AUTOMORPHISMS OF ABELIAN GROUPS INDUCED BY INVOLUTORY MATRICES, MODULO $p > 2$

By Jack Levine and Robert R. Korfhage

1. Introduction. This paper is a continuation of a previous one [3] which treated the case of involutory matrices, mod 2. Here, the situation where the modulus is a prime $p > 2$ is discussed.

Let $G_{n,p}$ be an abelian group of order p^n and type $[1^n]$, and let $M_{n,p}$ be the set of all involutory $n \times n$ matrices, modulo p.

$G_{n,p}$ is defined by the mapping

$$(1.1) \qquad (\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \to \sum_{i=0}^{n-1} \alpha_i p^{n-i-1},$$

where

$$(1.2) \qquad (\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \varepsilon Z_p^n = Z_p \times Z_p \times \cdots \times Z_p, \text{ (n factors)},$$

Z_p being the additive group of integers, mod p.

An automorphism μ^* on $G_{n,p}$ is defined by

$$\mu^*: \sum \alpha_i p^{n-i-1} \to \sum \beta_i p^{n-i-1},$$

where $\mu \varepsilon M_{n,p}$ determines an automorphism on Z_p^n :

$$\mu: (\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \to (\beta_0, \beta_1, \cdots, \beta_{n-1}).$$

Let $M_{n,p}^*$ denote the set of all automorphisms on $G_{n,p}$. Then $\mu^* \varepsilon M_{n,p}^*$. We refer to all such mappings μ^* as involutory mappings.

In [3] it was shown that the set of elements of $G_{n,p}$ which remain fixed under μ^* form a subgroup, F, of $G_{n,p}$.

In §2 we show the existence of another subgroup Z of $G_{n,p}$ whose elements are mapped into their negatives under μ^*, and such that $G_{n,p} = F \oplus Z$, $F \cap Z = \{0\}$. This is in contrast to the situation when $p = 2$, where there is no such group Z, but there is a subgroup $F' \subseteq F$ such that $\theta + \mu^*(\theta) \varepsilon F'$, where $\theta \varepsilon G_{n,p}$.

Based on the above expression for $G_{n,p}$ in terms of F and Z a formula for the total number of matrices in the set $M_{n,p}$ is obtained in §3, this being in agreement with the corresponding result of Hodges [2].

§4 considers groups of involutory automorphisms, and it is proved the maximum order of such a group is 2^n. In the case $p = 2$ we had previously shown the existence of such groups of orders $\leq 2^{q^2}$, where $q \leq [n/2]$.

In §5 a method is outlined for the actual construction of involutory matrices of any order, mod $p > 2$, and in the last section a simplified method when $p = 2$ is explained. Another method for this construction had been given in [3].

Received March 19, 1962.