TWO-ELEMENT GENERATION OF THE SYMPLECTIC GROUP(1)

BY

PETER STANEK

1. **Introduction.** Several authors have discussed the problem of finding pairs of generators for the known simple groups of finite, composite order (see [1; 2; 7; 8; 9]). In this paper we examine the symplectic group, the group of all $2n$ by $2n$ matrices, X, with entries from $\mathrm{GF}(q)$, which satisfy

$$(1) \qquad XHX^T = H, \qquad H = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}, \qquad X^T = X \text{ transpose},$$

0 and I the zero and identity matrices, respectively. We denote this group by $\mathrm{Sp}(2n,q)$, and by $\mathrm{PSp}(2n, q)$ the factor group of $\mathrm{Sp}(2n,q)$ by its center, $\{\pm I\}$. $\mathrm{PSp}(2n,q)$ is a simple group of order

$$\frac{1}{d} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1),$$

d the g.c.d. of 2 and $q - 1$, except for $\mathrm{PSp}(2,2) = S_3$, $\mathrm{PSp}(2,3) = A_4$, $\mathrm{PSp}(4,2) = S_6$ (see [4; 5]). We prove

THEOREM. *The group* $\mathrm{PSp}(2n, q)$, *for* $n \geqq 3$, *has two generators, one of period* (*group order*) *two.*

In [1] the corresponding result is proved for the projective unimodular group. In [8] it is proved that $\mathrm{PSp}(2n,q)$, q a prime, is generated by two of its elements, while in [9] this is proved for all of the known simple finite groups other than the alternating and Mathieu groups.

For $q = 2$, T. G. Room [7], has proved this theorem. The result has certain geometric implications [3].

2. **Known generators of the symplectic group.** The following is originally due to Dickson [4]. The form in which we state it is convenient for our purposes; and, for a proof, that of Hua and Reiner [6], may be easily modified.

LEMMA 1. $\mathrm{Sp}(2n,q)$ *is generated by the following matrices*:

(i) *translations*

Received by the editors August 21, 1962.

(1) This work is in part an excerpt from the author's doctoral thesis, supported by NSF grant G-9504. I am greatly indebted to Professor A. A. Albert for suggesting the problem and giving valuable criticism.

$$T = \begin{pmatrix} I & S \\ 0 & I \end{pmatrix}, \qquad S^T = S;$$

(ii) *rotations*

$$R = \begin{pmatrix} U & 0 \\ 0 & (U^T)^{-1} \end{pmatrix}, \qquad \det U \neq 0;$$

(iii) *semi-involutions*

$$S = \begin{pmatrix} Q & I - Q \\ Q - I & Q \end{pmatrix},$$

where Q is a diagonal matrix of zeros and ones.

In all of what follows, E_{ij} will be the n by n matrix with a one in the ijth position and zero elsewhere.

For $x \in \mathrm{GF}(q)$, define

$$T_i(x) = \begin{pmatrix} I & xE_{ii} \\ 0 & I \end{pmatrix};$$

$$T_{ij}(x) = \begin{pmatrix} I & xE_{ij} + xE_{ji} \\ 0 & I \end{pmatrix};$$

$$R_{ij}(x) = \begin{pmatrix} I + xE_{ij} & 0 \\ 0 & I - xE_{ji} \end{pmatrix};$$

for $i \neq j$. The T's commute, while the rotations satisfy $(R_{ij}(x))^{-1} = R_{ij}(-x)$, $(R_{ij}(x), R_{jk}(y)) = R_{ik}(xy)$ if $i \neq k \neq j$, where (U, V) is the commutator $UVU^{-1}V^{-1}$.

3. $n \geqq 3$ **and** q **odd.**

LEMMA 2. $\mathrm{Sp}(2n, q)$ *is generated by*

$$D = \begin{bmatrix} \sum_{i=1}^{n-1} E_{i,i+1} & -E_{n1} \\ E_{n1} & \sum_{i=1}^{n-1} E_{i,i+1} \end{bmatrix}$$

and $J' = R_{21}(a)$, where a is primitive in $\mathrm{GF}(q)$.

Clearly D and J' belong to $\mathrm{Sp}(2n, q)$. Consider the conjugates of J' by D:

$$\begin{aligned} D^{-1}J'D &= R_{32}(a) \\ D^{-1}R_{32}(a)D &= R_{43}(a) \\ &\vdots \\ D^{-1}R_{n,n-1}(a)D &= (T_{n1}(a))^T \\ D^{-1}(T_{n1}(a))^T D &= R_{12}(-a) \\ &\vdots \\ D^{-1}R_{n-1,n}(-a)D &= T_{n1}(-a) \\ D^{-1}T_{n1}(-a)D &= R_{21}(a). \end{aligned} \tag{2}$$

Since $R_{ij}(-x) = (R_{ij}(x))^{-1}$, the group generated by D and J' contains every rotation of the form $R_{i,i+1}(\pm a)$ and $R_{i+1,i}(\pm a)$, for all possible values of i.

$$(3)\qquad \begin{aligned} (R_{12}(a), R_{23}(a)) &= R_{13}(a^2) \\ (R_{13}(a^2), R_{32}(a)) &= R_{12}(a^3) \\ &\vdots \\ (R_{12}(a^{2j+1}), R_{23}(a)) &= R_{13}(a^{2j+2}) \\ (R_{13}(a^{2i}), R_{32}(a)) &= R_{12}(a^{2i+1}), \end{aligned}$$

so that every $R_{13}(a^{2i})$ and $R_{12}(a^{2j+1})$, for every integer value of i and j, is obtained. Now q is odd, so $q-1$ is even and we have $R_{13}(1)$. But there exist in $GF(q)$ solutions x, y of $x^2+y^2=a^{-1}$. Let $x=a^i$ and $y=a^j$; then $x^2=a^{2i}$, $y^2=a^{2j}$ and

$$(4)\qquad R_{13}(a^{2i})R_{13}(a^{2j}) = R_{13}(x^2+y^2) = R_{13}(a^{-1}).$$

So

$$(5)\qquad (R_{13}(a^{-1}), R_{32}(a)) = R_{12}(1)$$

is available.

By replacing a by 1 in (2), we see that the conjugates of $R_{12}(1)$ under D contain every $R_{i,i+1}(1)$ and $R_{i+1\ i}(1)$. Then

$$(6)\qquad \begin{aligned} (R_{12}(1), R_{23}(1)) &= R_{13}(1) \\ (R_{13}(1), R_{34}(1)) &= R_{14}(1) \\ &\vdots \\ (R_{1i}(1), R_{i,i+1}(1)) &= R_{1,i+1}(1) \\ &\vdots \\ (R_{32}(1), R_{21}(1)) &= R_{31}(1) \\ &\vdots \\ (R_{i+1,i}(1), R_{i,1}(1)) &= R_{i+1,1}(1) \end{aligned}$$

so that we get every $R_{i1}(1)$ and $R_{1j}(1)$, for all possible i and j.

Now let $i \neq j$. If $i \neq 1 \neq j$,

$$(7)\qquad (R_{i1}(1), R_{1j}(1)) = R_{ij}(1);$$

and since

$$(8)\qquad (R_{13}(a^{2k}), R_{32}(1)) = R_{12}(a^{2k}),$$

then,

$$(9)\qquad \begin{aligned} (R_{i1}(1), R_{12}(u)) &= R_{i2}(u), \quad i \neq 2; \\ (R_{i2}(u), R_{2k}(1)) &= R_{ik}(u), \quad i \neq k \neq 2. \end{aligned}$$

We know that every n by n matrix, U, of determinant one can be written as a product of matrices of the form $I + xE_{ij}$. Hence, the group generated by D and J' contains every rotation (ii) with det $U = 1$.

Now,

$$D^{-1}R_{1n}(x)D = T_{12}(x), \tag{10}$$

$$\left(R_{12}\left(\frac{1}{2}\right), T_{12}(x)\right) = T_1(x), \tag{11}$$

and we get every $T_1(x)$ and every $T_{12}(x)$. Also, $(T_1(x))^T = D^{-n-1}T_1(-x)D^{n+1}$. If $S_1(x) = T_1(x)\,(T_1(-x^{-1}))^T T_1(x)$, then

$$S_1(-a)S_1(1) = \begin{pmatrix} I - E_{11} + aE_{11} & 0 \\ 0 & I - E_{11} + a^{-1}E_{11} \end{pmatrix}. \tag{12}$$

Every n by n matrix of nonzero determinant is a product of a matrix of determinant one and a matrix $I - E_{11} + xE_{11}$, $x \neq 0$ in GF(q). Since a is primitive, every element in GF(q) is some power of a, and we see that the group generated by D and J' contains every matrix of the form (ii), with det $U \neq 0$.

We have obtained the matrices $T_1(x)$ and $T_{12}(x)$ from D and J'. Since

$$\begin{aligned} \begin{pmatrix} I & S \\ 0 & I \end{pmatrix} \begin{pmatrix} I & S' \\ 0 & I \end{pmatrix} &= \begin{pmatrix} I & S+S' \\ 0 & I \end{pmatrix}, \\ \begin{pmatrix} U & 0 \\ 0 & (U^T)^{-1} \end{pmatrix} \begin{pmatrix} I & S \\ 0 & I \end{pmatrix} \begin{pmatrix} U^{-1} & 0 \\ 0 & U^T \end{pmatrix} &= \begin{pmatrix} I & USU^T \\ 0 & I \end{pmatrix}, \end{aligned} \tag{13}$$

we see that every translation can be obtained by simultaneously interchanging rows and corresponding columns of the symmetric matrices xE_{11} and $xE_{12} + xE_{21}$ of $T_1(x)$ and $T_{12}(x)$, respectively, and then taking their products.

Now define

$$S_{i,j,k,\dots} = \begin{pmatrix} Q & I - Q \\ Q - I & Q \end{pmatrix},$$

where Q has zeros in the iith, jjth, kkth,$\cdots$ positions, and ones in all other diagonal positions. Then $S_2, \cdots, S_n$ are among the conjugates of S_1 under D; and since

$$(S_{i,j,k,\dots})(S_{i_1,j_1,k_1,\dots}) = S_{i,j,k,\ \dots,i_1,j_1,k_1,\dots} \tag{14}$$

we see that every generator of the group Sp($2n, q$) can be obtained from D and J' for $n > 2$ and q odd. We return now to the case of characteristic two.

4. $n \geqq 4$ **and** q **a power of two.**

LEMMA 3. Sp($2n, 2^m$) *is generated by the matrix D of Lemma* 2 *and* J':

$$J' = \begin{pmatrix} I + aE_{21} & E_{nn} \\ 0 & I + aE_{12} \end{pmatrix},$$

a primitive in GF(q).

$$D^{-1}J'D = \begin{pmatrix} I + aE_{32} & 0 \\ E_{11} & I + aE_{12} \end{pmatrix} = B. \tag{15}$$

$$(J', B) = R_{31}(a^2). \tag{16}$$

$$(J', R_{31}(a^2)) = R_{23}(a^3). \tag{17}$$

Notice that for i_0 and j_0 fixed, the conjugates of $R_{i_0 j_0}(x)$ under D (see (2)) contain the matrices $R_{st}(x)$, where $|s-t| = |i_0 - j_0|$.

$$(R_{23}(a^3), R_{31}(a^2)) = R_{21}(a^5) \tag{18}$$

$$(R_{21}(a^5), R_{13}(a^2)) = R_{23}(a^7). \tag{19}$$

$$\vdots$$

Now $a^{q-1} = 1$ is an odd power of a, so we obtain from D and J' every $R_{i,i+1}(1)$ and $R_{i+1,i}(1)$ for all possible i (see (2)). As in the case of odd characteristic, we also obtain every $R_{ij}(1)$.

Now,

$$(R_{32}(1), J') = R_{31}(a); \tag{20}$$

and

$$(R_{13}(a), R_{32}(a^3)) = R_{12}(a^4). \tag{21}$$

But squaring is an automorphism of a field of characteristic two, so a^4 is primitive if a is. Hence, using equations (2) through (9), we obtain every rotation (ii) with

$$R_{21}(a)J' = T_{nn}(1) \tag{22}$$

for any y in GF(q),

$$(R_{1n}(y), T_{nn}(1)) = \begin{pmatrix} I & yE_{n1} + yE_{1n} + y^2E_{11} \\ 0 & I \end{pmatrix}. \tag{23}$$

Also

$$D^{-1}R_{n-1,n}(y)D = T_{1n}(y); \tag{24}$$

$$(R_{1n}(y), T_{nn}(1))T_{1n}(y) = T_1(y^2). \tag{25}$$

Again, since squaring is an automorphism, y^2 is arbitrary. The proof may now be completed as above.

5. **The group** Sp($6, 2^m$). In this section we show

LEMMA 4. *$\mathrm{Sp}(6,2^m)$ is generated by D and J':*

$$J' = \begin{pmatrix} I + aE_{21} & a^{-1}E_{33} \\ 0 & I + aE_{12} \end{pmatrix},$$

where a is primitive in $\mathrm{GF}(q)$.

Computing $A_1 = D^{-1}J'D$, $A_2 = D^{-2}J'D^2$, $A_3 = (J',D)$, we get

$$D^{-1}A_2D^{-1}A_2D^{-1}A_3D^3 = R_{13}(a^2)$$

and $D^{-1}R_{13}(a^2)D = T_{12}(a^2)$. Then since $D^{-1}(R_{13}(x),A_1)^2 = R_{13}(x^2)$, we get every $R_{13}(a^{2^k})$, $k > 0$. Now $a^q = a$ is some power of two, so we get the matrix $R_{13}(a)$. We have shown that the matrix $T_{12}(a^2)$ can be obtained from D and J'. Assume that we have obtained the matrix $T_{12}(a^k)$. But then, because

$$(R_{13}(a), D^{-1}T_{12}(a^k)D) = T_{12}(a^{k+1}), \tag{26}$$

we can get every matrix of the form $T_{12}(x)$, for any x in $\mathrm{GF}(q)$. Hence we have shown that every $R_{13}(x)$, for any x in $\mathrm{GF}(q)$ is obtained from D and J'.

Now we compute $A_4=(R_{13}(a^2),A_1)$, $A_5=(D^{-1}R_{31}(a^2)D)(D^{-2}R_{31}(a^4)D^2)A_4A_2$, $A_6 = R_{13}(1)R_{31}(1)D^{-2}A_5D^2R_{31}(1)R_{13}(1)$, $A_7 = (R_{13}(1),A_6)$, and finally $(D^{-1}A_7D, R_{13}(x)) = R_{23}(yx)$, with $y = a^{-1} + a^5$. If the field is neither GF(2) or GF(4), $y \neq 0$ and x can be chosen so that $yx = a$. Then the group generated by D and J' contains every rotation (ii) with $\det U = 1$.

$$R_{21}(a)J' = T_3(a^{-1}). \tag{27}$$

Hence, the proof may now be completed as before.

Now consider the case of the field GF(4). GF(4) is generated over GF(2) by a root of $1 + x + x^2$. If a is a primitive element then the three nonzero elements are 1, a, $1 + a = a^2 = a^{-1}$. We shall now show that the group $\mathrm{Sp}(6,4)$ is generated by the matrix D and the matrix J' defined by

$$J' = \begin{pmatrix} I + aE_{21} & aE_{33} \\ 0 & I + aE_{12} \end{pmatrix}.$$

First,

$$(J', D^{-1}J'D) = R_{31}(a^2), \tag{28}$$

$$D^{-3}R_{31}(a^2)D^3 = R_{13}(a^2). \tag{29}$$

Moreover,

$$\begin{aligned}(D^{-2}R_{31}(a^2)D^2)(D^{-3}J'D^3)(D^{-1}R_{31}(a^2)D)& \\ (R_{13}(1), D^{-1}J'D)(D^{-2}J'D^2) &= \begin{pmatrix} I & 0 \\ a^{-1}E_{22} & I \end{pmatrix}.\end{aligned} \tag{30}$$

Then $T_3(a^{-1})$ is a conjugate of this matrix by D and

$$R_{13}(1)T_3(a^{-1})R_{13}(1)D^2T_3(a^{-1})D^{-2} = T_{13}(a^{-1}), \tag{31}$$

$$D^{-1}T_{13}(a^{-1})D = R_{21}(a^{-1}). \tag{32}$$

Now surely a^{-1} is primitive if a is, so we may proceed as before.

The case of GF(2) is best handled in [7] where Room exhibits two generators for the group Sp(6,2), one of which has period two.

6. **The main theorem.** We have thus far seen that the group $\mathrm{Sp}(2n,q)$ has two generators for $n > 2$. We are now in a position to prove the theorem of the introduction.

For q a power of two, the matrix J' of §§4 and 5 have period two. For q odd the matrices D as above and J defined by

$$J = \begin{pmatrix} I + bE_{12} - 2E_{22} & 0 \\ 0 & I + bE_{21} - 2E_{22} \end{pmatrix},$$

where $b = a/2$, a primitive, generate the symplectic group.

Among the conjugates of J and D are the following

$$\begin{aligned} J_1 &= \begin{pmatrix} I + bE_{21} - 2E_{22} & 0 \\ 0 & I + bE_{12} - 2E_{22} \end{pmatrix}, \\ J_2 &= \begin{pmatrix} I + bE_{32} - 2E_{33} & 0 \\ 0 & I + bE_{23} - 2E_{33} \end{pmatrix}. \end{aligned} \tag{33}$$

Then,

$$(J, J_1, J_2) = R_{32}(x), \tag{34}$$

where $x = b^3 + 4b$, and the commutator (X, Y, Z) is defined to be $(X,(Y, Z))$. Also,

$$(J, J_1 J_2 J_1) = R_{32}(y), \tag{35}$$

where $y = b^3 + 2b$. Now,

$$R_{32}(x)(R_{32}(y))^{-1} = R_{32}(x - y) = R_{32}(2b) = R_{32}(a), \tag{36}$$

and this matrix, together with D are known generators.

In the natural map $\mathrm{Sp}(2n,q)$ onto $\mathrm{PSp}(2n,q)$, D and J' are mapped onto generators, and the coset containing J has period two.

References

1. A. A. Albert and John Thompson, *Two element generation of the projective unimodular group*, Illinois J. Math. 3 (1959), 421–439.

2. H. R. Brahana, *Pairs of generators for the known simple groups of order less than one million*, Ann. of Math. (2) 31 (1930), 529–549.

3. ———, *Regular maps and their groups*, Amer. J. Math. **49** (1927), 266–284.

4. L. E. Dickson, *The theory of linear groups*, Dover, New York, 1958.

5. J. Dieudonné, *Sur les groupes classiques*, Actualités Sci. Ind. No. 1040, Hermann, Paris, 1958.

6. L. K. Hua and I. Reiner, *On the generators of the symplectic modular group*, Trans. Amer. Math. Soc. **65** (1949), 415–426.

7. T. G. Room, *The generation by two operators of the symplectic group over* GF(2), J. Austral. Math. Soc. **1** (1959), 38–46.

8. T. G. Room and R. J. Smith, *A generation of the symplectic group*, Quart. J. Math. Oxford Ser. (2) **9** (1958), 177–182.

9. R. Steinberg, *Generators for simple groups*, Canad. J. Math. **14** (1962), 277–283.

UNIVERSITY OF CHICAGO,
CHICAGO, ILLINOIS
INSTITUTE FOR DEFENSE ANALYSES,
PRINCETON, NEW JERSEY