

## TWO ELEMENT GENERATION OF THE PROJECTIVE UNIMODULAR GROUP<sup>1</sup>

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  $i$ th row and  $j$ th column, and  $k$  be a primitive element of the field  $\mathfrak{F}_q$ . If  $n \geq 5$  it is not difficult to show that the cosets  $C\mathfrak{N}$  and  $D\mathfrak{N}$  generate  $\mathfrak{G}(n, q)$  if we take

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

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

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

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  $\mathfrak{S}$  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  $\mathfrak{S}$  contains  $C$ , it is easy to show that  $\mathfrak{S}$  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

<sup>1</sup> The research which yielded these results was supported in part by NSF grant G-4792.