TWO ELEMENT GENERATION OF THE SYMPLECTIC GROUP[1]

P. F. G. STANEK

Communicated by Irving Kaplansky, November 7, 1960

Albert and Thompson [1] have given two generators for the projective unimodular group over any finite field, one of which has period (group order) two. Using the same method, it is possible to prove a similar result for the symplectic group, which may be described as the group of linear transformations on an even-dimensional vector space which leave invariant a skew-symmetric bilinear form.

Let

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

be a $2n$ by $2n$ matrix and let $G(2n, q)$ be the group of all matrices X, with entries from $GF(q)$, which satisfy $XHX^T = H$, where X^T is the transpose of X. Denote by $S(2n, q)$ the group $G(2n, q)$ modulo its center. $S(2n, q)$ is known to be simple, except for $n = 1$, $q = 2$ or 3, and $n = 2$, $q = 2$.

The following three types of matrices are known to be generators of $G(2n, q)$ (see [2]):

(i) translations:

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

(ii) rotations:

$$R = \begin{pmatrix} U & 0 \\ 0 & U^{T^{-1}} \end{pmatrix}, \quad \text{where} \quad \det U \neq 0;$$

(iii) semi-involutions:

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

where Q is a diagonal matrix of 0's and 1's, so that $Q^2 = Q$, $(I-Q)^2 = I-Q$.

Denote by E_{ij} the n by n matrix with a 1 in the ijth entry and zeros elsewhere. With α primitive in $GF(q)$, set

[1] This research was supported in part under NSF G-9504.

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

and

$$J' = \begin{pmatrix} I - \alpha E_{21} & 0 \\ 0 & I + \alpha E_{12} \end{pmatrix}.$$

It can be shown that for q odd and $n>2$, $G(2n, q)$ is the group generated by D and J', i.e., every matrix of types (i), (ii), and (iii) is derivable from them.

Now, if we set

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

where $\beta=\alpha/2$, then J has period two and the group generated by D and J contains the matrix J'.

For the case of q even, re-define J by

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

where α is primitive in $GF(2^m)$. Then J has period two, and the group generated by D and J is $G(2n, 2^m)$, for $n>3$.

The group $G(6, 2^m)$ can be generated by D and the matrix

$$J = \begin{pmatrix} I + \alpha E_{21} & \alpha^{-1} E_{33} \\ 0 & I + \alpha E_{12} \end{pmatrix}.$$

In the natural map of $G(2n, q)$ onto $S(2n, q)$, the matrices D and J are mapped onto generators, and the coset containing J has period two.

The group $S(2, q)$ is the projective unimodular group, for which two generators are known (see [1]). Our method does not extend to the case $n=2$. However, the group $S(4, 2)$ is isomorphic with S_6, the symmetric group on six letters, and so has two generators, one of period two.

In [3; 4] Room and Smith have described a generation of the symplectic group over prime fields $GF(p)$ by two elements, one of which has period p. I am also informed by letter that Miss E. A. Whight of the University of Sydney has extended their theorem to include all finite fields.

References

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

2. L. E. Dickson, *The theory of linear groups*, New York, Dover (reprint), 1958.

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

4. T. G. Room and R. J. Smith, *A generation of the symplectic group*, Quart. J. Math. vol. 9 (1958) pp. 177–182.

University of Chicago