

AN ACTION OF THE SYMPLECTIC MODULAR GROUP

LOUIS SOLOMON*

To the memory of TADASI NAKAYAMA

1. Let V be a free \mathbf{Z} -module of rank $2n$. Let $G = \mathbf{Sp}(2n, \mathbf{Z})$ be the symplectic modular group and let ϕ be the non-singular alternating bilinear form on V left invariant by G . Let $p \in \mathbf{Z}$ be a prime and let X be the set of all endomorphisms ξ of V such that

$$\phi(\xi x, \xi y) = p\phi(x, y)$$

for all $x, y \in V$. In the theory of transformation of theta functions [3] one encounters the natural action of G on X by left multiplication. The number of G orbits is known to be finite and the point of this note is a proof of the following

THEOREM. *The number of orbits of X under G is $\prod_{i=1}^n (1 + p^i)$*

The case $n=2$ is due to Hermite [2] and the case $n=3$ to Weber [4] who compute explicit sets of representatives for the orbits in these cases. The idea in the present argument is to reduce the problem to a question about the finite symplectic group $\mathbf{Sp}(2n, \mathbf{F}_p)$. In the new situation Witt's theorem is available for counting purposes. The number $\prod_{i=1}^n (1 + p^i)$ is the number of maximal totally isotropic subspaces of a $2n$ dimensional symplectic space over \mathbf{F}_p .

2. Let V be a free \mathbf{Z} -module of rank $2n$. Let $\phi: V \times V \rightarrow \mathbf{Z}$ be a non-singular alternating bilinear form on V . We assume that V has a basis v_1, \dots, v_{2n} such that the matrix of $\phi(v_i, v_j)$ is

$$J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

where I is the identity matrix of degree n . We call v_1, \dots, v_{2n} a symplectic basis for V . The symplectic modular group $\mathbf{Sp}(2n, \mathbf{Z})$ consists of all automor-

Received March 22, 1965.

* This work was supported in part by the National Science Foundation under grant GP 1452.

phisms τ of V such that $\emptyset(\tau x, \tau y) = \emptyset(x, y)$ for all $x, y \in V$. We let $\mathbf{F} = \mathbf{Z}/p\mathbf{Z}$ denote the field of p elements and set $E = V/pV$. We view E as vector space over \mathbf{F} . The form \emptyset defines, by reduction mod p , a non-singular alternating bilinear form $\Psi: E \times E \rightarrow \mathbf{F}$. Similarly, an endomorphism of $\text{Hom}_{\mathbf{Z}}(V, V)$ defines an endomorphism of $\text{Hom}_{\mathbf{F}}(E, E)$. In this way we get a homomorphism of $\mathbf{Sp}(2n, \mathbf{Z})$ into the group $\mathbf{Sp}(2n, \mathbf{F})$ of all non-singular \mathbf{F} -linear transformations of E which preserve the form Ψ . A transvection

$$\tau: v \rightarrow v + a\emptyset(v, w)w \quad w \in V, a \in \mathbf{Z}$$

of $\mathbf{Sp}(2n, \mathbf{Z})$ maps into a transvection of $\mathbf{Sp}(2n, \mathbf{F})$. Since every transvection in $\mathbf{Sp}(2n, \mathbf{F})$ may be obtained in this way by reduction mod p , and since the transvections generate $\mathbf{Sp}(2n, \mathbf{F})$ we see that the map $\mathbf{Sp}(2n, \mathbf{Z}) \rightarrow \mathbf{Sp}(2n, \mathbf{F})$ is an epimorphism. We use $x \rightarrow x^*$ as a notation for each of the reductions

$$\mathbf{Z} \rightarrow \mathbf{F}, \quad V \rightarrow E, \quad \mathbf{Sp}(2n, \mathbf{Z}) \rightarrow \mathbf{Sp}(2n, \mathbf{F})$$

modulo p . We use those facts about symplectic spaces over a field which center around Witt's theorem. These facts are proved in [1].

LEMMA 1. *Let e_1, \dots, e_{2n} be a symplectic basis for E . Then there exists a symplectic basis w_1, \dots, w_{2n} for V such that $w_i^* = e_i$.*

Proof. Let v_1, \dots, v_{2n} be a symplectic basis for V . Then v_1^*, \dots, v_{2n}^* is a symplectic basis for E . Define an \mathbf{F} -linear transformation β of E by $\beta v_i^* = e_i$. Then $\beta \in \mathbf{Sp}(2n, \mathbf{F})$ and, since $\mathbf{Sp}(2n, \mathbf{Z})$ maps onto $\mathbf{Sp}(2n, \mathbf{F})$ we may choose $\alpha \in \mathbf{Sp}(2n, \mathbf{Z})$ with $\alpha^* = \beta$. Set $w_i = \alpha v_i$. Then w_1, \dots, w_{2n} is a symplectic basis for V and $w_i^* = \alpha^* v_i^* = e_i$.

LEMMA 2. *Let $\xi \in X$. Then $\text{Ker } \xi^*$ and $\text{Im } \xi^*$ are maximal totally isotropic subspaces of E .*

Proof. If $a, b \in \text{Ker } \xi^*$ choose $x, y \in V$ with $x^* = a, y^* = b$. Then $\xi x, \xi y \in pV$ so $\xi x = px', \xi y = py'$ for some $x', y' \in V$. Then

$$p\emptyset(x, y) = \emptyset(\xi x, \xi y) = p^2\emptyset(x', y') \in p^2\mathbf{Z}$$

so $\emptyset(x, y) \in p\mathbf{Z}$ and $\Psi(a, b) = 0$. Thus $\text{Ker } \xi^*$ is totally isotropic. Similarly, if $a, b \in \text{Im } \xi^*$ write $a = \xi^* x^*, b = \xi^* y^*$ for some $x, y \in V$ and then

$$\Psi(a, b) = \emptyset(\xi x, \xi y)^* = p^*\emptyset(x, y)^* = 0$$

so that $\text{Im } \xi^*$ is totally isotropic. We must prove that $\dim \text{Ker } \xi^* = n = \dim \text{Im } \xi^*$.

Let T be the matrix for ξ in the symplectic basis v_1, \dots, v_{2n} . Since $\mathcal{O}(\xi x, \xi y) = p\mathcal{O}(x, y)$ we have $TJT^t = pJ$ where T^t denotes the transpose of T . Thus $(\det T)^2 = p^{2n}$ so $|\det \xi| = p^n$. Imbed V in the vector space $V \otimes \mathbf{Q}$ over the rational field \mathbf{Q} . Then \mathcal{O} extends to a form, denoted again \mathcal{O} , on $V \otimes \mathbf{Q}$ and ξ defines a linear transformation, denoted again ξ , of $V \otimes \mathbf{Q}$. Then $\mathcal{O}(\xi x, \xi y) = p\mathcal{O}(x, y)$ for all $x, y \in V \otimes \mathbf{Q}$. Since $\det \xi \neq 0$, ξ is invertible, and for any $x, v \in V$ we have

$$\mathcal{O}(\xi^{-1}px, v) = \mathcal{O}(\xi^{-1}px, \xi^{-1}\xi v) = p^{-1}\mathcal{O}(px, \xi v) = \mathcal{O}(x, \xi v) \in \mathbf{Z}$$

Now letting v range over a symplectic basis for V we see that $\xi^{-1}px \in V$. Thus $\xi^{-1}pV \subseteq V$, so $pV \subseteq \xi V$. Let $d_1, \dots, d_{2n} \in \mathbf{Z}$ be the elementary divisors of ξ viewed as endomorphism of V , where we choose the d_i non-negative and such that d_{i+1} divides d_i . Choose \mathbf{Z} -bases x_1, \dots, x_{2n} and y_1, \dots, y_{2n} for V so that $\xi x_i = d_i y_i$. Since $pV \subseteq \xi V$ we must have $py_i \in \mathbf{Z}d_i y_i$ so each d_i divides p . But $d_1, \dots, d_{2n} = |\det \xi| = p^n$ so we have $d_1 = \dots = d_n = p$ and $d_{n+1} = \dots = d_{2n} = 1$. Thus the elementary divisors of ξ^* are $d_1^* = \dots = d_n^* = 0$ and $d_{n+1}^* = \dots = d_{2n}^* = 1$. Thus ξ^* has rank n and hence $\dim \text{Ker } \xi^* = n = \dim \text{Im } \xi^*$. This proves the lemma.

LEMMA 3. *Suppose $\xi, \eta \in X$. If $\text{Ker } \xi^* = \text{Ker } \eta^*$ then ξ and η are in the same orbit under G .*

Proof. Lemma 2 tells us that $D = \text{Ker } \xi^*$ is a maximal totally isotropic subspace of E . The theorem on Witt decomposition of symplectic spaces over a field asserts the existence of a maximal totally isotropic subspace D' of E such that $E = D + D'$, direct sum. Furthermore there exist bases e_1, \dots, e_n for D and e_{n+1}, \dots, e_{2n} for D' such that e_1, \dots, e_{2n} is a symplectic basis for E . Lemma 1 shows the existence of a symplectic basis w_1, \dots, w_{2n} for V such that $w_i^* = e_i$. Define $\theta \in X$ by

$$\begin{aligned} \theta w_i &= pw_i & i &= 1, \dots, n \\ \theta w_i &= w_i & i &= n+1, \dots, 2n \end{aligned}$$

Then $\text{Ker } \theta^* = D$. Since $\text{Im } \xi^* = \xi^* D'$ and $\text{Im } \theta^* = \theta^* D'$ we see from Lemma 2 that $\xi^* D'$ and $\theta^* D'$ are totally isotropic subspaces of E of the same dimension

n . Define a non singular \mathbb{F} -linear transformation $\beta: \xi^*D' \rightarrow \theta^*D'$ by $\beta\xi^*e_i = \theta^*e_i$ for $i = n+1, \dots, 2n$. Since ξ^*D' and θ^*D' are totally isotropic, β is an isometry, and, by Witts theorem, may be extended to an element, denoted again β , of $\mathbf{Sp}(2n, \mathbb{F})$. Since both ξ^* and θ^* annihilate D we have $\beta\xi^*e_i = \theta^*e_i$ for all $i = 1, \dots, 2n$ so $\beta\xi^* = \theta^*$. Choose $\alpha \in \mathbf{Sp}(2n, \mathbb{Z})$ with $\alpha^* = \beta$. Then $(\alpha\xi)^* = \alpha^*\xi^* = \theta^*$. In particular $\alpha\xi w_i \in pV$ for $i = 1, \dots, n$. Define $\sigma \in \text{Hom}_{\mathbb{Z}}(V, V)$ by

$$\begin{aligned} \sigma w_i &= \frac{1}{p} \alpha \xi w_i & i = 1, \dots, n \\ \sigma w_i &= \alpha \xi w_i & i = n+1, \dots, 2n \end{aligned}$$

Then $\alpha\xi = \sigma\theta$ so

$$\mathcal{O}(\sigma\theta x, \sigma\theta y) = \mathcal{O}(\alpha\xi x, \alpha\xi y) = p\mathcal{O}(x, y) = \mathcal{O}(\theta x, \theta y)$$

for all $x, y \in V$. Since θV has finite index in V the bilinearity of \mathcal{O} implies $\mathcal{O}(\sigma x, \sigma y) = \mathcal{O}(x, y)$ for all $x, y \in V$. Now, as in the proof of Lemma 1, we conclude $\det \sigma = 1$ so that $\sigma \in G$. Thus we have shown the existence of $\alpha, \sigma \in G$ with $\alpha\xi = \sigma\theta$. Similarly there exist $\beta, \tau \in G$ with $\beta\eta = \tau\theta$. Then $\eta = \beta^{-1}\tau\sigma^{-1}\alpha\xi$ so that ξ, η lie in the same orbit under G .

PROPOSITION. *The map $\xi \rightarrow \text{Ker } \xi^*$ induces a one to one correspondence between orbits of X under G and maximal totally isotropic subspaces of E .*

Proof. If $\xi, \eta \in X$ lie in the same orbit, say $\xi = \tau\eta$ with $\tau \in \mathbf{Sp}(2n, \mathbb{Z})$. Then $\xi^* = \tau^*\eta^*$. Since $\tau^* \in \mathbf{Sp}(2n, \mathbb{F})$ is non-singular we have $\text{Ker } \xi^* = \text{Ker } \eta^*$. Thus $\xi \rightarrow \text{Ker } \xi^*$ induces a map of orbits into the set of maximal totally isotropic subspaces of E . By Lemma 3 the map is one to one. To see that every maximal totally isotropic subspace D occurs as a kernel of some ξ^* , construct a Witt decomposition $E = D + D'$ as in the proof of Lemma 3, and note that the element $\theta \in X$ satisfies $\text{Ker } \theta^* = D$. This completes the proof.

3. We have thus reduced the problem to computing the number t of maximal totally isotropic subspaces of a $2n$ dimensional symplectic space over \mathbb{F} . The finite group $\mathbf{Sp}(2n, \mathbb{F})$ acts as a permutation group on the set of maximal totally isotropic subspaces of E . By Witt's theorem this permutation group is transitive, hence

$$t = |G : H|$$

where H is the group of all $\gamma \in \mathbf{Sp}(2n, \mathbf{F})$ which leave globally invariant a given maximal totally isotropic subspace D . The restriction map $\gamma \rightarrow \gamma|D$ defines a homomorphism of H into the full linear group $\mathbf{GL}(D) = \mathbf{GL}(n, \mathbf{F})$. By Witt's theorem this is an epimorphism. The kernel K consists of those elements of $\mathbf{Sp}(2n, \mathbf{F})$ which fix D . It is known, and it is easy to compute directly, that K is isomorphic to the additive group of $n \times n$ symmetric matrices over \mathbf{F} so that K has order $|K| = p^{n(n+1)/2}$. Thus

$$t = |\mathbf{Sp}(2n, \mathbf{F})| |\mathbf{GL}(n, \mathbf{F})|^{-1} p^{-n(n+1)/2}$$

If we insert the known formulas

$$|\mathbf{Sp}(2n, \mathbf{F})| = p^{n^2} \prod_{i=1}^n (p^{2i} - 1)$$

$$|\mathbf{GL}(n, \mathbf{F})| = p^{n(n-1)/2} \prod_{i=1}^n (p^i - 1)$$

we find

$$t = \prod_{i=1}^n (1 + p^i)$$

This proves the theorem.

REFERENCES

- [1] E. Artin, *Geometric Algebra*, Interscience, New York (1957).
- [2] C. Hermite, Sur la théorie de la transformation des fonctions abéliennes, *Comptes Rendus* **40** (1855), 249-254.
- [3] A. Krazer, *Lehrbuch der Thetafunktionen*, Teubner, Leipzig (1903).
- [4] H. Weber, Über die Transformationstheorie der Thetafunktionen, insbesondere derer von drei Veränderlichen, *Annali di mat.*, Ser. 2, **9** (1879), 126-166.

The Rockefeller Institute,
New York 21, N.Y.

