AUTOMORPHISMS OF ABELIAN GROUPS INDUCED BY INVOLUTORY MATRICES

BY JACK LEVINE AND ROBERT R. KORFHAGE

1. **Introduction.** The encipherment method of algebraic cryptography employs involutory matrices M_n of order n, and with elements in the ring of integers modulo m, to establish a unique reciprocal correspondence

$$(1.1)\qquad (p_1\,, p_2\,, \cdots\,, p_n) \leftrightarrow (c_1\,, c_2\,, \cdots\,, c_n)$$

between every n-tuple $(p_1\,,\ p_2\,,\ \cdots\,,\ p_n)$ of plain-letters and its associated n-tuple $(c_1\,, c_2\,, \cdots\,, c_n)$ of cipher letters. This is done by means of the matrix congruence

$$(1.2)\qquad C \equiv M_n P \qquad \text{mod } m,$$

where P and C represent the left and right sides of (1.1) respectively, considered as column vectors. (The letters are given unique numerical values selected from the ring.) The value m represents the number of letters in the "alphabet" being used, such as 2, or 10, or 26, etc. For further reference to the theory of algebraic cryptography, [4] may be consulted.

In the cryptanalysis of this type of encipherment, it is essential to deduce properties of the correspondence (1.1), and, as indicated briefly in [4], this may be done through a study of certain additive abelian groups and their automorphisms, these being dependent on n and prime factors of m. The present paper is primarily concerned with the case of the prime factor 2. Other cases will be taken up in later papers, as well as the applications to the cryptanalysis mentioned above.

To gain some idea of the groups and automorphisms involved, consider, for any prime $p > 2$, the additive group Z_p of integers modulo p. Define the group Z_p^n by

$$(1.3)\qquad Z_p^n = Z_p \times Z_p \times \cdots \times Z_p\,, \qquad (n \text{ factors}).$$

The abelian group $G_{n,p}$ of order p^n and type $[1^n]$ is then defined by the mapping

$$(1.4)\qquad (\alpha_0\,, \alpha_1\,, \cdots\,, \alpha_{n-1}) \rightarrow \sum_{i=0}^{n-1} \alpha_i p^{n-i-1},$$

where $(\alpha_0\,, \alpha_1\,, \cdots\,, \alpha_{n-1}) \,\varepsilon\, Z_p^n$. Hence, $G_{n,p}$ is isomorphic to Z_p^n.

Let $M_{n,p}$ be the set of all involutory $n \times n$ matrices, modulo p. Since these are non-singular, each determines an automorphism of Z_p^n. Hence there is an