CONGRUENCE SUBGROUPS OF MATRIX GROUPS

IRVING REINER AND J. D. SWIFT

1. Introduction. Let M_r^+ denote the modular group consisting of all integral $r \times r$ matrices with determinant $+1$. Define the subgroup G_n, of M_2^+ to be the group of all matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

of M_2^+ for which $c \equiv 0 \pmod{n}$. M. Newman [1] recently established the following theorem:

Let H be a subgroup of M_2^+ satisfying $G_{mn} \subset H \subset G_n$. Then $H = G_{an}$, where $a|m$.

In this note we indicate two directions in which the theorem may be extended: (i) Letting the elements of the matrices lie in the ring of integers of an algebraic number field, and (ii) Considering matrices of higher order.

2. Ring of algebraic integers. For simplicity, we restrict our attention to the group G of 2×2 matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{1}$$

where a, b, c, d lie in the ring $\mathscr{D}$ of algebraic integers in an algebraic number field. Small Roman letters denote elements of $\mathscr{D}$, German letters denote ideals in $\mathscr{D}$.

Let $G(\mathfrak{N})$ be the subgroup of G defined by the condition that $c \equiv 0 \pmod{\mathfrak{N}}$. We shall prove the following.

THEOREM 1. *Let H be a subgroup of G satisfying*

$$G(\mathfrak{M}\mathfrak{N}) \subset H \subset G(\mathfrak{N}), \tag{2}$$

where $(\mathfrak{M}, (6)) = (1)$. Then $H = G(\mathfrak{D}\mathfrak{N})$ for some $\mathfrak{D} \supset \mathfrak{M}$.

Proof. 1. As in Newman's proof, we use induction on the number of prime ideal factors of $\mathfrak{M}$. The result is clear for $\mathfrak{M} = (1)$. Assume it holds for a product of fewer than k prime ideals, and let $\mathfrak{M} = \mathfrak{Q}_1 \cdots \mathfrak{Q}_k$ $(k \geq 1)$, where the $\mathfrak{Q}_i$ are prime ideals (not necessarily distinct). For

Received June 17, 1955. The research of Professor Swift and the preparation of this paper were supported by the Office of Naval Research under Contract NR 045 141.

the remainder of this section of the proof, let $\mathfrak{R}$ denote a divisor of $\mathfrak{M}$, with $\mathfrak{R}\neq(1)$; set $\mathfrak{M}=\mathfrak{R}\mathfrak{M}'$. Intersecting the groups in (2) with $G(\mathfrak{R}\mathfrak{R})$, we obtain

$$G(\mathfrak{R}\mathfrak{M}'\mathfrak{R})\subset H\cap G(\mathfrak{R}\mathfrak{R})\subset G(\mathfrak{R}\mathfrak{R})\ .$$

Since $\mathfrak{M}'$ has fewer prime ideal factors than $\mathfrak{M}$, the induction hypothesis gives

$$H\cap G(\mathfrak{R}\mathfrak{R})=G(\mathfrak{R}'\mathfrak{R}\mathfrak{R})\ , \qquad \mathfrak{R}'\supset\mathfrak{M}'\ ,$$

and therefore

$$G(\mathfrak{R}'\mathfrak{R}\mathfrak{R})\subset H\subset G(\mathfrak{R})\ .$$

Suppose now that for some $\mathfrak{R}$ we have $\mathfrak{R}'\neq\mathfrak{M}'$. Then the induction hypothesis yields $H=G(\mathfrak{S}\mathfrak{R})$ with $\mathfrak{S}\supset\mathfrak{R}'\mathfrak{R}\supset\mathfrak{M}$, and we are through. Thus we may assume hereafter that $\mathfrak{R}'=\mathfrak{M}'$ for each $\mathfrak{R}$, so that

$$H\cap G(\mathfrak{R}\mathfrak{R})=G(\mathfrak{M}\mathfrak{R})$$

for each $\mathfrak{R}$. Therefore for every $A\in H$ given by (1), either $c\in\mathfrak{M}\mathfrak{R}$ or else ((c), $\mathfrak{M}\mathfrak{R})=\mathfrak{R}$.

2. Next we shall assume that $H\neq G(\mathfrak{M}\mathfrak{R})$, and try to establish that $H=G(\mathfrak{R})$. Let us suppose that $n_1, \cdots, n_t\in\mathscr{O}$ form a Z-basis[1] for $\mathfrak{R}$, and put

$$W_j=\begin{pmatrix}1 & 0\\ n_j & 1\end{pmatrix}, \qquad Y=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}. \tag{3}$$

It is easy to see that the W_j and the matrix Y generate a complete set of left coset representatives of $G(\mathfrak{R})$ relative to $G(\mathfrak{M}\mathfrak{R})$. Since obviously $Y\in G(\mathfrak{M}\mathfrak{R})\subset H$, it suffices to prove that each $W_j\in H$.

Let us now put $\mathfrak{M}=\prod_i\mathfrak{Q}_i^{a_i}$, $\mathfrak{R}=\prod_i\mathfrak{Q}_i^{b_i}$, where $a_i\geqq 0$, $b_i\geqq 0$, $a_i+b_i>0$, and $\mathfrak{Q}_i$, $\mathfrak{Q}_j$ are distinct prime ideals when $i\neq j$. (Notation: $\mathfrak{Q}_i^{a_i}\|\mathfrak{M}$). We shall show that the Z-basis $\{n_j\}$ of $\mathfrak{R}$ may be adjusted so that

$$\mathfrak{Q}_i^{b_i}\|(n_j) \qquad \text{for each } j \text{ and each } i. \tag{4}$$

For suppose the n_j chosen so that (4) holds for each j for $i=1, \cdots, r-1$; we show how to choose a new set $\{n_j'\}$ so that $\mathfrak{Q}_i^{b_i}\|(n_j')$ for all j for $i=1, \cdots, r$. By renumbering the n_j, we may assume that $\mathfrak{Q}_r^{b_r}\|(n_1)$. Choose $u\in\mathfrak{Q}_1^{b_1+1}\cdots\mathfrak{Q}_{r-1}^{b_{r-1}+1}$, $u\notin\mathfrak{Q}_r$, and replace each n_j for which $n_j\in\mathfrak{Q}_r^{b_r+1}$ by $n_j'=n_j+un_1$. Then

$$n_j'\equiv n_j \pmod{\mathfrak{Q}_i^{b_i+1}}\ , \qquad i=1, \cdots, r-1\ ,$$
$$n_j'\equiv un_1 \text{ or } n_j \pmod{\mathfrak{Q}_r^{b_r+1}}\ ,$$

[1] Z denotes the set of rational integers.

according as to whether $n_j \in \mathfrak{Q}_r^{b_r+1}$ or not. This implies the desired result.

3. Since the group H properly contains $G(\mathfrak{MN})$, by the preceding discussion it follows that there exists an element

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H \tag{5}$$

in which $(c)=\mathfrak{NC}$ with $(\mathfrak{C}, \mathfrak{M})=(1)$. Therefore H also contains, for each $x \in \mathfrak{D}$, the product

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a+xc & \cdot \\ c & \cdot \end{pmatrix}.$$

Since $(a, c)=(1)$, we may choose x so that $((a+xc), \mathfrak{M})=(1)$. Hence we may assume that H contains an element A given by (5), satisfying

$$((a), \mathfrak{M})=(1), \quad (c)=\mathfrak{NC}, \quad (\mathfrak{C}, \mathfrak{M})=(1). \tag{6}$$

Next we remark that

$$\begin{pmatrix} 1 & 0 \\ n_j y_j & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} \cdot & \cdot \\ n_j y_j a+c & \cdot \end{pmatrix},$$

so that if y_j is chosen to satisfy $n_j y_j a+c \in \mathfrak{MN}$, it will follow that

$$W_j^*=\begin{pmatrix} 1 & 0 \\ n_j y_j & 1 \end{pmatrix} \in H. \tag{7}$$

But now $n_j y_j a+c \in \mathfrak{MN}$ means that

$$n_j y_j a \equiv -c \pmod{\mathfrak{Q}_i^{a_i+b_i}} \text{ for each } i.$$

If $a_i=0$, then $\mathfrak{Q}_i^{b_i}$ divides both (n_j) and (c), and there is no condition on y_j. If $a_i>0$, then $\operatorname{ord}_{\mathfrak{Q}_i} a=0$, $\operatorname{ord}_{\mathfrak{Q}_i} n_j=b_i$, and $\operatorname{ord}_{\mathfrak{Q}_i} c=b_i$, so that the congruence is solvable for y_j. We remark further that y_j may be chosen coprime to any fixed ideal. Thus for each n_j, there exists an element $y_j \in \mathfrak{D}$ such that $((y_j), \mathfrak{MN})=(1)$, and for which $W_j^* \in H$. In order to complete the proof of the theorem, we need only show that if

$$\begin{pmatrix} 1 & 0 \\ ny & 1 \end{pmatrix} \in H. \tag{8}$$

where $\mathfrak{Q}_i^{b_i} \| (n)$ for each i, and where $((y), \mathfrak{MN})=(1)$, then also

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \in H.$$

4. Now let $d \in \mathfrak{D}$ be any element coprime to $\mathfrak{MN}$; then there

exists $a \in \mathscr{D}$ such that $ad \equiv 1 \pmod{\mathfrak{M}\mathfrak{N}}$. Setting $ad = 1 + c$, with $c \in \mathfrak{M}\mathfrak{N}$, we see that

$$\begin{pmatrix} a & 1+xa \\ c & d+xc \end{pmatrix} \in G(\mathfrak{M}\mathfrak{N}) \subset H$$

for all $x \in \mathscr{D}$. In particular, choosing x so that $1+xa \in \mathfrak{M}\mathfrak{N}$, we see that H contains a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in which both b and c lie in $\mathfrak{M}\mathfrak{N}$. Therefore H also contains

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ ny & 1 \end{pmatrix} \equiv \begin{pmatrix} a & \cdot \\ dyn & \cdot \end{pmatrix} \pmod{\mathfrak{M}\mathfrak{N}}.$$

But then

$$\begin{pmatrix} 1 & 0 \\ nu & 1 \end{pmatrix}\begin{pmatrix} a & \cdot \\ dyn & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & \cdot \\ n(ua+dy) & \cdot \end{pmatrix},$$

and so if $u \in \mathscr{D}$ is chosen satisfying $n(ua+dy) \in \mathfrak{M}\mathfrak{N}$, then the matrix

$$\begin{pmatrix} 1 & 0 \\ nu & 1 \end{pmatrix} \in H.$$

However, $n(ua+dy) \in \mathfrak{M}\mathfrak{N}$ if and only if

$$n(ua+dy) \equiv 0 \pmod{\mathfrak{Q}_i^{a_i+b_i}} \quad \text{for each } i,$$

that is,

$$u \equiv -dy/a \pmod{\mathfrak{Q}_i^{a_i}} \quad \text{for each } i.$$

Since $ad \equiv 1 \pmod{\mathfrak{Q}_i^{a_i}}$, this gives $u \equiv -yd^2 \pmod{\mathfrak{Q}_i^{a_i}}$.

We have thus shown that (8) implies

$$\begin{pmatrix} 1 & 0 \\ nyd^2 & 1 \end{pmatrix} \in H$$

for every d coprime to $\mathfrak{M}\mathfrak{N}$. Consequently H contains every product of such matrices, that is,

$$\begin{pmatrix} 1 & 0 \\ nyx & 1 \end{pmatrix} \in H \tag{9}$$

whenever $x = \sum d_i^2$, with each d_i coprime to $\mathfrak{M}\mathfrak{N}$. To complete the proof, it suffices to show that there exists such an x for which $yx \equiv 1 \pmod{\mathfrak{M}}$. For then $yx = 1 + m$ with $m \in \mathfrak{M}$, and

$$\begin{pmatrix} 1 & 0 \\ nyx & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -mn & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \in H .$$

Finally, $y\sum d_i^2 \equiv 1 \pmod{\mathfrak{M}}$ implies $y \equiv \sum(yd_i)^2 \pmod{\mathfrak{M}}$, and conversely, so we need only show the existence of numbers d_i coprime to $\mathfrak{M}\mathfrak{N}$ such that

$$y \equiv \sum d_i^2 \qquad (\mathrm{mod}\ \mathfrak{M}).$$

5. We begin by examining the finite field $\mathfrak{L}=\mathfrak{O}/\mathfrak{Q}_i$, where $\mathfrak{Q}_i|\mathfrak{M}$. The characteristic of $\mathfrak{L}$ is p, the unique rational prime in $\mathfrak{Q}_i$. Since $(\mathfrak{M}, (6))=(1)$, certainly $p>3$. The nonzero elements of $\mathfrak{L}$ form a multiplicative group, and the map $x \to x^2$ gives an endomorphism of this group with kernel ± 1. Hence exactly half of the nonzero elements of $\mathfrak{L}$ are squares, and we have the usual rules for multiplying quadratic residues and nonresidues. In particular, $\mathfrak{L}$ contains at least two distinct squares.

Now we show that $\mathfrak{M}$ is a power of a single prime. For let $\mathfrak{Q}_1|\mathfrak{M}$, $\mathfrak{Q}_2|\mathfrak{M}$, with $\mathfrak{Q}_1 \neq \mathfrak{Q}_2$, and let p be the characteristic of $\mathfrak{O}/\mathfrak{Q}_1$. If we choose $d_i \equiv 1 \pmod{\mathfrak{Q}_1}$ $(i=1, \cdots, p)$, then $x=\sum d_i^2 \equiv 0 \pmod{\mathfrak{Q}_1}$. On the other hand, since there are at least two distinct squares $(\mathrm{mod}\ \mathfrak{Q}_2)$ by the above argument, we may choose the d_i coprime to $\mathfrak{M}\mathfrak{N}$ such that $(\mathfrak{Q}_2, (x))=(1)$. But then the matrix given by (9) lies in H, which is impossible by virtue of the discussion at the end of Part 1 of this proof, for $\mathfrak{Q}_1\mathfrak{N}|((nyx), \mathfrak{M}\mathfrak{N})$, but $\mathfrak{Q}_2 \nmid ((nyx), \mathfrak{M}\mathfrak{N})$.

We need only prove now that

$$y \equiv \sum d_i^2 \qquad (\mathrm{mod}\ \mathfrak{Q}^a)$$

is solvable for a set of d_i each coprime to $\mathfrak{Q}$. Since $(\mathfrak{Q}, (2))=(1)$, we may show by a well-known procedure that for any d coprime to $\mathfrak{Q}$, and any $q \in \mathfrak{Q}$, there exists $\overline{d} \in \mathfrak{O}$ such that

$$d^2+q \equiv \overline{d}^2 \qquad (\mathrm{mod}\ \mathfrak{Q}^a).$$

Hence it suffices to prove that

$$y \equiv \sum d_i^2 \qquad (\mathrm{mod}\ \mathfrak{Q})$$

is solvable, that is, that every nonzero element in $\mathfrak{L}=\mathfrak{O}/\mathfrak{Q}$ is expressible as a sum of squares. We need only show that any non-square in $\mathfrak{L}$ is a sum of squares, and for this it is sufficient to show that at least one non-square is the sum of squares. For then all non-squares are obtained from the given non-square by multiplying by suitable squares.

Now if the sum of squares in $\mathfrak{L}$ were always a square, then the squares would form a subfield $\mathfrak{K}$, and we would have $[\mathfrak{L}: \mathfrak{K}]=2$. This

is impossible, since the number of elements in $\mathfrak{L}=\mathfrak{D}/\mathfrak{Q}$ is odd, being a power of the characteristic of $\mathfrak{D}/\mathfrak{Q}$.

3. Two examples. The hypothesis that $(\mathfrak{M}, (6))=(1)$ seems almost superfluous in the above proof, entering only in the discussion of squares (mod $\mathfrak{Q}_i^{a_i}$), and it might be thought that a different proof could be found which would obviate this restriction. To show that this is not the case, we give here two examples in which (2) holds, but where the conclusion of Theorem 1 is not valid; in the first example, $(\mathfrak{M}, (2)) \neq (1)$, and in the second, $(\mathfrak{M}, (3)) \neq (1)$. We shall use the notation $G(n)$ to denote $G((n))$, where (n) is a principal ideal.

Firstly, let $\mathfrak{D}$ be the ring of Gaussion integers. We shall exhibit a group H for which

$$G(4) \subset H \subset G(2) , \tag{10}$$

with both inclusions proper, and such that $H \neq G(2+2i)$. Since $G(2+2i)$ is the only congruence subgroup between $G(2)$ and $G(4)$, this shows that the conclusion of Theorem 1 does not hold here.

Let us set

$$B=\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}.$$

Let H be the group generated by B and $G(4)$; clearly (10) holds. Let X denote the general element of $G(4)$, say

$$X=\begin{pmatrix}a & b\\ c & d\end{pmatrix} \equiv \begin{pmatrix}a & b\\ 0 & d\end{pmatrix} \pmod 4 .$$

Then

$$BXB^{-1} \equiv \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}=\begin{pmatrix}\cdot & \cdot\\ 2(a+d) & \cdot\end{pmatrix} \pmod 4 .$$

However, $ad \equiv 1 \pmod 4$ implies (by consideration of cases) that $a+d \equiv 0 \pmod 2$. Therefore $BG(4)B^{-1}=G(4)$, and hence $G(4)$ is of index 2 in H. Since $G(4)$ has index 4 in $G(2)$, we see that H is neither $G(4)$ nor $G(2)$. Furthermore, $H \neq G(2+2i)$, since $B \notin G(2+2i)$.

For our second example, let us take $\mathfrak{D}$ to be the ring of integers in the field obtained by adjoining α to the rational field, where α is a zero of x^2+5. Then $\mathfrak{D}=\{a+b\alpha : a \in Z,\ b \in Z\}$. In this ring we have the factorization $(3)=\mathfrak{Q}_1\mathfrak{Q}_2$, where

$$\mathfrak{Q}_1=(3,\ 2+\alpha) , \quad \mathfrak{Q}_2=(3,\ 2-\alpha)$$

are prime ideals with norm 3. Let H be the group generated by B and $G(9)$, where

$$B=\begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix}.$$

Then clearly $G(9)\subset H\subset G(3)$, with the first inclusion proper. Certainly H is not an intermediate congruence subgroup, since $H=G(3\mathfrak{P})$ would imply (because $B\in H$) that $3\mathfrak{P}|(3)$. We need only prove that $H\neq G(3)$, which is the case since $[H: G(9)]=3$, whereas $[G(3): G(9)]=9$. For we have, as in the previous example, the result that $BG(9)B^{-1}=G(9)$, following easily from the fact that $ad\equiv 1 \pmod 9$ implies $a\equiv d \pmod 3$.

The question as to the necessary and sufficient conditions on the ideals $\mathfrak{M}$, $\mathfrak{N}$ to insure the validity of the conclusion of Theorem 1 seems more difficult, since the answer will certainly depend on the structure of $\mathscr{D}$. For example, it is possible to give certain special cases in which Theorem 1 holds, even though $(\mathfrak{M}, (6))\neq(1)$.

4. Higher dimension. Turning now to the domain of rational integers, there is no direct and complete generalization of Newman's theorem valid for higher dimensions, owing to the profusion of possible congruence subgroups. For example, we may define a 3-parameter family of subgroups $G(m, n, r)$ of M_3^+, where $r|(m, n)$, by setting

$$G(m, n, r)=\{(a_{ij})\in M_3^+ : m|a_{21},\ n|a_{32},\ r[m, n]|a_{31}\}\ .$$

(Here, $[m, n]$=L.C.M. of m and n.) It would be reasonable to conjecture that if H is a group satisfying $G(am, bn, cr)\subset H\subset G(m, n, r)$, where $cr|(am, bn)$, then $H=G(\alpha m, \beta n, \gamma r)$ with $\alpha|a$, $\beta|b$, $\gamma|c$, and $\gamma r|(\alpha m, \beta n)$. The proof of such a conjecture would be rather tedious, and would have no direct generalization to higher dimensions.

We shall therefore restrict our attention to two specific types of groups which are readily defined in all dimensions, the column groups

$$C_m=\{(a_{ij})\in M_r^+ : m|a_{21},\ m|a_{31},\ \cdots,\ m|a_{r1}\}$$

and the row groups

$$R_n=\{(a_{ij})\in M_r^+ : n|a_{r1},\ n|a_{r2},\ \cdots,\ n|a_{r,r-1}\}\ .$$

THEOREM 2.[2] *Let H be a subgroup of M_r^+ satisfying*

$$(C_{am}\cap R_{bn})\subset H\subset (C_m\cap R_n)\ ,$$

where $(am, bn)=1$. Then $H=C_{am}\cap R_{\beta n}$, where $\alpha|a$ and $\beta|b$.

Proof. We shall carrry out the proof for $r=3$, since higher dimen-

[2] M. Newman has informed the authors that he has independently obtained the results comprised in this theorem.

sions present little additional difficulty. We shall use induction on the number of prime factors of b, and begin with the case $b=1$. When $a=1$ also, the result is clear. Suppose it is true for all a with fewer than k prime factors, and now let a have k prime factors. Then by hypothesis

$$(C_{am} \cap R_n) \subset H \subset (C_m \cap R_n) .$$

As in the proof of Theorem 1, intersect this with C_{Am}, where $A \neq 1$ and $A|a$. Then either the desired result follows from the induction hypothesis on a, or else for each such A we have

$$H \cap C_{Am} = C_{am} \cap R_n .$$

Therefore for any element

$$T = \begin{pmatrix} a_{11} & . & . \\ ma_{21} & . & . \\ mna_{31} & . & . \end{pmatrix} \tag{11}$$

of H, either $(a_{21}, a_{31}, a)=1$ or $(a_{21}, a_{31}, a)=a$.

Now suppose that $H \neq C_{am} \cap R_n$. Then for some $T \in H$ the former alternative occurs. Then for any x, y, z, the matrix

$$T_1 = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & . & . \\ ma_{21} & . & . \\ mna_{31} & . & . \end{pmatrix} = \begin{pmatrix} a_{11}+m(xa_{21}+yna_{31}) & . & . \\ m(a_{21}+zna_{31}) & . & . \\ mna_{31} & . & . \end{pmatrix}$$

lies in H. Since $(a_{11}, ma_{21}, mna_{31})=1$, by proper choice of x, y, z we may make the elements in the (1, 1) and (2, 1) positions of T_1 coprime to a. Changing notation, we may now assume that H contains an element T given by (11), satisfying $(a_{11}, a)=(a_{21}, a)=1$.

Next, replacing T by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & nt & 1 \end{pmatrix} T \in H$$

leaves a_{11} and a_{21} unaltered, and replaces a_{31} by $a'_{31}=a_{31}+ta_{21}$. By proper choice of t, we may make $(a'_{31}, a)=1$. Again changing notation, H now contains an element T for which

$$(a_{11}, a)=(a_{21}, a)=(a_{31}, a)=1 .$$

We next observe that

$$(12)\qquad \begin{pmatrix} 1 & 0 & 0 \\ my & 1 & 0 \\ mnz & 0 & 1 \end{pmatrix} T = \begin{pmatrix} a_{11} & . & . \\ m(a_{11}y+a_{21}) & . & . \\ mn(a_{11}z+a_{31}) & . & . \end{pmatrix}.$$

If y and z are chosen so that

$$a_{11}y+a_{21} \equiv a_{11}z+a_{31} \equiv 0 \pmod{a},$$

then the right-hand side of (12) will lie in $C_{am} \cap R_n$, hence in H. Therefore H contains a matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ my & 1 & 0 \\ mnz & 0 & 1 \end{pmatrix}$$

with both y and z coprime to a.

But then

$$\begin{pmatrix} 1 & 0 & 0 \\ mau & 1 & t \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ my & 1 & 0 \\ mnz & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -t \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ m(au+y+ntz) & 1 & 0 \\ mnz & 0 & 1 \end{pmatrix} \in H,$$

and also

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ mnau & nt & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ my & 1 & 0 \\ mnz & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -nt & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ my & 1 & 0 \\ mn(au+ty+z) & 0 & 1 \end{pmatrix} \in H.$$

By proper choice of t and u in each case, we deduce that $P^y \in H$ and $S^z \in H$, where

$$P = \begin{pmatrix} 1 & 0 & 0 \\ m & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ mn & 0 & 1 \end{pmatrix}.$$

On the other hand, $P^a \in H$ and $S^a \in H$. Since $(y, a)=(z, a)=1$, it follows at once that P and S are both in H.

Now let

$$U = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad V = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then P, S, U, V generate a complete set of left coset representatives of $C_m \cap R_n$ with respect to $C_{am} \cap R_n$. Since P, S, U, V are all in H, this shows that $H = C_m \cap R_n$. Hence we have established the theorem

when $b=1$, for all a. A corresponding proof can be given when $a=1$, for all b.

Suppose now that the theorem has been proved for all a whenever b has fewer than k prime factors, and take b to have k prime factors. The result certainly holds when $a=1$. Assume it true for a having fewer than k' prime factors, and now let a have k' prime factors. By hypothesis

$$(C_{am} \cap R_{bn}) \subset H \subset (C_m \cap R_n) .$$

Intersect this with C_{Am}, where $A|a$ and $A \neq 1$. Then as before, the result holds (by virtue of the induction hypothesis) unless

$$H \cap C_{Am} = C_{am} \cap R_{bn} \tag{13}$$

for all such A. Likewise, the result holds unless for each $B \neq 1$, $B|b$ we have

$$H \cap R_{Bn} = C_{am} \cap R_{bn} . \tag{14}$$

From (13) and (14) we deduce that if

$$T = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ ma_{21} & a_{22} & a_{23} \\ mna_{31} & na_{32} & a_{33} \end{pmatrix} \in H ,$$

then either

$$(a_{21}, a_{31}, a) = a \quad \text{and} \quad (a_{31}, a_{32}, b) = b \tag{15}$$

or

$$(a_{21}, a_{31}, a) = (a_{31}, a_{32}, b) = 1 . \tag{16}$$

To complete the proof, we shall assume that $H \neq C_{am} \cap R_{bn}$, and obtain a contradiction. Under this hypothesis, (16) must hold for some $T \in H$. Replacing T by

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} T$$

with suitably chosen x, y, z, we may hereafter assume that $(a_{11}, ab) = (a_{21}, a) = 1$.

We now show that H contains a matrix T satisfying

$$(a_{11}, ab) = (a_{21}, a) = (a_{22}, b) = 1 , \qquad b|a_{12} . \tag{17}$$

Upon replacing T of the preceding paragraph by

$$T\begin{pmatrix}1 & k & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

a_{11} and a_{21} are unchanged, and a_{12} becomes $a'_{12}=a_{12}+ka_{11}$. If we choose k so that $b|a'_{12}$, we shall have a matrix (again denoted by T) in H, for which $(a_{11}, ab)=(a_{21}, a)=1$, $b|a_{12}$. Lastly, replace T by

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & ax\\ 0 & 0 & 1\end{pmatrix}T\in H\,.$$

This leaves a_{11} and a_{12} unaltered, does not change $a_{21} \pmod a$, and replaces a_{22} by $a'_{22}=a_{22}+anxa_{32}$. Since $(a_{22}, ana_{32}, b)=1$, we may choose x so that $(a'_{22}, b)=1$. This new matrix T will then satisfy (17).

Let us put

$$Y=\begin{pmatrix}1 & 0 & 0\\ mx & 1 & 0\\ mny & nz & 1\end{pmatrix}.$$

Then

$$YT=\begin{pmatrix}a_{11} & \cdot & \cdot\\ m(a_{21}+xa_{11}) & \cdot & \cdot\\ mn(a_{31}+ya_{11}+za_{21}) & n(a_{32}+mya_{12}+za_{22}) & \cdot\end{pmatrix}.$$

If x, y, z satisfy

$$a_{21}+xa_{11}\equiv 0 \pmod a\,, \tag{18}$$

$$a_{31}+ya_{11}+za_{21}\equiv 0 \pmod{ab}\,, \tag{19}$$

$$a_{32}+mya_{12}+za_{22}\equiv 0 \pmod b\,, \tag{20}$$

then the product YT will lie in $C_{am}\cap R_{bn}$, hence in H, and so $Y\in H$. We may certainly solve (18) with $(x, a)=1$. Since $b|a_{12}$, we may solve (20) for $z \pmod b$. Fixing z arbitrarily $(\mathrm{mod}\ a)$, we may then solve (19) for y, since $(a_{11}, ab)=1$. Therefore H contains a matrix Y in which $(x, a)=1$.

But now

$$Y^b\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & -bnz & 1\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\ mbx & 1 & 0\\ mny_1 & 0 & 1\end{pmatrix}\in H\,,$$

and so

$$W=\begin{pmatrix} 1 & 0 & 0 \\ mbx & 1 & 0 \\ mny_1 & 0 & 1 \end{pmatrix}^b=\begin{pmatrix} 1 & 0 & 0 \\ mb^2x & 1 & 0 \\ mnby_1 & 0 & 1 \end{pmatrix}\in H\,.$$

However, $W\in R_{bn}$, so by (14) since $b>1$, also $W\in C_{am}$. This is impossible, since $(a, b^2x)=1$. We thus have a contradiction, and so H must equal $C_{am}\cap R_{bn}$. This comptes the proof.

We remark in conclusion that various special theorems may be proved by similar methods. For example, using the notation at the beginning of this section, we may show that $G(m, n, rs)\subset H\subset G(m, n, s)$ implies $H=G(m, n, ts)$ with $t|r$.

REFERENCE

1. Morris Newman, *Structure theorems for modular subroups*, Duke Math. J., **22** (1955), 25–32,

INSTITUTE FOR ADVANCED STUDY; UNIVERSITY OF ILLINOIS.
INSTITUTE FOR ADVANCED STUDY; UNIVERSITY OF CALIFORNIA, LOS ANGELES.