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 $c\equiv 0$ $(\bmod\, \mathfrak{N})$. 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 $\mathfrak{M}=\mathfrak{Q}_1\cdots\mathfrak{Q}_k$ $(k\geqq 1)$, 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.