P. Ponomarev
Nagoya Math. J.
Vol. 62 (1976), 125-140

A CORRESPONDENCE BETWEEN QUATERNARY QUADRATIC FORMS

PAUL PONOMAREV*

Introduction

Let p be a prime $\equiv 1 \pmod 4$. Let $\mathfrak{A}$ denote the quaternion algebra of discriminant p^2 over the field of rational numbers $\boldsymbol{Q}$, and let V be a quaternary quadratic space over $\boldsymbol{Q}$ of discriminant $p(\boldsymbol{Q}^\times)^2$. In this note we establish a natural correspondence between the similitude classes of two-sided normal ideals of $\mathfrak{A}$ and certain similitude classes of the lattices of V which have reduced discriminant p or p^3. The classes for which it fails to be a function can be explicitly described, and at such classes it is at worst "one-to-two", the two associated classes merely being the duals of each other.

In the classical terminology, our correspondence is between classes of positive definite integral quaternary forms which have an improper automorphism, on the one hand, those of discriminant p^2, and, on the other hand, those of discriminant p or p^3. In both cases the classes having an improper automorphism can be obtained by taking the classes which represent 1 along with their adjoints. In § 5 we disprove a conjecture of Hecke ([4], p. 884) concerning the linear independence of the theta series coming from a fixed column of the Brandt matrices associated to $\mathfrak{A}$. We propose, instead, that the theta series coming from the classes having an improper automorphism should provide a basis for the corresponding space of modular forms. In the case of Nebentypus this reduces to a conjecture of Kitaoka ([5], p. 152). If the more general conjecture were verified, then our correspondence would have the property of associating a basis of modular forms of Nebentypus $\left(-2, p, \left(\frac{\ }{p}\right)\right)$ to a basis of modular forms of Haupttypus $(-2, p, 1)$.

Received February 18, 1976.

* This research was partially supported by NSF grand MPS 72-05055 A02 at the Institute for Advanced Study, Princeton.

§ 1. Symmetric normal ideals

Let $K = \boldsymbol{Q}(\sqrt{p})$ and let $\mathcal{O}$ denote the ring of integers of K. Put $\mathfrak{A}_K = \mathfrak{A} \otimes_{\boldsymbol{Q}} K$. Let $\alpha \mapsto \alpha^*$ be the canonical involution of $\mathfrak{A}_K$ and $N: \mathfrak{A}_K \mapsto K$ the reduced norm, $N(\alpha) = \alpha\alpha^*$. The conjugation $x \mapsto \bar{x}$ of K extends uniquely to a $\boldsymbol{Q}$-automorphism $\alpha \mapsto \bar{\alpha}$ of $\mathfrak{A}_K$ having $\mathfrak{A}$ as its ring of fixed elements. Let n be the norm map of K, $n(x) = x\bar{x}$ for $x \in K$.

NOTATION. For any associative ring R with 1 let $R^\times$ denote the multiplicative group of all invertible elements in R.

Let V be a definite quadratic space of dimension four over $\boldsymbol{Q}$. Let $f: V \to \boldsymbol{Q}$ be the quadratic form on V. The associated bilinear form B is defined by $B(v, w) = f(v + w) - f(v) - f(w)$, $v, w \in V$. The discriminant $\Delta(V)$ is the coset of $\det[B(v_i, v_j)]$ in $\boldsymbol{Q}^\times/(\boldsymbol{Q}^\times)^2$, where $\{v_i\}$ is a basis of $V, i, j = 1, 2, 3, 4$. We assume that $\Delta(V) = p(\boldsymbol{Q}^\times)^2$ and V_q is isotropic for each finite prime q. Then V is similar to the quadratic space $W = \{\alpha \in \mathfrak{A}_K: \bar{\alpha}^* = \alpha\}$, the quadratic form on W being the restriction of the norm form N ([8], § 2, Prop. 4). Since we will be concerned only with similitude classes of lattices of V, we may assume that $V = W, f = N$. The proper similitudes of V are then given by all mappings of the form $\xi \mapsto c\alpha\xi\bar{\alpha}^*$, where $c \in \boldsymbol{Q}^\times, \alpha \in \mathfrak{A}_K^\times$ ([8], § 1, Prop. 3).

For each rational prime q put $K_q = K \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_q, \mathfrak{A}_{K_q} = \mathfrak{A}_K \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_q = \mathfrak{A}_q \otimes_{\boldsymbol{Q}_q} K_q$. The conjugation on $\mathfrak{A}_K$ extends uniquely to $\mathfrak{A}_{K_q}$ and V_q may be identified with the subspace $\{\alpha_q \in \mathfrak{A}_{K_q}: \bar{\alpha}_q^* = \alpha_q\}$. The proper similitudes of V_q are all mappings of the form $\xi_q \mapsto c_q\alpha_q\xi_q\bar{\alpha}_q^*, c_q \in \boldsymbol{Q}_q^\times, \alpha_q \in \mathfrak{A}_{K_q}^\times$. Let $J_{\mathfrak{A}}, J_K, J_{\mathfrak{A}_K}$ denote the idele groups of $\mathfrak{A}, K, \mathfrak{A}_K$, respectively. For an $\mathcal{O}$-lattice Λ of $\mathfrak{A}_K$ we put $\Lambda_q = \Lambda \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_q$. Putting $\mathcal{O}_q = \mathcal{O} \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_q$, we see that Λ_q is an $\mathcal{O}_q$-lattice of $\mathfrak{A}_{K_q}$. If $\tilde{\alpha} = (\alpha_q), \tilde{\beta} = (\beta_q)$ are ideles of $\mathfrak{A}_K$, and Λ is an $\mathcal{O}$-lattice of $\mathfrak{A}_K$, then $\tilde{\alpha}\Lambda\tilde{\beta}$ is the $\mathcal{O}$-lattice defined by $(\tilde{\alpha}\Lambda\tilde{\beta})_q = \alpha_q\Lambda_q\beta_q$ for all rational q. Similarly, we can define $c\tilde{\alpha}L\bar{\tilde{\alpha}}^*$ for a lattice L of $V, c \in \boldsymbol{Q}^\times, \tilde{\alpha} \in J_{\mathfrak{A}_K}$; and $\tilde{\gamma}\Omega\tilde{\delta}$ for a lattice Ω of $\mathfrak{A}, \tilde{\gamma}, \tilde{\delta} \in J_{\mathfrak{A}}$.

An $\mathcal{O}$-lattice Λ of $\mathfrak{A}_K$ (resp. $\mathcal{O}_q$-lattice $\Lambda(q)$ of $\mathfrak{A}_{K_q}$) is *symmetric* if $\bar{\Lambda}^* = \Lambda$ (resp. $\overline{\Lambda(q)}^* = \Lambda(q)$). It is clear that Λ is symmetric if and only if Λ_q is symmetric for every rational q. A lattice of $\mathfrak{A}$ or $\mathfrak{A}_K$ is a *normal ideal* if its left and right orders are maximal. The existence of a symmetric maximal order is insured by [8], § 3, Prop. 5.

PROPOSITION 1. *Let Ω be a symmetric maximal order of $\mathfrak{A}_K$. An*

$\mathcal{O}$-lattice Λ of $\mathfrak{A}_K$ is a symmetric normal ideal of $\mathfrak{A}_K$ if and only if there exist $c \in \boldsymbol{Q}^\times, \tilde{\alpha} \in J_{\mathfrak{A}_K}$ such that either $\Lambda = c\tilde{\alpha}\Omega\bar{\tilde{\alpha}}^*$ or $\Lambda = c\sqrt{p}\tilde{\alpha}\Omega\bar{\tilde{\alpha}}^*$.

Proof. It is evident that a lattice in either of the latter two forms is a symmetric normal ideal of $\mathfrak{A}_K$. Suppose Λ is a symmetric normal ideal of $\mathfrak{A}_K$. We must show that $\Lambda_q = c_q\alpha_q\Omega_q\bar{\alpha}_q^*$ or $\Lambda_q = c_q\sqrt{p}\alpha_q\Omega_q\bar{\alpha}_q^*$ for each q, where $c_q \in \boldsymbol{Q}_q^\times, \alpha_q \in \mathfrak{A}_{K_q}^\times$. This assertion is trivial for q which split in K. Suppose q does not split in $K, q \neq p$. We can write $\Lambda_q = \alpha_q\Omega_q\beta_q$, $\alpha_q, \beta_q \in \mathfrak{A}_{K_q}^\times$. Then $\alpha_q\Omega_q\beta_q = \bar{\beta}_q^*\Omega_q\bar{\alpha}_q^*$, which implies that $\Omega_q\beta_q(\bar{\alpha}_q^*)^{-1}$ is a two-sided ideal. Since $\mathfrak{A}_K$ splits at every finite prime of K, we must have $\beta_q(\bar{\alpha}_q^*)^{-1} = x_q\varepsilon_q$ with $x_q \in K_q^\times, \varepsilon_q \in \Omega_q^\times$. Then $\Lambda_q = x_q\alpha_q\Omega_q\bar{\alpha}_q^* = \bar{\Lambda}_q^* = \bar{x}_q\alpha_q\Omega_q\bar{\alpha}_q^*$, which implies $\bar{x}_q^{-1}x_q \in \mathcal{O}_q^\times$. Using the fact that $H^1(\mathrm{Gal}\,(K_q/\boldsymbol{Q}_q), \mathcal{O}_q^\times) = 1$, we deduce that $x_q = c_qe_q$, where $c_q \in \boldsymbol{Q}_q^\times, e_q \in \mathcal{O}_q^\times$, which shows that $\Lambda_q = c_q\alpha_q\Omega_q\bar{\alpha}_q^*$. If $q = p$ we have the additional possibility $x_q = c_q\sqrt{p}e_q$.

If L is a lattice of V, its *norm* $N(L)$ is the unique positive rational number which generates the $\boldsymbol{Z}$-span of $\{N(v): v \in L\}$. The *reduced discriminant* $\Delta'(L)$ is defined to be $\det[N(L)^{-1}B(v_i, v_j)]$, where $\{v_i\}$ is a $\boldsymbol{Z}$-basis of $L, i, j = 1, 2, 3, 4$. For a lattice L of V, the lattices $L \otimes_{\boldsymbol{Z}} \mathcal{O}$, $\sqrt{p}(L \otimes_{\boldsymbol{Z}} \mathcal{O})$ are symmetric lattices of $\mathfrak{A}_K$ but are not normal ideals of $\mathfrak{A}_K$. If, however, $\Delta'(L) = p$, then we have

PROPOSITION 2. *For each lattice L of V with reduced discriminant p there exists a unique symmetric normal ideal $\hat{L}$ of $\mathfrak{A}_K$ such that $\hat{L} \cap V = L$. Any symmetric normal ideal Λ of $\mathfrak{A}_K$ is of the form $\Lambda = \hat{L}$ or $\Lambda = \sqrt{p}\hat{L}$ for some lattice L of V with reduced discriminant p.*

Proof. We can choose a symmetric maximal order Ω of $\mathfrak{A}_K$ so that $M = \Omega \cap V$ is a lattice of reduced discriminant p ([8], § 3, Prop. 5). The lattices of V with reduced discriminant p, being maximal, form an idealcomplex. Hence $L = c\tilde{\alpha}M\bar{\tilde{\alpha}}^*$ for some $c \in \boldsymbol{Q}^\times, \tilde{\alpha} \in J_{\mathfrak{A}_K}$. Put $\hat{L} = c\tilde{\alpha}\Omega\bar{\tilde{\alpha}}^*$. Then $\hat{L} \cap V = c\tilde{\alpha}(\Omega \cap V)\bar{\tilde{\alpha}}^* = L$. To prove uniqueness, suppose $c\tilde{\alpha}\Omega\bar{\tilde{\alpha}}^* \cap V = d\tilde{\beta}\Omega\bar{\tilde{\beta}}^* \cap V$. Then $d^{-1}c\tilde{\beta}^{-1}\tilde{\alpha}M(\overline{\tilde{\beta}^{-1}\tilde{\alpha}})^* = M$, which implies $d^{-1}c\tilde{\beta}^{-1}\tilde{\alpha}\Omega(\overline{\tilde{\beta}^{-1}\tilde{\alpha}})^* = \Omega$ ([8], § 4, Prop. 8), or $c\tilde{\alpha}\Omega\bar{\tilde{\alpha}}^* = d\tilde{\beta}\Omega\bar{\tilde{\beta}}^*$. To complete the proof we apply Proposition 1.

Remark. According to Proposition 2, the symmetric normal ideals Λ of $\mathfrak{A}_K$ are of two kinds: 1) $\Lambda = \hat{L}$ or 2) $\Lambda = \sqrt{p}\hat{L}$, L a lattice of V with

reduced discriminant p. If Λ is of the second kind, it is easily seen that $\Lambda \cap V$ is a non-maximal lattice with reduced discriminant p^3. If $\Lambda = \Omega$, a symmetric maximal order, then $(\sqrt{p})^{-1}\Omega \cap V$ is the dual lattice of $\Omega \cap V$ with respect to the bilinear form B. From this it follows that the lattices of V coming from Λ of the second kind are nothing more than the *dual* lattices of those coming from Λ of the first kind.

§ 2. Reflexive normal ideals

The quaternion algebra $\mathfrak{A}$ is split at all finite primes q except $q = p$. Let $\mathfrak{O}_p$ denote the unique maximal order of $\mathfrak{A}_p$ and $\mathfrak{P}_p$ the unique non-zero prime ideal of $\mathfrak{O}_p$.

LEMMA 1. *There exists a symmetric maximal order $\Omega(p)$ of $\mathfrak{A}_{K_p}$ with the properties*:

(i) $\Omega(p) \cap \mathfrak{A}_p = \mathfrak{O}_p$

(ii) $\sqrt{p}\Omega(p) = \pi\Omega(p)$ *for any generator* π *of* $\mathfrak{P}_p$.

Proof. We may assume that $\mathfrak{A}_{K_p} = M(2, K_p)$ and the conjugation on $\mathfrak{A}_{K_p}$ is given by

$$(1) \qquad \begin{bmatrix} x & y \\ z & w \end{bmatrix} \mapsto \begin{bmatrix} \overline{w} & u_p^{-1}\overline{z} \\ u_p\overline{y} & \overline{x} \end{bmatrix}, \qquad x, y, z, w \in K_p ,$$

where $u_p \in Z_q^{\times}$, $(u_p, p)_p = -1$ (cf. [8], § 2). Then we have

$$(2) \qquad \mathfrak{A}_p = \left\{ \begin{bmatrix} x & y \\ u_p\overline{y} & \overline{x} \end{bmatrix} : x, y \in K_p \right\}$$

$$(3) \qquad \mathfrak{O}_p = \left\{ \begin{bmatrix} x & y \\ u_p\overline{y} & \overline{x} \end{bmatrix} : x, y \in \mathcal{O}_p \right\}.$$

We take $\Omega(p) = M(2, \mathcal{O}_p)$. Then $\overline{\Omega(p)^*} = \Omega(p)$ and $\Omega(p) \cap \mathfrak{A}_p = \mathfrak{O}_p$. It is enough to verify (ii) for a particular generator π, say

$$\pi = \begin{bmatrix} \sqrt{p} & 0 \\ 0 & -\sqrt{p} \end{bmatrix} = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

LEMMA 2. *There exists a symmetric maximal order Ω_1 of $\mathfrak{A}_K$ with the properties*:

(i) $\mathfrak{O}_1 = \Omega_1 \cap \mathfrak{A}$ *is a maximal order of* $\mathfrak{A}$.

(ii) $\sqrt{p}\Omega_1 = \tilde{\pi}\Omega_1$ *for any* $\tilde{\pi} \in J_{\mathfrak{A}}$ *such that* $\tilde{\pi}\mathfrak{O}_1 =$ *the unique nonzero two-sided prime ideal of* $\mathfrak{O}_1$.

https://doi.org/10.1017/S0027763000024776 Published online by Cambridge University Press

Proof. Let $\mathfrak{O}$ be any maximal order of $\mathfrak{A}$. Then $\Omega = \mathfrak{O} \otimes_Z \mathcal{O}$ is a symmetric order of $\mathfrak{A}_K$ and Ω_q is maximal for $q \neq p$, since $\mathfrak{O}$ has discriminant p^2. Furthermore, $\Omega_q \cap \mathfrak{A}_q = \mathfrak{O}_q$ for $q \neq p$. We take Ω_1 so that $(\Omega_1)_q = \Omega_q$ for $q \neq p$ and $(\Omega_1)_p = \Omega(p)$ as in Lemma 1.

An $\mathcal{O}$-lattice Λ of $\mathfrak{A}_K$ is said to be *reflexive* if $\bar{\Lambda} = \Lambda$. For a maximal order Ω of $\mathfrak{A}_K$ we have $\Omega^* = \Omega$. Hence the notions of reflexivity and symmetry coincide for maximal orders of $\mathfrak{A}_K$.

PROPOSITION 3. *Let Ω be a symmetric maximal order of $\mathfrak{A}_K$. A lattice Λ of $\mathfrak{A}_K$ is a reflexive normal ideal of $\mathfrak{A}_K$ if and only if there exist $\tilde{\gamma}, \tilde{\delta} \in J_{\mathfrak{A}}$ such that $\Lambda = \tilde{\gamma}\Omega\tilde{\delta}$.*

Proof. It is clear that any Λ of the given form is reflexive. Suppose Λ is a reflexive normal ideal of $\mathfrak{A}_K$. For each rational prime q we can find $\alpha_q, \beta_q \in \mathfrak{A}_{K_q}^{\times}$ such that $\Lambda_q = \alpha_q \Omega_q \beta_q$. If q splits in K it is easily seen that α_q, β_q can be chosen from $\mathfrak{A}_q$. Suppose q does not split in K, so that K_q is a field. From $\bar{\alpha}_q \Omega \bar{\beta}_q = \alpha_q \Omega \beta_q$ it follows that $\alpha_q^{-1}\bar{\alpha}_q \Omega_q, \Omega \beta_q \bar{\beta}_q^{-1}$ are two-sided ideals. Furthermore, $N(\alpha_q^{-1}\bar{\alpha}_q) = N(\alpha_q)^{-1}\overline{N(\alpha_q)} \in \mathcal{O}_q^{\times}$. It follows that $\alpha_q^{-1}\bar{\alpha}_q \in \Omega_q^{\times}$ and, similarly, $\beta_q \bar{\beta}_q^{-1} \in \Omega_q^{\times}$. We may assume $\mathfrak{A}_{K_q} = M(2, K_q)$, $\Omega_q = M(2, \mathcal{O}_q)$, $\Omega_q^{\times} = GL(2, \mathcal{O}_q)$. If $q \neq p$ then $H^1(\mathrm{Gal}\,(K_q/\boldsymbol{Q}_q), GL(2, \mathcal{O}_q)) = 1$ implies that $\alpha_q = \gamma_q \varepsilon_q$, $\beta_q = \eta_q \delta_q$, where $\gamma_q, \delta_q \in \mathfrak{A}_q^{\times}$; $\varepsilon_q, \eta_q \in \Omega_q^{\times}$. If $q = p$ we have the additional possibilites $\alpha_q = \sqrt{p}\gamma_q \varepsilon_q$, $\beta_q = \sqrt{p}\eta_q \delta_q$. It follows that $\Lambda = \tilde{\gamma}\Omega\tilde{\delta}$ or $\Lambda = \sqrt{p}\tilde{\gamma}\Omega\tilde{\delta}$ for some $\tilde{\gamma}, \tilde{\delta} \in J_{\mathfrak{A}}$. Similarly, $\Omega = \tilde{\lambda}\Omega_1\tilde{\mu}$ or $\Omega = \sqrt{p}\tilde{\lambda}\Omega_1\tilde{\mu}$ for some $\tilde{\lambda}, \tilde{\mu} \in J_{\mathfrak{A}}$, where Ω_1 is chosen as in Lemma 2. Using property (ii) of Ω_1, we see that $\sqrt{p}\Omega = \tilde{\nu}\Omega$ for some $\tilde{\nu} \in J_{\mathfrak{A}}$. Thus $\Lambda = \tilde{\gamma}\Omega\tilde{\delta}$ or $\Lambda = \tilde{\gamma}\tilde{\nu}\Omega\tilde{\delta}$.

COROLLARY 1. *Let Ω_1, Ω_2 be symmetric maximal orders of $\mathfrak{A}_K$. Then there exists an element $\tilde{\alpha} \in J_{\mathfrak{A}}$ such that $\Omega_2 = \tilde{\alpha}\Omega_1\tilde{\alpha}^{-1}$.*

Proof. We know that $\Omega_2 = \tilde{\alpha}\Omega_1\tilde{\beta}$ for some $\tilde{\alpha}, \tilde{\beta} \in J_{\mathfrak{A}}$. The fact that $1 \in \Omega_2$ implies $\tilde{\beta} = \tilde{\gamma}\tilde{\alpha}^{-1}$ for some $\tilde{\gamma} \in J_{\mathfrak{A}_K}$. Then $\Omega_1\tilde{\gamma} = \tilde{\alpha}^{-1}\Omega_2\tilde{\alpha}$, which implies $\Omega_1\tilde{\gamma} = \Omega_1$, $\Omega_2 = \tilde{\alpha}\Omega_1\tilde{\alpha}^{-1}$.

COROLLARY 2. *Properties* (i) *and* (ii) *in Lemma* 2 *are valid for any symmetric maximal order Ω_1 of $\mathfrak{A}_K$.*

PROPOSITION 4. *For each normal ideal $\mathfrak{L}$ of $\mathfrak{A}$ there exists a unique reflexive normal ideal $\hat{\mathfrak{L}}$ of $\mathfrak{A}_K$ such that $\hat{\mathfrak{L}} \cap \mathfrak{A} = \mathfrak{L}$. Any reflexive normal ideal Λ of $\mathfrak{A}_K$ is of the form $\Lambda = \hat{\mathfrak{L}}$ for some normal ideal $\mathfrak{L}$ of $\mathfrak{A}$.*

Proof. Fix a symmetric maximal order Ω of $\mathfrak{A}_K$. Let $\mathfrak{O} = \Omega \cap \mathfrak{A}$. Then $\mathfrak{L} = \tilde{\alpha}\mathfrak{O}\tilde{\beta}$ for some $\tilde{\alpha}, \tilde{\beta} \in J_{\mathfrak{A}}$. We take $\hat{\mathfrak{L}} = \tilde{\alpha}\Omega\tilde{\beta}$. Proposition 3 shows that every reflexive normal ideal Λ is of the latter form. To prove uniqueness, suppose $\tilde{\alpha}\Omega\tilde{\beta} \cap \mathfrak{A} = \tilde{\gamma}\Omega\tilde{\delta} \cap \mathfrak{A}$. Then $\tilde{\alpha}\mathfrak{O}\tilde{\beta} = \tilde{\gamma}\mathfrak{O}\tilde{\delta}$, which implies $\tilde{\gamma}^{-1}\tilde{\alpha}\mathfrak{O} = \mathfrak{O}\tilde{\delta}\tilde{\beta}^{-1}$ is a two-sided ideal of $\mathfrak{O}$. Applying property (ii) and the fact that every two-sided ideal of $\mathfrak{O}$ is a rational multiple of a power of its two-sided prime ideal, we deduce $\tilde{\gamma}^{-1}\tilde{\alpha}\Omega = c(\sqrt{p})^m\Omega = \Omega\tilde{\delta}\tilde{\beta}^{-1}$, $c \in \boldsymbol{Q}^\times$, $m \in \boldsymbol{Z}$, which completes the proof.

COROLLARY. *The mapping $\mathfrak{O} \mapsto \hat{\mathfrak{O}}$ gives a one-to-one correspondence between the maximal orders of $\mathfrak{A}$ and the symmetric maximal orders of $\mathfrak{A}_K$.*

PROPOSITION 5. *A normal ideal Λ of $\mathfrak{A}_K$ is both symmetric and reflexive if and only if $\Lambda = c\Omega$ or $\Lambda = c\sqrt{p}\Omega$, $c \in \boldsymbol{Q}^\times$, for some symmetric maximal order Ω of $\mathfrak{A}_K$.*

Proof. A normal ideal in either of these two forms is clearly both reflexive and symmetric. Conversely, suppose Λ is reflexive and symmetric. Then $\Lambda = \hat{\mathfrak{L}}$ for a unique normal ideal $\mathfrak{L}$ of $\mathfrak{A}$. Let $\mathfrak{O}$ be the left order of $\mathfrak{L}$, so that $\hat{\mathfrak{O}} = \Omega$ is the left order of Λ. Then $\Lambda = \bar{\Lambda}^* = \Lambda^* = (\hat{\mathfrak{L}})^* = (\mathfrak{L}^*)\hat{}$, which implies $\mathfrak{L} = \mathfrak{L}^*$, or $\mathfrak{L}$ is a two-sided ideal of $\mathfrak{O}$. It follows that $\mathfrak{L} = c\mathfrak{P}^m$, $c \in \boldsymbol{Q}^\times$, $m \in \boldsymbol{Z}$, where $\mathfrak{P}$ is the two-sided prime ideal of $\mathfrak{O}$. Then $\Lambda = \hat{\mathfrak{L}} = c(\mathfrak{P}^m)\hat{} = c(\sqrt{p})^m\Omega$.

Remark. We have a one-to-one mapping $\mathfrak{O} \to \hat{\mathfrak{O}} \cap V$ from the set of maximal orders of $\mathfrak{A}$ into the set of lattices of V with reduced discriminant p, and a one-to-one mapping $\mathfrak{P} \mapsto \hat{\mathfrak{P}} \cap V$ from the set of all two-sided prime ideals of maximal orders of $\mathfrak{A}$ into the set of lattices of V with reduced discriminant p^3. Proposition 5 shows that these two mappings are essentially the *only* ones of this kind.

§ 3. Equivalences of symmetric maximal orders

The earlier discussion yields three possible notions of equivalence on the set of symmetric maximal orders of $\mathfrak{A}_K$.

I. Conjugacy: $\Omega_2 = \alpha\Omega_1\alpha^{-1}$, $\alpha \in \mathfrak{A}_K^\times$.

II. Similarity: $\Omega_2 = c\alpha\Omega_1\bar{\alpha}^*$, $c \in \boldsymbol{Q}^\times$, $\alpha \in \mathfrak{A}_K^\times$.

III. Strict conjugacy: $\Omega_2 = \alpha\Omega_1\alpha^{-1}$, $\alpha \in \mathfrak{A}^\times$.

Notion I is natural to $\mathfrak{A}_K$, being equivalent to: Ω_1, Ω_2 are isomorphic

as $\mathcal{O}$-orders. On the other hand, notion II is inherited from V, being equivalent to: $\Omega_1 \cap V, \Omega_2 \cap V$ are similar as lattices of V. Notion III comes from $\mathfrak{A}$, being equivalent to: $\Omega_1 \cap \mathfrak{A}, \Omega_2 \cap \mathfrak{A}$ are isomorphic as $\boldsymbol{Z}$-orders. In this section we will determine the relation between these three kinds of equivalence.

The implication III $\Rightarrow$ I is trivial. Suppose I holds, $\Omega_2 = \alpha\Omega_1\alpha^{-1}$, $\alpha \in \mathfrak{A}_K^\times$. We imitate the proof of Proposition 1 to deduce that $\Omega_2 = c\alpha\Omega_1\bar{\alpha}^*$ or $\Omega_2 = c\sqrt{p}\alpha\Omega_1\bar{\alpha}^*$, $c \in \boldsymbol{Q}^\times$. The latter case is not possible, as $\Omega_2 \cap V$ would then have reduced discriminant p^3 instead of p. Thus I $\Rightarrow$ II.

Now suppose II holds, $\Omega_2 = c\alpha\Omega_1\bar{\alpha}^*$, $c \in \boldsymbol{Q}^\times$, $\alpha \in \mathfrak{A}_K^\times$. The reflexivity of Ω_2 implies that $\bar{\alpha}^{-1}\alpha\Omega_1$ is a two-sided ideal of Ω_1. Then $\bar{\alpha}^{-1}\alpha = y\omega$, where $y \in K^\times$, $\omega \in \Omega_1^\times$, and ω can be taken to be a root of unity ([8], § 7, Prop. 14, Remark). Taking norms, we obtain $y^2 = \overline{N(\alpha)}^{-1}N(\alpha)$, $n(y)^2 = 1$, so that $n(y) = \pm 1$. If $n(y) = 1$, then $y = \bar{x}x^{-1}$, $x \in K^\times$, and $(\bar{x}\bar{\alpha})^{-1}(x\alpha) = \omega$. If $n(y) = -1$, then $y = e\bar{x}x^{-1}$, $x \in K^\times$, where e is the fundamental unit of K. Thus, without loss of generality, we may assume $\bar{\alpha}^{-1}\alpha = \omega$ or $\bar{\alpha}^{-1}\alpha = e\omega$. Multiplying α by $\sqrt{p}$ changes ω to $-\omega$. Hence we may assume that ω is a primitive m-th root of 1 for $m = 1, 3, 4, 5$. If $\bar{\alpha}^{-1}\alpha = e\omega$, then $\alpha = e\bar{\alpha}\omega = e(\bar{e}\alpha\bar{\omega})\omega = -\alpha\bar{\omega}\omega$, which shows $\bar{\omega}\omega = -1$. Hence $m = 4$, as $\bar{\omega}$ must have the same order as ω. Then $\bar{\omega} = -\omega^{-1} = \omega$, which implies $\omega \in \mathfrak{A}$, a contradiction to the fact that $\mathfrak{A}_p$ is not split, $p \equiv 1 \pmod 4$. We conclude that $\bar{\alpha}^{-1}\alpha = \omega$ is the only possibility and that $\bar{\omega}\omega = 1$. We now consider the various cases.

1. $\omega = 1$. If $\bar{\alpha}^{-1}\alpha = 1$, then $\alpha \in \mathfrak{A}^\times$ and $\Omega_2 = c\alpha\Omega_1\bar{\alpha}^* = c\alpha\Omega_1\alpha^* = cN(\alpha)\alpha\Omega_1\alpha^{-1}$, which implies $cN(\alpha) = \pm 1$, $\Omega_2 = \alpha\Omega\alpha^{-1}$.

2. $\omega = \zeta$, a primitive third root of 1. Then $\zeta = \bar{\zeta}\zeta^{-1}$ which shows $\alpha\zeta = \beta \in \mathfrak{A}^\times$, $\Omega_2 = \beta\Omega_1\beta^{-1}$.

3. $\omega = i$, $i^2 = -1$. Then $\bar{i} = -i$, which implies $i = \overline{(1+i)}^{-1}(1+i)$. Thus $\alpha = \beta(1+i)$, $\beta \in \mathfrak{A}^\times$, and $\Omega_2 = \beta(1+i)\Omega_1(1+i)^{-1}\beta^{-1}$.

4. $\omega^5 = 1$, $\omega \neq 1$. Then $\bar{\omega} = \omega^{-1} = \omega^4$, which shows $\omega = \overline{(\omega^2)}(\omega^2)^{-1}$, $\alpha\omega^2 = \beta \in \mathfrak{A}^\times$, $\Omega_2 = \beta\Omega_1\beta^{-1}$.

As a particular consequence, we have shown II $\Rightarrow$ I.

PROPOSITION 6. *Let Ω_0 be a fixed symmetric maximal order of $\mathfrak{A}_K$. Another symmetric maximal order is similar to Ω_0 if and only if it is conjugate to Ω_0. If Ω_0 does not contain a primitive fourth root of 1, then any symmetric maximal order conjugate to Ω_0 is actually strictly*

https://doi.org/10.1017/S0027763000024776 Published online by Cambridge University Press

conjugate to Ω_0. *If* Ω_0 *does contain a primitive fourth root of* 1, *then it contains one satisfying* $\bar{i} = -i$ *and, for any such* i, *a symmetric maximal order which is conjugate to* Ω_0 *is strictly conjugate either to* Ω_0 *or to* $(1+i)\Omega_0(1+i)^{-1}$.

Proof. It remains for us to prove the last statement. Let G be the group of roots of 1 in Ω_0 modulo $\{\pm 1\}$. If Ω_0 contains a primitive fourth root of 1, then the set of elements of order 2 in G has an odd number of elements. Hence at least one element of order 2 in G must be fixed by the conjugation, that is, $\bar{i} = \pm i$ for some primitive fourth root i. Since $\mathfrak{A}$ does not have a primitive fourth root of 1, we must have $\bar{i} = -i$. Suppose i, j are two fourth roots of 1 in Ω_0 satisfying $\bar{i} = -i$, $\bar{j} = -j$. Then $ij \in \Omega_0^\times$ and $\overline{ij} = ij$. This implies that ij is a unit of the maximal order $\mathfrak{O}_0 = \Omega_0 \cap \mathfrak{A}$. If $ij = \pm 1$, then $(1+i)\Omega_0(1+i)^{-1}$ $=(1+j)\Omega_0(1+j)^{-1}$. The only other possibility is $ij = \pm\zeta, \zeta$ a primitive third root of 1. In this case $\mathfrak{O}_0$ is the unique maximal order of $\mathfrak{A}$ (up to isomorphism) which contains a non-trivial unit. The elements $\sqrt{\bar{p}}i$, $\sqrt{\bar{p}}j$ are generators of the two-sided prime ideal of $\mathfrak{O}_0$ and as such are conjugate by a unit ε of $\mathfrak{O}_0$ (cf. § 4, Lemma 2, Proof), $\sqrt{\bar{p}}i = \varepsilon\sqrt{\bar{p}}j\varepsilon^{-1}$, $\varepsilon \in \mathfrak{O}_0^\times$. It follows that $(1+i)\Omega_0(1+i)^{-1} = \varepsilon(1+j)\Omega_0(1+j)\varepsilon^{-1}$.

§ 4. The correspondence

The mapping $\mathfrak{O} \mapsto \hat{\mathfrak{O}}$ induces a mapping $\{\mathfrak{O}\} \mapsto \{\hat{\mathfrak{O}}\}$ from the set of conjugacy classes of maximal orders of $\mathfrak{A}$ onto the set of conjugacy classes of symmetric maximal orders of $\mathfrak{A}_K$. Proposition 6 shows that this mapping is one-to-one on the classes of orders $\mathfrak{O}$ for which $\hat{\mathfrak{O}}$ does not contains a primitive fourth root of 1. Suppose, on the other hand, that $\hat{\mathfrak{O}}$ contains a primitive fourth root i such that $\bar{i} = -i$. Then $\pi = \sqrt{\bar{p}}i$ satisfies $\pi^2 = -p$, $\bar{\pi} = \pi$, so that $\pi \in \mathfrak{O}$. Conversely, if $\mathfrak{O}$ contain an element π with $\pi^2 = -p$, then $\pi/\sqrt{\bar{p}} \in \hat{\mathfrak{O}}$ (§ 2, Prop. 3, Cor. 2) and $\pi/\sqrt{\bar{p}}$ is a primitive fourth root of 1. Thus we must study the mapping on the classes of maximal orders which have a *principal* two-sided prime ideal. The first step is to give explicitly a complete set of representatives for the conjugacy classes of such maximal orders.

Suppose first that the Legendre symbol $\left(\frac{2}{p}\right) = -1$, that is, $p \equiv 5 \pmod 8$. Then $(-2, -p)_p = (-2, -p)_\infty = -1$ and $(-2, -p)_q = 1$ for all

rational primes $q \neq p$. Hence there exist $\lambda, \mu \in \mathfrak{A}$ such that $\lambda^2 = -p$, $\mu^2 = -2$, $\lambda\mu = -\mu\lambda$. Then $(1 + \lambda)^{-1}\mu$ is a pure element of $\mathfrak{A}$ with norm $2(1 + p)^{-1}$, a unit of $\boldsymbol{Z}_2$. Hence there is a maximal order $\mathfrak{O}$ of $\mathfrak{A}$ such that $\{\lambda, \mu\} \subset \mathfrak{O}$, $(1 + \lambda)^{-1}\mu \in \mathfrak{O}_2^\times$. We put $F = \boldsymbol{Q}(\lambda)$, $\mathcal{O}_F$ = ring of integers of F, $\mathfrak{p}$ = the prime ideal of $\mathcal{O}_F$ such that $\mathfrak{p}^2 = (2)$. Then $\mathfrak{p}(\mathcal{O}_F)_\mathfrak{p} = (1 + \lambda)(\mathcal{O}_F)_\mathfrak{p}$, which gives

$$\mathfrak{p}\mathfrak{O}\mathfrak{p}^{-1} = \mu\mathfrak{O}\mu^{-1} . \tag{4}$$

More generally, if $\mathfrak{c}$ is an ideal of F, then

$$\mathfrak{c}\mathfrak{p}\mathfrak{O}\mathfrak{p}^{-1}\mathfrak{c}^{-1} = \mu\mathfrak{c}^*\mathfrak{O}(\mathfrak{c}^*)^{-1}\mu^{-1} . \tag{5}$$

This follows from the fact that $\mu\alpha\mu^{-1} = \alpha^*$ for all $\alpha \in F$. Let $\{\mathfrak{c}_1, \cdots, \mathfrak{c}_g\}$ be a complete set of representatives for the principal genus of F. Then $\{\mathfrak{c}_1, \cdots, \mathfrak{c}_g ; \mathfrak{c}_1\mathfrak{p}, \cdots, \mathfrak{c}_g\mathfrak{p}\}$ is a complete set of representatives for the ideal classes of F, and, by the Chevalley-Hasse-Noether Theorem ([2], p. 134), the set $\{\mathfrak{c}_j\mathfrak{O}\mathfrak{c}_j^{-1}, \mathfrak{c}_j\mathfrak{p}\mathfrak{O}(\mathfrak{c}_j\mathfrak{p})^{-1} : j = 1, \cdots, g\}$ represents all the conjugacy classes of maximal orders containing an element π with $\pi^2 = -p$. Since * preserves the principal genus of F, (5) implies that $\{\mathfrak{c}_j\mathfrak{O}\mathfrak{c}_j^{-1} : j = 1, \cdots, g\}$ already represents all such conjugacy classes.

Suppose now that $\left(\frac{2}{p}\right) = 1$. Choose a rational prime r such that $(r, -p)_p = (r, -p)_2 = -1$. Then $r \neq p$, 2 and $(-r, -p)_p = -1$, $(-r, -p)_2 = 1$. By the product formula, $(-r, -p)_r = (r, -p)_r = 1$. Hence we can find $\lambda, \mu \in \mathfrak{A}$ such that $\lambda^2 = -p$, $\mu^2 = -r$, $\lambda\mu = -\mu\lambda$. We put $F = \boldsymbol{Q}(\lambda)$ and define $\mathcal{O}_F, \mathfrak{p}$ as before. It follows from $(r, -p)_r = 1$ that $r = N(\mathfrak{r})$ for a prime ideal $\mathfrak{r}$ of F. Since $(r, -p)_p = -1$, $\mathfrak{r}$ is in the nonprincipal genus of F. Take $a, b \in \boldsymbol{Z}$ such that $\mathfrak{r}(\mathcal{O}_F)_\mathfrak{r} = (a + b\lambda)(\mathcal{O}_F)_\mathfrak{r}$. We can choose a maximal order $\mathfrak{O}$ of $\mathfrak{A}$ so that $\{\lambda, \mu\} \subset \mathfrak{O}$, $(a + b\lambda)^{-1}\mu \in \mathfrak{O}_\mathfrak{r}^\times$. It follows that

$$\mathfrak{c}\mathfrak{r}\mathfrak{O}\mathfrak{r}^{-1}\mathfrak{r}^{-1} = \mu\mathfrak{c}^*\mathfrak{O}(\mathfrak{c}^*)^{-1}\mu^{-1} \tag{6}$$

for any ideal $\mathfrak{c}$ of F. Reasoning exactly as before, with $\mathfrak{r}$ instead of $\mathfrak{p}$, we see that if $\{\mathfrak{c}_j : j = 1, \cdots, g\}$ is a complete set of representatives for the principal genus of F, then $\{\mathfrak{c}_j\mathfrak{O}\mathfrak{c}_j^{-1} : j = 1, \cdots, g\}$ represents all conjugacy classes of maximal orders containing an element π with $\pi^2 = -p$.

LEMMA 1. *Let $\mathfrak{O}$ be a maximal order of $\mathfrak{A}$ containing an element*

λ such that $\lambda^2 = -p$. Let $\mathfrak{c}$ be an ideal of $F = \boldsymbol{Q}(\lambda)$. If $\mathfrak{c}\mathfrak{O}\mathfrak{c}^{-1} = \mathfrak{O}$, then $\mathfrak{c}$ is principal.

Proof. If $\mathfrak{c}\mathfrak{O}\mathfrak{c}^{-1} = \mathfrak{O}$, then $\mathfrak{c}\mathfrak{O}$ is a two-sided ideal of $\mathfrak{O}$. Thus $\boldsymbol{c}\mathfrak{O} = a\lambda^e\mathfrak{O}$ for some $a \in \boldsymbol{Q}^\times$, $e \in \boldsymbol{Z}$. Since $p \equiv 1 \pmod 4$, $\{1, \lambda\}$ is a $\boldsymbol{Z}$-basis for $\mathcal{O}_F$. It follows that $\mathfrak{O} \cap F = \mathcal{O}_F$, $\mathfrak{O}_q^\times \cap F_q = (\mathcal{O}_F)_q^\times$, all rational q. Hence $\mathfrak{c} = a\lambda^e\mathcal{O}_F$.

LEMMA 2. *Let $\mathfrak{O}, \mathfrak{O}'$ be maximal orders of $\mathfrak{A}$, both containing an element λ with $\lambda^2 = -p$. Let $F = \boldsymbol{Q}(\lambda)$. If $\alpha\mathfrak{O}\alpha^{-1} = \mathfrak{O}'$, $\alpha \in \mathfrak{A}^\times$, then $\alpha = \beta\varepsilon$, where $\varepsilon \in \mathfrak{O}^\times$ and $\beta F\beta^{-1} = F$.*

Proof. By assumption, $\lambda, \alpha^{-1}\lambda\alpha \in \mathfrak{O}$. Then $\lambda, \alpha^{-1}\lambda\alpha$ must be generators for the two-sided prime ideal of $\mathfrak{O}$, which implies $\alpha^{-1}\lambda\alpha = \delta\lambda$, $\delta \in \mathfrak{O}^\times$. If $\delta = \pm 1$, we take $\beta = \alpha, \varepsilon = 1$. If $\delta \neq \pm 1$, then $\delta = \pm\zeta$, ζ a primitive third root of 1. There is only one maximal order (up to isomorphism) with a non-trivial unit group, satisfying the relation $\lambda\zeta = \zeta^{-1}\lambda$. Then $\alpha^{-1}\lambda\alpha = \pm\zeta\lambda = \pm\zeta^{-2}\lambda = \pm\zeta^{-1}\lambda\zeta$, and we take $\beta = \alpha\zeta^{-1}, \varepsilon = \zeta$.

PROPOSITION 7. *Let r be any rational prime such that $(r, -p)_p = (r, -p)_2 = -1$. Then we can find $\lambda, \mu \in \mathfrak{A}$ such that $\lambda^2 = -p, \mu^2 = -r$, $\lambda\mu = -\mu\lambda$. Let $F = \boldsymbol{Q}(\lambda)$. Then $r = N(\mathfrak{r})$ for a prime $\mathfrak{r}$ of F and we can find a maximal order $\mathfrak{O}_0$ of $\mathfrak{A}$ containing λ, μ such that $\mathfrak{r}\mathfrak{O}_0\mathfrak{r}^{-1} = \mu\mathfrak{O}_0\mu^{-1}$. For each such $\mathfrak{O}_0$ and any complete set of representatives $\{\mathfrak{c}_1, \cdots, \mathfrak{c}_g\}$ of the principal genus of F, the set $\{\mathfrak{c}_j\mathfrak{O}_0\mathfrak{c}_j^{-1} : j = 1, \cdots, g\}$ is a complete set of representatives for the conjugacy classes of maximal orders of $\mathfrak{A}$ containing an element π with $\pi^2 = -p$.*

Proof. We observe that we can take $r = 2, \mathfrak{r} = \mathfrak{p}$ if $\left(\frac{2}{p}\right) = -1$. Suppose $\alpha\mathfrak{c}_j\mathfrak{O}_0\mathfrak{c}_j^{-1}\alpha^{-1} = \mathfrak{c}_\ell\mathfrak{O}_0\mathfrak{c}_\ell^{-1}$ for some j, ℓ; $\alpha \in \mathfrak{A}^\times$. According to Lemma 2, we may assume $\alpha F\alpha^{-1} = F$. If $\alpha\lambda\alpha^{-1} = \lambda$, then $\alpha \in F^\times$ and we may apply Lemma 1 to deduce that $j = \ell$. If $\alpha\lambda\alpha^{-1} = -\lambda$, then $\alpha = \beta\mu, \beta \in F^\times$, and we have $\mathfrak{c}_\ell\mathfrak{O}_0\mathfrak{c}_\ell^{-1} = \beta\mu\mathfrak{c}_j\mathfrak{O}_0\mathfrak{c}_j^{-1}\mu^{-1}\beta^{-1} = \beta\mathfrak{c}_j^*\mathfrak{r}\mathfrak{O}_0\mathfrak{r}^{-1}(\mathfrak{c}_j^*)^{-1}\beta^{-1}$. Applying Lemma 1, we see that $\mathfrak{c}_\ell, \mathfrak{c}_j^*\mathfrak{r}$ are in the same class, which contradicts the fact that $\mathfrak{r}$ is not in the principal genus of F.

Proposition 7 enables us to determine the effect of the mapping $\{\mathfrak{O}\} \mapsto \{\hat{\mathfrak{O}}\}$ on the classes of $\mathfrak{O}$ which contain an element π with $\pi^2 = -p$. We take $\mathfrak{O}_0, \{\mathfrak{c}_j\}$ as in Proposition 7 with the stipulation that $\mathfrak{r} = \mathfrak{p}$ when

$\left(\frac{2}{p}\right) = -1$. Let $\Omega_0 = \hat{\mathfrak{O}}_0$. It is clear that $(\mathfrak{c}_j\mathfrak{O}_0\mathfrak{c}_j^{-1})\hat{} = \mathfrak{c}_j\Omega_0\mathfrak{c}_j^{-1}$. Let $i = \lambda/\sqrt{p}$, a primitive fourth root of 1. Then $i \in \mathfrak{c}_j\Omega_0\mathfrak{c}_j^{-1}$ for all j, and $\bar{i} = -i$. We note that

$$(1 + i)\Omega_0(1 + i)^{-1} = \mathfrak{p}\Omega_0\mathfrak{p}^{-1} \tag{7}$$

Suppose $\mathfrak{c}_j\Omega_0\mathfrak{c}_j^{-1}, \mathfrak{c}_\ell\Omega_0\mathfrak{c}_\ell^{-1}$ are conjugate. Then, using (7) and Proposition 6, we deduce that either (a) $j = \ell$ or (b) $\mathfrak{c}_j\mathfrak{O}_0\mathfrak{c}_j^{-1}, \mathfrak{c}_\ell\mathfrak{p}\mathfrak{O}_0\mathfrak{p}^{-1}\mathfrak{c}_\ell^{-1}$ are conjugate.

If $\left(\frac{2}{p}\right) = -1$, then (b) implies, by virtue of (5), that $\mathfrak{c}_j, \mathfrak{c}_\ell^*$ are equivalent, that is, $\mathfrak{c}_j, \mathfrak{c}_\ell^{-1}$ are equivalent. Conversely, if $\mathfrak{c}_j, \mathfrak{c}_\ell^{-1}$ are equivalent, then $\mathfrak{c}_j\Omega_0\mathfrak{c}_j^{-1}, \mathfrak{c}_\ell\Omega_0\mathfrak{c}_\ell^{-1}$ are conjugate. Hence the total number of conjugacy classes of symmetric maximal orders containing a primitive fourth root of 1 is the total number of elements in the principal genus of F upon identifying inverse elements, namely $(g + 1)/2$.

If $\left(\frac{2}{p}\right) = 1$, then $\mathfrak{p}$ is in the principal genus and the total number of conjugacy classes of symmetric maximal orders containing a primitive fourth root of 1 is the number of elements in the principal genus modulo they subgroup generated by the class of $\mathfrak{p}$, namely $g/2$.

We have completed the proof of

THEOREM. *The mapping* $\{\mathfrak{O}\} \mapsto \{\hat{\mathfrak{O}}\}$, *from conjugacy classes of maximal orders of* $\mathfrak{A}$ *to conjugacy classes of symmetric maximal orders of* $\mathfrak{A}_K$, *is one-to-one on the classes of* $\mathfrak{O}$ *which do not have a principal two-sided prime ideal. Let* $r, \mathfrak{O}_0, \{\mathfrak{c}_j\}$ *be chosen as in Proposition* 7, *with* $r = 2$ *if* $\left(\frac{2}{p}\right) = -1$. *Then*

(i) *If* $\left(\frac{2}{p}\right) = -1$, $(\mathfrak{c}_j\mathfrak{O}_0\mathfrak{c}_j^{-1})\hat{}$ *is conjugate to* $(\mathfrak{c}_\ell\mathfrak{O}_0\mathfrak{c}_\ell^{-1})\hat{} \Leftrightarrow \ell = j$ *or* $\mathfrak{c}_\ell \sim \mathfrak{c}_j^{-1}$.

(ii) *If* $\left(\frac{2}{p}\right) = 1$, $(\mathfrak{c}_j\mathfrak{O}_0\mathfrak{c}_j^{-1})\hat{}$ *is conjugate to* $(\mathfrak{c}_\ell\mathfrak{O}_0\mathfrak{c}_\ell^{-1})\hat{} \Leftrightarrow \ell = j$ *or* $\mathfrak{c}_\ell \sim \mathfrak{p}\mathfrak{c}_j$, *where* $\mathfrak{p}^2 = (2)$.

COROLLARY. *Let* $\hat{t}$ *denote the number of conjugacy classes of symmetric maximal orders of* $\mathfrak{A}_K$, *and* t *the number of conjugacy classes of maximal orders of* $\mathfrak{A}$. *Then*

$$\hat{t} = t - (g - a)/2 \tag{8}$$

where $g = h(\sqrt{-p})/2$ *and* $a = 0, 1$ *according as* $\left(\frac{2}{p}\right) = 1, -1$, *respectively* (*cf.* [5], § 12).

Remark. We note that the mapping $\{\mathfrak{O}\} \mapsto \{\hat{\mathfrak{O}}\}$ is two-to-one on the classes of $\mathfrak{O}$ having a principal two-sided prime ideal except if $\left(\frac{2}{p}\right) = -1$, $\mathfrak{O} = \mathfrak{O}_0$; in the latter case $\{\hat{\mathfrak{O}}_0\}$ uniquely determines $\{\mathfrak{O}_0\}$.

The algebras $\mathfrak{A}_K, \mathfrak{A}$ may be regarded as quadratic spaces over $K, \boldsymbol{Q}$, resp., with quadratic forms $N, N|\mathfrak{A}$, resp.; the proper similitudes are all the mappings of the form $\xi \mapsto \alpha\xi\beta$, where $\alpha, \beta \in \mathfrak{A}_K^{\times}$, $\alpha, \beta \in \mathfrak{A}^{\times}$, resp. We observe that two-sided normal ideals with the same norm are conjugate if and only if they are similar. Let $\mathfrak{O}$ be a maximal order of $\mathfrak{A}$ and $\mathfrak{P}$ its two-sided prime ideal. Then $\hat{\mathfrak{P}} = \sqrt{p}\hat{\mathfrak{O}}$, from which it follows that the mapping $\{\mathfrak{P}\} \mapsto \{\hat{\mathfrak{P}}\}$, from similitude classes of two-sided prime ideals of $\mathfrak{A}$ to similitude classes of two-sided symmetric prime ideals of $\mathfrak{A}_K$, is one-to-one on the classes of nonprincipal $\mathfrak{P}$ and satisfies the rest of the Theorem upon replacing $\mathfrak{O}_0$ by its two-sided prime ideal $\mathfrak{P}_0$. Noting that any two-sided normal ideal of $\mathfrak{A}$ is similar either to a maximal order $\mathfrak{O}$ or to a prime ideal $\mathfrak{P}$, we can combine the above two mappings and intersect with V to obtain a correspondence $\{\mathfrak{J}\} \mapsto \{\hat{\mathfrak{J}} \cap V\}$ from the set of similitude classes of two-sided normal ideals of $\mathfrak{A}$ into the set of similitude classes of lattices of V with reduced discriminant p or p^3. This correspondence is a function except on the classes of $\mathfrak{O}$ which are similar to their prime ideals, that is, $\mathfrak{O}$ which have *principal* $\mathfrak{P}$. For such $\mathfrak{O}$ we have $\{\mathfrak{O}\} \mapsto \{\hat{\mathfrak{O}} \cap V\}$ and $\{\mathfrak{O}\} \mapsto \{\hat{\mathfrak{P}} \cap V\}$. On the other hand, for each such $\mathfrak{O}$, excluding $\mathfrak{O}_0$ when $\left(\frac{2}{p}\right) = -1$, we have exactly one other class $\{\mathfrak{O}'\}$ such that $\{\mathfrak{O}'\} \mapsto \{\hat{\mathfrak{O}} \cap V\}, \{\mathfrak{O}'\} \mapsto \{\hat{\mathfrak{P}} \cap V\}$. Thus our correspondence is "two-to-two" on all such classes, except for $\{\mathfrak{O}_0\}$ when $\left(\frac{2}{p}\right) = -1$, where it is "one-to-two". On all other classes it is one-to-one. Furthermore, since the dual lattice of an order $\mathfrak{O}$ is $\mathfrak{P}^{-1}$, which is similar to $\mathfrak{P}$, our correspondence takes classes of dual lattices to classes of dual lattices. The total number of similitude classes $\{\mathfrak{J}\}$ is h, the ideal class number of $\mathfrak{A}$ ([6], p. 306, (11)), while the total number of similitude classes $\{\hat{\mathfrak{J}} \cap V\}$ is $2\hat{t}$. In particular, we have

$$(9)\qquad \begin{aligned} h &= 2\hat{t} && \text{if } \left(\frac{2}{p}\right) = 1 \\ &= 2\hat{t} - 1 && \text{if } \left(\frac{2}{p}\right) = -1 \end{aligned}$$

§ 5. Quadratic forms and theta series

We fix an ordered basis of V and call another ordered basis of V positively oriented if its tranformation matrix relative to the fixed basis has positive determinant. To each lattice L of V we can associate an integral quadratic form f_L by setting

$$(10)\qquad f_L(x_1, x_2, x_3, x_4) = N(L)^{-1}N\left(\sum_{i=1}^{4} x_i v_i\right)$$

for all $x_i \in \boldsymbol{Q}, i = 1, 2, 3, 4$, where $\{v_i\}$ is a positively oriented $\boldsymbol{Z}$-basis of L. The discriminant of f_L is the reduced discriminant of L. Different choices of positively oriented $\boldsymbol{Z}$-bases of L yield properly equivalent quadratic forms and in this way we obtain a one-to-one correspondence between proper similitude classes of lattices and proper equivalence classes of integral quadratic forms. If we let L vary over the integral lattices of reduced discriminant p, then the classes $\{f_L\}$ will vary over all the classes of integral positive definite quaternary forms of discriminant p ([8], § 6, Th. 3 (a)). In particular, the number of proper classes of such forms is equal to T, the number of conjugacy classes of maximal orders of $\mathfrak{A}_K$ ([8], § 4, Prop. 9 (a)).

If $\hat{L}$ is an order of $\mathfrak{A}_K$, then f_L represents 1. Conversely, suppose f_L represents 1. Let Ω be a symmetric maximal order of $\mathfrak{A}_K$. We may assume $\hat{L} = \tilde{\alpha}\Omega\bar{\tilde{\alpha}}^*$ for some $\tilde{\alpha} \in J_{\mathfrak{A}_K}$. Then $N(L) = n(N(\tilde{\alpha}))$, where $N(\tilde{\alpha})$ is the ideal of K such that $N(\tilde{\alpha})_\mathfrak{q} = N(\alpha_\mathfrak{q})\mathcal{O}_\mathfrak{q}$ for all finite primes $\mathfrak{q}$ of K. Since K has only one strict genus, we can find $\alpha \in \mathfrak{A}_K$ such that $n(N(\alpha)) = N(L)$. Let $M = \alpha^{-1}L(\overline{\alpha^{-1}})^*$. Then $N(M) = 1$ and M contains an element μ with $N(\mu) = 1$. It follows that $\hat{M} = \Omega_1\mu$, where Ω_1 is the left order of $\hat{M}$. Furthermore, $\mu = \lambda\bar{\lambda}^{-1}$ for some $\lambda \in \mathfrak{A}_K$ with $N(\lambda) \in \boldsymbol{Q}^\times$. Then $\hat{M} = \lambda\Omega_2\bar{\lambda}^{-1}$ with $\Omega_2 = \lambda^{-1}\Omega_1\lambda$. The symmetry of $\hat{M}$ implies that the maximal order Ω_2 is symmetric. We have shown

PROPOSITION 8. *Let L be a lattice of reduced discriminant p in V. Then f_L represents $1 \Leftrightarrow \hat{L}$ is similar to a symmetric maximal order of $\mathfrak{A}_K$.*

https://doi.org/10.1017/S0027763000024776 Published online by Cambridge University Press

COROLLARY. *The number of classes of integral quaternary forms of discriminant p which represent* 1 *is equal to* $\hat{t}$.

In the manner of (10), we can associate to each lattice $\mathfrak{L}$ of $\mathfrak{A}$ an integral quadratic form $f_{\mathfrak{L}}$. The class of $f_{\mathfrak{L}}$ depends only on the similitude class of $\mathfrak{L}$, and the mapping $\{\mathfrak{L}\} \mapsto \{f_{\mathfrak{L}}\}$ is one-to-one. Furthermore, as $\mathfrak{L}$ ranges over the normal ideals of $\mathfrak{A}$, $f_{\mathfrak{L}}$ will range over all integral positive definite quaternary forms of discriminant p^2. As before, $f_{\mathfrak{L}}$ represents $1 \Leftrightarrow \mathfrak{L}$ is a maximal order of $\mathfrak{A}$. It follows that the number of proper classes of integral positive definite quaternary forms of discriminant p^2 which represent 1 is equal to t. In [6], § 3 we gave the following formula for H, the number of proper similitude classes of normal ideals of $\mathfrak{A}$,

$$H = \frac{1}{2}\left(h^2 + \left(\frac{h(\sqrt{-p})}{2}\right)^2\right). \tag{11}$$

From [1] we have the following formula for t

$$t = \frac{1}{2}\left(h + \frac{h(\sqrt{-p})}{2}\right). \tag{12}$$

Let H_0 denote the number of *improper* classes of integral positive definite quaternary forms of discriminant p^2. Then $2H_0 - H$ is the number of classes $\{f_{\mathfrak{L}}\}$ which have an improper automorphism, and $f_{\mathfrak{L}}$ has an improper automorphism $\Leftrightarrow \mathfrak{L}$ is properly similar to $\mathfrak{L}^* \Leftrightarrow \mathfrak{L}$ is two-sided. It follows that $2H_0 - H = h$ or

$$H_0 = \frac{1}{2}(H + h). \tag{13}$$

We have just observed that the quadratic forms $f_{\mathfrak{L}}$ associated to the two-sided ideals of $\mathfrak{A}$ are characterized by the property that they have an *improper* automorphism. Kitaoka [5] gave an analogous characterization for quaternary forms of discriminant p which represent 1; in fact, he showed that $f_{\mathfrak{L}}$ represents $1 \Leftrightarrow o(L) \neq \{\pm 1\}$. (This stronger result is not true for square discriminant). Thus our correspondence has the property that it associates quaternary forms of discriminant p^2 with improper automorphisms to quaternary forms of discriminant p or p^3 with improper automorphisms. The significance of this for theta series is as follows.

Eichler [3] showed that the theta series associated to positive definite quaternary forms of discriminant p^2 span the space of all modular forms of *Haupttypus* $(-2, p, 1)$. However, the matter of providing an explicit basis of theta series has not yet been settled. The space of modular forms of type $(-2, p, 1)$ has dimension h, and Hecke ([4], p. 884) conjectured that the theta series coming from a fixed column of the Brandt matrices (of size $h \times h$) are a basis. He claims to have verified this for $p \leq 37$. In fact, it is false for $p = 37$. To see this, we first observe that all unit groups of maximal orders of $\mathfrak{A}$ are trivial since $\left(\frac{-1}{37}\right) = \left(\frac{-3}{37}\right) = 1$. Hence the Brandt matrices are all *symmetric* ([2], § 5, (22)). For $p = 37$ we have $t = 2, h = 3, H = 5, H_0 = 4$. If we arrange the improper classes $\{f_\varrho\}$ in a 3×3 symmetric matrix array in accordance with the Brandt matrices, we see that the diagonal has 2 distinct classes. The remaining 2 improper classes must then be placed in the 3 places above the diagonal. There is no way of doing this without having at least one column in the matrix array having 2 identical improper classes. It follows that at least one column will yield 2 *identical* theta series. Another way of showing this is to find normal ideals L, M with the property that they have the same left and right orders, are left inequivalent but right equivalent. This can be done whenever h/t is not an integral power of 2. We need only take $L, M = L\alpha$ as in [6], § 7, Remark 2. In this way we obtain an infinite number of counterexamples.

The question still remains as to which set of h classes should be chosen to provide h linearly independent theta series. A reasonable conjecture would be the classes $\{f_\mathfrak{z}\}$ coming from the two-sided normal ideals of $\mathfrak{A}$. Indeed, Hecke's own computations ([4]. p. 900–903) show this to be true for $p \leq 31$ ($p \equiv 3 \pmod 4$ is permissible in the case of Haupttypus). Kitaoka [5] has conjectured that the theta series coming from the quadratic forms of discriminant p representing 1, and their adjoints, form a basis for the modular forms of Nebentypus $\left(-2, p, \left(\frac{\ }{p}\right)\right)$. Both of these conjectures can be summarized in the statement that the theta series coming from quadratic forms which have an *improper* automorphism form a basis for the corresponding space of modular forms. The correspondence $\{\mathfrak{J}\} \mapsto \{\hat{\mathfrak{J}} \cap V\}$ induces a correspondence of the associated theta series. If the preceding conjectures are true, then this

correspondence has the virtue of associating a basis of modular forms of type $(-2, p, 1)$ to a basis of modular forms of type $\left(-2, p, \left(\frac{-}{p}\right)\right)$.

REFERENCES

[1] M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl, Jber. DMV **54** (1950), 24–41.
[2] M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren, J. Reine Angew. Math. **195** (1955), 127–151.
[3] ——, Über die Darstellbarkeit von Modulformen durch Thetareihen, J. Reine Angew. Math. **195** (1955), 156–171.
[4] E. Hecke, Mathematische Werke, Vandenhoeck & Ruprecht, Göttingen, 1970.
[5] Y. Kitaoka, Quaternary even positive definite quadratic forms of prime discriminant, Nagoya Math. J. **52** (1973), 147–161.
[6] P. Ponomarev, Class numbers of definite quaternary forms with square discriminant, J. No. Theory **6** (1974), 291–317.
[7] ——, Class numbers of definite quaternary forms with nonsquare discriminant, Bull. AMS **79** (1973), 594–598.
[8] ——, Arithmetic of quaternary quadratic forms, Acta Arithmetica **29** (1976), 1–48.

Department of Mathematics
The Ohio State University