SIMILAR INVOLUTORY MATRICES MODULO R

By Joel V. Brawley, Jr.

1. Preliminaries. If A is an $n \times n$ matrix over a ring R with an identity, then A is called involutory if $A^2 = I$ where I denoted the $n \times n$ identity matrix over R. Such involutory matrices while of interest in themselves have a practical application in the area of algebraic cryptography [6], [7], [8]. One characteristic of an involutory matrix is that it remains involutory under a similarity transformation; i.e., A is involutory if and only if $P^{-1}AP$ is involutory where P is any nonsingular matrix over R. Thus, in studying involutory matrices one is led to a study of the effect of similarity transformations on such matrices, and one question which arises is the following: What kind of canonical forms for involutory matrices can be obtained through similarity transformations? To be more specific we make the following definitions.

Definitions. A set C of $n \times n$ matrices is called a *canonical set* for the involutory matrices if each $n \times n$ involutory matrix is similar to one and only one matrix in C. For a fixed canonical set C and for an arbitrary involutory matrix A, that matrix in C to which A is similar will be called the *canonical form* of A (relative to C).

Usually, when one speaks of a canonical form, he means a matrix that is in some sense simpler than the original matrix. Therefore, in obtaining a canonical set C it is desired to have the member matrices as "simple" as possible. The question above is now rephrased as follows: What is a canonical set for the involutory matrices with the property that the members of the set are in some sense simple?

This question is easily answered when the ring R is a field F. Indeed, the set C may be taken as the *Jordan* canonical set. This Jordan set is shown by Hodges [5] to be

$$C_1 = \{\operatorname{diag}(I_t, -I_{n-t}) \mid t = 0, 1, 2, \cdots, n\}$$

for fields not of characteristic 2 and

$$C_2 = \left\{\operatorname{diag}(I_{n-2t}, Z_1, \cdots, Z_t) \mid t = 0, 1, 2, \cdots \left[\frac{n}{2}\right]\right\}$$

for fields of characteristic 2. Here I_k denotes the $k \times k$ identity matrix, $Z_i = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ for $i = 1, 2, \cdots t$, and $[n/2]$ is the greatest integer in $n/2$. (Actually, Hodges' work refers to finite fields, but his arguments are valid for arbitrary fields.)

Received October 29, 1966.