ACTA ARITHMETICA
XI (1966)

# Generalization of the symplectic modular group*

by

S. K. Kolmer (St. Louis)

**1.** In this paper we are concerned with certain groups of rational integral matrices, and *all matrices considered here will be of this kind.* The phrases *lower triangular matrix* and *upper triangular matrix* will always refer to a square matrix having zeroes above or below the main diagonal and all the diagonal elements $+1$.

Let $J$ be the $2t\times 2t$ matrix defined by

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

where $I$ is the $t\times t$ identity matrix. Let $\Gamma = \Gamma_J$ be the group of automorphs of $J$; that is, the set of matrices $M$ such that $MJM' = J$. Clearly, $J$ is skew-symmetric, that is, $J' = -J$. The group $\Gamma$ is called the *symplectic modular group*. This group has been studied extensively by M. Newman, J. R. Smart, I. Reiner, and L. K. Hua. L. K. Hua and I. Reiner determined the independent generators of the symplectic group in [1]. M. Newman and J. R. Smart, having developed results for modulary groups of $t\times t$ matrices in [3] extended their study to the symplectic modulary groups in [4].

The purpose of the present paper is to extend the work of M. Newman and J. R. Smart on symplectic modulary groups. To this end automorphs of arbitrary non-singular skew-symmetric matrices which are not necessarily unimodular are considered. A number of difficulties arise since the skew-symmetric matrix $K$ may not be unimodular and $K$ itself is not in general a member of the group.

Several theorems for unimodular matrices with rational integral elements are proved in section 2 which can be applied in section 3. These theorems, although they are stronger than is strictly necessary for this paper, are of interest in themselves.

---

* Dissertation submitted to the Faculty of the Graduate School of Arts and Sciences of the Catholic University of America in Partial Fulfilment of the Requirements for the Degree of Doctor of Philosophy.

In section 3 after the definitions of the $K$-symplectic group and the $K$-symplectic group modulo $n$, a few observations are made concerning the structure of elements of the $K$-symplectic group. There follows a discussion of matrices modulo $n$ in lemmas 3, 4, and 5. Finally in theorem 3 there is shown that given $M$, a $K$-symplectic matrix modulo $n$, there is a $K$-symplectic matrix $N$ such that

$$N \equiv M \pmod{n}.$$

Having established the key theorem 3, applications to modulary groups can be made in a very similar manner as in [4]. This discussion is treated in section 4.

**2.** In this section we establish several results concerning unimodular matrices, that is, matrices $A$ with rational integral elements and determinant $\pm 1$.

LEMMA 1. *The group of $t\times t$ unimodular matrices is generated by lower triangular matrices and upper triangular matrices.*

Proof. Let

$$P_t = \begin{bmatrix} 0 & 0 & \dots & 0 & (-1)^{t-1} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix},$$

$$T_t = T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \dotplus I_{t-2}, \qquad S_t = S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \dotplus I_{t-2},$$

where $\dotplus$ is the direct sum. Then $TP_t = (1)\dotplus P_{t-1}$ and $T = SWS$, where $W = S'^{-1}$. Hence $T$ is the product of upper triangular matrices and lower triangular matrices. Suppose that $P_{t-1}$ is the product of such matrices. Then $P_t$ is also. But $P_2$ satisfies

$$P_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = S_2^{-1} W_2^{-1} S_2^{-1}.$$

It follows that $P_t$ is always of the desired form. Since $S$ and $P_t$ generate the unimodular group [1], the truth of lemma 1 follows.

THEOREM 1. *Let $f$ be an integer such that $(f, n) = 1$. Let $A^*$ be an arbitrary unimodular matrix. Then there is a unimodular matrix $A$ such that $A \equiv A^* \pmod{n}$ and $A$ is in upper triangular form modulo $f$.*

Proof. By lemma 1, $A^* = L_1^* U_1 L_2^* U_2 \dots L_m^* U_m$ for some $m$, where each $L_k^*$ denotes a unimodular matrix in lower triangular form and each $U_k$ a unimodular matrix in upper triangular form. Set $L_k^* = l_{ij}^*(k)$. Since $(f, n) = 1$ there is a solution to the congruence $fr_{ij} \equiv l_{ij}^*(k) \pmod{n}$, $i > j$. Define

$$L_k = l_{ij}(k) \quad \text{where} \quad l_{ij} = \begin{cases} 0, & i < j, \\ 1, & i = j, \\ fr_{ij}, & i > j. \end{cases}$$

Then $L_k \equiv I \pmod{f}$ and $L_k^* \equiv L_k \pmod{n}$. So

$$A^* = L_1^* U_1 L_2^* U_2 \dots L_m^* U_m \equiv L_1 U_1 L_2 U_2 \dots L_m U_m \pmod{n}.$$

Set

$$A = L_1 U_1 L_2 U_2 \dots L_m U_m.$$

Then

$$A \equiv A^* \pmod{n}$$

and $A$ modulo $f$ is the product of unimodular matrices in upper triangular form. Clearly, a product of such matrices is again such a matrix. So $A$ modulo $f$ is of the desired form and the theorem is proved.

We remark that the following lemma is true.

LEMMA 2. *The set of unimodular matrices which are in upper triangular form modulo $f$ forms a group.*

We are now prepared to give the proofs of the theorems of section 3.

**3.** Let $M$ be a $2t\times 2t$ rational integral matrix of the form $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ where $A$, $B$, $C$, and $D$ are $t\times t$ matrices. Let $K$ be the rational integral matrix

$$K = \begin{bmatrix} 0 & H \\ -H & 0 \end{bmatrix} \tag{1}$$

where $H = \operatorname{diag}(h_1, h_2, \dots, h_t)$, $h_{i-1}$ divides $h_i$, and $h_i > 0$, for all $i$, $1 \leqslant i \leqslant t$. Then $K$ is skew-symmetric and it is known that an arbitrary non-singular skew-symmetric matrix, $K^*$, is necessarily equivalent to one of this form.

If $K^*$ is an arbitrary non-singular skew-symmetric matrix, define

$$\Gamma_{K^*} = \{M \mid MK^*M' = K^*\}.$$

If $M$ is a member of $\Gamma_{K^*}$ then $M$ is called *$K^*$-symplectic*. The set $\Gamma_{K^*}$ forms a group which we call the *$K^*$-symplectic group*. It is easy to show that if $K$ is given by (1) then $M$ is $K$-symplectic if and only if

$$AHD' - BHC' = H, \quad AHB' = BHA', \quad CHD' = DHC'.$$

$M$ is called *$K^*$-symplectic modulo $n$* if $M$ belongs to

$$\Gamma_{K^*}(\operatorname{mod} n) = \{M \mid MK^*M' \equiv K^* \pmod{n},\ (\det K^*, n) = 1,\ n \text{ is an integer}\}.$$

Notice that a $K^*$-symplectic matrix modulo $n$ is not necessarily $K^*$-symplectic.

Let $K^*$ be an arbitrary non-singular skew-symmetric matrix. Then there is a matrix $K$ of the form (1) with the properties given with (1) and a matrix $V$ such that $VK^*V' = K$. Thus if $M$ is a member of $\Gamma_{K^*}$ then $M(V^{-1}KV^{-1'})M' = V^{-1}KV^{-1'}$ or $VM(V^{-1}KV^{-1'})M'V' = K$ and $(VMV^{-1})K(VMV^{-1})' = K$. So

$$\Gamma_K = V\Gamma_{K^*}V^{-1}.$$

Hence it is sufficient to treat skew-symmetric matrices $K$ of the form (1) with the properties given with (1). Thus in the remainder of this section $K$ will refer to a skew-symmetric matrix of this type.

We first make some observations concerning the structure of elements of the $K$-symplectic group of the form $\begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}$. Let $M$ be a member of the $K$-symplectic group and of the form $M = \begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}$. Then $AHD' = H$ or $D = HA^{-1'}H^{-1}$. Let $A^{-1'} = G$. Then

$$\begin{bmatrix} d_{11} & d_{12} & \dots & d_{1t} \\ d_{21} & d_{22} & \dots & d_{2t} \\ \dots & \dots & \dots & \dots \\ d_{t1} & d_{t2} & \dots & d_{tt} \end{bmatrix} = \begin{bmatrix} h_1 & & & \\ & h_2 & 0 & \\ 0 & & \ddots & \\ & & & h_t \end{bmatrix} \begin{bmatrix} g_{11} & g_{12} & \dots & g_{1t} \\ g_{21} & g_{22} & \dots & g_{2t} \\ \dots & \dots & \dots & \dots \\ g_{t1} & g_{t2} & \dots & g_{tt} \end{bmatrix} \begin{bmatrix} 1/h_1 & & & \\ & 1/h_2 & 0 & \\ 0 & & \ddots & \\ & & & 1/h_t \end{bmatrix}$$

$$= \begin{bmatrix} g_{11} & (h_1/h_2)g_{12} & \dots & (h_1/h_t)g_{1t} \\ (h_2/h_1)g_{21} & g_{22} & \dots & (h_2/h_t)g_{2t} \\ \dots & \dots & \dots & \dots \\ (h_t/h_1)g_{t1} & (h_t/h_2)g_{t2} & \dots & g_{tt} \end{bmatrix}.$$

Thus $d_{ij}$, $i > j$, is a multiple of $h_i/h_j$, since the elements of $G$ are rational integers.

Having made these observations we can prove theorem 2.

THEOREM 2. *Let $A$ be a unimodular matrix with $A$ modulo $h_t$ in upper triangular form, where $h_t$ is the largest invariant factor of $H$. Then there is a matrix $D$ such that $\begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}$ is a $K$-symplectic matrix.*

Proof. If $A$ is unimodular and $A$ is in upper triangular form modulo $h_t$, then by lemma 2 $A^{-1}$ is in upper triangular form modulo $h_t$. Hence $HA^{-1'}H^{-1}$ has rational integral elements. Then $AH(HA^{-1'}H^{-1})' = AH(H^{-1}A^{-1}H) = H$. Thus the choice $D = HA^{-1'}H^{-1}$ makes the matrix $\begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}$ $K$-symplectic.



Now in theorem 3 it will be shown that given a matrix $M$ which is $K$-symplectic modulo $n$ there is a $K$-symplectic matrix $N$ such that $N \equiv M \pmod{n}$. The theorem is preceded by several lemmas.

LEMMA 3. *Let $n$ be an integer such that $(\det H, n) = 1$. Let $A$ be a matrix with $AH \equiv (AH)' \pmod{n}$, that is, $A$ is $H$-symmetric modulo $n$ or $AH$ is symmetric modulo $n$. Then there is an $H$-symmetric matrix $S$ such that $S \equiv A \pmod{n}$.*

Proof. Let $AH \equiv (AH)' \pmod{n}$ where $A = (a_{ij})$, $H = \operatorname{diag}(h_1, h_2, \dots, h_t)$. There is a $g_{ij}$ which satisfies $a_{ij} + ng_{ij} \equiv 0 \pmod{h_i}$ since $(n, h_i) = 1$. This determines a matrix $G$ such that $A + nG = A_0 \equiv A \pmod{n}$ and

$$HA_0'H^{-1} = \left((a_{ij} + ng_{ij})\frac{h_j}{h_i}\right)$$

has integral elements. Then $A_0H \equiv HA_0' \pmod{n}$ and $A_0H \equiv HA_0'H^{-1}H \pmod{n}$ or

$$(A_0 - HA_0'H^{-1})H \equiv 0 \pmod{n}.$$

Define $H_1$ so that $HH_1 \equiv H_1H \equiv I \pmod{n}$. Then

$$(A_0 - HA_0'H^{-1})HH_1 \equiv 0 \pmod{n} \quad \text{or} \quad A_0 \equiv HA_0'H^{-1} \pmod{n}.$$

So $A_0 = HA_0'H^{-1} - nE$ where $E$ is integral. And $A_0H - HA_0' = nEH$. Also by taking transposes, $HA_0' - A_0H = nHE'$. So $HE' = (EH)' = -EH$ or $EH$ is skew-symmetric. Let $EH = (e_{ij}h_j)$. Define $(EH)^+ = \frac{1}{2}(e_{ij}h_j + |e_{ij}h_j|)$. Then $(EH)^+$ is obtained from $EH$ by replacing all negative entries of $E$ by zero. Also since $EH$ is skew-symmetric, $(EH)^{+'} = \frac{1}{2}(-e_{ij}h_j + |e_{ij}h_j|)$. Thus

$$EH = (EH)^+ - (EH)^{+'}, \quad \text{and} \quad AH - (AH)' = nEH = n\left((EH)^+ - (EH)^{+'}\right)$$

or

$$A_0H - n(EH)^+ = \left((A_0H) - n(EH)^+\right)'.$$

Note that $(EH)^+ = E^+H$ since all elements $h_i$ in $H$ are positive, and $H$ is a diagonal matrix. So $S$ may be chosen as $S = A_0 - nE^+ = A + n(G + E^+)$ and

$$S \equiv A \pmod{n}.$$

LEMMA 4. *Given $M$ where $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, a $K$-symplectic matrix modulo $n$, then there is an $H$-symmetric matrix $X$ with $(\det(A + BX), n) = 1$.*

Proof. It is sufficient to show that for every prime $p$, where $p$ divides $n$, there exists an $H$-symmetric matrix $X_p$ such that $p \nmid \det(A + BX_p)$. For then, since clearly a linear combination of $H$-symmetric matrices is an $H$-symmetric matrix, by the Chinese remainder theorem there is an $H$-symmetric matrix $X$ such that $X \equiv X_p (\bmod p)$ for every $p$ dividing $n$. Since

$$\det(A+BX) \equiv \det(A+BX_p)(\bmod p)$$

this implies that

$$\big(\det(A+BX), n\big) = 1.$$

Let $p$ divide $n$ and let $U$ and $V$ be unimodular matrices such that $A_p = UAV$ is diagonal and $\det A_p \not\equiv 0(\bmod p)$. The case $A \equiv 0(\bmod p)$ will be treated at the end of the proof. Let $Q = \{h_1, h_2, \ldots, h_t\}$ be the set of invariant factors of $H$. Then clearly $h_t$ is the least common multiple of the elements of $Q$ and $(h_t, n) = 1$. So by theorem 1 there are unimodular matrices $U_p$ and $V_p$ which are in upper triangular form modulo $h_t$ and such that

$$U_p \equiv U(\bmod p) \quad \text{and} \quad V_p \equiv V(\bmod p).$$

By theorem 2 $U_p$ and $V_p$ determine unimodular matrices $W_p$ and $Z_p$ such that

$$\begin{bmatrix} U_p & 0 \\ 0 & W_p \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} V_p & 0 \\ 0 & Z_p \end{bmatrix}$$

are $K$-symplectic. Then

$$\begin{bmatrix} U_p & 0 \\ 0 & W_p \end{bmatrix}\begin{bmatrix} A & B \\ C & D \end{bmatrix}\begin{bmatrix} V_p & 0 \\ 0 & Z_p \end{bmatrix} = \begin{bmatrix} U_pAV_p & U_pBZ_p \\ W_pCV_p & W_pDZ_p \end{bmatrix} \equiv \begin{bmatrix} A_p & B_p \\ C_p & D_p \end{bmatrix}(\bmod p).$$

Let $Y_p = Z_p^{-1}X_pV_p$. Then

$$A_p+B_pY_p \equiv U_pAV_p+U_pBZ_pZ_p^{-1}X_pV_p = U_p(A+BX_p)V_p(\bmod p).$$

Hence if

$$p \nmid \det(A_p+B_pY_p) \quad \text{then} \quad p \nmid \det(A+BX_p).$$

Determine $X$ by the Chinese remainder theorem such that $X \equiv X_p(\bmod p)$ for every $p$ dividing $n$. Then $\big(\det(A+BX), n\big) = 1$.

So we need only determine an $H$-symmetric matrix $Y_p$ such that $p \nmid \det(A_p+B_pY_p)$ for every $p$ dividing $n$. We know $A_p \equiv \begin{bmatrix} E & 0 \\ 0 & 0 \end{bmatrix}(\bmod p)$ where $E$ is diagonal and non-singular modulo $p$. $B_p$ can be written $B_p = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$ where $B_{11}$ has the dimension of $E$. We compute that

$$A_pHB_p' \equiv \begin{bmatrix} E & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}\begin{bmatrix} B_{11}' & B_{21}' \\ B_{12}' & B_{22}' \end{bmatrix} = \begin{bmatrix} EH_1B_{11}' & EH_1B_{21}' \\ 0 & 0 \end{bmatrix}(\bmod p)$$



where $H$ is partitioned so that $H_1$ has the dimension of $E$. By symmetry modulo $p$ we conclude that $B_{21} \equiv 0(\bmod p)$ and so $B_p \equiv \begin{bmatrix} B_{11} & B_{12} \\ 0 & B_{22} \end{bmatrix}(\bmod p)$. Hence the $t \times 2t$ matrix $[A_p\ B_p]$ satisfies

$$[A_p\ B_p] \equiv \begin{bmatrix} E & 0 & B_{11} & B_{12} \\ 0 & 0 & 0 & B_{22} \end{bmatrix}(\bmod p),$$

so that $\det B_{22} \not\equiv 0(\bmod p)$ since $(\det M)^2 \equiv 1(\bmod n)$. Let

(2) $$Y_p = \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix}$$

where $I$ is the identity and has the dimension of $B_{22}$. Obviously $Y_p$ is $H$-symmetric. Then

$$A_p+B_pY_p \equiv \begin{bmatrix} E & B_{12} \\ 0 & B_{22} \end{bmatrix}(\bmod p)$$

and

$$\det(A_p+B_pY_p) \equiv (\det E)(\det B_{22})(\bmod p)$$

so that

$$p \nmid \det(A_p+B_pY_p) \quad \text{since} \quad p \nmid \det E \quad \text{and} \quad p \nmid \det B_{22}.$$

The above is true for all $p$ where $p$ divides $n$. Thus $Y_p$ as in (2) is the required $H$-symmetric matrix.

$X_p$ is $H$-symmetric since $Y_p = Z_p^{-1}X_pV_p$ or $Y_pH = Z_p^{-1}X_pV_pH$. Then $Z_p = HV_p'^{-1}H^{-1}$ and $Y_pH = (HV_p'H^{-1})(X_pH)(HV_p'H^{-1})'$. Thus $X_pH$ is symmetric or $X_p$ is $H$-symmetric, and the lemma is proved except for the special case $A \equiv 0(\bmod p)$.

If $A \equiv 0(\bmod p)$ where $p$ divides $n$, then $M \equiv \begin{bmatrix} 0 & B \\ C & D \end{bmatrix}(\bmod p)$. But $\det B \not\equiv 0(\bmod p)$. Let $X = I$. Then $\det(A+BX) \equiv \det BX \equiv \det B \not\equiv 0(\bmod p)$. Thus $\big(\det(A+BX), p\big) = 1$ where $p$ divides $n$.

LEMMA 5. *Let $P$, $Q$ be $H$-symmetric matrices which commute such that $M = \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix}$ is $K$-symplectic modulo $n$. Then there is a $K$-symplectic matrix $N$ such that*

$$M \equiv N(\bmod n).$$

Proof. Since $M = \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix}$ is $K$-symplectic modulo $n$, $PHQ' \equiv H(\bmod n)$ or $PQH \equiv H(\bmod n)$. Since $(\det H, n) = 1$, it follows that $PQH = H - nEH$ where $E$ is $H$-symmetric and commutes with $P$ and $Q$. Then it is easy to show that

$$N = \begin{bmatrix} P+nEP & -nE \\ nE & Q \end{bmatrix}$$

is a $K$-symplectic matrix and $N \equiv M(\bmod n)$.

THEOREM 3. *Given* $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, *a K-symplectic matrix modulo n, there is a K-symplectic matrix N such that* $N \equiv M(\bmod n)$.

Proof. Let $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ be a $K$-symplectic matrix modulo $n$. By lemma 4 there is an $H$-symmetric matrix $X$ such that $(\det(A+BX), n) = 1$. Let

$$M_1 = \begin{bmatrix} A & B \\ C & D \end{bmatrix}\begin{bmatrix} I & 0 \\ X & I \end{bmatrix} = \begin{bmatrix} A+BX & B \\ C+DX & D \end{bmatrix} = \begin{bmatrix} A_1 & B \\ C_1 & D \end{bmatrix}.$$

Then $M_1$ is $K$-symplectic modulo $n$ and $(\det A_1, n) = 1$. Let $\alpha$ be a real number such that $\alpha \det A_1 \equiv 1(\bmod n)$. Then $-\alpha A_1^{\mathrm{adj}} BH$ is symmetric modulo $n$ since $A_1 HB'$ is symmetric modulo $n$. By lemma 3 there is an $H$-symmetric matrix $S$ such that $S \equiv -\alpha A_1^{\mathrm{adj}} B(\bmod n)$. Put

$$M_2 = \begin{bmatrix} A_1 & B \\ C_1 & D \end{bmatrix}\begin{bmatrix} I & S \\ 0 & I \end{bmatrix} = \begin{bmatrix} A_1 & A_1S+B \\ C_1 & C_1S+D \end{bmatrix}.$$

Then $A_1S+B \equiv 0(\bmod n)$. So $M_2 \equiv \begin{bmatrix} A_1 & 0 \\ C_1 & D_1 \end{bmatrix}(\bmod n)$. Since $(\det A_1)(\det D_1) \equiv \pm 1(\bmod n)$ we can set $\det A_1 = \beta$ so that $\beta \det D_1 \equiv \pm 1(\bmod n)$. Then $\mp\beta D_1^{\mathrm{adj}} C_1 H$ is symmetric modulo $n$. By lemma 3 there is an $H$-symmetric matrix $S_1$ such that $S_1 \equiv \mp\beta D_1^{\mathrm{adj}} C_1(\bmod n)$. Put

$$M_3 = \begin{bmatrix} A_1 & 0 \\ C_1 & D_1 \end{bmatrix}\begin{bmatrix} I & 0 \\ S_1 & I \end{bmatrix} = \begin{bmatrix} A_1 & 0 \\ C_1+D_1S_1 & D_1 \end{bmatrix}.$$

Then $C_1+D_1S_1 \equiv 0(\bmod n)$ and so $M_3 \equiv \begin{bmatrix} A_1 & 0 \\ 0 & D_1 \end{bmatrix}(\bmod n)$.

Determine $U$, $V$ unimodular such that $UA_1V = P$ where $P$ is diagonal. By theorem 1 there are unimodular matrices $U_1$ and $V_1$ which are in upper triangular form modulo $h_i$ and such that $U_1 \equiv U(\bmod n)$ and $V_1 \equiv V(\bmod n)$. By theorem 2 $U_1$ and $V_1$ determine the $K$-symplectic matrices $\begin{bmatrix} U_1 & 0 \\ 0 & W_1 \end{bmatrix}$ and $\begin{bmatrix} V_1 & 0 \\ 0 & Z_1 \end{bmatrix}$. Then

$$M_4 = \begin{bmatrix} U_1 & 0 \\ 0 & W_1 \end{bmatrix}\begin{bmatrix} A_1 & 0 \\ 0 & D_1 \end{bmatrix}\begin{bmatrix} V_1 & 0 \\ 0 & Z_1 \end{bmatrix} \equiv \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix}(\bmod n)$$

where $P \equiv U_1A_1V_1(\bmod n)$ is diagonal and $Q \equiv W_1D_1Z_1(\bmod n)$. But $Q$ is diagonal modulo $n$ as $Q \equiv W_1D_1Z_1 = H(U_1A_1V_1)^{-1'}H^{-1}(\bmod n)$. Hence by lemma 5 there is a $K$-symplectic matrix $N_1$ such that $N_1 \equiv M_4(\bmod n)$. Since we have $M_4 = RMS$ where $R = \begin{bmatrix} U_1 & 0 \\ 0 & W_1 \end{bmatrix}$ and



$S = \begin{bmatrix} I & 0 \\ X & I \end{bmatrix}\begin{bmatrix} I & S \\ 0 & I \end{bmatrix}\begin{bmatrix} I & 0 \\ S_1 & I \end{bmatrix}\begin{bmatrix} V_1 & 0 \\ 0 & Z_1 \end{bmatrix}$. We define $N = R^{-1}N_1S^{-1}$. Then $N$ is $K$-symplectic and

$$N = R^{-1}N_1S^{-1} \equiv M(\bmod n).$$

We now give some applications of theorem 3.

**4.** We now define $\Gamma_K(n) = \{N \mid N \in \Gamma_K \text{ and } N \equiv I(\bmod n)\}$. $\Gamma_K(n)$ is called the *principal congruence subgroup of* $\Gamma_K$ *of level* $n$. $N$, a member of the principal congruence subgroup, is said to be *K-symplectic of level n*.

Clearly $\Gamma_K(n)$ is a normal subgroup of finite index in $\Gamma_K$. Given the natural homomorphism of $\Gamma_K$ into $\Gamma_K(\bmod n)$, it is easy to show that $\Gamma_K(n)$ is the kernel of the homomorphism. It follows that

$$\Gamma_K/\Gamma_K(n) \cong \Gamma_K(\bmod n).$$

In the remainder of the section let $d = (m, n)$ be the greatest common divisor of $m$ and $n$, and let $\delta = [m, n]$ be the least common multiple of $m$ and $n$. The proofs of the lemmas and theorems that follow up to and including lemma 8 are completely analogous to those of the corresponding lemmas and theorems given in [3] and [4].

LEMMA 6. *Let M be a K-symplectic matrix of level d. Then there is a matrix Y where Y is K-symplectic of level m and* $Y \equiv M(\bmod n)$.

LEMMA 7. *Let M be K-symplectic of level d. Then there is an* $M_1$, *K-symplectic of level m and an* $M_2$, *K-symplectic of level n such that* $M = M_1M_2$.

THEOREM 4. *The normal subgroups* $\Gamma_K(m)$, $\Gamma_K(n)$ *of* $\Gamma_K$ *satisfy*

$$\Gamma_K(m)\Gamma_K(n) = \Gamma_K(d), \qquad \Gamma_K(m) \cap \Gamma_K(n) = \Gamma_K(\delta).$$

THEOREM 5. *The following isomorphism exists* $\boldsymbol{M}(d, m) \cong \boldsymbol{M}(n, \delta)$ *where we define* $\boldsymbol{M}(a, b) = \Gamma_K(a)/\Gamma_K(b)$, *a divides b, the K-symplectic modulary group.*

THEOREM 6. *Let "×" represent the direct product. Then*

$$\boldsymbol{M}(d, \delta) \cong \boldsymbol{M}(d, m) \times \boldsymbol{M}(d, n).$$

COROLLARY. *If r is arbitrary and* $d = 1$ *then*

$$\boldsymbol{M}(r, rmn) \cong \boldsymbol{M}(r, rm) \times \boldsymbol{M}(r, rn).$$

THEOREM 7. *Let r and s be arbitrary and* $s = \prod_{p|s} p^{\beta_p}$. *For each prime p dividing s write r as* $r = r_p p^{\alpha_p}$ *where* $(r_p, p) = 1$. *Then* $\boldsymbol{M}(r, rs)$ *is isomorphic to the direct product*

$$\prod_{p|s} \boldsymbol{M}(p^{\alpha_p}, p^{\alpha_p+\beta_p}).$$

LEMMA 8. *If $s$ divides $r$, the $\boldsymbol{M}(r, rs)$ is abelian.*

We now consider the structure of $\boldsymbol{M}(m, mp^u)$ where $p$ is a prime and $p^u$ divides $m$. Let $E_{ij}$ be the matrix with 1 in the $(i, j)$ position and 0 elsewhere, and put $x_{ji} = h_j/h_i$, $j > i$, where $h_j$ and $h_i$ are invariant factors of $H$. Set

$$S_{ij} = \begin{cases} \begin{bmatrix} I & mE_{ii} \\ 0 & I \end{bmatrix}, & \text{if} \quad i = j, \\ \begin{bmatrix} I & m(E_{ij}+x_{ji}E_{ji}) \\ 0 & I \end{bmatrix}, & \text{if} \quad i < j, \end{cases} \tag{3}$$

$$W_{ij} = \begin{cases} \begin{bmatrix} I & 0 \\ mE_{ii} & I \end{bmatrix}, & \text{if} \quad i = j, \\ \begin{bmatrix} I & 0 \\ m(E_{ij}+x_{ji}E_{ji}) & I \end{bmatrix}, & \text{if} \quad i < j, \end{cases} \tag{4}$$

$$R_{ij} = \begin{bmatrix} I+mE_{ij} & 0 \\ 0 & I-mx_{ji}E_{ji} \end{bmatrix}. \tag{5}$$

There are $\frac{1}{2}(t^2+t)$ matrices $S_{ij}$, $\frac{1}{2}(t^2+t)$ matrices $W_{ij}$, and $t^2$ matrices $R_{ij}$. Matrices $S_{ij}$, $W_{ij}$ are $K$-symplectic as are matrices $R_{ij}$, $i \neq j$. Matrices $R_{ii}$ are not $K$-symplectic but are $K$-symplectic modulo $m^2$ and so modulo $mp^u$ since $p^u$ divides $m$. This suffices in view of theorem 3.

THEOREM 8. *Let $p$ be a prime where $p^u$ divides $m$ for some $m$. Then $\boldsymbol{M}(m, mp^u)$ is an abelian group of order $p^{u(2t^2+t)}$ and of type $(p^u, p^u, \ldots, p^u)$. The generators are given modulo $mp^u$ by the matrices* (3), (4), *and* (5).

Proof. By lemma 8 $\boldsymbol{M}(m, mp^u)$ is abelian since $p^u$ divides $m$. Let $M$ be $K$-symplectic of level $m$ and of the form

$$M = \begin{bmatrix} I+mA & mB \\ mC & I+mD \end{bmatrix}.$$

Then $M$ is $K$-symplectic which implies $AH \equiv -HD' (\operatorname{mod} m)$, $BH \equiv HB' (\operatorname{mod} m)$, and $CH \equiv HC' (\operatorname{mod} m)$. Since $p^u$ divides $m$ the congruences hold modulo $p^u$. By lemma 3 there is an $H$-symmetric matrix $X$ and an $H$-symmetric matrix $Y$ such that $X \equiv B (\operatorname{mod} p^u)$ and $Y \equiv C (\operatorname{mod} p^u)$. And by the method used in lemma 3, $A_0$ can be determined such that $A_0 \equiv A (\operatorname{mod} m)$ and $HA_0'H^{-1}$ has integral elements. Then

$$M \equiv \begin{bmatrix} I & mX \\ 0 & I \end{bmatrix} \begin{bmatrix} I & 0 \\ mY & I \end{bmatrix} \begin{bmatrix} I+mA_0 & 0 \\ 0 & I-mHA_0'H^{-1} \end{bmatrix} (\operatorname{mod} mp^u).$$

The matrices

$$\begin{bmatrix} I & mX \\ 0 & I \end{bmatrix}, \quad \begin{bmatrix} I & 0 \\ mY & I \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} I+mA_0 & 0 \\ 0 & I-mHA_0'H^{-1} \end{bmatrix}$$



are all expressible modulo $mp^u$ in an obvious way in terms of matrices (3), (4), and (5) so that these indeed generate $\Gamma_K(m)$ modulo $\Gamma_K(mp^u)$. Furthermore they are independent modulo $mp^u$ and have period $p^u$ modulo $\Gamma_K(mp^u)$.

Let $m = p^v$ and there follows

COROLLARY. *If $1 \leqslant u \leqslant v$ then $\boldsymbol{M}(p^v, p^{u+v})$ is an abelian group of order $p^{u(2t^2+t)}$ and of type $(p^u, p^u, \ldots, p^u)$. The generators modulo $p^{u+v}$ may be chosen as the matrices* (3), (4), *and* (5) *with $m = p^v$.*

Theorem 7 and the corollary to theorem 8 imply

THEOREM 9. *Let $n$ divide $m$ and $n = \prod_{p|n} p^{\beta_p}$. For each prime $p$ dividing $n$ write $m$ as $m = m_p p^{\alpha_p}$ where $(m_p, p) = 1$. Then $1 \leqslant \beta_p \leqslant \alpha_p$ and $\boldsymbol{M}(m, mn)$ is isomorphic to the direct product $\prod_{p|n} \boldsymbol{M}(p^{\alpha_p}, p^{\alpha_p+\beta_p})$.*

Hence the structure of the group $\boldsymbol{M}(m, mn)$ where $n$ divides $m$ is determined in view of the corollary above and theorem 9.

The above does not apply if $\beta_p > \alpha_p$. A simple calculation shows that two different groups of the same order have centers of different orders and hence have different structures. Thus no group with $\beta_p > \alpha_p$ can be isomorphic to a different group with $\beta_{p'} > \alpha_{p'}$.

**References**

[1] L. K. Hua and I. Reiner, *On the generators of the symplectic modular group*, Trans. Amer. Math. Soc. 65 (1949), pp. 415-426.

[2] M. Newman and I. Reiner, *Inclusion theorems for congruence subgroups*, Trans. Amer. Math. Soc. 91 (1959), pp. 369-379.

[3] M. Newman and J. R. Smart, *Modulary groups of t×t matrices*, Duke Math. Journal 30 (1963), pp. 253-257.

[4] — — *Symplectic modulary groups*, Acta Arith. 9 (1964), pp. 83-90.

*Reçu par la Rédaction le 22. 12. 1964*