A THEOREM ON THE AUTOMORPHS OF A SKEW-SYMMETRIC MATRIX

Morris Newman

In this note we consider certain groups of integral matrices, and without further qualification all matrices that appear will be assumed to have integral entries. The propositions obtained below remain true when the matrix elements belong to an arbitrary principal ideal ring, with essentially no change in the proofs.

Let I stand for the identity matrix of order t, and J for the $2t \times 2t$ matrix

$$J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The group of automorphs of J is the multiplicative group Γ of matrices M such that

$$MJM' = J,$$

and it is called the *symplectic group.*

An element M of Γ is said to be *symplectic.* A matrix M_0 satisfying the condition

$$M_0 J M_0' \equiv J \pmod{n},$$

is said to be *symplectic modulo* n.

The following result, proved in [3], was the key theorem in the determination of the structure of certain quotient groups of matrices.

THEOREM 1. *Suppose that* M_0 *is symplectic modulo* n. *Then a symplectic matrix* M *exists such that* $M \equiv M_0 \pmod{n}$.

Suppose that K is a nonsingular skew-symmetric matrix. The K-*symplectic group* Γ_K is defined as the multiplicative group of matrices N such that

$$NKN' = K,$$

and an element N of Γ_K is said to be K-*symplectic.* If N_0 is a matrix such that

$$N_0 K N_0' \equiv K \pmod{n},$$

then N_0 is said to be K-*symplectic* modulo n.

In her doctoral dissertation [1], Sister Kenneth Kolmer proved the following result for the group Γ_K, which corresponds to Theorem 1 for Γ:

THEOREM 2. *Suppose that* n *is an integer such that* $(n, \det K) = 1$, *and that* N_0 *is* K-*symplectic modulo* n. *Then there exists a* K-*symplectic matrix* N *such that* $N \equiv N_0 \pmod{n}$.

Received October 16, 1964.

She went on to determine the structure of the corresponding quotient groups of matrices. Her proof proceeded from first principles. Using Theorem 1, we shall give a short proof of her result.

LEMMA 1. *Let* a, b *be relatively prime integers, and* A, B *symplectic matrices. Then a symplectic matrix* W *can be determined such that*

$$W \equiv A \pmod{a}, \tag{1}$$

$$W \equiv B \pmod{b}. \tag{2}$$

Proof. Determine b' so that $bb' \equiv 1 \pmod{a}$, and set

$$W_0 = B + bb'(A - B).$$

Then W_0 satisfies each of the congruences (1), (2). Hence W_0 is symplectic modulo a and modulo b, hence also modulo ab, since $(a, b) = 1$. By Theorem 1, there exists a symplectic matrix W such that

$$W \equiv W_0 \pmod{ab},$$

and this W satisfies the requirements of the lemma. Lemma 1 is thus proved.

We continue our discussion. Since K is nonsingular and skew-symmetric, K is of even order 2t. It is known [2, p. 52] that K is congruent by a unimodular integral matrix to a matrix of the form

$$\begin{pmatrix} 0 & H \\ -H & 0 \end{pmatrix},$$

where H is a symmetric matrix of order t and

$$\det H = p \neq 0.$$

(In fact, H may be taken in Smith normal form, but we do not need the full result.) We may therefore assume without loss of generality that

$$K = \begin{pmatrix} 0 & H \\ -H & 0 \end{pmatrix},$$

so that $\det K = p^2$. Set

$$T = \begin{pmatrix} H & 0 \\ 0 & I \end{pmatrix}.$$

Then T is symmetric, $\det T = p$, and

$$TJT' = K. \tag{3}$$

If N is K-symplectic, (3) implies that

$$(T^{-1}NT)J(T^{-1}NT)' = J.$$

This implies the following Lemma.

LEMMA 2. *If* M *is symplectic and* $N = TMT^{-1}$ *has integral elements, then* N *is* K-*symplectic.*

We are now prepared to give a proof of Theorem 2. Let n be an integer such that (p, n) = 1, and suppose that N_0 is K-symplectic modulo n. Then

$$N_0 K N_0' \equiv K \pmod{n},$$

$$N_0 TJT' N_0' \equiv TJT' \pmod{n}. \tag{4}$$

Set $H_0 = p' H^{adj}$, where $pp' \equiv 1 \pmod{n}$. Then H_0 is symmetric, H_0 commutes with H, and $HH_0 \equiv I \pmod{n}$. Put

$$T_0 = \begin{pmatrix} H_0 & 0 \\ 0 & I \end{pmatrix}.$$

Then T_0 is symmetric, T_0 commutes with T, and $TT_0 \equiv I \pmod{n}$. From (4) we find that

$$(T_0 N_0 T) J (T_0 N_0 T)' \equiv J \pmod{n}.$$

Hence $T_0 N_0 T$ is symplectic modulo n, and Theorem 1 guarantees the existence of a symplectic matrix S such that

$$S \equiv T_0 N_0 T \pmod{n}. \tag{5}$$

By Lemma 1, a symplectic matrix W can be determined such that

$$W \equiv S^{-1} \pmod{p}, \tag{6}$$

$$W \equiv I \pmod{n}. \tag{7}$$

Define $N = TSWT^{-1}$. Then (6) implies that N is an integral matrix (since pT^{-1} is an integral matrix), and Lemma 2 implies that N is K-symplectic. We need only show that $N \equiv N_0 \pmod{n}$. Since NT = TSW, (5) and (7) imply that

$$NT \equiv TT_0 N_0 T \equiv N_0 T \pmod{n};$$

since T has an inverse modulo n, it follows that $N \equiv N_0 \pmod{n}$. This completes the proof of Theorem 2.

REFERENCES

1. Sister K. Kolmer, *Generalization of the symplectic modular group*, Dissertation, Catholic University of America (1964).
2. C. C. MacDuffee, *The theory of matrices*, Chelsea, New York (1946).
3. M. Newman and J. R. Smart, *Symplectic modulary groups*, Acta Arith. 9 (1964), 83-89.

National Bureau of Standards
Washington, D. C.