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 $m | n$.

The proof given was by an induction and made use of properties of the representatives of $G_0(n \mathbb{N})$ 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
$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad W = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$ 

We note that
$$S^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad W^k = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}.$$ 

$S$ 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 \(a_0y = c \mod n\). Then

\[
W^{-y}M_0 = \begin{pmatrix} 1 & 0 \\ -y & 1 \end{pmatrix} \begin{pmatrix} a_0 & b_0 \\ c & d \end{pmatrix} = \begin{pmatrix} a_0 & b_0 \\ c - a_0y & d - b_0y \end{pmatrix} \in G_0(n).
\]

Hence \(W^{-y}M_0 \in H\), and so \(W^{-y} \in H\). Thus \(W^{a_0y} \in H\). Since \(a_0y = c \mod n\) 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

\[
S^xM = \begin{pmatrix} a_0 & b_0 \\ mc & d \end{pmatrix},
\]

where \((a_0, n) = 1\). Since \((a_0, n) = 1\), we can determine \(y\) so that \(a_0y = -1 \mod n\). For this \(y\),
\[
W^{mcy}S^z M = \begin{pmatrix}
1 & 0 \\
mc y & 1
\end{pmatrix}
\begin{pmatrix}
a_0 \\
mc d
\end{pmatrix}
\begin{pmatrix}
a_0 \\
mc b_0 + dj
\end{pmatrix}
\in G_0(n).
\]

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

REFERENCES


NATIONAL BUREAU OF STANDARDS