Owing to (1) we do not lose control of the number of sign-changes after applying δ. On the other hand if we write the Mellin inversion formula for f in the form:

$$f(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \bar{f}(s)\, x^s\, ds, \qquad c > 0,$$

then the computation of $\delta(f)$ becomes very easy since owing to (2) we have

$$\delta(f)(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \bar{f}(s) \frac{x^s}{s}\, ds.$$

Let us notice that the factor $1/s$ improves the convergence of the above integral. This makes the whole analysis simpler especially if we repeat this procedure a number of times.

References

[1] G. H. Hardy and J. E. Littlewood, *Contribution to the theory of the Riemann Zeta function and the theory of the distribution of primes*, Acta Math. 41 (1918), pp. 119–196.

[2] A. E. Ingham, *A note on the distribution of primes*, Acta Arith. 1 (1936), pp. 201–211.

[3] J. Kaczorowski, *On sign-changes in the remainder-term in the prime-number formula, I*, ibid. 44 (1984), pp. 365–377.

[4] S. Knapowski, *On sign changes in the remainder term in the prime-number formula*, J. London Math. Soc. 36 (1961), pp. 451–560.

[5] — *On sign-changes of the difference* $\pi(x) - \mathrm{li}\, x$, Acta Arith. 7 (1962), pp. 107–120.

[6] S. Knapowski and P. Turán, *On the sign-changes of* $\pi(x) - \mathrm{li}\, x$, *I*, Coll. Math. Soc. J. Bolyai 13 (1974), pp. 153–165.

[7] — — *On sign-changes of* $\pi(x) - \mathrm{li}\, x$, *II*, Monatsh. für Math. 82 (1976), pp. 163–175.

[8] N. Levinson, *On the number of sign changes of* $\pi(x) - \mathrm{li}\, x$, Coll. Math. Soc. J. Bolyai 13 (1974), pp. 171–177.

[9] J. E. Littlewood, *Sur la distribution des nombres premiers*, C. R. Acad. Sci. Paris 158 (1914), pp. 1869–1872.

[10] J. Pintz, *Bemerkungen zur Arbeit von S. Knapowski und P. Turán*, Monatsh. für Math. 82 (1976), pp. 199–206.

[11] — *On the remainder term of the prime number formula, III, IV*, Studia Sci. Math. Hungar., 12 (1977), pp. 343–369; 13 (1978), pp. 29–42.

[12] G. Pólya, *Über das Vorzeichen des Restgliedes im Primzahlsatz*, Gött. Nachrichten, 1930, pp. 19–27, revised form in *Number Theory and Analysis*, Landau Memorial Volume, ed. by P. Turán, Plenum Press, 1969.

INSTITUTE OF MATHEMATICS OF THE ADAM MICKIEWICZ UNIVERSITY
Poznań, Poland

Received on 17. 10. 1983
and in revised form on 28. 2. 1984 (1378)

ACTA ARITHMETICA
XLV (1985)

Theta series of quaternary quadratic forms over Z and $Z[(1+\sqrt{p})/2]$

by

J. S. Hsia* and D. C. Hung (Columbus, Ohio)

In an earlier work [3] we mentioned that the arithmetic method introduced to prove linear independence of theta series should be applicable to other genera as well as to number fields provided the basic structural features of the quadratic forms in these genera could be overcome. In this paper, we give evidence to this remark. All quadratic forms shall be even positive definite and all genera will be uniquely determined by their discriminants. For convenience we denote by $G := G(n, D)$ the genus of n-ary quadratic forms over Z of discriminant D, and if G is replaced by $\mathfrak{G}$ the corresponding genus over the ring of integers in $Q(\sqrt{p})$, where p throughout shall be an arbitrarily fixed prime congruent to 1 (mod 4). Specifically, we investigate the linear independence of theta series of degrees one and two arising from the forms in $G(4, p^2)$ and $\mathfrak{G}(4, 1)$. We consider each genus separately even though both are closely linked to the genus $G(4, p)$ studied in [3].

A key ingredient of our arithmetic approach is to analyze for each form f its theta series $\theta_f^{(d)}$ (of degree d) modulo q-powers where q is a prime factor of the order of the unit group $O(f)$ of f. For this, we need a rather detailed, albeit technical, knowledge of the arithmetic structures of f and $O(f)$ which we shall determine. However, several new phenomena arise; e.g. (1) the symmetries of f – in the $G(4, p^2)$ case – are not controlled by the minimal vectors, (2) the unit groups $O(f)$ – in the $\mathfrak{G}(4, 1)$ case – are not generated by ± symmetries of f, (3) the "glueing" construction process of a form $\tilde{f} \in \mathfrak{G}(4,1)$ from an $f \in G(4, p)$ may introduce new minimal vectors. The latter, in the language of quaternion algebras, means that if $\mathfrak{A}$ is the rational quaternion algebra with discriminant p^2 and $\tilde{\mathfrak{A}} = \mathfrak{A} \otimes Q(\sqrt{p})$ then the

* Research supported by N.S.F. Grant MCS 82-02065.

symmetric maximal orders of $\tilde{\mathfrak{A}}$ corresponding to the maximal orders of $\mathfrak{A}$ may have different roots-system types (when viewing the orders as quadratic forms with respect to their reduced norms). On the other hand, it is somewhat surprising that the roots-system type of *any* maximal order of $\tilde{\mathfrak{A}}$ must already belong to a roots-system type of some symmetric maximal order (Prop. II.2.4). One notes that the ratio "symmetric" type number of $\tilde{\mathfrak{A}}$/ /type number of $\tilde{\mathfrak{A}}$ tends to zero as $p \to \infty$.

Instead of quadratic forms we adopt the geometric language of (quadratic) lattices, and the presentation goes as follows. After a systematic study of the arithmetic structures of lattices in the genera $G(4, p^2)$ and $\mathfrak{G}(4, 1)$ we categorize the lattices having *improper* automorphisms according to their "types" or roots-system types. Next, we examine their unit groups, which in the $\mathfrak{G}(4, 1)$ case is treated partially via the theory of quaternion algebras over $Q(\sqrt{p})$. Finally, we study theta series along the lines of [3]. In particular, we prove that the theta series of degree two for lattices in $G(4, p^2)$ and $\mathfrak{G}(4, 1)$ having improper automorphisms are linearly independent (Thms I.4.4 and II.3.3).

I. Even positive definite quaternary lattices of discriminant p^2

I.1. Basic structures. Any unexplained notation or terminology may be found in [11]. We fix a prime $p \equiv 1 \pmod 4$. Let L be an even positive definite quaternary $\boldsymbol{Z}$-lattice of discriminant p^2. Then L is maximal and 2-adically L_2 is hyperbolic. One computes easily that the Hasse symbols satisfy: $S_2(QL) = S_p(QL) = -1$ and $S_r(QL) = 1$ at all $r \neq 2, p$. Hence, there is just one genus $G(4, p^2)$ of such quaternary lattices. By a minimal vector we mean one of quadratic length 2. Suppose $L \in G(4, p^2)$ contains a minimal vector e, then it is clear that $K := \langle e\rangle^{\perp}$ is a lattice in $G(3, 2p^2)$ and also maximal.

I.1.1. Proposition. *Let $K \in G(3, 2p^2)$. Then there is a unique $L \in G(4, p^2)$ containing $\boldsymbol{Z}e \perp K$, where e is a minimal vector.*

Proof. It suffices to show that there is a unique even unimodular 2-adic lattice containing $\boldsymbol{Z}_2 e \perp K_2$. By local theory, K_2 is isometric to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp$ $\perp \langle -2p^2\rangle$, which we suppose is adapted to a basis $\{x, y, z\}$. Since $\boldsymbol{Z}_2 e \perp \boldsymbol{Z}_2 z$ is isotropic there is a unimodular lattice $N = \boldsymbol{Z}_2 u + \boldsymbol{Z}_2 v$ containing it and such that $Q(u) = Q(v) = 0$, $B(u, v) = 1$. If M is any 2-adic unimodular lattice also containing $\boldsymbol{Z}_2 e \perp \boldsymbol{Z}_2 z$ then $M = \boldsymbol{Z}_2 e + \boldsymbol{Z}_2(au + bv)$, $a, b \in \boldsymbol{Q}_2$. Since M is even integral, a, b lie in $\boldsymbol{Z}_2$, i.e. $M = N$.

I.1.2. Lemma. *Let $K \in G(3, 2p^2)$. Then $2t^2 \notin Q(K)$ for any $t > 0$, $(t, p) = 1$. In particular, K has no minimal vector.*

Proof. Suppose there is a $w \in K$ with $Q(w) = 2t^2$; then at the prime spot p we have $K_p = \boldsymbol{Z}_p w \perp N_p$ where $N = \langle w\rangle^{\perp}$. Since dN_p is a square and $p \equiv 1 \pmod 4$, N_p is isotropic. Hence, K_p is not maximal which gives the contradiction.

I.1.3. Corollary. *Let $K \in G(3, 2p^2)$ and L the unique lattice in $G(4, p^2)$ containing $\boldsymbol{Z}e \perp K$, then any minimal vector u in L is mapped onto $\pm e$ by some symmetry of L.*

Proof. Lemma I.1.2 implies that $u \notin K$. Hence, $B(e, u) \neq 0$. We may suppose $u \neq \pm e$. $Q(e \pm u) > 0$ implies that $B(e, u) = \pm 1$, whence follows that either S_{u-e} or S_{u+e} maps u onto $\pm e$.

I.1.4. Remarks. (i) It follows from Corollary I.1.3 that if K_1, K_2 are two lattices in $G(3, 2p^2)$ and L_1, L_2 the corresponding lattices in $G(4, p^2)$ then $L_1 \cong L_2$ implies $K_1 \cong K_2$. Therefore, the map $K \mapsto L \supset \boldsymbol{Z}e \perp K$ induces a one-to-one correspondence between the classes of lattices in $G(3, 2p^2)$ and those classes in $G(4, p^2)$ which represent 2.

(ii) Since L cannot contain two orthogonal minimal vectors by Lemma I.1.2, the only possible roots-systems for lattices in $G(4, p^2)$ are $\emptyset$, A_1, A_2.

(iii) In an analogous manner, given $K \in G(3, 2p^2)$ there is a unique sublattice $\bar{K}$ of index p and the norm $n(\bar{K}_p) = p\boldsymbol{Z}_p$. If $\bar{K}$ is scaled by a factor p^{-1} one obtains a lattice $K' \in G(3, 2p)$. The mapping $K \mapsto K'$ induces a one-to-one correspondence between classes in $G(3, 2p^2)$ and classes in $G(3, 2p)$. See [5] for more details.

I.1.5. Proposition. *Let $K \in G(3, 2p^2)$ and L the unique lattice in $G(4, p^2)$ containing $\boldsymbol{Z}e \perp K$. Let K' be the lattice in $G(3, 2p)$ uniquely associated with K according to Remark* I.1.4 (iii). *Then L has a roots-system of type A_2 if and only if K' does.*

Proof. We first observe that L has roots-system type A_2 if and only if K has a vector x satisfying $Q(x) = 6$, $B(x, K) \subseteq 2\boldsymbol{Z}$. For, let L be of type A_2 then L has a basis $\{e, f, u, v\}$ such that $Q(e) = Q(f) = 2$, $B(e, f) = 1$, $B(e, u) = B(e, v) = 0$ by Minkowski reduction. Take $x = e - 2f$. Conversely, if such a vector $x \in K$ exists then $L = \boldsymbol{Z}e \perp K + \boldsymbol{Z}\left(\frac{e+x}{2}\right)$ which shows that L has type A_2.

Suppose now K' has type A_2. Then, $K' \supset A_2 \perp \langle 6p\rangle$ and $K \supset K'^p$ $\supset \begin{pmatrix} 2p & p \\ p & 2p \end{pmatrix} \perp \langle 6p^2\rangle$. Since $Q_p K_p$ is anisotropic with $K_p \cong \langle -2\Delta\rangle \perp$ $\perp \langle p\rangle \perp \langle -\Delta p\rangle$ the vector of length $6p^2$ is imprimitive, say, px. (Here Δ denotes a non-square p-adic unit as in [11].) Hence, $x \in K$ has $Q(x) = 6$, $B(x, K) \subseteq 2\boldsymbol{Z}$ so that L has type A_2. Conversely, if L has type A_2 then such a vector x in K exists. As x splits K_2, $K \supset \boldsymbol{Z}x \perp J$ for some binary J of discriminant $3p^2$. Now J_p is p-modular and anisotropic; hence, $Z(px) \perp J$ is contained in a sublattice of index p in K. Therefore, $Z(px) \perp J \subset K'^p$ and $J^{p^{-1}} \subset K'$. But, there is only one even positive binary lattice of discriminant 3, implying $J^{p^{-1}} \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and so K' has type A_2.

I.1.6. Lemma. *Let $L \in G(4, p^2)$. Suppose that L contains vectors e and u such that $Q(e) = 2$ and $Q(u) = 2p$, then $e \perp u$.*

Proof. Let T be the orthogonal complement of u in L. If $e \notin T$ then $e \notin \langle u \rangle \perp T$. Write $e = \frac{1}{2}(au+w)$ with $a \neq 0$, $w \in T$. But, $Q(e) = \frac{1}{4}(2pa^2+Q(w)) > 2$, a contradiction.

I.2. Classification by types. The usual roots-systems are concerned with minimal vectors. In the case of $G(4, p^2)$ symmetries of a lattice may also be defined from vectors of length $2p$. We introduce here a classification of lattices via "types" which takes into account both the minimal vectors and the vectors of length $2p$. We reserve the symbols K, L, K' for those lattices stated in the hypothesis of Proposition I.1.5.

I.2.1. Definition. We say L has *type* A_1^0 if the roots-system of L is A_1 while the roots-system of K' is $\emptyset$. L has *type* A_1^1 if the roots-systems of L and K' are both A_1. L has *type* A_2^2 if it has roots-system A_2.

I.2.2. Remark. Lemma I.1.6 implies the number $a_L(2p)$ of representations of $2p$ by L is the same as those $a_K(2p)$ by K. But, $a_K(2p) = a_{K'}(2)$ by Remark I.1.4 (iii). Hence $a_L(2p) = 0$, 2, or 6 as L has types A_1^0, A_1^1, or A_2^2. Combining Remarks I.1.4, the above notations, and the structural results for the genera $G(3, 2p)$ and $G(4, p)$ in [6] one deduces the following: the mapping $L \mapsto K \mapsto K' \mapsto L'$ (the last stage is Kitaoka's construction of $L' \in G(4, p)$ from $K' \in G(3, 2p)$ described in [6]) induces a correspondence between the classes of lattices in $G(4, p^2)$ which represent 2 and those classes in $G(4, p)$ that represent 2. This correspondence is one-to-one on the classes of L of type A_1^0. It is two-to-one on the classes of L of type A_1^1 or A_2^2 with the exceptional case when K' contains an ambiguous nice binary lattice (in the sense of [6]), which occurs only when $p \equiv 5 \pmod 8$. This correspondence has been proved in [12] via the arithmetic of quaternion algebra while the above sketch is wholly lattice-theoretic. More specifically, using the classification by types and the roots-systems of lattices $L' \in G(4, p)$ described in [3], we have:

Type of L		*Roots-system of L′*
A_1^0	$\xleftrightarrow{\text{1-1}}$	$\begin{cases} A_1 \\ A_2 \end{cases}$
A_1^1	$\xleftrightarrow{\text{2-1}}$	$A_1 \oplus A_1$
A_1^1	$\xleftrightarrow{\text{1-1}}$	A_3 when $p \equiv 5 \pmod 8$
A_1^1, A_2^2	$\xleftrightarrow{\text{2-1}}$	$A_1 \oplus A_2$ when $p \equiv 2 \pmod 3$

Let $L \in G(4, p^2)$. Recall that the *reciprocal* $\tilde{L}$ of L is the dual $L^\#$ scaled by the factor dL/Ω, where Ω is the greatest common divisor of the entries in the adjoint matrix of the matrix of L. Here $\Omega = p$ and $\tilde{L} \in \mathfrak{G}(4, p^2)$. There is a classical duality between representations by a form and those by its primitive adjoint form (i.e., the reciprocal) that already appeared in the works of Gauss, Smith, Minkowski and others. In terms of lattices it asserts the following:

I.2.3. Proposition. *For any lattice L of discriminant D there is a one-to-one correspondence between the primitive sublattices of L of codimension one and discriminant Δ and the pairs of primitive vectors in the reciprocal lattice $\tilde{L}$ of length Δ/Ω.*

I.2.4. Lemma. *Let $L \in G(4, p^2)$. Then L represents 2 if and only if $\tilde{L}$ represents $2p$. Furthermore, we have $a_L(2) = a_{\tilde{L}}(2p)$.*

Proof. If e is a minimal vector of L then $K = \langle e \rangle^\perp$ is a primitive sublattice of discriminant $2p^2$ and the classical duality implies that $\tilde{L}$ represents $2p^2/p = 2p$. Conversely, if $u \in \tilde{L}$ with $Q(u) = 2p$, it suffices to show that $\langle u \rangle^\perp$ has discriminant $2p$ (since $\tilde{\tilde{L}} \cong L$). To see this, localize at the primes 2 and p. One easily checks that $d(\langle u \rangle_2^\perp) \in 2Z_2^\times$ and $d(\langle u \rangle_p^\perp) \in pZ_p^\times$ by noting that $\tilde{L}_p \cong \langle 1 \rangle \perp \langle -\Delta \rangle \perp \langle p \rangle \perp \langle -\Delta p \rangle$.

To prove the last statement, we observe that if K is any ternary sublattice of L of discriminant $2p^2$, then there is a minimal vector e in L such that $e \perp K$. This is clear, since locally at p, we have $K_p \cong \langle -2\Delta \rangle \perp \langle p \rangle \perp \perp \langle -\Delta p \rangle$; hence, the p-modular component of K_p splits L_p. Therefore, if e is a primitive vector in the orthogonal complement of K, then $Q(e) \in Z_p^\times$. Thus, e is a minimal vector. Now, the number of (primitive) ternary sublattices of L of discriminant $2p^2$ equals exactly the number of pairs $\{\pm e\}$ of minimal vectors in L. On the other hand, this number also equals the number of pairs $\{\pm u\}$ of vectors in $\tilde{L}$ with $Q(u) = 2p$ by the classical duality.

I.2.5. Definition. Let $L \in G(4, p^2)$. We say that L has *type* A_0^1 if $a_L(2) = 0$ but $a_L(2p) = 2$. L has *type* $\emptyset$ if L represents neither 2 nor $2p$.

I.2.6. Remark. It follows from Lemma I.2.4 that L has type A_1^0, A_1^1, or A_2^2 if and only if $\tilde{L}$ has type A_0^1, A_1^1, or A_2^2, respectively. In the last two cases, we have $\tilde{L} \cong L$, for if L has type A_2^2, then $a_L(2p) = 6$ so that $a_{\tilde{L}}(2) = 6$. This means that $\tilde{L}$ has type A_2^2, but there is only one lattice class of type A_2^2 in $G(4, p^2)$. Hence, $\tilde{L} \cong L$. Similarly, for the case L of type A_1^1. Summarizing, we have partitioned the classes in $G(4, p^2)$ according to their types: $\emptyset$, A_1^0, A_0^1, A_1^1, A_2^2.

I.3. Unit groups. Let $G'(4, p^2)$ denote those lattices in $G(4, p^2)$ which represent either 2 or $2p$. We need a result from [5] which asserts that if $K \in G(3, 2p^2)$ and K' the associated lattice in $G(3, 2p)$ then $O(K) = O(K')$. Since $O(K')$ is generated by symmetries and ± 1 by [6], so does $O(K)$. In particular, $|O(K)| = 2, 4, 8, 12$ as $a_K(2p) = 0, 2, 4, 6$ respectively. Suppose first that L has type A_1^0 and e is minimal vector of L and $K = \langle e\rangle^{\perp}$. A automorphism φ of L maps e onto $\pm e$ and acts trivially on K. Thus, $O(L$ generated by S_e and ± 1. The same applies to L having type A_0^1 since $\tilde{L}$ l type A_1^0 and $O(L) \cong O(\tilde{L})$. Next, let L have type A_1^1 with minimal vecto and a vector u with $Q(u) = 2p$. Then $|O(K)| = 4$ and $O(L)$ is generated by S_u and ± 1. If L has type A_2^2 then $L \supset (Ze_1 + Ze_2) \perp (Zu_1 + Zu_2)$, wh $Ze_1 + Ze_2 \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $Zu_1 + Zu_2 \cong \begin{pmatrix} 2p & p \\ p & 2p \end{pmatrix}$. It is easy to see tl $O(L)$ is generated by S_{e_1}, S_{e_2}, $S_{e_1-e_2}$, S_{u_1}, S_{u_2}, $S_{u_1-u_2}$, and ± 1. Finally L has type $\emptyset$ then $O(L)$ is trivial. This can be seen using the main c respondence between lattices in $G(4, p^2)$ and $G(4, p)$. Summarizing, we ha

I.3.1. Proposition. *Let $L \in G(4, p^2)$. Then $O(L)$ is generated by sy metries of L and ± 1. We have $O(L) \cong C_2$, $C_2 \times C_2$, $C_2 \times C_2 \times C_2$, or $(S_3 \times S_3$ $\times C_2$ as the type of L is $\emptyset$, A_1^0 or A_0^1, A_1^1, or A_2^2 respectively. $G'(4,$ consists of precisely those lattices in $G(4, p^2)$ which have improper au morphisms.*

I.4. Theta series. The main objective of this section is to prove in ful linear independence result for theta series of degree two, and to state soı results about degree one theta series. The method is the same as tl introduced in [3].

Let $L_1, \ldots, L_t$ be a full set of non-isometric lattices in $G'(4, p^2)$. F each i, choose a binary sublattice J_i in L_i according to its type:

(i) L_i type A_2^2. Let J_i be the unique sublattice of L_i which is generat by its roots-system $A_2 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

(ii) L_i type A_0^1. Let $u_i \in L_i$ such that $Q(u_i) = 2p$ and $K_i' = \langle u_i\rangle^{\perp}$. Sir $K_i' \in G(3, 2p)$ we can choose $J_i \subset K_i'$ of discriminant q_i for some prime $q_i \neq$ or p.

(iii) L_i type A_1^0 or A_1^1. Let e_i be a minimal vector and $K_i = \langle e_i\rangle^{\perp}$. As [3], we can choose $J_i \subset K_i$ of discriminant pq_i, where q_i is a prime $\neq 2$ oı by Lemma 1.6, [4]. Furthermore, we can do so that J_i contains a vector length $2p$ if L_i has type A_1^1.

I.4.1. Lemma. *Suppose L_i has type A_0^1 and $\varphi\colon J_i \to L_j$ is an isometı embedding of J_i into L_j. Then we have*

(1) $\varphi(J_i)$ is not orthogonal to any minimal vector in L_j;

(2) If $\varphi(J_i) \perp u$ for some vector u of length $2p$, then $L_i \cong L_j$; hence, $i =$

Proof. (1) If $\varphi(J_i) \perp e$ for some minimal vector $e \in L_j$ then $(L_j$ $= \varphi(J_i) \perp Z_p e \perp Z_p w$ for some w with $Q(w) \in p^2 Z_p^{\times}$. This is impossit since $(L_j)_p$ is maximal.

(2) It suffices to show that $Zu_i \perp J_i$ is a characteristic sublattice of L_i the sense of [7]. But this is clear since J_i is characteristic in $K_i' = \langle u_i\rangle^{\perp}$

I.4.2. Lemma. *Let L_i be of type A_1^0 and $\varphi\colon J_i \to L_j$ an isometric embedding of J_i into L_j. If $\varphi(J_i) \perp e$ for some minimal vector $e \in L_j$ then $L_i \cong L_j$; hence, $i = j$.*

I.4.3. Lemma. *Suppose L_i has type A_1^1 and $\varphi\colon J_i \to L_j$ is an isometric embedding of J_i into L_j. Then we have*

(1) $\varphi(J_i)$ is not orthogonal to any vector u of length $2p$ in L_j;

(2) If $\varphi(J_i) \perp e$ for some minimal vector $e \in L_j$ then $L_i \cong L_j$; hence, $i = j$.

The proofs of these two lemmas are analogous.

I.4.4. Theorem. *The theta series $\theta_L^{(2)}(Z)$ of degree two for lattices L coming from the classes of even positive definite quaternary lattices of discriminant p^2 having an improper automorphism group are linearly independent.*

Proof. Let L_i and J_i be as before, $i = 1, \ldots, t$. Let a_{ij} be the number of isometric embeddings of J_i into L_j. Let 2^{n_j} be the exact power of 2 in $|O(L_j)|$. We want to measure the size of an $O(L_j)$-orbit. Consider the following cases:

Case (i). L_i has type A_0^1, then no symmetries of $O(L_j)$ can fix $\varphi(J_i)$ by Lemma I.4.1, unless $i = j$ and φ is in the orbit of the inclusion map, where the stabilizer H_φ of φ is $\{1, S_{u_i}\}$. Hence,

$$\frac{|O(L_j)|}{|H_\varphi|} = \begin{cases} 2^{n_j - 1} & \text{if } i = j \text{ and } \varphi \in \text{orbit of inclusion}, \\ 2^{n_j} & \text{otherwise}. \end{cases}$$

By Proposition I.3.1 we have

$$a_{ij} = \sum_{\substack{\varphi \text{in} \\ \text{distinct orbit}}} \frac{|O(L_j)|}{|H_\varphi|} \equiv 0 (\text{mod } 2^2) \quad \text{if} \quad i \neq j,$$

$$a_{ii} = \frac{|O(L_j)|}{|H_\alpha|} + \sum_{\varphi \notin \text{orbit}\,\alpha} \frac{|O(L_j)|}{|H_\varphi|} \equiv 2 (\text{mod } 2^2)$$

but, $a_{ii} \not\equiv 0 (\text{mod } 2^2)$. Here α is the inclusion map.

Case (ii). L_i has type A_1^0. If L_j has type A_2^2 or A_1^1 then by Lemma I.4.2, no symmetries of the kind S_e for some minimal vector e can fix $\varphi(J_i)$, and at most one symmetry S_u, $Q(u) = 2p$, can fix $\varphi(J_i)$. Similarly for L_j of type A_0^1. If L_j has type A_1^0, then H_φ is trivial, except when $i = j$ and φ lies in the inclusion orbit, in which case $H_\varphi = \{1, S_{e_i}\}$. Thus,

$$\frac{|O(L_j)|}{|H_\varphi|} = \begin{cases} 2^{n_j} \quad \text{or} \quad 2^{n_j - 1} & \text{if} \quad L_j \text{ has type } A_2^2, A_1^1, \text{ or } A_0^1, \\ 2^{n_j} & \text{if} \quad L_j \text{ has type } A_1^0, i \neq j, \text{ or } i = j, \text{ but} \\ & \qquad \varphi \notin \text{inclusion orbit}, \\ 2^{n_j - 1} & \text{if} \quad i = j \text{ and } \varphi \in \text{inclusion orbit}. \end{cases}$$

Hence,

$$a_{ij}\equiv 0\ (\mathrm{mod}\ 2^2)\quad \text{for}\quad i\neq j \text{ and } L_j \text{ of type } A_2^2,\ A_1^1,\ A_1^0;$$

$$a_{ij}\equiv 0 \text{ or } 2\ (\mathrm{mod}\ 2^2)\quad \text{for}\quad L_j \text{ of type } A_0^1;$$

$$a_{ii}\equiv 0\ (\mathrm{mod}\ 2),\quad \text{but}\quad a_{ii}\not\equiv 0\ (\mathrm{mod}\ 2^2).$$

Case (iii). L_i has type A_1^1. Lemma I.4.3 gives this time

$$\frac{|O(L_j)|}{|H_\varphi|}=\begin{cases}2^{n_j-1} & \text{if}\quad i=j,\ \varphi\in\text{inclusion orbit},\\ 2^{n_j} & \text{otherwise.}\end{cases}$$

Thus,

$$a_{ij}\equiv 0\ (\mathrm{mod}\ 2^3)\quad \text{for}\quad L_j \text{ of type } A_2^2 \text{ or } A_1^1,\ i\neq j;$$

$$a_{ij}\equiv 0\ (\mathrm{mod}\ 2^2)\quad \text{for}\quad L_j \text{ of type } A_1^0 \text{ or } A_0^1;$$

$$a_{ii}\equiv 0\ (\mathrm{mod}\ 2^2),\quad \text{but}\quad a_{ii}\not\equiv 0\ (\mathrm{mod}\ 2^3).$$

Case (iv). L_i has type A_2^2, then $a_{ij}=0$ if $i\neq j$, but $a_{ii}=12$, since $J_i\cong\begin{pmatrix}2&1\\1&2\end{pmatrix}$.

Suppose now there is a non-trivial linear relation

$$\sum_j c_j\,\theta_{L_j}^{(2)}(Z)=0,$$

where we may assume the c_j's are relatively prime integers. Evaluating at each J_i, we obtain $\sum_j c_j a_{ij}=0$.

(1) If L_i has type A_2^2, then $c_i=0$.

(2) If L_i has type A_0^1, then $\sum_j c_j a_{ij}\equiv 0\ (\mathrm{mod}\ 2^2)$ yields $c_i\equiv 0\ (\mathrm{mod}\ 2)$.

(3) If L_i has type A_1^0, then $\sum_j c_j a_{ij}\equiv 0\ (\mathrm{mod}\ 2^2)$ also yields $c_i\equiv 0\ (\mathrm{mod}\ 2)$.

(4) If L_i has type A_1^1, then $\sum_j c_j a_{ij}\equiv 0\ (\mathrm{mod}\ 2^3)$ yields $c_i\equiv 0\ (\mathrm{mod}\ 2)$.

This gives a contradiction, and our proof is completed.

I.4.5. Corollary. *Let L_1 and L_2 be two lattices in $G'(4, p^2)$. Then $L_1\cong L_2$ if and only if $\theta_{L_1}^{(2)}(Z)\equiv\theta_{L_2}^{(2)}(Z)\ (\mathrm{mod}\ 8)$.*

Proof. Looking at the representations of $\begin{pmatrix}2&0\\0&0\end{pmatrix}$ and $\begin{pmatrix}2p&0\\0&0\end{pmatrix}$ one sees that the theta series of degree two modulo 8 classifies lattices in $G'(4, p^2)$ up to type. Suppose L_1 and L_2 have the same type, then we choose J_1 in L_1 according to the proof of the theorem. We have $a_{L_1}(J_1)\equiv 2$ or $6\ (\mathrm{mod}\ 8)$, but $a_{L_2}(J_1)\equiv 0$ or $4\ (\mathrm{mod}\ 8)$ if L_1 and L_2 have type A_0^1 or A_1^0. And if both lattices are of type A_1^1 then $a_{L_1}(J_1)\equiv 4\ (\mathrm{mod}\ 8)$ while $a_{L_2}(J_1)\equiv 0\ (\mathrm{mod}\ 8)$. This finishes the proof.

We now briefly discuss theta series od degree one. Recall that the classes of lattices in $G'(4, p)$ with roots-systems containing $A_1\oplus A_1$ have linearly independent ordinary theta series. The counterpart in $G'(4, p^2)$ is slightly different. Each $L\in G'(4, p)$ with roots-system containing $A_1\oplus A_1$ corresponds to *two* lattices in $G'(4, p^2)$, according to Remark I.2.2, of type A_1^1 or A_2^2. Let L be any such lattice with minimal vector e and a vector u with $Q(u)=2p$, and $e\perp u$. Then $L\supset Ze\perp Zu\perp M$ for some nice binary lattice M. Choose a vector $v\in M$ such that $Q(v)=2q$, q a prime (via Lemma 1.6, [4]). Let Zf be the orthogonal complement of v in M. Then $Q(f)=2pq$ and one can prove the following: There exist exactly four lattices in $G(4, p^2)$ containing $Ze\perp Zu\perp Zv\perp Zf$ which are partitioned into two disjoint sets of isometric lattices with each set containing two lattices. Lattices from one set are not isometric to those from the other, except in the case when an even maximal lattice containing $Zv\perp Zf$ is ambiguous. Therefore, the quaternary lattice $\langle 2\rangle\perp\langle 2p\rangle\perp\langle 2q\rangle\perp\langle 2pq\rangle$ classifies the lattices of type A_1^1 or A_2^2 up to "twins". If we let G_0 be a subset of $G'(4, p^2)$ consisting of exactly one member from each twin set, then the following holds:

I.4.6. Theorem. *The theta series of degree one for lattices coming from distinct classes of G_0 are linearly independent.*

I.4.7. Remark. Similar to Corollary I.4.5 one can show that lattices in G_0 are classified by their theta series of degree one modulo 4. The number of classes in G_0 is essentially $h(Q(\sqrt{-p}))/4$.

II. Even positive definite quaternary unimodular lattices over $Q(\sqrt{p})$

Fix a prime $p\equiv 1\ (\mathrm{mod}\ 4)$. Let $F=Q(\sqrt{p})$, $\mathfrak{O}=Z\left[\frac{1+\sqrt{p}}{2}\right]$ its ring of integers, $\mathfrak{O}^\times$ the group of units of $\mathfrak{O}$. Let V be a positive definite quaternary F-space of discriminant 1. We assume V admits a lattice L over $\mathfrak{O}$ such that $L_\mathfrak{p}$ is unimodular at every finite prime $\mathfrak{p}$ of F and $Q(x)\in 2\mathfrak{O}$ for any $x\in L$. One easily sees that $V_\mathfrak{p}$ is hyperbolic at each $\mathfrak{p}<\infty$. Let $\mathfrak{A}$ denote the quaternion algebra of discriminant p^2 over Q and $\tilde{\mathfrak{A}}=\mathfrak{A}\otimes F$, then $V\cong\tilde{\mathfrak{A}}$ with the quadratic map on $\tilde{\mathfrak{A}}$ being $2N(-)$, N the reduced norm. We assume throughout this chapter that $V=\tilde{\mathfrak{A}}$ and $Q(x)=2N(x)$. Unexplained notations and basic facts about quaternion algebras and their arithmetic may be found in [13], [14]. These even unimodular lattices L on V are free (see [8]) and constitute a single genus denoted by $\mathfrak{G}(4, 1)$. We study the arithmetic structures of the lattices in $\mathfrak{G}(4, 1)$, the relations of some of them with the genus $G(4, p)$; we characterize the roots-systems, calculate the unit groups, and finally consider the theta series of degrees one and two.

II.1. Basic structures. Suppose R is a maximal order of $\tilde{\mathfrak{A}}$. Then $R_{\mathfrak{p}} = M_2(\mathfrak{O}_{\mathfrak{p}})$ at every finite prime $\mathfrak{p}$. Hence, $R_{\mathfrak{p}}$ is unimodular at every $\mathfrak{p}$ and $R \in \mathfrak{G}(4, 1)$. For any lattice $L \in \mathfrak{G}(4, 1)$, and any maximal order R there exist $\tilde{a} = (a_{\mathfrak{p}})$, $\tilde{b} = (b_{\mathfrak{p}})$ in the idèle group $J_{\tilde{\mathfrak{A}}}$ such that $N(a_{\mathfrak{p}} b_{\mathfrak{p}}) = 1$ and $L = \tilde{a} R \tilde{b}$. In particular, L is a normal ideal.

II.1.1. Proposition. *Let $L \in \mathfrak{G}(4, 1)$ represent 2. Then L is isometric to a maximal order.*

Proof. Let e be a minimal vector in L, then $N(e) = 1$. If $R'$and R'' are the left and resp. right order of L, then $R', R'' \in \mathfrak{G}(4, 1)$. We have $L(L^{-1} e) = R' e \subset L$, so $L^{-1} e \subset R''$. We claim that $L^{-1} e = R''$. It suffices to prove that $L^{-1} e \in \mathfrak{G}(4, 1)$. Write $L = \tilde{a} R \tilde{b}$ for some maximal order R, $\tilde{a} = (a_{\mathfrak{p}})$, $\tilde{b} = (b_{\mathfrak{p}}) \in J_{\tilde{\mathfrak{A}}}$, $N(a_{\mathfrak{p}} b_{\mathfrak{p}}) = 1$ for all $\mathfrak{p}$. At each $\mathfrak{p}$, $L_{\mathfrak{p}}^{-1} = b_{\mathfrak{p}}^{-1} R_{\mathfrak{p}} a_{\mathfrak{p}}^{-1}$. Since $N(b_{\mathfrak{p}}^{-1} a_{\mathfrak{p}}^{-1} e) = 1$, $L_{\mathfrak{p}}^{-1} e$ and $R_{\mathfrak{p}}$ are locally isometric. Hence, $L^{-1} e \in \mathfrak{G}(4, 1)$. Now, $L^{-1} e = R''$ implies that $LL^{-1} e = LR''$, i.e., $R' e = L$. Equivalently, L is isometric to R'.

II.1.2. Remark. For a maximal order the algebraic isomorphism class (= conjugacy class) is the same as the isometry class. Thus, the number of lattice-classes in $\mathfrak{G}(4, 1)$ that represent 2 is the type number $t(\tilde{\mathfrak{A}})$ of $\tilde{\mathfrak{A}}$. On the other hand, Kitaoka proved in [8] that the class number of the genus $\mathfrak{G}(4, 1)$ is $\frac{1}{2} H(H+1)$, where $H = h(\tilde{\mathfrak{A}})/h(F)$, $h(\tilde{\mathfrak{A}})$ and $h(F)$ being respectively the ideal class number of $\tilde{\mathfrak{A}}$ and F. Tamagawa proved (unpublished) that $t(\tilde{\mathfrak{A}}) = H =$ proper class number of $G(4, p)$. Since H also equals the number of classes in $\mathfrak{G}(4, 1)$ which have nontrivial automorphisms ([8], Lemma 2), it follows that the classes in $\mathfrak{G}(4, 1)$ which represent 2 are precisely those classes which have improper automorphism groups. Since the class number of $\mathfrak{G}(4, 1)$ is 1 when $p = 5$ (due to Maass, [9]), we shall henceforth assume in our discussion that $p > 5$.

Let $\mathfrak{G}'(4, 1) \subset \mathfrak{G}(4, 1)$ consist of those L which admit improper automorphisms. It follows from the preceeding remark that such an L represents 2, and so has symmetries. We wish to determine the different roots-system types in $\mathfrak{G}'(4, 1)$. One knows from [10] that the only (non-empty) indecomposable 2-lattices over $\mathfrak{O}$ are: A_n, $1 \leqslant n \leqslant 4$, and D_4 since $p > 5$. (When $p = 5$ there is also F_4.) Let R_L denote the roots-system of an $L \in \mathfrak{G}'(4, 1)$. The possibilities for R_L are then: A_1, $2A_1$, $3A_1$, $4A_1$, A_2, $A_1 \oplus A_2$, $2A_1 \oplus A_2$, $2A_2$, A_3, $A_1 \oplus A_3$, A_4, and D_4. The cases $2A_1 \oplus A_2$, $A_1 \oplus A_3$, and A_4 are impossible by discriminant consideration. The next three propositions restrict further.

II.1.3. Proposition. *Suppose there exists $L \in \mathfrak{G}'(4, 1)$ with $R_L \supset 3A_1$. Then we have $p \equiv 5 \pmod 8$ and $R_L = D_4$.*

Proof. Let e_1, e_2, e_3 be mutually orthogonal minimal vectors in L and let N be its orthogonal complement. If $p \equiv 1 \pmod 8$ then a simple Hasse symbol computation at a dyadic prime leads to a contradiction. So, $p \equiv 5 \pmod 8$. We claim that $N \cong \langle 2 \rangle$. At each non-dyadic prime this is clear. So, it suffices to verify at the unique dyadic prime $2\mathfrak{O}$. Using local integral theory (e.g., 93:29, [11]) and the fact that the local degree $[F_2 \colon Q_2] = 2$, one readily sees that $N_2 \cong \langle 2 \rangle$. Therefore, R_L contains $4A_1$. To prove $R_L = D_4$ it is enough to show that $R_L \supsetneqq 4A_1$ since $p > 5$. Putting $N = \mathfrak{O} e_4$ we know L_2 contains a vector $\frac{1}{2}(ae_1 + be_2 + ce_3 + de_4)$ not in $\mathfrak{O}_2 e_1 \perp \mathfrak{O}_2 e_2 \perp \mathfrak{O}_2 e_3 \perp \mathfrak{O}_2 e_4$. We may suppose that a, b, c, d are either units or 0. Furthermore, if $\{0, 1, \omega, 1+\omega\}$ is a representative set of the residue class field at $2\mathfrak{O}$, then we may assume that $a, b, c, d \in \{0, 1, \omega, 1+\omega\}$. Since $Q\left(\frac{1}{2}(ae_1 + be_2 + ce_3 + de_4)\right) \in 2\mathfrak{O}_2$ we have $a = b = c = d$, and thus finding a new minimal vector $\frac{1}{2}(e_1 + e_2 + e_3 + e_4)$.

II.1.4. Proposition. *There exists at most one class of lattices L in $\mathfrak{G}'(4, 1)$ such that the roots-system $R_L \supset A_3$. It exists if and only if $p \equiv 5 \pmod 8$; furthermore, in that case $R_L = D_4$.*

Proof. Let $L \supset T = \mathfrak{O} e_1 + \mathfrak{O} e_2 + \mathfrak{O} e_3$, where e_i are minimal vectors and $B(e_1, e_2) = B(e_2, e_3) = 1$, $B(e_1, e_3) = 0$. If $p \equiv 1 \pmod 8$, localizing at a dyadic prime $\mathfrak{p}$ gives: $T_{\mathfrak{p}} = (\mathfrak{O}_{\mathfrak{p}} e_1 + \mathfrak{O}_{\mathfrak{p}} e_2) \perp \mathfrak{O}_{\mathfrak{p}} w$, $Q(w) = 12$ and $L_{\mathfrak{p}} = (\mathfrak{O}_{\mathfrak{p}} e_1 + \mathfrak{O}_{\mathfrak{p}} e_2) \perp J$ where J is anisotropic and $F_{\mathfrak{p}} J$ represents only odd-ordered field elements. Thus, $w \in F_{\mathfrak{p}} J$ is a contradiction. Thus, $p \equiv 5 \pmod 8$ and $J \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, say, adapted to a local basis $\mathfrak{O}_{\mathfrak{p}} u + \mathfrak{O}_{\mathfrak{p}} v$. We now claim that T is a (global) characteristic sublattice of L even though at the dyaic prime $\mathfrak{p} = (2)$, $T_{\mathfrak{p}}$ is not (locally) characteristic in $L_{\mathfrak{p}}$. (See [7] for the definitions of local and global characteristic sublattices.) Let $T^{\perp} = \langle x \rangle$. We may suppose that $w = u + 6v$ and $\langle x \rangle = \langle u - 6v \rangle$ over $\mathfrak{p}$. T is clearly locally characteristic at all primes away from $\mathfrak{p}$. Therefore, any even unimodular global lattice on $\tilde{\mathfrak{A}}$ containing T is either L or else $S_x(L)$, proving the claim. This proves the first statement. When $p \equiv 5 \pmod 8$ we know that there is a lattice $\Lambda \in G(4, p)$ having roots-system exactly A_3 (see [2]) or equivalently, there is a symmetric maximal order R_Λ on $\tilde{\mathfrak{A}}$ whose intersection with $W := \{a \in \tilde{\mathfrak{A}} \colon \bar{a}^* = a\}$ is Λ; here $-$ is the non-trivial galois automorphism of F/Q and $*$ the main involution of $\mathfrak{A}$, both extended to $\tilde{\mathfrak{A}}$. Finally, $R_L = D_4$ follows from the next section on unit groups, specifically, II.2.4.

II.1.5. Proposition. *There exists at most one class of lattices L in $\mathfrak{G}'(4, 1)$ such that roots-system $R_L \supset A_1 \oplus A_2$. It exists if and only if $p \equiv 2 \pmod 3$; furthermore, in that case $R_L = 2A_2$.*

Proof. Let $L \supset K = (\mathfrak{O} e_1 + \mathfrak{O} e_2) \perp \mathfrak{O} e_3$, e_i minimal vectors and $B(e_1, e_2) = 1$. Suppose $p \equiv 1 \pmod 3$, then $(3) = \mathfrak{p}\mathfrak{p}'$. Localization at $\mathfrak{p}$ shows that if $X := (\langle e_2 \rangle \perp \langle e_3 \rangle)^{\perp}$ in $L_{\mathfrak{p}}$ then X is anisotropic since $\left(\frac{-1}{\mathfrak{p}}\right) = \left(\frac{-1}{3}\right)$

$= -1$. Hence, X should represent only even-ordered elements. But, $e_2 - 2e_1 \in X$ and $\operatorname{ord}_{\mathfrak{p}}(Q(e_2-2e_1)) = 1$. This contradiction gives $p \equiv 2 \pmod 3$. As $dK = 6$, K is now a characteristic sublattice of L which proves the first statement of the proposition. Again, from the structure of the genus $G(4, p)$ it is known that when $p \equiv 2 \pmod 3$ there is a lattice $\Gamma \in G(4, p)$ with roots-system $A_1 \oplus A_2$, and hence a symmetric maximal order R_Γ as well. That $R_L = 2A_2$ follows from II.2.4.

To complete the investigation of roots-systems we need to know the roots of unity in a maximal order which we next discuss.

II.2. Unit groups. The structure of unit groups for lattices in $\mathfrak{G}'(4, 1)$ is more conveniently treated by means of the arithmetic ot quaternion algebra $\mathfrak{A}$.

II.2.1. LEMMA. *Let R be a maximal order of $\mathfrak{A}$ and $W(R)$ the group of roots of unity of R. Then $W(R) = \{x \in R\colon N(x) = 1\}$.*

Proof. If $x \in R$ is a root of unity, then $x^n = 1$ for some n; hence, $N(x)^n = 1$. Since $N(-)$ is totally positive and the only roots of unity of F are ± 1, it follows that $N(x) = 1$. The converse is an immediate consequence of the fact that the group of all units of R having norm 1 is a finite group ([1]), p. 129).

II.2.2. PROPOSITION. *Let R be a maximal order of $\mathfrak{A}$, $W(R)$ the group of roots of unity of R, and U_F the group of units of F. Then $R^\times \cong W(R) \times U_F/\{\pm 1\}$. In particular, $|W(R)| = 2|R^\times/U_F|$.*

Proof. Define the homomorphism $\varphi\colon W(R) \times U_F \to R^\times$ by $\varphi(x, u) = xu$. If $c \in R^\times$ then $N(c) = u^2$ for some $u \in U_F$ since the norm of the fundament unit is -1. From $N(cu^{-1}) = 1$ follows that $c = xu$ for some $x \in W(R)$; hence, φ is surjective. If now $xu = 1$ then $x = u^{-1} \in W(R) \cap U_F$ $= \{\pm 1\}$. Hence, $x = u = \pm 1$.

II.2.3. Remark. If R is a symmetric maximal order of $\mathfrak{A}$, then from [2] one knows that $|R^\times/U_F| = 1, 2, 3, 6$, or 12. From II.2.1 and II.2.2 the number of minimal vectors in R is $a_R(2) = 2, 4, 6, 12$, or 24. Lattices $\Lambda \in G'(4, p)$ lift up to symmetric maximal orders R_Λ. Therefore, we have the roots-systems A_1, $A_1 \oplus A_1$, A_2, $A_1 \oplus A_2$, A_3 from $G'(4, p)$ lift up to roots-systems A_1, $A_1 \oplus A_1$, A_2, $A_2 \oplus A_2$, D_4 of symmetric maximal orders in $\mathfrak{G}(4, 1)$. In particular, we see that this lifting (or "glueing" construction) can introduce new minimal vectors. At $p = 5$, A_4 lifts to F_4. On the other hand, from the elimination process in this section we extract the following rather surprising result.

II.2.4. PROPOSITION. *The only possible types of roots-systems for lattices in $\mathfrak{G}'(4, 1)$ are: A_1, $A_1 \oplus A_1$, A_2, $A_2 \oplus A_2$, and D_4. These roots-systems are already realized from the roots-systems of the symmetric maximal orders of $\mathfrak{A}$ (i.e., equivalently, from the liftings of lattices from $G'(4, p)$).*

II.2.5. PROPOSITION. *Let $L \in \mathfrak{G}(4, 1)$, R' and R'' the left and right orders of L. Let $W(R')$ and $W(R'')$ be the groups of roots of unity of R' and R'' respectively. Then $O^+(L) \cong W(R') \times W(R'')/\{\pm 1\}$.*

Proof. Every rotation of L is of the form $x \mapsto \alpha x \beta^{-1}$ where $\alpha, \beta \in \mathfrak{A}$ satisfy $N(\alpha) = N(\beta)$. Let R', R'' be the left and right order of L respectively. Since $\alpha R' \alpha^{-1} = R'$ and $\beta R'' \beta^{-1} = R''$, both $R'\alpha$ and $R''\beta$ are principal two-sided ideals. But, $\mathfrak{A}$ splits at every finite prime. It follows that $R'\alpha = R'I$ and $R''\beta = R''J$ for some ideals I and J in F. Taking norms, we have $I^2 = (N(\alpha))$, $J^2 = (N(\beta))$. Since the class number of F is odd, I and J are principal. Thus, $R'\alpha = R'a$, $R''\beta = R''b$ for some $a, b \in F$. Write $\alpha = ua$, $\beta = vb$, $u \in R'^\times$, $v \in R''^\times$. Since $N(u) \in U_F$ is totally positive and the norm of the fundamental unit of F is -1, we have $N(u) = \varepsilon^2$ for some $\varepsilon \in U_F$; hence, $u = \varepsilon w$ for some $w \in W(R')$. Replacing a by εa, we may assume that $u \in W(R')$. Similarly, we may assume that $v \in W(R'')$. Hence, $N(\alpha) = a^2$, $N(\beta) = b^2$, and so $a = \pm b$. The original rotation reduces to $x \mapsto \pm uxv^{-1}$. This means the mapping $\varphi\colon W(R') \times W(R'') \to O^+(L)$ defined by $(u, v) \mapsto uxv^{-1}$ is surjective. One easily checks that $\ker(\varphi) = \{\pm 1\}$.

II.2.6. COROLLARY. *Let $L \in \mathfrak{G}'(4, 1)$. Then the order of the unit group of L, $|O(L)|$, is 4, 16, 36, 144, or 576, according to the roots-system of L being A_1, $A_1 \oplus A_1$, A_2, $A_2 \oplus A_2$, or D_4 respectively.*

Proof. By Proposition II.1.1, L is isometric to a maximal order R of $\mathfrak{A}$. We may assume $L = R$. Thus, $R' = R'' = R$, and the corollary follows from the proposition together with II.2.2 and II.2.3.

Our next result shows that, contrary to the $G(4, p^2)$ case, the symmetries of a lattice L in $\mathfrak{G}'(4, 1)$ are fully controlled by the minimal vectors. To see this, suppose that $u \in \mathfrak{A}$ and the symmetry $S_u \in O(L)$. We may suppose that $u \in L$. Consider it at each finite prime $\mathfrak{p}$. We may express $u = \pi_{\mathfrak{p}}^{s_{\mathfrak{p}}} u'$, where $\pi_{\mathfrak{p}}$ is a fixed uniformizer at $\mathfrak{p}$, $s_{\mathfrak{p}} \geqslant 0$, and u' is primitive in $L_{\mathfrak{p}}$. Since $L_{\mathfrak{p}}$ is unimodular and $S_{u'} \in O(L_{\mathfrak{p}})$, we see that $Q(u') \in \mathfrak{O}_{\mathfrak{p}}^\times$ if $\mathfrak{p}$ is non-dyadic, and $Q(u') \in 2\mathfrak{O}_{\mathfrak{p}}^\times$ at dyadic $\mathfrak{p}$. Therefore $Q(u)\mathfrak{O} = 2\prod_{\mathfrak{p}\nmid 2} \mathfrak{p}^{2s_{\mathfrak{p}}}$. Since the class number of F is odd, $\prod_{\mathfrak{p}\nmid 2} \mathfrak{p}^{s_{\mathfrak{p}}}$ is principal, say, $= (a)$. Since norm (fundamental unit) $= -1$, $Q(a^{-1}u) = 2\varepsilon^2$ for some $\varepsilon \in U_F$. Replacing u by $\varepsilon^{-1}a^{-1}u$ we may take $Q(u) = 2$ as $S_{\varepsilon^{-1}a^{-1}u} = S_u$. We record this.

II.2.7. PROPOSITION. *Every symmetry of a lattice $L \in \mathfrak{G}'(4, 1)$ is of the form S_e where e is a minimal vector in L.*

II.2.8. Remark. Corollary II.2.6 implies that $O(L)$ may not be generated by $\pm$ symmetries of L in view of Proposition II.2.7.

II.3. Theta series of degree two. The objective here is to prove Theorem II.3.3 below. Let $L_1, \ldots, L_t$ be a full set of non-isometric lattices in $\mathfrak{G}'(4, 1)$. For each i, fix a minimal vector e_i in L_i and denote by K_i the orthogonal complement of e_i in L_i. Then K_i is free with discriminant $dK_i = 2$. We choose a binary lattice J_i in K_i according to the following lemma. (We drop the subscript i.)

II.3.1. Lemma. *There exists a principal prime ideal $\mathfrak{q} = \mathfrak{O}\pi$ of F such that K contains binary free lattice J with discriminant $dJ = \pi$, where π is a totally positive prime element.*

Proof. At a dyadic prime $\mathfrak{p}$, $K_\mathfrak{p} = X \perp \mathfrak{O}_\mathfrak{p} x$, where X is binary unimodular. Using Lemma 1.6 [4] generalized to totally real number fields, there is a binary $\mathfrak{O}$-lattice J and a principal prime ideal $\mathfrak{q} = \mathfrak{O}\pi$ such that $2 \notin \mathfrak{q}$, $dJ_\mathfrak{r}$ a unit at all $\mathfrak{r} \neq \mathfrak{q}$ and $dJ_\mathfrak{q} = \pi$. J is free with discriminant π by [8], p. 97.

The orthogonal complement of J in K is clearly also free, say, $\mathfrak{O}f$, $Q(f) = 2\pi$. The next result may be proved in a similar way as in I.4, by noting that $\mathfrak{O}e \perp J$ is a characteristic sublattice of L since there are exactly two lattices in $\mathfrak{G}(4, 1)$ containing it and the two are interchanged by the symmetry S_f. We skip the details.

II.3.2. Lemma. *If $\varphi\colon J_i \to L_j$ is an isometric embedding such that L_j contains a minimal vector e perpendicular to $\varphi(J_i)$ then φ can be extended to an isometry of L_i onto L_j. In particular, $i = j$.*

II.3.3. Theorem. *The generalized theta series $\theta_L^{(2)}(\mathbf{Z})$ of degree two for even positive definite quaternary unimodular lattices over $Q(\sqrt{p})$ having improper automorphisms are linearly independent.*

Proof. Let L_i, e_i, J_i, $dJ_i = \pi_i$ and $\mathfrak{q}_i = \mathfrak{O}\pi_i$ be as above. Let 2^{n_i} be the exact power of 2 dividing $|O(L_i)|$. Then $n_i = 2$ for L_i of roots-system type A_1 or A_2; $n_i = 4$ for type $A_1 \oplus A_1$ or $A_2 \oplus A_2$; $n_i = 6$ for type D_4. Clearly, $O(L_j)$ acts on the set of isometric embeddings of J_i into L_j. If $\varphi\colon J_i \to L_j$ is any isometric embedding, then the number of elements in the $O(L_j)$-orbit of φ is $|O(L_j)|/|H_\varphi|$, where H_φ is the stabilizer of φ. We want to determine the exact power of 2 in this quotient. Let $\sigma \in H_\varphi$ be an involution. Then, there is a splitting $V = V^- \perp V^+$ for which $\sigma = -1 \perp 1$.

If $\dim V^+ = 3$, then σ is a symmetry of L_j, so that by Proposition II.2.7 there is a minimal vector $e \in L_j$ such that $\sigma = S_e$. Since e is orthogonal to $\varphi(J_i)$ we have $i = j$ and φ lies in the orbit of the inclusion map by Lemma II.3.2. If $\dim V^+ = 2$, then $V^+ = F(\varphi(J_i))$. Put $X := \varphi(J_i)^\perp$ in L_j. We have

$$(L_j)_{\mathfrak{q}_i} \supset (\varphi(J_i))_{\mathfrak{q}_i} \perp X_{\mathfrak{q}_i} = \mathfrak{O}_{\mathfrak{q}_i} u \perp \mathfrak{O}_{\mathfrak{q}_i} v \perp \mathfrak{O}_{\mathfrak{q}_i} x \perp \mathfrak{O}_{\mathfrak{q}_i} y,$$

where $(\varphi(J_i))_{\mathfrak{q}_i} = \mathfrak{O}_{\mathfrak{q}_i} u \perp \mathfrak{O}_{\mathfrak{q}_i} v$, $X_{\mathfrak{q}_i} = \mathfrak{O}_{\mathfrak{q}_i} x \perp \mathfrak{O}_{\mathfrak{q}_i} y$, $Q(u)$, $Q(x) \in \mathfrak{O}_{\mathfrak{q}_i}^\times$, and $Q(v)$, $Q(y) \in \pi_i \mathfrak{O}_{\mathfrak{q}_i}^\times$. It follows that

$$(*) \qquad (L_j)_{\mathfrak{q}_i} = (\varphi(J_i))_{\mathfrak{q}_i} \perp X_{\mathfrak{q}_i} + \mathfrak{O}_{\mathfrak{q}_i} \frac{1}{\pi_i}(v + ay)$$

for some $a \in \mathfrak{O}_{\mathfrak{q}_i}^\times$. Since $\sigma(L_j) = L_j$ we also have an equation as $(*)$ except with av replaced by $-ay$. Hence, $2v/\pi_i \in L_j$, which is impossible since $\pi_i^2 \nmid Q(v)$. Therefore, the exact power of 2 in $|O(L_j)|/|H_\varphi|$ is determined by the chart below:

Type of L_j	When $i = j$ and φ lies in the orbit of the inclusion	When $i \neq j$ or φ does not lie in the orbit of inclusion
A_1 or A_2	2^1	2^2
$A_1 \oplus A_1$ or $A_2 \oplus A_2$	2^3	2^4
D_4	2^5	2^6

Let a_{ij} be the number of isometric embeddings of J_i into L_j. It follows that if the type of L_j is A_1 or A_2, then

$$a_{ij} \equiv 0 (\mathrm{mod}\ 2^2) \quad \text{for} \quad i \neq j,$$

$$a_{jj} \equiv 0 (\mathrm{mod}\ 2), \quad a_{jj} \not\equiv 0 (\mathrm{mod}\ 2^2);$$

if the type of L_j is $A_1 \oplus A_1$ or $A_2 \oplus A_2$, then we have

$$a_{ij} \equiv 0 (\mathrm{mod}\ 2^4) \quad \text{for} \quad i \neq j,$$

$$a_{jj} \equiv 0 (\mathrm{mod}\ 2^3), \quad a_{jj} \not\equiv 0 (\mathrm{mod}\ 2^4);$$

if the type of L_j is D_4, we have

$$a_{ij} \equiv 0 (\mathrm{mod}\ 2^6) \quad \text{for} \quad i = j,$$

$$a_{jj} \equiv 0 (\mathrm{mod}\ 2^5), \quad a_{jj} \not\equiv 0 (\mathrm{mod}\ 2^6).$$

Suppose there is a non-trivial linear relation over $\boldsymbol{Z}$ (since the generalized theta series of degree two are integral automorphic forms) $\sum c_j \theta_{L_j}^{(2)}(\mathbf{Z}) = 0$ where c_j's are relatively prime integers. Evaluating at each J_i, we obtain $\sum c_j a_{ij} = 0$. We consider this equation modulo various congruences:

mod $2^2 \Rightarrow c_j \equiv 0 (\mathrm{mod}\ 2)$ for $n_j = 2$ (i.e. for L_j with type A_1 or A_2);
mod $2^3 \Rightarrow c_j \equiv 0 (\mathrm{mod}\ 2^2)$ for $n_j = 2$;
mod $2^4 \Rightarrow c_j \equiv 0 (\mathrm{mod}\ 2)$ for $n_j = 4$ (L_j of type $A_1 \oplus A_1$ or $A_2 \oplus A_2$).
$\Rightarrow c_j \equiv 0 (\mathrm{mod}\ 2^3)$ for $n_j = 2$;
mod $2^5 \Rightarrow c_j \equiv 0 (\mathrm{mod}\ 2^2)$ for $n_j = 4$,
$\Rightarrow c_j \equiv 0 (\mathrm{mod}\ 2^4)$ for $n_j = 2$;
mod $2^6 \Rightarrow c_j \equiv 0 (\mathrm{mod}\ 2)$ for $n_j = 6$ (L_j of type D_4).

This shows all c_j's are even, and the contradiction proves the theorem.

A careful examination of the proof of the theorem shows the following classification result.

II.3.4. Corollary. *Let L_1 and L_2 be two lattices in $\mathfrak{G}'(4, 1)$. If $\theta^{(2)}_{L_1}(\mathbf{Z}) \equiv \theta^{(2)}_{L_2}(\mathbf{Z})(\mathrm{mod}\ 16)$ then $L_1 \cong L_2$.*

II.4. Theta series of degree one. Again we shall merely state some of the results for degree one theta series and say a few words about their proofs.

II.4.1. Theorem. *Let $p \equiv 5(\mathrm{mod}\ 8)$. Then the generalized theta series $\theta_L(\mathbf{z})$ of degree one for lattices L coming from distinct classes in $\mathfrak{G}'(4, 1)$ of roots-system type $A_1 \oplus A_1$ are linearly independent.*

II.4.2. Corollary. *For $p \equiv 5(\mathrm{mod}\ 8)$, lattices in $\mathfrak{G}'(4, 1)$ of roots-system type $A_1 \oplus A_1$ are classified by their generalized theta series of degree one modulo* 8.

II.4.3. Theorem. *Let $p \equiv 2(\mathrm{mod}\ 3)$. Then the generalized theta series $\theta_L(\mathbf{z})$ of degree one for lattices in $\mathfrak{G}'(4, 1)$ of roots-system type A_2 are linearly independent.*

II.4.4. Corollary. *For $p \equiv 2(\mathrm{mod}\ 3)$, lattices in $\mathfrak{G}'(4, 1)$ of roots-system type A_2 are classified by their generalized theta series of degree one modulo* 3.

Remarks on the proofs. Consider first a lattice $L \in \mathfrak{G}'(4, 1)$ of roots-system type $A_1 \oplus A_1$, and let e_1 and e_2 be minimal vectors of L. Then the orthogonal complement M of $\langle e_1 \rangle \perp \langle e_2 \rangle$ in L is free with discriminant 4. There exist a vector $u \in M$ and a principal prime ideal $\mathfrak{q} = \mathfrak{O}\pi$ such that $Q(u) = 2\pi$. Let $\langle v \rangle := \langle u \rangle^{\perp}$ in M. Then $Q(v) = 2\pi$. Define an isometry $\tau \in O(V)$ by $\tau(e_1) = e_2$, $\tau(e_2) = e_1$, and τ fixes M. For $p \equiv 5(\mathrm{mod}\ 8)$ there are exactly four lattices in $\mathfrak{G}(4, 1)$ which contain $\mathfrak{O}e_1 \perp \mathfrak{O}e_2 \perp \mathfrak{O}u \perp \mathfrak{O}v$, and they are transitively permuted by $S_{\mathfrak{p}}$ and τ.

Now, let L have roots-system type A_2, and $\mathfrak{O}e_1 + \mathfrak{O}e_2 \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \subset L$ and T its orthogonal complement. Then T is free with discriminant 3. There is a principal prime ideal $\mathfrak{q} = \pi\mathfrak{O}$ and $\mathfrak{O}u_1 + \mathfrak{O}u_2 = \begin{pmatrix} 2\pi & \pi \\ \pi & 2\pi \end{pmatrix} \subset T$. When $p \equiv 2(\mathrm{mod}\ 3)$, there are precisely four lattices again in $\mathfrak{G}(4, 1)$ containing $(\mathfrak{O}e_1 + \mathfrak{O}e_2) \perp \mathfrak{O}u_1 \perp \mathfrak{O}v$, and they are transitively permuted by $S_{\mathfrak{p}}$ and the isometry ϱ defined by $\varrho(u_1) = -u_1$, $\varrho(v) = -v$, and ϱ fixes e_1, e_2. Here $v = u_1 - 2u_2$.

II.4.5. Remarks. (i) If $p \equiv 1(\mathrm{mod}\ 8)$, then 2 splits in F and there will be eight lattices in $\mathfrak{G}(4, 1)$ containing $\mathfrak{O}e_1 \perp \mathfrak{O}e_2 \perp \mathfrak{O}u \perp \mathfrak{O}v$ forming two sets of four lattices which are isometric amongst members within each set, but not necessarily isometric to members of the other set. Hence, the proof of Theorem II.4.1 would yield independence for only half the classes of type $A_1 \oplus A_1$. (ii) If $p \equiv 1(\mathrm{mod}\ 3)$ then 3 splits in F. Again, eight lattices in $\mathfrak{G}(4, 1)$ will contain $(\mathfrak{O}e_1 + \mathfrak{O}e_2) \perp \mathfrak{O}u_1 \perp \mathfrak{O}v$ with a similar behaviour. It is, of course, possible that the congruence condition in Theorems II.4.1, II.4.3 is superfluous.

References

[1] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. 195 (1955), pp. 127–151.

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

[3] J. S. Hsia and D. C. Hung, *Theta series of ternary and quaternary quadratic forms*, Invent. Math. 73 (1983), pp. 151–156.

[4] J. S. Hsia, Y. Kitaoka and M. Kneser, *Representations of positive definite quadratic forms*, J. Reine Angew. Math. 301 (1978), pp. 132–141.

[5] D. C. Hung, *Theta series of ternary quadratic forms*, in preparation.

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

[7] — *Representations of quadratic forms and their application to Selberg's zeta functions*, ibid. 63 (1976), pp. 153–162.

[8] — *Class numbers of quadratic forms over real quadratic fields*, ibid. 66 (1977), pp. 89–98.

[9] H. Maass, *Modulformen und quadratische Formen über dem quadratischen Zahlkörper* $R(\sqrt{5})$, Math. Ann. 118 (1941), pp. 65–84.

[10] Y. Mimura, *On 2-lattices over real quadratic integers*, Math. Sem. Notes 7 (1979), pp. 327–342.

[11] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, New York 1963.

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

[13] I. Reiner, *Maximal Orders*, Academic Press, New York 1975.

[14] M. F. Vigneras, *Arithmétique des Algèbres de Quaternions*, Springer-Verlag, New York 1980.

Received on 25. 10. 1983 (1381)

DEPARTMENT OF MATHEMATICS
OHIO STATE UNIVERSITY
Columbus, Ohio, USA

Current address of D.C. Hung
DEPARTMENT OF MATHEMATICS
SUNY ETR. AT BINGHAMTON
Binghamton, N. Y. 13901, USA