AN ALTERNATIVE PROOF OF A THEOREM ON UNIMODULAR GROUPS

MORRIS NEWMAN

Introduction. Let G denote the multiplicative group of matrices

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

where a, b, c, d are integers and $ad-bc=1$, and $G_0(n)$ the subgroup of G characterized by $c\equiv 0 \pmod{n}$, where n is an integer different from 0. In a forthcoming paper [1] the author has proved the following theorem:

THEOREM 1. *Let H be a subgroup of G containing $G_0(n)$. Then $H=G_0(m)$, where $m \mid n$.*

The proof given was by an induction and made use of properties of the representatives of $G_0(nN)$ in $G_0(n)$. The referee for [1] furnished the author with an ingenious proof of Theorem 1 which avoided the induction. Since then the author has found a simpler proof which is more illuminating. This proof of Theorem 1 will be given here.

Set

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad W = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

We note that

$$S^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \qquad W^k = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}.$$

S is an element of $G_0(n)$ for every n, and so $S\in H$.

LEMMA 1. *Let*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H.$$

Then $W^c\in H$.

PROOF. We have

$$S^x M = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+xc & b+xd \\ c & d \end{pmatrix} \in H.$$

Received by the editors January 21, 1955.

Since $(a, c)=1$, there is an x such that $(a+xc, n)=1$. (This is a consequence of Dirichlet's theorem, but can be proved in an elementary fashion. See e.g., p. 17 [2].) Thus associated with every matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$$

there is a matrix

$$M_0 = \begin{pmatrix} a_0 & b_0 \\ c & d \end{pmatrix} \in H$$

such that $(a_0, n)=1$.

Since $(a_0, n)=1$, we can determine y such that $a_0 y \equiv c \pmod{n}$. Then

$$W^{-v}M_0 = \begin{pmatrix} 1 & 0 \\ -y & 1 \end{pmatrix}\begin{pmatrix} a_0 & b_0 \\ c & d \end{pmatrix} = \begin{pmatrix} a_0 & b_0 \\ c - a_0 y & d - b_0 y \end{pmatrix} \in G_0(n).$$

Hence $W^{-v}M_0 \in H$, and so $W^{-v} \in H$. Thus $W^{a_0 v} \in H$. Since $a_0 y \equiv c \pmod{n}$ and $W^n \in G_0(n) \subseteq H$, $W^c \in H$. Lemma 1 is thus proved.

LEMMA 2. *Let Z denote the totality $\{c\}$, where*

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

Then Z is an ideal in the ring of integers and hence a principal ideal.

PROOF. This is immediate, since if $c_1, c_2 \in Z$ then $W^{c_1}, W^{c_2} \in H$ by Lemma 1, and so for arbitrary integers p, q

$$(W^{c_1})^p (W^{c_2})^q = W^{pc_1 + qc_2} \in H,$$

whence $pc_1 + qc_2 \in Z$.

We turn now to the proof of Theorem 1. Put $Z=(m)$. Since $G_0(n) \subseteq H$, $(n) \subseteq Z$, and so $m \mid n$. Trivially, $H \subseteq G_0(m)$. Furthermore, let

$$M = \begin{pmatrix} a & b \\ mc & d \end{pmatrix} \in G_0(m).$$

Reasoning as before, we can find an x such that

$$S^x M = \begin{pmatrix} a_0 & b_0 \\ mc & d \end{pmatrix},$$

where $(a_0, n)=1$. Since $(a_0, n)=1$, we can determine y so that $a_0 y \equiv -1 \pmod{n}$. For this y,

$$W^{mcy}S^{x}M = \begin{pmatrix} 1 & 0 \\ mcy & 1 \end{pmatrix}\begin{pmatrix} a_0 & b_0 \\ mc & d \end{pmatrix}$$

$$= \begin{pmatrix} a_0 & b_0 \\ mc(a_0y + 1) & mcyb_0 + d \end{pmatrix} \in G_0(n).$$

Hence $W^{mcy}S^{x}M \in H$. But Lemmas 1 and 2 imply that $W^{mcy} \in H$. Since also $S^{x} \in H$, $M \in H$. Thus $G_0(m) \subseteq H$, and so $H = G_0(m)$. This completes the proof of Theorem 1.

References

1. M. Newman, *Structure theorems for modular subgroups*, Duke Math. J., March 1955.

2. L. E. Dickson, *Modern elementary theory of numbers*, University of Chicago Press, 1943.

National Bureau of Standards