WITT'S THEOREM FOR SYMPLECTIC MODULAR FORMS [1]

D. G. JAMES

(Received 25 July 1967)

Let L denote a free Z-module of rank $2n$ and Φ an alternating bilinear mapping from $L \times L$ into the rational integers Z. Writing $\alpha \cdot \beta$ for $\Phi(\alpha, \beta)$, where $\alpha, \beta \in L$, we have

$$\alpha \cdot \beta = -\beta \cdot \alpha \quad \text{and} \quad \alpha^2 = 0.$$

We shall assume that Φ is non-singular and unimodular (see Bourbaki [1]). L is now a (*symplectic*) *lattice*.

The automorphisms φ of L that preserve Φ, that is satisfying

$$\varphi(\alpha) \cdot \varphi(\beta) = \alpha \cdot \beta$$

for all $\alpha, \beta \in L$, are called (*symplectic*) *isometries* and form the *symplectic modular group* $Sp(2n, Z)$. It is the purpose of this paper to give necessary and sufficient conditions for a map Θ between two sublattices of L to extend to an isometry in $Sp(2n, Z)$. This is an extension of the problem first considered by Witt [6] for an orthogonal geometry over fields. More general forms (in both the symplectic and orthogonal cases) can be found in Bourbaki [1] and Dieudonné [2]. There are also many integral generalizations of this result in the literature, some of which are mentioned in O'Meara [5] and James [3].

Let J_1 and J_2 be two sublattices of L and $\Theta : J_1 \to J_2$ a bijective, linear transformation that preserves Φ, that is for each $\alpha, \beta \in J_1$

$$\Theta(\alpha) \cdot \Theta(\beta) = \alpha \cdot \beta.$$

A vector $\alpha \in L$ is called *imprimitive* if it can be written $d\beta$ with $\beta \in L$ and d not a unit of Z; otherwise α is *primitive*. The maximal d, as above, will be called the *divisor* of α. It is clear from linearity, that an isometry of L must preserve the divisor of each vector. We shall prove the following:

THEOREM. *A bijective linear transformation $\Theta : J_1 \to J_2$ between two sublattices J_1 and J_2 of L extends to an isometry in $Sp(2n, Z)$ if and only if*

[1] This research was partially supported by the National Science Foundation through grant GP-6663.

(i) *it preserves the symplectic form* Φ

(ii) *it preserves the divisor of each vector in* J_1.

Although the proof will be given for Z-modules, it immediately generalizes to R-modules with R any principal ideal domain.

1. Preliminaries

We recall first some results about L and $Sp(2n, Z)$. Denote by $\langle \alpha_1, \alpha_2, \cdots, \alpha_r \rangle$ the sublattice of L spanned over Z by the vectors α_i. The vectors α and β in L are said to be *orthogonal* if $\alpha \cdot \beta = 0$. The notation $L = J \oplus K$ indicates that L is the orthogonal sum of the two sublattices J and K. We may decompose L into the orthogonal sum of binary sublattices (Bourbaki [1, p. 79]):

$$L = \langle \lambda_1, \mu_1 \rangle \oplus \langle \lambda_2, \mu_2 \rangle \oplus \cdots \oplus \langle \lambda_n, \mu_n \rangle$$

where $\lambda_i \cdot \mu_i = 1$, $1 \leqq i \leqq n$. The vectors λ_i, μ_i form a symplectic basis of L. More than this, any chosen primitive vector in L may be taken as λ_1. In fact any pair $\lambda, \mu \in L$ where $\lambda \cdot \mu = 1$, may be split off into an orthogonal component of L

$$L = \langle \lambda, \mu \rangle \oplus J.$$

For fixed primitive $\tau \in L$, we denote by φ_τ the mapping

$$\varphi_\tau(\alpha) = \alpha + (\tau \cdot \alpha)\tau.$$

Then $\varphi_\tau \in Sp(2n, Z)$; in fact, although we do not need this, $\varphi_\tau(\tau \in L)$ generate the symplectic modular group. Notice, for $t \in Z$,

$$\varphi_\tau^t(\alpha) = \alpha + t(\tau \cdot \alpha)\tau.$$

The following lemma establishes the theorem in the case where the rank of J_1 (and J_2) is one.

LEMMA. *Let α and β be two vectors in L with the same divisor. Then there exists an isometry $\varphi \in Sp(2n, Z)$ such that*

$$\varphi(\alpha) = \beta.$$

PROOF. By linearity it suffices to consider the case where α and β are primitive vectors. Take two symplectic bases of L, one with α as the first basis vector, the other with β as the first vector. The mapping which takes the j-th vector in the first basis into the j-th vector in the second basis, $1 \leqq j \leqq 2n$, is the desired isometry.

A general consideration of transitivity in symplectic forms, not necessarily unimodular, is given in James [4].

https://doi.org/10.1017/S1446788700007333 Published online by Cambridge University Press

2. Proof of the theorem

We start by making a few simplifications.

It suffices to consider the case where J_1 and J_2 are primitive sublattices of L. That is, if $\alpha \in J_1$ is primitive in J_1, then α is also primitive in L. For suppose $\alpha \in J_1$ may be written $\alpha = d\beta$ with $\beta \in L$. By condition (ii) of the theorem $\Theta(\alpha)$ is of the form $d\gamma, \gamma \in L$. We may therefore extend Θ to β by defining $\Theta(\beta) = \gamma$. We shall therefore assume in future that J_1 and J_2 are primitive.

Since J_1 is a symplectic lattice, it has a basis $\xi_i, \eta_i, \zeta_j, 1 \leqq i \leqq s, 1 \leqq j \leqq t$, such that $\xi_i \cdot \eta_i = a_i$ and all other products are zero. Furthermore each a_i divides a_{i+1}. We may make a further simplification if $a_1 = 1$. For then we have

$$L = \langle \xi_1, \eta_1 \rangle \oplus K_1 = \langle \Theta(\xi_1), \Theta(\eta_1) \rangle \oplus K_2.$$

Since K_1 and K_2 have the same rank, there is an obvious isometry of L mapping ξ_1, η_1 and K_1 into $\Theta(\xi_1), \Theta(\eta_1)$ and K_2, respectively. We may therefore assume $\Theta(\xi_1) = \xi_1$ and $\Theta(\eta_1) = \eta_1$. The remaining basis vectors of J_1 and J_2 are in the orthogonal complement of $\langle \xi_1, \eta_1 \rangle$. In this case we complete the proof by induction on the rank of J_1. We therefore assume that for no vectors ξ and η in J_1 is $\xi \cdot \eta = 1$.

We now outline the method of proof. We first relabel any vectors of the type ζ_j in the basis of J_1 alternately as ξ_i and η_i; thus $\zeta_1 = \xi_{s+1}$, $\zeta_2 = \eta_{s+1}, \zeta_1 = \xi_{s+2}, \cdots$. Then

$$\xi_{s+i} \cdot \eta_{s+i} = a_{s+i} = 0.$$

(If the rank of J_1 is odd the last ξ_i will have no mate η_i). Then, including these new a_{s+i}, we have

$$(a_1, a_2, a_3, \cdots) = a_1 > 1. \tag{1}$$

We shall show that L has a symplectic basis $\lambda_i, \mu_i, 1 \leqq i \leqq n$, such that

$$\xi_i = \lambda_i, \qquad 1 \leqq i \leqq m,$$

and

$$\eta_i = a_i \mu_i + \lambda_{m+i}, \qquad 1 \leqq i \leqq m \text{ (or } m-1).$$

Having done this the proof of the theorem is simple, for if we embed $\Theta(\xi_i)$, $\Theta(\eta_i)$ in a similar symplectic basis λ'_i, μ'_i of L, the isometry $\varphi(\lambda_i) = \lambda'_i$, $\varphi(\mu_i) = \mu'_i$, $1 \leqq i \leqq n$, will map J_1 onto J_2.

We now show how to construct the basis λ_i, μ_i. It will suffice to show that an isometric image $\psi(J_1) = \langle \psi(\xi_1), \psi(\eta_1), \cdots \rangle$, with $\psi \in Sp(2n, Z)$, has such a basis, for applying the inverse isometry ψ^{-1} we transform the basis obtained for $\psi(J_1)$ into the basis required for J_1.

We shall use induction. Let λ_i, μ_i be a symplectic basis for L. Suppose that

$$\xi_i = \lambda_i, \quad \eta_i = a_i\mu_i + \lambda_{m+i} \tag{2}$$

for $1 \leqq i \leqq r$. We shall explain how to put ξ_{r+1} and η_{r+1} into this form.

Let

$$L_r = \langle\lambda_1, \mu_1\rangle \oplus \cdots \oplus \langle\lambda_r, \mu_r\rangle \oplus \langle\lambda_{m+1}, \mu_{m+1}\rangle \oplus \cdots \oplus \langle\lambda_{m+r}, \mu_{m+r}\rangle$$

so that $L = L_r \oplus U$, where U is the orthogonal complement of L_r. We show first that ξ_{r+1} has a component in U. Suppose on the contrary that

$$\xi_{r+1} = \sum_{i=1}^{r} (x_i\lambda_i + y_i\mu_i + u_i\lambda_{m+i} + v_i\mu_{m+i}) \in L_r.$$

Then, since $\xi_{r+1} \cdot \xi_i = \xi_{r+1} \cdot \eta_i = 0$ for $1 \leqq i \leqq r$, we have, using (2), $y_i = 0$ and $v_i = a_i x_i$. Now consider

$$\xi_{r+1} - \sum_{i=1}^{r} (x_i\xi_i + u_i\eta_i) = \sum_{i=1}^{r} (-a_i u_i \mu_i + a_i x_i \mu_{m+i}).$$

The left hand side is a primitive vector since J_1 is primitive, but the vector on the right hand side has divisor at least $a_1 > 1$ by (1). This contradiction means that ξ_{r+1} must have a component in U, which after applying an isometry in U (as in the lemma), we may assume to be $u\lambda_{r+1}$. Thus ξ_{r+1} has the form

$$\xi_{r+1} = \sum_{i=1}^{r} (x_i\lambda_i + u_i\lambda_{m+i} + a_i x_i \mu_{m+i}) + u\lambda_{r+1}. \tag{3}$$

Moreover, $\xi_{r+1} - \sum_{i=1}^{r} (x_i\xi_i + u_i\eta_i)$ is primitive, since J_1 is a primitive sublattice, so that

$$(a_1x_1, \cdots, a_rx_r, a_1u_1, \cdots, a_ru_r, u) = 1. \tag{4}$$

We shall now apply isometries to L that leave ξ_i, η_i, $1 \leqq i \leqq r$, invariant, but transform ξ_{r+1} into λ_{r+1}. We first transform ξ_{r+1} into the form (3) with $u = 1$. Let

$$\sigma_i = \mu_{r+1} + \lambda_{m+i}, \qquad 1 \leqq i \leqq r,$$

and

$$\tau_i = \mu_{r+1} + \lambda_i + a_i\mu_{m+i}, \qquad 1 \leqq i \leqq r.$$

Then $\sigma_i \cdot \xi_j = \sigma_i \cdot \eta_j = \tau_i \cdot \xi_j = \tau_i \cdot \eta_j = 0$ for $1 \leqq i, j \leqq r$. Hence φ_{σ_i} and φ_{τ_i} leave all the vectors ξ_j, η_j invariant, $1 \leqq i, j \leqq r$. However,

$$\begin{aligned} \varphi_{\sigma_i}(\xi_{r+1}) &= \xi_{r+1} + (\sigma_i \cdot \xi_{r+1})\sigma_i \\ &= \xi_{r+1} + (a_i x_i - u)\sigma_i. \end{aligned}$$

The component of $\varphi_{\sigma_i}(\xi_{r+1})$ in $H_{r+1} = \langle \lambda_{r+1}, \mu_{r+1} \rangle$ is $u\lambda_{r+1} + (a_i x_i - u)\mu_{r+1}$. By applying the lemma in H_{r+1} we may map this into $u'\lambda_{r+1}$ where $u' = (u, a_i x_i - u)$, so that u' divides $a_i x_i$. We do this for all σ_i, $1 \leqq i \leqq r$, in turn. Similarly

$$\begin{aligned} \varphi_{\tau_i}(\xi_{r+1}) &= \xi_{r+1} + (\tau_i \cdot \xi_{r+1})\tau_i \\ &= \xi_{r+1} - (u + a_i u_i)\tau_i. \end{aligned}$$

The component of $\varphi_{\tau_i}(\xi_{r+1})$ in H_{r+1} is $u\lambda_{r+1} - (u + a_i u_i)\mu_{r+1}$, so that as above we may replace u with a new u' dividing $a_i u_i$. It now follows from (4) that $u = 1$ (or $u = -1$, which we can easily transform to $u = 1$).

We now show how, by a similar argument, to reduce the coefficients x_i, u_i in (3) to zero. First put

$$\pi_i = \lambda_{m+i} + (u_i + a_i x_i)\mu_{r+1}, \qquad 1 \leqq i \leqq r,$$

and apply the isometry φ_{π_i}. Again, since $\pi_i \cdot \xi_j = \pi_i \cdot \eta_j = 0$ for $1 \leqq i$, $j \leqq r$, ξ_j and η_j are left invariant by φ_{π_i}. However,

$$\varphi_{\pi_i}(\xi_{r+1}) = \xi_{r+1} - u_i \pi_i,$$

so that the coefficient of λ_{m+i} in $\varphi_{\pi_i}(\xi_{r+1})$ is zero. The component of $\varphi_{\pi_i}(\xi_{r+1})$ in H_{r+1}, namely $\lambda_{r+1} - u_i(u_i + a_i x_i)\mu_{r+1}$, may be restored to λ_{r+1} by an isometry as in the lemma. Thus each of the u_i in (3) may, in turn, be reduced to zero.

Finally, put

$$\rho_i = \lambda_i + a_i \mu_{m+i} + x_i \mu_{r+1}, \qquad 1 \leqq i \leqq r,$$

and apply φ_{ρ_i}. As before ξ_j, η_j, $1 \leqq j \leqq r$, are invariant, but now

$$\varphi_{\rho_i}(\xi_{r+1}) = \xi_{r+1} - x_i \rho_i.$$

The coefficients of both λ_i and μ_{m+i} are now zero. We have therefore succeeded in mapping ξ_{r+1} into λ_{r+1}.

We now consider η_{r+1}. We show first that $\eta_{r+1} \notin L_r \oplus H_{r+1}$. For if

$$\eta_{r+1} = \sum_{i=1}^{r} (x_i \lambda_i + y_i \mu_i + u_i \lambda_{m+i} + v_i \mu_{m+i}) + u\lambda_{r+1} + v\mu_{r+1},$$

using the various orthogonality conditions on η_{r+1}, we obtain $y_i = 0$, $v_i = a_i x_i$ and $v = a_{r+1}$. Then as before

$$\eta_{r+1} - \sum_{i=1}^{r} (x_i \xi_i + u_i \eta_i) - u\xi_{r+1} = \sum_{i=1}^{r} (-a_i u_i \mu_i + a_i x_i \mu_{m+i}) + a_{r+1}\mu_{r+1}$$

leads to a contradiction. Therefore we may assume (again using the lemma)

$$\eta_{r+1} = \sum_{i=1}^{r} (x_i \lambda_i + u_i \lambda_{m+i} + a_i x_i \mu_{m+i}) + u\lambda_{r+1} + a_{r+1}\mu_{r+1} + v\lambda_{m+r+1}.$$

We proceed as before, first reducing v to 1, and then the coefficients u, x_i and u_i to zero. Since $\eta_{r+1}-\sum_{i=1}^{r}(x_i\xi_i+u_i\eta_i)-u\xi_{r+1}$ is primitive, we obtain

$$(a_1x_1, \cdots, a_rx_r, a_1u_1, \cdots, a_ru_r, a_{r+1}, v) = 1. \tag{5}$$

First let $\sigma = \mu_{m+r+1}+\lambda_{r+1}$ and apply φ_σ. Then φ_σ leaves ξ_i, $1 \leqq i \leqq r+1$, and η_j, $1 \leqq j \leqq r$, invariant. But

$$\varphi_\sigma(\eta_{r+1}) = \eta_{r+1}+(a_{r+1}-v)\sigma,$$

so that by the usual argument, we replace v by v' with v' dividing a_{r+1}. As in the discussion with ξ_{r+1} (after replacing μ_{r+1} by μ_{m+r+1} in the definitions of σ_i and τ_i), v may be further assumed to divide each of a_ix_i and a_iu_i, $1 \leqq i \leqq r$, so that by (5) we must have $v = 1$.

Now let $\pi = \lambda_{r+1}+(a_{r+1}+u)\mu_{m+r+1}$. Then φ_π leaves each of ξ_i, $1 \leqq i \leqq r+1$, and η_j, $1 \leqq j \leqq r$, invariant. However,

$$\varphi_\pi(\eta_{r+1}) = \eta_{r+1}-u\pi,$$

so that the coefficient of λ_{r+1} in $\varphi_\pi(\eta_{r+1})$ becomes zero. As with ξ_{r+1}, we may reduce in turn, all the coefficients x_i and u_i in η_{r+1} to zero. We have therefore succeeded in mapping η_{r+1} into the desired form $a_{r+1}|\mu_{r+1}+\lambda_{m+r+1}$.

This completes the inductive construction of ξ_i and η_i. Of course, if the rank of J_1 is odd, we stop after constructing ξ_m. The construction given above also includes, as a special case, the construction of $\xi_1 = \lambda_1$ and $\eta_1 = a_1\mu_1+\lambda_{m+1}$, to start the induction. As mentioned before, the embedding of an isometric image of J_1 in this form makes the proof of the theorem trivial.

References

[1] Bourbaki, *Algèbre* ch. 9, (Hermann, Paris, 1959).

[2] J. Dieudonné, *La géométrie des groupes classiques*, (Springer-Verlag, Berlin, 1963).

[3] D. G. James, 'Integral invariants for vectors over local fields', *Pac. J. Math.* 15 (1965), 905—916.

[4] D. G. James, 'Transitivity in integral symplectic forms', *J. Aust. Math. Soc.* 8 (1968), 43—48.

[5] O. T. O'Meara, 'Quadratic forms over local fields', *Amer. J. Math.* 77 (1955), 87—116.

[6] E. Witt, 'Theorie der quadratischen Formen in beliebigen Körpern', *J. reine angew. Math.* 176 (1937), 31—44.

The Pennsylvania State University