AN INCLUSION THEOREM FOR MODULAR GROUPS

MORRIS NEWMAN

Let $G$ denote the multiplicative group of $2 \times 2$ matrices

\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix},
\]

where $a$, $b$, $c$, $d$ are rational integers and $ad - bc = 1$. Let $G(m, n)$ denote the subgroup of $G$ characterized by $b \equiv 0 \pmod{m}$ and $c \equiv 0 \pmod{n}$, where $m$ and $n$ are nonzero rational integers. In a previous paper [1] the author has proved Theorem I below:

**Theorem I.** Let $H$ be a subgroup of $G$ containing $G(1, n)$. Then $H = G(1, n_1)$, where $n_1 \mid n$.

More generally, let $R$ be the ring of algebraic integers in a fixed algebraic number field of finite degree over the rationals. Let $G_R$ denote the multiplicative group of $2 \times 2$ matrices

\[
\begin{pmatrix}
\alpha & \beta \\
\gamma & \delta
\end{pmatrix},
\]

where $\alpha, \beta, \gamma, \delta$ are elements of $R$ and $\alpha \delta - \beta \gamma = 1$. Let $G_R(m, n)$ denote the subgroup of $G_R$ characterized by $\beta \in m$ and $\gamma \in n$, where $m$ and $n$ are nonzero ideals in $R$. Then Theorem I has been generalized by Reiner and Swift in a forthcoming paper [2] in the following manner:

**Theorem II.** Suppose that $(n, (6)) = (1)$, and let $H$ be a subgroup of $G_R$ containing $G_R((1), n)$. Then $H = G_R((1), n_1)$, where $n_1$ is an ideal dividing $n$.

The restriction that $n$ be prime to $(6)$ is necessary in general, examples being given in [2] which show that Theorem II may be false otherwise.

We propose to prove here the following generalizations of Theorems I and II:

**Theorem 1.** Suppose that $(m, n) = 1$. Let $H$ be a subgroup of $G$ containing $G(m, n)$. Then $H = G(m_1, n_1)$, where $m_1 \mid m$ and $n_1 \mid n$.

**Theorem 2.** Suppose that $(m, (6)) = (n, (6)) = (m, n) = (1)$. Let $H$ be

Received by the editors September 16, 1953.

1 The preparation of this paper was supported (in part) by the Office of Naval Research.
a subgroup of $G_R$ containing $G_R(m, n)$. Then $H = G_R(m_1, n_1)$, where $m_1$ and $n_1$ are ideals dividing $m$ and $n$ respectively.

The restriction that $(m, n) = 1$ (or that $(m, n) = (1)$) is not superfluous. We prove as a companion theorem to these theorems the following:

**Theorem 3.** Suppose that $(m, n) = k > 1$. Then there are subgroups of $G$ containing $G(m, n)$ which are not of the form $G(m_1, n_1)$ where $m_1 | m$ and $n_1 | n$.

Theorem 3 of course applies to both Theorems 1 and 2.

The proofs of Theorems 1 and 2 are not different, and we give only the proof of Theorem 2.

Since $(m, n) = (1)$, there is an element $\mu$ of $m$ and an element $\nu$ of $n$ such that $\mu - \nu = 1$. Thus the matrix

$$X = \begin{pmatrix} \mu & 1 \\ \nu & 1 \end{pmatrix}$$

is an element of $G_R$.

Suppose now that

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G_R(m, n).$$

Then the element in the (2, 1) place of $K^{-1}AK$ is $\mu\nu\delta - \mu\nu\alpha + \mu^2\gamma - \nu^2\beta$, and so $K^{-1}AK \subseteq G_R((1), mn)$ since $\mu\nu$, $\mu\gamma$, and $\nu\beta$ are all elements of $mn$. Thus $K^{-1}G_R(m, n)K \subseteq G_R((1), mn)$.

Similarly, if $A \subseteq G_R((1), mn)$, we can show that $KAK^{-1} \subseteq G_R(m, n)$, which implies that $KG_R((1), mn)K^{-1} \subseteq G_R(m, n)$, so that $K^{-1}G_R(m, n)K \subseteq G_R((1), mn)$. This together with the preceding relationship proves that $K^{-1}G_R(m, n)K = G_R((1), mn)$. In this manner we can show that for the same $K$

(1) If the ideals $m_1$, $n_1$ are any divisors of the ideals $m$, $n$ respectively, then $K^{-1}G_R(m_1, n_1)K = G_R((1), m_1n_1)$.

Suppose now that $H$ is a group such that

$$G_R(m, n) \subseteq H \subseteq G_R.$$

Then

$$K^{-1}G_R(m, n)K \subseteq K^{-1}HK \subseteq K^{-1}G_RK.$$

Using (1), we have

$$G_R((1), m, n) \subseteq K^{-1}HK \subseteq G_R.$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Since $K^{-1}HK$ is a subgroup of $G_R$, and $(mn, (6)) = (1)$, Theorem II applies and we find that $K^{-1}HK = G_R((1), I)$, where $I | mn$. Since $(m, n) = (1)$, we have $I = m_1n_1$, where $m_1 | m, n_1 | n$. Using (1) once again we find that $H = KG_R((1), m_1n_1)K^{-1} = G_R(m_1, n_1)$. Theorem 2 is thus proved.

The only difference in the proof of Theorem 1 is that the restriction $(m, (6)) = (n, (6)) = (1)$ is unnecessary and that Theorem I is used above, instead of Theorem II.

We turn now to Theorem 3. We have that $(m, n) = k > 1$. Let $p$ be any prime divisor of $k$, so that $G(p, p) \supseteq G(m, n)$. (Here and in what follows we use the fact that $G(m_1, n_1) \supseteq G(m, n)$ if and only if $m_1 | m, n_1 | n$). Let $T$ be the element

$$
\begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix}
$$

of $G$, and let $F$ be the smallest subgroup of $G$ containing $T$ and $G(p, p)$. Since $T^2 = -I$ and $T$ commutes with $G(p, p)$, $F$ consists of the totality $T^\epsilon G(p, p)$, where $\epsilon$ is 0 or 1. Thus if

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

is any element of $F$, either $b \equiv c \equiv 0 \pmod{p}$ or $a \equiv d \equiv 0 \pmod{p}$. We now note the following:

(i) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is an element of $G(1, p)$ but not of $F$.

(ii) $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is an element of $G(p, 1)$ but not of $F$.

(iii) $F$ contains $G(p, p)$ properly, and is properly contained in $G$.

Thus $F$ is not any of the groups $G(1, 1), G(1, p), G(p, 1), G(p, p)$. $F$ therefore is a group containing $G(m, n)$ which is not itself of the form $G(m_1, n_1)$ for any divisors $m_1, n_1$ of $m, n$ respectively and so furnishes an example for Theorem 3.

References