TWO ELEMENT GENERATION OF THE PROJECTIVE UNIMODULAR GROUP[1]

BY A. A. ALBERT AND JOHN THOMPSON

Communicated February 21, 1958

In volume 31 (1930) of the Annals of Mathematics H. R. Brahana gave pairs of generators of the known simple groups whose orders are less than one million, and showed that one of the generators can be taken to have period two. In this note we shall outline our proof of the corresponding result for the general case of the projective unimodular group.

Let $\mathfrak{F}=\mathfrak{F}_q$ be the field of $q=p^n$ elements, $\mathfrak{M}(n, q)$ be the multiplicative group of all n-rowed square matrices with elements in $\mathfrak{F}$ and determinant unity, $\mathfrak{N}=\mathfrak{N}(n, q)$ be the center of $\mathfrak{M}(n, q)$, that is, the set of all scalar matrices of determinant unity. Then the projective unimodular group $\mathfrak{G}(n, q)=\mathfrak{M}(n, q)/\mathfrak{N}(n, q)$ is known to be simple. We have proved that it is generated by two cosets $A\mathfrak{N}$ and $B\mathfrak{N}$, where $A\mathfrak{N}$ has period two.

Let e_{ij} be the n-rowed square matrix with 1 in the ith row and jth column, and k be a primitive element of the field $\mathfrak{F}_q$. If $n\geqq 5$ it is not difficult to show that the cosets $C\mathfrak{N}$ and $D\mathfrak{N}$ generate $\mathfrak{G}(n, q)$ if we take

$$(1)\quad C = I + ke_{n-1,2} + e_{n1}, \qquad D = (-1)^n\left(e_{12} - e_{23} + \sum_{i=3}^{n} e_{i,i+1}\right).$$

The matrix C has period p and we have obtained the required pair of generators in the case $p=2$. Hence let $p=2t+1$ and take

$$(2)\quad A = C - 2(e_{11} + e_{22}), \qquad B = D + (-1)^n t(e_{n2} - ke_{n-1,3}),$$

so that A has period two. Then $B^{-1}AB=A_1=I-2(e_{22}+e_{33})$ and $(A_1A)^2=I+2ke_{n-1,2}$. Using this result it can be shown that the subgroup $\mathfrak{H}$ generated by the elements of $A\mathfrak{N}$ and $B\mathfrak{N}$ contains $I-(2e_{n-1,n-1}+e_{nn})=J_n$, contains J_nA, and so contains $(J_nA)^2=I+2(ke_{n-1,2}+e_{n1})$. Then $\mathfrak{H}$ contains C, it is easy to show that $\mathfrak{H}$ contains D, and so $A\mathfrak{N}$ and $B\mathfrak{N}$ are the required generators.

The argument in the case above fails when $n=2, 3, 4$ as there is too little space in the matrices to carry out the computations needed. However, when $n=4$ and $q\neq 9$ we have shown that the selection

[1] The research which yielded these results was supported in part by NSF grant G-4792.

$$C = I + ke_{41}, \qquad D = e_{12} - e_{23} + e_{34} + e_{41} \tag{3}$$

yield generators, as before, and then provide the pair required when $p=2$. If $p=2t+1$ we use

$$A = e_{11} - e_{22} + e_{33} - e_{44} + ke_{41}, \quad B = e_{12} - e_{23} + e_{34} - kte_{42}. \tag{4}$$

When $n=4$ and $q=9$ the group is generated by $A\mathfrak{N}$ and $B\mathfrak{N}$ where

$$\begin{aligned} A &= -e_{11} + e_{22} - e_{33} + e_{44} + k(e_{32}) + e_{41}, \\ B &= e_{12} - e_{23} + e_{34} + e_{41} + e_{42} + k(e_{33}). \end{aligned} \tag{5}$$

In the case where $n=3$ there is even less room to operate but we can take

$$C = I + k(e_{31}), \qquad D = e_{12} + e_{23} + e_{31}, \tag{6}$$

where C has period p. As before, if $p=2t+1$, we use

$$A = 2(e_{33}) - C, \qquad B = D - (kt)e_{32}, \tag{7}$$

where A has period two.

There remains the more difficult case where $n=2$. In this case the matrices

$$B = \begin{pmatrix} k & 0 \\ 0 & k^{-1} \end{pmatrix}, \qquad C = \begin{pmatrix} 0 & 1 \\ -1 & k \end{pmatrix} \tag{8}$$

generate if $q>3$. Then A and B will generate if we select

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}, \tag{9}$$

and choose a, b and c so that A is unimodular and so that

$$AB^jA = \begin{pmatrix} 0 & d \\ -d^{-1} & f \end{pmatrix} \tag{10}$$

for some j. This can always be achieved. The case $n=2$, $q=2$ or 3 is contained, of course, in the tables of Brahana.

THE UNIVERSITY OF CHICAGO