrak{q}$, so there is an ideal $\mathfrak{q}'$ of $\boldsymbol{Z} + \boldsymbol{Z}(1 + \alpha)/2$ such that $(aq\kappa) = \mathfrak{a}^2\mathfrak{q}\mathfrak{q}'$ and $N(\mathfrak{q}') = q'$. So, by Proposition 2.1, the proof is completed. q.e.d.

Proof of Proposition 4.1. First, assume that $m \not\equiv 3 \bmod 4$. We have $O(q, r) \subset (o/2) + \mathfrak{q}\mathfrak{a}^2\beta/2qa$. In this case, optimal subrings of $\mathfrak{a}O(q, r)\mathfrak{a}^{-1}$ which are isomorphic to o may not be unique. But we can take an isomorphism $\mathfrak{a}O(q, r)\mathfrak{a}^{-1} \cong O(q', r')$ such that the image of o is o. Let β' be the image of $\beta_{q'}$ of this isomorphism, as before. So we have $\beta' \in \mathfrak{q}\mathfrak{a}^2\beta/2qa$. Put $\kappa = aq\beta'\beta^{-1}$. Then, $N(\kappa) = a^2qq' \in \boldsymbol{Z}$ and $\mathrm{tr}(\kappa) \in \boldsymbol{Z}$, since $\kappa \in \mathfrak{q}\mathfrak{a}^2/2 \subset (\boldsymbol{Z} + \boldsymbol{Z}\alpha)/2$. So, we have $\kappa \in \boldsymbol{Z} + \boldsymbol{Z}\alpha$. By the assumption that $\mathfrak{a}$ is prime to 2, there is an integral ideal $\mathfrak{q}'$ such that $(\kappa) = \mathfrak{q}\mathfrak{q}'\mathfrak{a}^2$ and $N(\mathfrak{q}') = q'$. Now, we show that $(\kappa) \in P_{\boldsymbol{Z}}(2)$. We have

$$(1+\beta')/2 \in \mathfrak{a}O(q,r)\mathfrak{a}^{-1}, \quad \text{so} \quad (aq+\kappa\beta)/2q \in a\mathfrak{a}^{-1}O(q,r)\mathfrak{a} \subset O(q,r).$$

Then, putting $\kappa = c + d\alpha$, we have

$$(aq+\kappa\beta)/2q = (aq - c + dr)/2q + (c - dr)(1+\beta)/2q + d(r+\alpha)\beta/2q .$$

So, we have $2 \mid d$ and $(\kappa) \in P_Z(2)$. When $m \equiv 3 \bmod 4$, the proof is virtually the same and we omit it here. q.e.d.

Next, let p be a prime integer such that $p \equiv 1 \bmod 4$. Let D be a definite quaternion algebra with discriminant p. Put $B = D \otimes_{\boldsymbol{Q}} \boldsymbol{Q}(\sqrt{p})$. Let σ be a non trivial automorphism of $\boldsymbol{Q}(\sqrt{p})$. Lift it to B by putting $(a \otimes b)^{\sigma} = a \otimes b^{\sigma}$. Following Ponomarev [9], a maximal order $\hat{O}$ of B is called symmetric, if $\hat{O}^{\sigma} = \hat{O}$. Then we have

PROPOSITION 4.3. *Let $\hat{O}$ be a symmetric maximal order of B which contains a primitive fourth root of unity. Then, there exists a prime integer q, satisfying* (1), (2), *such that*

$$\hat{O} \cong o + o(1+\beta)/2 + o\alpha(1+\beta)/2\sqrt{p} + o(r+\alpha)\beta/\sqrt{p}\,q$$

where $o = Z + Z(1+\sqrt{p})/2$, r is any integer such that $p + r^2 \equiv 0 \bmod q$, $r \equiv 0 \bmod p$, and α, β, are as before.

Proof. This is an easy corollary of our Theorem 1 by virtue of Ponomarev [9] and Hashimoto [7]. q.e.d.

REFERENCES

[1] A. A. Albert, Integral domains of rational generalized quaternion algebras, Bull. Amer. Math. Soc., **40** (1934), 164–176.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischen Funktionen-körper, Abh. Hamburg, **14** (1941), 197–272.

[3] ——, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl, Jahresbericht der Deutschen Math., **54** (1951), 24–41.

[4] M. Eichler, Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z., **43** (1938), 102–109.

[5] ——, Zur Zahlentheorie der Quaternionen-Algebren, J. reine angew. Math., **195** (1955), 127–151.

[6] K. Hashimoto, Twisted trace formula of the Brandt matrix, Proc. Japan Acad., **53**, Ser. A (1977), 98–102.

[7] ——, Some examples of integral definite quaternary quadratic forms with prime discriminant, Nagoya Math. J., **77** (1980), 167–175.

[8] T. Ibukiyama, A basis and maximal orders in quaternion algebras over the rational number field (in Japanese), Sugaku, **24** (1972), 316–318.

[9] P. Ponomarev, A correspondence between quaternary quadratic forms, Nagoya Math. J., **62** (1976), 125–140.

[10] H. Shimizu, On zeta functions of quaternion algebras, Ann. Math., **81** (1965), 166–193.
[11] ——, Some examples of new forms, J. Fac. Sci. Univ. Tokyo, **24-1** (1977), 97–113.

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan

Current Address:
Department of Mathematics
College of General Education
Kyushu University
Chuo-ku, Fukuoka
810 Japan