

TRANSITIVITY IN INTEGRAL SYMPLECTIC FORMS

D. G. JAMES

(Received 1 June 1966)

A *symplectic lattice* L is a free Z -module of finite rank endowed with a non-degenerate alternating bilinear form. Thus we have a bilinear mapping Φ of $L \times L$ into the domain of integers Z ; we denote $\Phi(\alpha, \beta)$ by $\alpha \cdot \beta$ (where $\alpha, \beta \in L$). Then $\alpha^2 = 0$ and $\alpha \cdot \beta = -\beta \cdot \alpha$.

The *symplectic group* $\text{Sp}(L, Z)$ is the group of all automorphisms ϕ of L such that $\phi(\alpha) \cdot \phi(\beta) = \alpha \cdot \beta$ for all α, β in L . The purpose of this note is to give necessary and sufficient conditions on vectors α and β for there to exist an automorphism ϕ of $\text{Sp}(L, Z)$ such that $\phi(\alpha) = \beta$. If such an automorphism exists we write $\alpha \sim \beta$ and call α and β *associated vectors*. The group $\text{Sp}(L, Z)$ will act transitively on the equivalence class of α .

Although the results will be given for lattices over Z , they may be immediately interpreted for any principal ideal domain. Similar results for orthogonal groups over the p -adic integers have been obtained by S. Rosenzweig and the author [2], and for unimodular quadratic forms by Wall [5]. See also Kneser [3] for results on the representation of integers by quadratic forms. For the local integral structure of the symplectic group see Riehm [4].

We describe first the (well known) structure of the lattice L . Then, after investigating invariants of a typical vector α in L , we shall give the conditions for α and β to be associated.

We say that α and β are *orthogonal* if $\alpha \cdot \beta = 0$. Write $L = L_1 \oplus L_2$ if L is the direct sum of two sublattices L_1 and L_2 with α in L_1 orthogonal to all β in L_2 . We shall call this an *orthogonal splitting* of L (with two components). $\langle \lambda, \mu \rangle$ denotes the sublattice $\{l\lambda + m\mu \mid l, m \in Z\}$.

LEMMA 1. *The lattice L has an orthogonal splitting*

$$L = \langle \lambda, \mu \rangle \oplus L_1$$

if and only if $\lambda \cdot \mu = q$ and q divides $\lambda \cdot \alpha$ and $\mu \cdot \alpha$ for all α in L .

PROOF. The necessity of the conditions is immediate. Suppose now that the conditions are satisfied. Then, for arbitrary α in L , we can write

$$\begin{aligned} \alpha &= q^{-1}(\alpha \cdot \mu)\lambda - q^{-1}(\alpha \cdot \lambda)\mu + \beta \\ \beta &= \alpha - q^{-1}(\alpha \cdot \mu)\lambda + q^{-1}(\alpha \cdot \lambda)\mu \in L. \end{aligned}$$

where

Then $\beta \cdot \lambda = \beta \cdot \mu = 0$. Let L_1 be the sublattice of all β in L orthogonal to λ and μ . The result is now clear.

We call a sublattice $\langle \lambda, \mu \rangle$ as in the lemma a *q-modular hyperbolic plane* and denote it by H_q . A sublattice M of L is called *q-modular* if it is the orthogonal sum of *q-modular hyperbolic planes* of L .

PROPOSITION 1. *A symplectic lattice L has an orthogonal splitting*

$$L = L_1 \oplus L_2 \oplus \cdots \oplus L_n$$

where each L_i , $1 \leq i \leq n$, is a q_i -modular sublattice. Furthermore $q_i \mid q_{i+1}$, $1 \leq i \leq n-1$, and with the condition $q_{i+1} \neq q_i$, the q_i and the rank of each L_i are invariants of L .

PROOF. A splitting of the given type can be easily obtained with the help of the lemma; see Bourbaki [1, § 5]. The q_i (with multiplicities) are the invariants of the abelian group defined as the quotient of $\text{Hom}(L, Z)$ by the subgroup of homomorphisms of the form $\mu \rightarrow \lambda \cdot \mu$. I wish to thank the referee for this observation.

COROLLARY 1. *The rank of L is even.*

COROLLARY 2. *We can take λ_{ij}, μ_{ij} , $1 \leq j \leq n_i = \frac{1}{2} \text{rank } L_i$, $1 \leq i \leq n$, as a basis for L , where $\lambda_{ij} \cdot \mu_{ij} = q_i$ and all other products are zero.*

A basis as in Corollary 2 is called a *symplectic basis*.

We shall now investigate conditions on α and β for them to be associated. α in L is called *imprimitive* if $\alpha = d\gamma$ where $\gamma \in L$ and $d (\neq \pm 1)$ is an integer. Otherwise α is said to be *primitive*. It suffices in future to consider α and β primitive since the automorphisms are linear transformations on L .

A primitive vector α is called *q-modular* if it can be embedded in a *q-modular hyperbolic plane*. We now obtain a decomposition of a general vector α into the orthogonal sum of modular vectors.

For the rest of this note $a \mid b$ shall mean *a divides b* and $|a| \neq |b|$.

LEMMA 2. *If M is a q-modular sublattice of L and $\eta \in M$ is primitive, then η is q-modular (and can be taken as the leading element in a symplectic basis of M).*

PROOF. Let λ_j, μ_j , $1 \leq j \leq m$, be a symplectic basis for M . Then

$$\eta = \sum_{j=1}^m (a_j \lambda_j + b_j \mu_j)$$

with $(a_1, \dots, a_m, b_1, \dots, b_m) = 1$. Hence there exist integers x_j, y_j such that

$$\sum_{j=1}^m (a_j x_j - b_j y_j) = 1.$$

Put

$$\xi = \sum_{j=1}^m (y_j \lambda_j + x_j \mu_j) \in M$$

so that $\eta \cdot \xi = q$. Using Lemma 1 we can now split off a q -modular hyperbolic plane $\langle \eta, \xi \rangle$. η is thus a q -modular vector.

PROPOSITION 2. Any $\alpha (\neq 0)$ in L can be written in the form

$$\alpha = \sum_{i=1}^t r_i \alpha_i,$$

where $\alpha_i, 1 \leq i \leq t$ (with $1 \leq t \leq n$), are p_i -modular mutually orthogonal vectors, such that

$$r_{i+1} | r_i \text{ and } r_i p_i | r_{i+1} p_{i+1} \quad 1 \leq i \leq t-1.$$

PROOF. Take an orthogonal splitting of L , as in Proposition 1, and write $\alpha = a_1 \eta_1 + \dots + a_n \eta_n$ where $\eta_i \in L_i, 1 \leq i \leq n$, are primitive vectors. By Lemma 2 they are q_i -modular, η_i being embedded in $\langle \eta_i, \xi_i \rangle$ with $\eta_i \cdot \xi_i = q_i$.

By a previous remark it suffices to consider α primitive, so that $r_i = 1$. We shall consider first the special case $n = 2$. Write

$$\alpha = r d_1 \eta_1 + d_2 \eta_2$$

where $(r d_1, d_2) = 1$ and r is maximal with the property $r q_1 s = q_2 (s \in \mathbb{Z})$. Put

$$\begin{aligned} \alpha_1 &= d_1 \eta_1 + d_2 s \xi_1 - d_1 \xi_2 \\ \alpha_2 &= d_2 \eta_2 - d_2 r s \xi_1 + d_1 r \xi_2. \end{aligned}$$

Then $\alpha = r \alpha_1 + \alpha_2$ and $\alpha_1 \cdot \alpha_2 = 0, \alpha_1$ is q_1 -modular and α_2 is q_2 -modular. Since, by choice of $r, (d_1, d_2 s) = 1$, there exist integers x and y such that $x d_2 s - y d_1 = 1$. Put

$$\gamma_1 = x \eta_1 + y \xi_1 - x \xi_2.$$

Then $\gamma_1 \cdot \alpha_1 = q_1$ and $\gamma_1 \cdot \alpha_2 = 0$, so that, by Lemma 1

$$\langle \eta_1, \xi_1 \rangle \oplus \langle \eta_2, \xi_2 \rangle = \langle \gamma_1, \alpha_1 \rangle \oplus H.$$

But $\alpha_2 \in H$, so that by Lemma 2 we have $H = \langle \gamma_2, \alpha_2 \rangle$. The proof is now complete in this case except for the two possibilities

(i) $r = 1$: but now $\alpha_1 + \alpha_2$ is q_1 -modular, since it can be embedded in the hyperbolic plane $\langle \gamma_1, \alpha_1 + \alpha_2 \rangle$;

(ii) $s = 1$: and now $r = q_2 q_1^{-1}$, so that $r \alpha_1 + \alpha_2$ is q_2 -modular, being embedded in $\langle \gamma_2, \alpha_2 + r \alpha_1 \rangle$.

We now consider the general case. Write

$$\alpha = a_1\eta_1 + \dots + a_n\eta_n$$

where η_i are q_i -modular vectors in L_i . Applying the case $n = 2$ to $a_1\eta_1 + a_2\eta_2$ we can reduce it to the form $s_1\beta_1 + c_2\gamma_2$ where $c_2 = (a_1, a_2)$, s_1q_1 divides c_2q_2 and c_2 divides s_1 . In the same manner reduce $c_2\gamma_2 + a_3\eta_3$ to the form $s_2\beta_2 + c_3\gamma_3$ where $c_3 = (c_2, a_3)$, s_2q_2 divides c_3q_3 and s_2 divides c_2 and hence s_1 . Proceeding in this manner we reduce α to the form

$$\alpha = s_1\beta_1 + \dots + s_n\beta_n$$

where s_{i+1} divides s_i , $1 \leq i \leq n-1$.

However, we need not have $s_iq_i | s_{i+1}q_{i+1}$. This can be achieved by further applications of the case $n = 2$. Put $r_n = s_n$. Starting now with $s_{n-1}\beta_{n-1} + r_n\beta_n$ we may change it to $r_{n-1}\delta_{n-1} + r_n\alpha_n$ with $r_{n-1}q_{n-1} | r_nq_n$ (absorbing $r_{n-1}\delta_{n-1}$ in $r_n\alpha_n$ if $r_{n-1}q_{n-1} = r_nq_n$). The relation s_{n-1} divides s_{n-2} will become r_{n-1} divides s_{n-2} since r_{n-1} divides s_{n-1} . Proceed now with $s_{n-2}\beta_{n-2} + r_{n-1}\delta_{n-1}$.

If $r_i = r_{i+1}$ for any i , $\alpha_i + \alpha_{i+1}$ is q_i -modular, so that the $i+1$ -component may be absorbed in the i -component. The proof is now complete, the β_i being a subset of the q_i .

Let $L(\beta)$ be the set of all β -modular vectors in L ; hence for $\beta \in L(\beta)$ we have that $\beta \cdot \gamma$ is divisible by β , for any γ in L . Denote by $\nu(\beta, \alpha)$ the greatest common divisor of $\alpha \cdot \gamma$ as γ varies over $L(\beta)$.

LEMMA 3. If $\alpha = \sum_{i=1}^t r_i\alpha_i$ as in Proposition 2, then

$$\nu(\beta_i, \alpha) = r_i\beta_i, \quad 1 \leq i \leq t.$$

PROOF. If we multiply α by γ in $L(\beta_i)$ the terms $r_j\gamma \cdot \alpha_j$, $1 \leq j \leq i$, are divisible by $r_j\beta_i$, and hence by $r_i\beta_i$; while the terms $r_j\gamma \cdot \alpha_j$, $i < j \leq t$, are divisible by $r_j\beta_j$, which in turn is divisible by $r_i\beta_i$. Thus $r_i\beta_i \leq \nu(\beta_i, \alpha)$. On the other hand, Lemma 2 shows there exists $\xi_i \in L(\beta_i)$ such that $\alpha_i \cdot \xi_i = \beta_i$ and $\alpha_j \cdot \xi_i = 0$ ($j \neq i$). Thus $\nu(\beta_i, \alpha) \leq \alpha \cdot \xi_i = r_i\beta_i$. This proves the lemma.

It is clear from this lemma that the r_i of any α are uniquely determined by the β_i . However, the β_i as they stand need not be invariant, except in the case where the q_i are all powers of the same prime. (For example, if $r_2\beta_2 = (r_1\beta_2, r_3\beta_3)$, the term $r_2\alpha_2$ can be removed.) By placing further restrictions on the choice of β_i an invariant set can be obtained, for example as follows.

Consider all the decompositions of $\alpha = \sum r_i\alpha_i$ as in Proposition 2. Restrict consideration now to those with maximal β_1 , which now becomes an invariant of α . Amongst these decompositions we now restrict our attention to those with β_2 maximal. In general, after choosing β_i , we take β_{i+1} maximal. We therefore arrive finally at an uniquely determined set

of p_i and hence also r_i . We shall consider these p_i and r_i as the invariants of α .

An alternative method of characterizing an invariant set of p_i for α would be to make p_1 minimal, then p_2 minimal, and so on. Any such choice of invariants is sufficient; in fact for α and β to be associated it suffices for them to have decompositions with the same p_i and r_i .

THEOREM. $\alpha \sim \beta$ if and only if α and β have the same invariants r_i and p_i , $1 \leq i \leq t$.

PROOF. The necessity of these invariants is clear from Proposition 3; an automorphism will preserve the invariants. Consider now α and β with the same invariants

$$\begin{aligned} \alpha &= r_1\alpha_1 + \cdots + r_t\alpha_t \\ \beta &= r_1\beta_1 + \cdots + r_t\beta_t \end{aligned}$$

where α_i and β_i are p_i -modular vectors, $1 \leq i \leq t$. We can embed the α_i in mutually orthogonal hyperbolic planes $\langle \alpha_i, \gamma_i \rangle = H_{p_i}$, so that we get an orthogonal splitting of L

$$L = H_{p_1} \oplus \cdots \oplus H_{p_t} \oplus J.$$

Similarly we can embed β_i in $\langle \beta_i, \delta_i \rangle = H_{p_i}^*$ and get another splitting of L

$$L = H_{p_1}^* \oplus \cdots \oplus H_{p_t}^* \oplus J^*.$$

From the invariance of rank L_i in an orthogonal splitting of L , the invariants of J and J^* must be the same. Thus they split in the same manner into modular hyperbolic planes. We now take the automorphism ϕ in $\text{Sp}(L, Z)$ with $\phi(\alpha_i) = \beta_i$, $\phi(\gamma_i) = \delta_i$, $1 \leq i \leq t$, and extend it to L , in the obvious way, through corresponding hyperbolic planes in J and J^* . Then $\phi(\alpha) = \beta$ and the theorem is established.

Note added in proof. We originally expected that the p_i in Proposition 2 would be global invariants of α (as they are in the local case, compare [2]); but this is not the case. We have shown above how an invariant subset of p_i can be obtained by imposing maximal conditions. It would be desirable to have algebraic conditions that would ensure this. For example we must have $r_2 p_2 | (r_1 p_2, r_3 p_3)$, but this is not enough. Moreover, the conditions appear to depend on L (the q_i) and not only α . One should also be able to prove that if α and β are associated locally at all primes, then they are globally associated.

References

[1] N. Bourbaki, *Algèbre*, Ch. 9 (Hermann, Paris, 1959).
 [2] D. G. James, 'Integral invariants for vectors over local fields', *Pac. J. Math.* 15 (1965), 905–916.

- [3] M. Kneser, 'Darstellungsmasse indefiniter quadratischer Formen', *Math. Z.* 77 (1961), 188—194.
- [4] Carl R. Riehm, 'The structure of the symplectic group over a valuation ring', *Amer. J. Math.* 88 (1966), 106—128.
- [5] C. T. C. Wall, 'On the orthogonal group of unimodular quadratic forms', *Math. Ann.* 147 (1962), 328—338.

The Pennsylvania State University