INDEFINITE QUADRATIC FORMS OF DETERMINANT $\pm 2p$

D. G. JAMES[1]

1. **Introduction.** In [4] C. T. C. Wall gives a set of invariants which determine the transitivity class of a vector in an indefinite unimodular lattice under the action of its orthogonal group. We give here a generalization of this argument for indefinite lattices L with determinant $\delta(L) = \pm 2p$ where p is an odd prime. We do not handle all such lattices, only a large class of them, including all the odd lattices when $p \equiv 3 \pmod 4$ and the rank $r(L)$ and signature $s(L)$ satisfy $r(L) - |s(L)| \geqq 5$. Wall's invariants are essentially local invariants, and by placing the restriction $r(L) - |s(L)| \geqq 4$ on the lattice, he works in a situation where the local invariants are enough to determine the global behaviour in $\boldsymbol{Z}$. For general lattices the local situation can be very complex (see James and Rosenzweig [2]); we have also chosen a case where the local behaviour is reasonably simple.

Let L be a free $\boldsymbol{Z}$-module and $\Phi: L \times L \to \boldsymbol{Z}$ a symmetric bilinear mapping into the integers $\boldsymbol{Z}$ with $\det \Phi = \pm 2p$. For $\alpha, \beta \in L$ we shall denote $\Phi(\alpha, \beta)$ by $\alpha \cdot \beta$. L is called an *odd* lattice if α^2 takes both odd and even values as α ranges over L; and an *even* lattice if α^2 is always even. The orthogonal group $O(L, \boldsymbol{Z})$ of L is the set of all isometries ϕ of L; that is the set of all linear bijective mappings on L such that $\phi(\alpha) \cdot \phi(\beta) = \alpha \cdot \beta$ for all $\alpha, \beta \in L$. We wish to determine necessary and sufficient conditions on $\alpha, \beta \in L$ for there to exist a $\phi \in O(L, \boldsymbol{Z})$ such that $\phi(\alpha) = \beta$. If such a ϕ exists we write $\alpha \sim \beta$.

2. **Transitivity of vectors.** A vector $\alpha \in L$ is called *primitive* if it cannot be written in the form $\alpha = d\beta$ with $\beta \in L$ and $d \neq \pm 1$. For a general α $(\neq 0) \in L$ there exists a unique positive integer $d(\alpha)$ such that $\alpha = d(\alpha)\beta$ with β primitive. $d(\alpha)$ is called the *divisor* of α. It is clearly an invariant of the transitivity class of α. Clearly the *norm* α^2 is another. Let $i(\alpha) = \text{g.c.d. } \alpha \cdot \beta$ as β ranges over L. Since $\phi(\alpha) \cdot \phi(\beta) = \alpha \cdot \beta$ for any $\phi \in O(L, \boldsymbol{Z})$, and $\phi(\beta)$ ranges over all L, we have $i(\phi(\alpha)) = i(\alpha)$. We call $i(\alpha)$ the *index* of α. For odd lattices a vector α is called *ordinary* if there exists a $\beta \in L$ such that $\alpha \cdot \beta = 0$ and β^2 is odd; otherwise α is called *characteristic*. Thus for odd lattices there are two

Received by the editors May 6, 1968.

[1] This research was partially supported by an N.S.F. Grant.

types of vectors: ordinary and characteristic. For even lattices all vectors are of the same type.

Let $H=\langle\lambda, \mu\rangle$ denote the hyperbolic plane spanned by λ and μ over $\boldsymbol{Z}$ where $\lambda^2=\mu^2=0$ and $\lambda\cdot\mu=1$. $I=\langle\xi, \rho\rangle$ is the plane spanned by ξ and ρ where $\xi^2=\xi\cdot\rho=1$ and $\rho^2=0$, and $\langle\eta\rangle$ is the line $\boldsymbol{Z}\eta$. $J_1\perp J_2$ denotes the orthogonal sum of the sublattices J_1 and J_2.

THEOREM 1. *The invariants norm, divisor, index and type determine the transitivity class of a vector α in the two lattices*

$$L_1 = I_1 \perp I_2 \perp \langle\eta\rangle = \langle\xi_1, \rho_1\rangle \perp \langle\xi_2, \rho_2\rangle \perp \langle\eta\rangle,$$

and

$$L_2 = H_1 \perp H_2 \perp \langle\eta\rangle = \langle\lambda_1, \mu_1\rangle \perp \langle\lambda_2, \mu_2\rangle \perp \langle\eta\rangle$$

where $\eta^2=d=\pm 2p$.

PROOF. Notice that L_1 is an odd lattice and L_2 an even lattice. Both have determinant d, rank 5 and signature ± 1. We shall only prove the result for L_1; L_2 is similar and simpler.

Let $\alpha=\sum_{i=1}^{2}(a_i\xi_i+b_i\rho_i)+c\eta\in L_1$. We shall prove the theorem by applying mappings from $O(L, \boldsymbol{Z})$ to α to reduce it to a form where the coefficients are uniquely determined by the invariants. Clearly it suffices to consider only primitive vectors so that we may assume $d(\alpha)=(a_1, a_2, b_1, b_2, c)=1$. Let $q=i(\alpha)=(a_1, a_2, b_1, b_2, cd)$. Then q divides d and hence q has one of the four values 1, 2, p, $2p$.

Consider $\sum_{i=1}^{2}(a_i\xi_i+b_i\rho_i)=e\alpha_1\in I_1\perp I_2$ where α_1 is primitive. Our first simplification is to reduce e to q. From Wall [**4**, p. 333] or James [**1**, Lemma 2] there exists an element $\theta\in O(I_1\perp I_2, \boldsymbol{Z})$ (which extends to $\theta\in O(L_1, \boldsymbol{Z})$ by defining $\theta(\eta)=\eta$) such that $\theta(\alpha_1)$ is contained in a binary sublattice B_1 of $I_1\perp I_2=B_1\perp B_2$. More specifically, either

(i) $\theta(\alpha_1)=\lambda+a\mu$ if α_1 ordinary with α_1^2 even: $B_1=H$, $B_2=I$,

(ii) $\theta(\alpha_1)=\xi_1+a\rho_1$ if α_1 ordinary with α_1^2 odd: here $B_2=I_2$, or,

(iii) $\theta(\alpha_1)=2\xi+a\rho$ if α_1 characteristic: here $B_1=I$, $B_2=H$.

Case 1. $B_2=I_2=\langle\xi_2, \rho_2\rangle$ (this is (ii) above). We denote by σ_x, $x\in\mathbf{Z}$, the isometry on $I_2\perp\langle\eta\rangle$ defined by

$$\sigma_x(\xi_2) = \xi_2 - x\eta - \tfrac{1}{2}dx^2\rho_2, \qquad \sigma_x(\rho_2) = \rho_2, \qquad \sigma_x(\eta) = \eta + xd\rho_2.$$

σ_x extends to an element of $O(L, \boldsymbol{Z})$ by defining σ_x to be the identity mapping on B_1. Then $\sigma_1\theta(\alpha)=\sigma_1(e(\xi_1+a\rho_1)+c\eta)=e(\xi_1+a\rho_1)+cd\rho_2+c\eta$. But now $e(\xi_1+a\rho_1)+cd\rho_2\in I_1\perp I_2$ and its divisor is $(cd, e)=(cd, a_1, a_2, b_1, b_2)=q$. After applying an isometry on $I_1\perp I_2$ again we can map α into the form $q\zeta+c\eta$ where ζ is primitive and is one of the three forms $\xi_2+a\rho_2$, $2\xi+a\rho$ or $\lambda+a\mu$ as above.

Case 2. $B_2=I$ (this is (i) above). By a similar argument we can map α into the form $q\zeta+c\eta$ as in Case 1.

Case 3. $B_2=H=\langle\lambda, \mu\rangle$. Instead of σ_x we use τ_x, where

$$\tau_x(\lambda) = \lambda - x\eta - \tfrac{1}{2}dx^2\mu, \qquad \tau_x(\mu) = \mu, \qquad \tau_x(\eta) = \eta + xd\mu.$$

Again we can map α into the form $q\zeta+c\eta$ with ζ primitive of one of the three forms $\xi_2+a\rho_2$, $2\xi+a\rho$ or $\lambda+a\mu$.

We now show how to further transform α so that the coefficient c of η is invariantly determined. Consider first α ordinary with $\alpha\sim q(\xi_2+a\rho_2)+c\eta$. The map σ_x changes the coefficient of η from c to $c-qx$. If $q=1$ we can reduce c to 0, and α is mapped into the form $\xi_2+\frac{1}{2}(\alpha^2-1)\rho_2$, where the coefficients are determined uniquely by the invariants of α. For $q>1$, since we can change the sign of c, and move it through any multiple of q, we can move it into the range $0<c \leqq \frac{1}{2}q$. If $q=2$, c becomes 1. If p divides q then $\alpha^2\equiv c^2d \pmod{q^2}$, and since p exactly divides d, $c^2 \pmod q$ is an invariant of α. Hence c is uniquely determined in the range $0<c\leqq\frac{1}{2}q$ (by α^2 and q). Then α is mapped into the form $q(\xi_2+a\rho_2)+c\eta$, c fixed as above, and a fixed by the equation $\alpha^2=q^2(2a+1)+c^2d$.

α ordinary of the form $\alpha\sim q(\lambda+a\mu)+c\eta$ can be handled in an analogous manner. Here a is fixed by the equation $\alpha^2=q^2 2a+c^2d$. These two cases with α ordinary are distinct. In the first $q^{-2}(\alpha^2-c^2d)$ is odd, and in the second it is even.

It now remains to consider the case where α is characteristic with $\alpha\sim q(2\xi+a\rho)+c\eta$ · 'σ_x' now changes the coefficient of η from c to $c-2xq$. But $\alpha^2\equiv c^2d \pmod{8q^2}$. If $q=1$ this congruence determines whether c is even or odd, and hence whether we take the coefficient of η to be 0 or 1 respectively. Here again α has been mapped into a form invariantly determined by the norm, divisor, index and type of α. If $q=2$ then we can take $c=1$. If $q=p$ we can move c into the range $0<c<p$. But $\alpha^2\equiv c^2d \pmod{8p^2}$ makes $c^2 \pmod{4p}$ an invariant of α and hence fixes c in this range. Thus α is mapped into an invariant form.

If $q=2p$, so that c is odd, we need the isometry ψ on $\langle\xi, \rho\rangle \perp\langle\eta\rangle$ defined in the case where $d=2p$ by

$$\begin{aligned}
\psi(\xi) &= (2-p)\xi + \tfrac{1}{4}(p-1)(p+3)\rho + \tfrac{1}{2}(p-1)\eta,\\
\psi(\rho) &= 4\xi - (p+2)\rho - 2\eta,\\
\psi(\eta) &= -4p\xi + p(p+3)\rho + (1+2p)\eta.
\end{aligned}$$

Applying ψ to $q(2\xi+a\rho)+c\eta$ the coefficient of η becomes $(2p+1)c+q(p-1)-2aq\equiv c+qc \pmod{2q}$. It is therefore moved by an odd

multiple of q. But we can already move it by an arbitrary multiple of $2q$ and change its sign. Hence we can arrange $0<c<p$, and c is uniquely determined in this range by $\alpha^2 \equiv c^2 d \pmod{8q^2}$. Thus $\alpha \sim q(2\xi + a\rho) + c\eta$ with c uniquely determined by the above restrictions and a determined by α^2. Thus in all cases α is transformed into a form uniquely determined by the invariants norm, divisor, index and type. Therefore these invariants determine the transitivity class of α.

THEOREM 2. *Let $L = U \perp \langle \eta \rangle$ where U is an odd unimodular lattice with $r(U) - |s(U)| \geqq 4$. Then the transitivity class of a vector $\alpha \in L$ with respect to the orthogonal group $O(L, \boldsymbol{Z})$ is uniquely determined by the invariants norm, divisor, index and type.*

PROOF. This follows immediately from Theorem 1 and the results of Wall [4]. First $U = I_1 \perp I_2 \perp U_1$ with U_1 unimodular. Write $\alpha = \alpha_1 + c\eta$ with $\alpha_1 \in U$. Then there exists a $\phi \in O(U, \boldsymbol{Z})$ such that $\phi(\alpha_1) \in I_1 \perp I_2$. Now apply Theorem 1 to $\phi(\alpha_1) + c\eta \in L_1$.

3. **Odd lattices with $p \equiv 3 \pmod 4$.** The question now arises as to how many lattices are included in Theorem 2. We shall prove

THEOREM 3. *Let L be an odd indefinite lattice with determinant $d = \pm 2p$ where p is a prime and $p \equiv 3 \pmod 4$. Then if $r(L) \geqq 3$, L has an orthogonal basis $\xi_1, \cdots, \xi_{r-1}, \eta$ such that $\xi_i^2 = \pm 1$, $1 \leqq i \leqq r-1$ and $\eta^2 = \pm d$.*

We first observe that the theorem is not necessarily true if $p \equiv 1 \pmod 4$.

EXAMPLE. Let $p = 41$ and $L = I_1 \perp \cdots \perp I_8 \perp \langle \alpha, \beta \rangle$ where $\alpha^2 = 13$, $\alpha \cdot \beta = 41$, $\beta^2 = 123$ so that $\delta(L) = (-1)^{s+1} 2.41$. If L has an orthogonal basis then $L = \langle \zeta \rangle \perp J$ where ζ^2 equals ± 41 or ± 2.41. But 41 must divide $\zeta \cdot \gamma$ for all $\gamma \in L$. Hence

$$\zeta = 41 \sum_{i=1}^{8} (a_i \xi_i + b_i \rho_i) + 41u\alpha + v\beta$$

for some integers a_i, b_i, u, v. Therefore $\zeta^2 \equiv 123 v^2 \pmod{41^2}$ and hence $3v^2 \equiv \pm 1, \pm 2 \pmod{41}$. But $\pm 1, \pm 2$ are all quadratic residues modulo 41, and 3 is not. Hence such a ζ cannot exist.

The following proof of Theorem 3, suggested by the referee, is an improvement of our original proof.

Construct a $\boldsymbol{Z}$-lattice $K = \langle \zeta_1 \rangle \perp \cdots \perp \langle \zeta_t \rangle \perp \langle \alpha \rangle \perp \langle \beta \rangle$ with either $\alpha^2 = 1$ and $\beta^2 = -2p$, or $\alpha^2 = -1$ and $\beta^2 = 2p$. The $\zeta_i^2 = \pm 1$ are chosen so that K is isometric to L locally at the infinite prime (that is K

and L have the same signature and rank). The two different possibilities for α and β give distinct Hasse symbols S_pK since $p \equiv 3 \pmod 4$. We choose that K which makes $S_pK = S_pL$. Clearly K and L have the same rank and discriminant. The local classification theorems for fields [3, 63:20] give now that K and L are locally equivalent at all prime spots, except possibly at the prime 2. But by the Hilbert Reciprocity Theorem they will also be locally equivalent at the prime 2. So by the Hasse-Minkowski Theorem K and L are rationally equivalent. We can now assume K and L are on the same quadratic space.

Now K and L are locally integrally equivalent at all primes and hence in the same genus [3, 91:2 or 92:2 and 93:29]. Finally we shall show that there is only one class in each genus. For by simple calculation, locally K_2 represents all 2-adic units. Hence $\theta(O^+(K_2))$ contains all 2-adic units, so gen $K = \text{spn } K$ by [3, 102:9 and 102:10]. Hence $L \in \text{spn } K$. But since K is indefinite $\text{spn } K = \text{cls } K$ by [3, 104:5] and hence $L \in \text{cls } K$. That is L has an orthogonal basis as stated.

References

1. D. G. James, *On Witt's theorem for unimodular quadratic forms*, Pacific J. Math. 26 (1968), 303–316.

2. D. G. James and S. M. Rosenzweig, *Associated vectors in lattices over valuation rings*, Amer. J. Math. 90 (1968), 295–307.

3. O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, Berlin, 1963.

4. C. T. C. Wall, *On the orthogonal groups of unimodular quadratic forms*, Math. Ann. 147 (1962), 328–338.

Pennsylvania State University