COMMUTATORS OF MATRICES WITH COEFFICIENTS FROM THE FIELD OF TWO ELEMENTS

BY R. C. THOMPSON

Let $GL(n, K)$ denote the multiplicative group of all nonsingular $n \times n$ matrices with coefficients in a field K, and let $SL(n, K)$ denote the subgroup of $GL(n, K)$ consisting of the matrices in $GL(n, K)$ with determinant unity. Let $GF(p^n)$ denote the finite field with p^n elements. In [1] the author determined when a matrix in $SL(n, K)$ can be expressed as a commutator $XYX^{-1}Y^{-1}$ of matrices X, Y in $SL(n, K)$ or in $GL(n, K)$, for $K \neq GF(2)$ or $GF(3)$. In this note we determine when a matrix $A \in SL(n, GF(2))$ can be expressed as a commutator $XYX^{-1}Y^{-1}$ of matrices X, Y in $SL(n, GF(2)) = GL(n, GF(2))$. Our result is the following theorem.

THEOREM. *Let $n > 2$. Then every element of $SL(n, GF(2))$ is a commutator of $SL(n, GF(2))$.*

The present paper will not use any of the results of [1]. Our principal tool is the similarity theory of matrices; see [2, Chapter 8].

We begin by introducing suitable notation. We denote the two elements of $GF(2)$ by 0 and 1. All polynomials, matrices and equations appearing in this paper are assumed to have coefficients in $GF(2)$. By I_n we denote the $n \times n$ identity matrix. If $g(x) = x^t + a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_0$ is a polynomial, $C(g(x))$ will denote the companion matrix of $g(x)$; see [2; 148]. The Jordan canonical form of $C((x + 1)^e)$ is denoted by $J_e : J_1 = I_1$ and for $e > 1$, J_e is the matrix (23) of [2; 163] where, in (23), $a = 1$. By $A \dotplus B$ we denote the direct sum of the two matrices A and B:

$$A \dotplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

If $n = 0$ we interpret $A \dotplus I_n \dotplus B$ as $A \dotplus B$.

LEMMA 1. *For $n > 3$, the matrix $M_n = J_2 \dotplus J_{n-2}$ is a commutator of $SL(n, GF(2))$.*

Proof. We first dispose of the cases $n = 3, 4, 5, 6$. Let

$$U_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \qquad V_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

Received June 29, 1961. The author wishes to acknowledge his debt to Dr. O. Taussky-Todd for suggesting the problem considered here. He also wishes to thank the National Research Council of Canada for its financial support.