TWO-ELEMENT GENERATION OF THE PROJECTIVE UNIMODULAR GROUP[1]

BY

A. A. ALBERT AND JOHN THOMPSON

1. Introduction

Let $\mathfrak{F} = \mathfrak{F}_q$ be the field of $q = p^m$ elements, $\mathfrak{M} = \mathfrak{M}(n, q)$ the multiplicative group of all n-rowed square matrices with elements in $\mathfrak{F}$ and determinant 1, and $\mathfrak{N} = \mathfrak{N}(n, q)$ the subgroup of $\mathfrak{M}$ consisting of its scalar matrices ρI with $\rho^n = 1$. We assume, of course, that $n > 1$. Then $\mathfrak{N}$ is a normal subgroup of $\mathfrak{M}$, and the quotient group

$$(1) \qquad \mathfrak{G} = \mathfrak{G}(n, q) = \mathfrak{M}/\mathfrak{N}$$

is a well-known simple group called the *projective unimodular group.*

In 1930 H. R. Brahana[2] gave a list of simple groups of orders less than 1,000,000. An examination of his list reveals the fact that every group there is generated by two elements, one of which has period (group order) two. The purpose of this paper is to prove the corresponding result for a general class of simple groups. We shall derive the following property.[3]

THEOREM. *The projective unimodular group is generated by two elements $A\mathfrak{N}$ and $B\mathfrak{N}$, where the coset $A\mathfrak{N}$ has period two.*

The nature of our proof is such that it is necessary to consider a number of special cases for small matrix orders n. We shall begin with a treatment of the general case $n \geqq 5$, and shall then handle these special cases, the most difficult being the case $n = 2$.

2. The group $\mathfrak{G}$ for $n \geqq 5$

The nonzero elements of $\mathfrak{F}_q$ form a cyclic group $\mathfrak{F}_q^*$ of order $q - 1$, and the set of all elements ρ of $\mathfrak{F}_q^*$, such that $\rho^n = 1$, is a subgroup of $\mathfrak{F}_q^*$ isomorphic to $\mathfrak{N} = \mathfrak{N}(n, q)$. This is a cyclic group generated by an element λ whose period divides both n and $q - 1$, and we observe that, when $n = 2$, the group $\mathfrak{N}$ is the identity group if $p = 2$, and is generated by $-I$ when p is odd.

Our theorem is clearly equivalent to the property that $\mathfrak{M}(n, q)$ is generated by A, B, and λI. We let e_{ij} be the n-rowed square matrix with 1 in its i^{th} row and j^{th} column and zeros elsewhere, and I the n-rowed identity matrix. Then the theory of the reduction of a matrix to diagonal form by elementary

Received April 28, 1958.

[1] This paper was sponsored, in part, by the National Science Foundation.

[2] See the Annals of Mathematics, vol. 31 (1930), pp. 529–549 for this list.

[3] Our theorem was first proved for the case where q is a prime by I. Kaplansky in an unpublished note. It was later proved by L. J. Paige in the cases where $q = 4$ and $q = 8$.