K. Hashimoto
Nagoya Math. J.
Vol. 77 (1980), 167-175

SOME EXAMPLES OF INTEGRAL DEFINITE QUATERNARY QUADRATIC FORMS WITH PRIME DISCRIMINANT

KI-ICHIRO HASHIMOTO

Introduction

In the theory of integral quadratic forms or the related theory such as modular forms, it is important to give examples of forms with given discriminant for various computational purposes. However, little is known about this problem even in the case where the explicit formula for the class number has been given. Among the works that deal with satisfactorily many examples or give a constructive method of them, there are [1] for ternary forms, and [5] for quaternary forms with square discriminants. As for quaternary forms with prime discriminant, P. Ponomarev [8] gave an explicit way to construct such forms from ternary forms with discriminant $2q$. It was based on the result of his previous work [7] and that of Y. Kitaoka [6], but was rather complicated.

The purpose of this brief note is to give some examples of quaternary forms with prime discriminant q, by first constructing the examples of "symmetric" maximal orders of a quaternion algebra over $Q(\sqrt{q})$. So this could be regarded as a numerical supplement to [2], [6], [7], or [3], [4].

As the numerical table suggests, it is likely that our examples cover a complete representatives of isometric classes of such forms. Unfortunately we could not prove this.

§1. Symmetric maximal orders

Let B_0 be the definite quaternion algebra over Q with discriminant q, where q is a prime number such that $q \equiv 1 \pmod 4$. Let $F = Q(\sqrt{q})$ be the real quadratic field and $B = B_0 \otimes F$ be the base extension of B_0; it is the definite quaternion algebra over F with discriminant (1). As in [3, Prop. 1], we take and fix a Q-automorphism σ of B of order 2, that induces the non-trivial automorphism on F, and that is trivial on B_0. A

Received February 23, 1979.

https://doi.org/10.1017/S0027763000018742 Published online by Cambridge University Press

maximal order of B will be called "symmetric" if it is stable under the action of σ.

We collect some known facts that could be found in [3], [4], [7].

PROPOSITION 1. *Let $\mathcal{O}$ be a symmetric maximal order of B. Then $\mathcal{O}_0 = B_0 \cap \mathcal{O}$ is a maximal order of B_0. Conversely, for every maximal order of B_0, there is a unique maximal order of B containing it; and this is symmetric.*

In B_0 or B, the set of isomorphic (maximal) orders coincides the set of conjugate classes, which is called a type. The number of types of maximal orders is called the type number. Note that, the groups $\mathcal{O}_0^\times/E_0$, $\mathcal{O}^\times/E$ have finite order and are type invariants. (E_0, E are the groups of units in Q, F, respectively.)

PROPOSITION 2. *The mapping $\mathcal{O}_0 \to \mathcal{O}$ in Prop.* 1 *induces the map from the set of types in B_0 to that of B. This is one-to-one at the types where $\mathcal{O}^\times/E$ has order* 1, 3, *or* 12. *It is two-to-one where $\mathcal{O}^\times/E$ has order* 2, *or* 6. (*We exclude the case for $q = 5$, where both type numbers are* 1, *$\mathcal{O}^\times/E$ has order* 60.)

PROPOSITION 3. *The number of types in B, which contains a symmetric maximal order is* $[(q + 19)/24]$.

Now we give the example of symmetric maximal orders of B. Let p be a prime number satisfying $(p/q) = -1$ and $p \equiv 3 \bmod 4$, and let s be any positive divisor of $(p + 1)/4$. Then we can write

$$B_0 = Q + Qi + Qj + Qij\,, \quad i^2 = -sq\,, \quad j^2 = -p\,, \quad ij = -ji\,.$$

Following proposition is a generalization of [5].

PROPOSITION 4. *We can find an integer a such that $a^2q + s \equiv 0 \pmod{p}$. Then*

$$\mathcal{O}_0(p, s) = Z + Z(1 + j)/2 + Zi(1 + j)/2s + Z(aq + i)j/p$$

is a maximal order of B_0. The type of $\mathcal{O}_0(p, s)$ is independent of the choice of a.

Proof. Evidently $\mathcal{O}_0(p, s) = \mathcal{O}_0$ is a lattice in B_0 that contains 1. To show that $\mathcal{O}_0$ is a ring, we put $e_1 = 1$, $e_2 = (1 + j)/2$, $e_3 = i(1 + j)/2s$,

https://doi.org/10.1017/S0027763000018742 Published online by Cambridge University Press

$e_4 = (aq + i)j/p$, and then express $e_h e_k$ as a linear combination of e_k's with integral coefficients. In fact:

$$\begin{aligned}
e_2^2 &= -(1+p)/4\cdot e_1 + e_2\,,\\
e_2e_3 &= (1+p)aq/4s\cdot e_1 - (1+p)aq/2s\cdot e_2 + (1+p)/2\cdot e_3 + p(1+p)/4s\cdot e_4\,,\\
e_2e_4 &= -aq\cdot e_1 + aq\cdot e_2 + s\cdot e_3 + (1-p)/2\cdot e_4\,,\\
e_3e_2 &= (1+p)aq/4s\cdot e_1 - (1+p)aq/2s\cdot e_2 + (1-p)/2\cdot e_3 + p(1+p)/4s\cdot e_4\,,\\
e_3^2 &= -(1+p)q/4s\cdot e_1\,,\\
e_3e_4 &= (sq - sqp + a^2q^2 + a^2q^2p)/2sp\cdot e_1 - (sq + a^2q^2 + a^2q^2p)/sp\cdot e_2 - aq\cdot e_3\\
&\quad + (1+p)aq/2s\cdot e_4\,,\\
e_4e_2 &= -aq\cdot e_2 - s\cdot e_3 + (1+p)/2\cdot e_4\,,\\
e_4e_3 &= -(sq + sqp + a^2q^2 + a^2q^2p)/2sp\cdot e_1 + (sq + a^2q^2 + a^2q^2p)/sp\cdot e_2\\
&\quad + aq\cdot e_3 - (1+p)aq/2s\cdot e_4\,,\\
e_4^2 &= -(sq + a^2q^2)/p\cdot e_1\,.
\end{aligned}$$

Finally, the discriminant of $\mathcal{O}_0$ is

$$\det(\mathrm{Tr}\,(e_he_k)) = \det\begin{bmatrix} 2 & 1 & 0 & 0\\ 1 & (1-p)/2 & 0 & -aq\\ 0 & 0 & -(1+p)q/2s & -q\\ 0 & -aq & -q & -2(sq + a^2q^2)/p\end{bmatrix} = -q^2\,,$$

and this proves that $\mathcal{O}_0$ is maximal.

THEOREM 1. *Let $\mathcal{O}(p, s)$ be the symmetric maximal order of B that contains $\mathcal{O}_0(p, s)$. This is given by*

$$\mathcal{O}(p, s) = O_F + O_F(1+j)/2 + O_F i^*(1+j)/2s + O_F(a\sqrt{q} + i^*)j/p\,,$$

where we write O_F the ring of integers of F, and $i^* = i/\sqrt{q}$.

Proof. This may be proved by exactly the same way as Prop. 4, and we omit the calculation. Another way to prove it consists in compairing the integral basis of $\mathcal{O}(p, s)$ to that of $\mathcal{O}_0(p, s)$: if we note the simple relation $i^*(1+j)/2s = e_3/\sqrt{q}$, $(a\sqrt{q} + i^*)j/p = e_4/\sqrt{q}$, we can easily get to the conclusion. The symmetricity of $\mathcal{O}(p, s)$ is evident.

Remark 1. If we let p and s vary, there arise infinitely many symmetric maximal orders $\mathcal{O}(p, s)$ of B. So there are many isomorphisms among them, because the type number is finite (Prop. 3). For example, we can prove

https://doi.org/10.1017/S0027763000018742 Published online by Cambridge University Press

(i) $\mathcal{O}(p, s) \cong \mathcal{O}(p, s^*)$ if $4ss^* = x^2 + py^2$ for some $x, y \in Z$

(ii) $\mathcal{O}(p, 1) \cong \mathcal{O}(p^*, 1)$ if and only if $pp^* = x^2 + qy^2$ for some $x, y \in Z$.

§ 2. Integral quaternary forms with discriminant q

It is well known that quaternary quadratic space with nonsquare discriminant D is realized as a subspace of its second clifford algebra, which is a quaternion algebra over the quadratic field $Q(\sqrt{D})$. In our case, where $D = q$ is a prime as in § 1, it is isomorphic to B. Thus we consider

$$V = \{x \in B \mid {}^{\sigma}x = \bar{x}\} = Q + Qi^* + Q\sqrt{q}j + Qi^*j$$

equipped with the restriction of the reduced norm of B ($x \to \bar{x}$ denotes the canonical involution of B).

We quote the following result from [7]:

Proposition 5. *Let $\mathcal{O}$ be a symmetric maximal order of B. Then $L = \mathcal{O} \cap V$ is a lattice in V, with discriminant q and has a vector of length* 1. *Conversely, every such lattice can be written in this way (up to a similitude of V). Moreover for $L_k = \mathcal{O}_k \cap V$, $k = 1, 2$, we have: $L_1 \cong L_2$ if and only if $\mathcal{O}_1 \cong \mathcal{O}_2$.*

An easy consequence of the above correspondence is

Proposition 6. *Let $\mathcal{O}$ and $L = \mathcal{O} \cap V$ be as in Prop.* 5, *and let $O(L)$ ($O^+(L)$) be the group of (proper) automorphisms of L. Then we have*

$$O^+(L) \cong \mathcal{O}^\times/E \times \{\pm 1\}\,,$$
$$O(L) \cong \mathcal{O}^\times/E \times \{\pm 1\} \times \{1, \sigma\}\,,$$

the automorphism corresponding to $u \in \mathcal{O}^\times/E$ being $x \to ux\,{}^{\sigma}u^{-1}$, where we take u to be a root of unity.

The proof is easy and therefore omitted. (cf. [2, Prop. 3])

As a direct application, we get

Theorem 2. *Let p be a prime with $(p/q) = -1$ and $p \equiv 3 (\mathrm{mod}\, 4)$, and let s be any positive divisor of $(1 + p)/4$, and $a \in Z$ be such that $a^2q + s \equiv 0$ (mod p). Then*

$$L(p, s) = Z + Z(1 + \sqrt{q}j)/2 + Zi^*(1 + j)/2s + Z(a\sqrt{q} + i^*)j/p$$

https://doi.org/10.1017/S0027763000018742 Published online by Cambridge University Press

is a nice lattice in V, i.e, it has discriminant q and has a vector of length 1. *Therefore,*

$$\begin{aligned} f(p, s; x) &= f_L(x) \\ &= (2x_1 + x_2)^2/4 + (px_2 + 2ax_4)^2 q/4p + x_3^2/4s + (px_3 + 2sx_4)^2/4sp \end{aligned}$$

is a nice form, i.e, it is an integral quaternary form of discriminant q that represent 1.

Let a_n, $n = 1, 2, 3, \cdots$, be the number of vectors in L with length n. It is the n-th Fourier coefficient of the theta series associated to $f_L(x)$. Proposition 6 can be interpreted as giving a_1. Namely we can show easily

PROPOSITION 7. (i) $a_1 = 2.\sharp(\{u \in \mathcal{O}^\times; u^{\sigma}u = 1\}/E^1)$,

(ii) $a_1 = 2, 4, 6, 8, 12$, *according as* $\sharp(\mathcal{O}^\times/E) = 1, 2, 3, 6, 12$, *where E^1 denotes the group of units in F with norm* 1.

(In (ii) of the Proposition 7, and following Proposition 8, we are excluding the case for $q = 5$).

PROPOSITION 8. *Let H_j denotes the number of classes of nice lattices for which $\mathcal{O}^\times/E$ has order j, $j = 1, 2, 3, 6, 12$. They are determined by the following formulae*:

$$\begin{cases} H_1 + H_2 + H_3 + H_6 + H_{12} = [(q + 19)/24] \\ H_6 = \begin{cases} 0 & q \equiv 1 \pmod 3 \\ 1 & q \not\equiv 1 \pmod 3), \end{cases} \qquad H_{12} = \begin{cases} 0 & q \equiv 1 \pmod 8 \\ 1 & q \not\equiv 1 \pmod 8 \end{cases} \\ 4H_2 + 4H_6 + 2H_{12} = h(-q)\ , \qquad 4H_3 + 2H_6 + 4H_{12} = h(-3q) \end{cases}$$

where $h(n)$ is the class number of $Q(\sqrt{n})$.

This is a direct consequence of [3, Theorem 2], and [6].

§ 3. Numerical examples

In the following table we give the examples of (p, s, a)'s so that $f(p, s)$'s form a complete set of representatives of classes of nice quaternary forms. ($f(p, s; x) = x_1^2 + x_1x_2 + a^*x_2^2 + b^*x_2x_4 + c^*x_3^2 + x_3x_4 + d^*x_4^2$, $a^* = (1 + pq)/4$, $b^* = aq$, $c^* = (1 + p)/4s$, $d^* = (a^2q + s)/p$)

https://doi.org/10.1017/S0027763000018742 Published online by Cambridge University Press

q	(p, s, a)	$\sharp(\mathcal{O}^\times/E)$	$(a_1, a_2, a_3, a_4, a_5, \cdots)$
5	(3, 1, 1)	60	(20, 30, 60, ⋯)
13	(11, 1, 4)	12	(12, 14, 48, ⋯)
17	(3, 1, 1)	6	(8, 24, 18, ⋯)
29	(3, 1, 1)	6	(8, 12, 18, 32, ⋯)
	(19, 1, 6)	12	(12, 6, 24, 20, ⋯)
37	(23, 3, 10)	3	(6, 8, 30, 24, ⋯)
	(23, 1, 8)	12	(12, 6, 24, 12, ⋯)
41	(11, 1, 2)	2	(4, 16, 12, ⋯)
	(3, 1, 1)	6	(8, 12, 6, ⋯)
53	(23, 3, 4)	3	(6, 6, 18, 26, 30, 18, 64, ⋯)
	(3, 1, 1)	6	(8, 12, 6, 20, 36, 12, 60, ⋯)
	(31, 1, 10)	12	(12, 6, 24, 12, 24, 12, 56, ⋯)
61	(7, 1, 5)	2	(4, 8, 20, 16, 36, 20, ⋯)
	(23, 3, 3)	3	(6, 2, 24, 18, 30, 30, ⋯)
	(31, 1, 1)	12	(12, 6, 24, 12, 24, 8, ⋯)
73	(59, 3, 2)	1	(2, 12, 14, 22, 12, ⋯)
	(7, 1, 3)	2	(4, 8, 12, 24, 20, ⋯)
	(31, 2, 11)	3	(6, 6, 12, 24, 8, ⋯)
89	(23, 2, 4)	1	(2, 10, 10, ⋯)
	(19, 1, 4)	2	(4, 12, 0, ⋯)
	(59, 1, 23)	2	(4, 8, 8, ⋯)
	(3, 1, 1)	6	(8, 12, 6, ⋯)
97	(23, 2, 8)	1	(2, 10, 10, ⋯)
	(71, 2, 29)	1	(2, 8, 14, ⋯)
	(7, 1, 1)	2	(4, 8, 8, ⋯)
	(59, 3, 28)	3	(6, 6, 12, ⋯)
101	(7, 2, 2)	2	(4, 8, 8, 12, 32, 12, 34, 32, 48, 28)
	(11, 3, 2)	2	(4, 4, 12, 16, 36, 12, 28, 20, 36, 42)
	(83, 3, 22)	3	(6, 0, 12, 20, 30, 12, 36, 30, 30, 24)
	(3, 1, 1)	6	(8, 12, 6, 20, 24, 0, 24, 36, 20, 36)
	(103, 13, 26)	12	(12, 6, 24, 12, 24, 8, 48, 6, 36, 24)
109	(23, 2, 10)	1	(2, 6, 18, 12, 22, 12, 32, 24, 54, 24)
	(11, 1, 1)	2	(4, 4, 12, 12, 32, 20, 28, 16, 48, 26)
	(47, 2, 12)	3	(6, 2, 18, 6, 18, 24, 30, 20, 60, 30)

q	(p, s, a)	$\sharp(\mathcal{O}^\times/E)$	$(a_1, a_2, a_3, a_4, a_5, \cdots)$
	(47, 3, 13)	3	(6, 0, 12, 18, 24, 18, 36, 20, 48, 18)
	(59, 1, 20)	12	(12, 6, 24, 12, 24, 8, 48, 6, 36, 24)
113	(23, 3, 6)	1	(2, 10, 6, 20, 14, 26, 26, 44, 22, 28)
	(47, 4, 11)	1	(2, 8, 8, 26, 14, 14, 22, 50, 22, 40)
	(23, 6, 7)	2	(4, 12, 0, 20, 12, 22, 24, 48, 24, 52)
	(47, 6, 8)	3	(6, 6, 12, 18, 0, 18, 32, 48, 24, 42)
	(3, 1, 1)	6	(8, 12, 6, 20, 24, 0, 24, 36, 8, 36)
137	(23, 2, 5)	1	(2, 6, 10, 20, 12, 18, 18, 48, 16, 38)
	(47, 3, 6)	1	(2, 8, 4, 24, 14, 14, 26, 40, 18, 32)
	(47, 6, 5)	1	(2, 10, 4, 16, 12, 26, 24, 42, 24, 26)
	(43, 1, 4)	2	(4, 12, 0, 20, 8, 14, 20, 44, 24, 52)
	(79, 2, 7)	3	(6, 6, 12, 18, 0, 12, 26, 36, 24, 36)
	(3, 1, 1)	6	(8, 12, 6, 20, 24, 0, 24, 36, 8, 24)
149	(23, 2, 2)	1	(2, 6, 10, 12, 24, 6, 36, 22, 30, 20)
	(11, 1, 3)	2	(4, 4, 4, 16, 28, 12, 32, 12, 32, 28)
	(23, 1, 5)	2	(4, 4, 8, 8, 32, 8, 28, 24, 32, 38)
	(59, 5, 6)	3	(6, 0, 12, 12, 18, 6, 38, 24, 36, 30)
	(139, 5, 25)	3	(6, 0, 6, 14, 24, 18, 36, 24, 24, 18)
	(3, 1, 1)	6	(8, 12, 6, 20, 24, 0, 24, 36, 8, 24)
	(79, 20, 13)	12	(12, 6, 24, 12, 24, 8, 48, 6, 36, 24)
157	(23, 3, 8)	1	(2, 2, 18, 12, 16, 14, 18, 20, 46, 22)
	(103, 2, 24)	1	(2, 4, 14, 10, 18, 20, 24, 12, 46, 8)
	(7, 2, 2)	2	(4, 8, 8, 8, 16, 12, 18, 28, 52, 16)
	(79, 2, 9)	3	(6, 6, 12, 18, 0, 12, 24, 20, 36, 12)
	(79, 5, 20)	3	(6, 0, 12, 12, 14, 12, 30, 24, 48, 6)
	(139, 5, 39)	3	(6, 2, 18, 6, 12, 12, 18, 14, 60, 18)
	(83, 21, 14)	12	(12, 6, 24, 12, 24, 8, 48, 6, 36, 24)
173	(59, 3, 24)	1	(2, 4, 10, 14, 22, 6, 28, 20, 32, 16)
	(7, 2, 1)	2	(4, 8, 8, 8, 16, 8, 14, 32, 40, 20)
	(11, 3, 1)	2	(4, 4, 4, 12, 24, 16, 28, 12, 32, 20)
	(79, 2, 11)	3	(6, 6, 12, 18, 0, 12, 24, 18, 24, 14)
	(127, 4, 28)	3	(6, 0, 12, 12, 12, 6, 36, 24, 30, 14)
	(191, 4, 19)	3	(6, 0, 6, 14, 18, 12, 30, 30, 30, 18)
	(3, 1, 1)	6	(8, 12, 6, 20, 24, 0, 24, 36, 8, 24)
	(127, 1, 14)	12	(12, 6, 24, 12, 24, 8, 48, 6, 36, 24)

https://doi.org/10.1017/S0027763000018742 Published online by Cambridge University Press

q	(p, s, a)	$\sharp(\mathcal{O}^\times/E)$	$(a_1, a_2, a_3, a_4, a_5, \cdots)$
181	(23, 2, 4)	1	(2, 2, 14, 12, 20, 14, 16, 12, 38, 20)
	(31, 2, 9)	1	(2, 2, 16, 8, 18, 18, 16, 18, 38, 22)
	(47, 3, 9)	1	(2, 4, 10, 12, 20, 12, 26, 14, 42, 12)
	(7, 1, 1)	2	(4, 8, 8, 8, 16, 8, 10, 28, 48, 20)
	(19, 5, 3)	2	(4, 4, 8, 4, 28, 12, 20, 16, 40, 26)
	(71, 6, 7)	3	(6, 0, 12, 12, 12, 6, 30, 20, 36, 18)
	(103, 2, 13)	3	(6, 2, 18, 6, 12, 12, 12, 8, 54, 18)
	(131, 1, 29)	12	(12, 6, 24, 12, 24, 8, 48, 6, 36, 24)
193	(47, 6, 11)	1	(2, 6, 8, 10, 10, 24, 18, 32, 20, 28)
	(71, 2, 8)	1	(2, 10, 4, 10, 4, 26, 16, 36, 32, 18)
	(71, 6, 11)	1	(2, 4, 8, 18, 6, 22, 20, 32, 22, 18)
	(79, 4, 6)	1	(2, 4, 6, 20, 12, 22, 10, 24, 26, 22)
	(127, 16, 20)	1	(2, 4, 10, 14, 6, 28, 12, 28, 30, 24)
	(11, 1, 3)	2	(4, 4, 4, 12, 16, 24, 12, 28, 24, 32)
	(79, 10, 13)	3	(6, 6, 12, 18, 0, 12, 24, 18, 18, 12)
	(127, 4, 10)	3	(6, 0, 6, 12, 8, 30, 18, 36, 24, 24)
197	(31, 4, 5)	1	(2, 6, 8, 8, 18, 8, 30, 26, 32, 12)
	(71, 3, 7)	1	(2, 4, 8, 14, 18, 6, 36, 14, 26, 14)
	(11, 1, 1)	2	(4, 4, 4, 12, 20, 8, 28, 16, 36, 28)
	(79, 4, 18)	3	(6, 0, 6, 12, 12, 18, 30, 18, 36, 20)
	(103, 13, 14)	3	(6, 6, 12, 18, 0, 12, 24, 18, 18, 8)
	(167, 7, 27)	3	(6, 0, 6, 8, 18, 12, 42, 24, 18, 18)
	(227, 3, 39)	3	(6, 0, 12, 12, 12, 0, 32, 24, 30, 12)
	(3, 1, 1)	6	(8, 12, 6, 20, 24, 0, 24, 36, 8, 24)
	(103, 26, 17)	12	(12, 6, 24, 12, 24, 8, 48, 6, 36, 24)

(Calculation was done by hand up to $q = 97$, by electric machine for $100 < q < 200$)

References

[1] H. Brandt and O. Intrau, Tabellen reduzierter positiver ternärer quadratischer Formen, Akademie-Verlag, Berlin, 1958.

[2] M. Eichler, Theta function over Q and $Q(\sqrt{q})$, Lecture Notes in Math. Nr. 627, Springer-Verlag, Berlin-New York, 1977, 197–225.

[3] K. Hashimoto, Twisted trace formula of the Brandt matrix, Proceedings of the Japan Academy, Vol. **53**, Ser A, No. 3 (1977), 98–102.

[4] ——, On the arithmetic of quadratic extension of quaternion algebras (Japanese), master thesis, University of Tokyo, 1977.

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

[6] Y. Kitaoka, Quaternary even positive definite quadratic forms of prime discriminant, Nagoya Math. J., **52** (1973), 147–161.

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

[8] P. Ponomarev, Ternary quadratic forms and an explicit quaternary correspondences, Conference on Quadratic Forms, Queen's Papers in Pure and Applied Math. No. **46** (1977), 582–594.

Department of Mathematics
University of Tokyo