THE NORMALIZER OF CERTAIN MODULAR SUBGROUPS

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 $ad - bc = 1$. G is one of the well-known modular groups. Let $G_0(n)$ denote the subgroup of G characterized by $c \equiv 0 \pmod{n}$, where n is a positive integer. In this note we determine the normalizer of $G_0(n)$ in G, denoted by $\bar{G}_0(n)$. We shall prove the following theorem:

THEOREM 1. *If* $n = 2^\alpha\, 3^\beta\, n_0 \geqslant 1$, *where* $(n_0, 6) = 1$, *then*

$$\bar{G}_0(n) = G_0(n/2^u\, 3^v),$$

where $u = \min(3, [\tfrac{1}{2}\alpha]), v = \min(1, [\tfrac{1}{2}\beta])$.

Thus in all cases $\bar{G}_0(n) = G_0(n/\Delta)$, where $\Delta|24$. An interesting consequence of this theorem is that if H is a subgroup of G which has $G_0(n)$ for a normal subgroup, then $H = G_0(d)$, where $d|n$ and $(n/d)|24$. This is so since H is included between the groups $G_0(n)$ and $\bar{G}_0(n) = G_0(n/\Delta)$, and so H must be of the form given above by virtue of the theorem quoted in Lemma 1 below.

In addition, Theorem 1 shows that for certain n there are inner automorphisms of $G_0(n)$ arising from elements of G which are not in $G_0(n)$.

We go on now to the proof of Theorem 1. Put

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

and note that

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

LEMMA 1. *If* $n = \sigma^2 Q \geqslant 1$ *where* Q *is square-free, then* $\bar{G}_0(n) = G_0(n/\Delta)$, *where* $\Delta|\sigma$.

Proof. The author has shown in **(1)** that if H is a subgroup of G containing $G_0(n)$, then $H = G_0(m)$, where $m|n$. Since $\bar{G}_0(n) \supseteq G_0(n)$, we may put $\bar{G}_0(n) = G_0(m)$, $m|n$. The matrix W^m therefore belongs to $\bar{G}_0(n)$. Since $S \in G_0(n)$ for all n, $W^{-m}\, S\, W^m \in G_0(n)$. This implies that $m^2 \equiv 0 \pmod{n}$, or that $(m/\sigma)^2 \equiv 0 \pmod{Q}$, so that $(m/\sigma) \equiv 0 \pmod{Q}$, since Q is square-free. Hence $\sigma Q|m$, and also $m|\sigma^2 Q$. Thus $m = n/\Delta$, where $\Delta|\sigma$.

Received April 4, 1955.

https://doi.org/10.4153/CJM-1956-005-5 Published online by Cambridge University Press

LEMMA 2. *Suppose there is some divisor ϵ of σ such that for every element*

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

of $G_0(n)$, $\epsilon | (d - a)$. *Then* $\epsilon | \Delta$.

Proof. It is only necessary to show that $W^{n/\epsilon} \in \bar{G}_0(n)$, since then $(n/\Delta) | (n/\epsilon)$, and so $\epsilon | \Delta$. We have

$$W^{-n/\epsilon} A \; W^{n/\epsilon} = \begin{pmatrix} * & * \\ nc + n(d - a)\epsilon^{-1} - nb \cdot n\epsilon^{-2} & * \end{pmatrix}.$$

But $\epsilon^2 | n$ (since $\epsilon | \sigma$), and $\epsilon | (d - a)$ by hypothesis. Thus $W^{-n/\epsilon} A \; W^{n/\epsilon} \in G_0(n)$, and so $W^{n/\epsilon} \in \bar{G}_0(n)$.

LEMMA 3. *Suppose* $(k, n) = 1$. *Then* $\Delta | (k^2 - 1)$.

Proof. Since $(k, n) = 1$ we can find a, b such that $ak - bn = 1$. The matrix

$$A = \begin{pmatrix} a & b \\ n & k \end{pmatrix}$$

therefore belongs to $G_0(n)$. Since $W^{n/\Delta} \in \bar{G}_0(n)$, $W^{-n/\Delta} A \; W^{n/\Delta} \in G_0(n)$. Performing the multiplications, we see that

$$\frac{n}{\Delta}(k - a) + n\left(1 - \frac{n}{\Delta^2} b\right) \equiv 0 \pmod{n}.$$

This implies Lemma 3, since $\Delta^2 | n$ by Lemma 1 and $ak \equiv 1 \pmod{n}$.

LEMMA 4. $\Delta | 2^u \cdot 3$.

Proof. If n is odd, we may choose $k = 2$ in Lemma 3, which implies that $\Delta | 3$. If n is even, put $n = 2^\alpha n_1$, where n_1 is odd and $\alpha \geqslant 1$. Choose λ so that $\lambda n_1 \equiv -1 \pmod{2^\alpha}$. Then λ is odd. We may choose $k = \lambda n_1 - 2$ in Lemma 3 since

$$\begin{aligned}(k, n) &= (\lambda n_1 - 2, 2^\alpha n_1) \\ &= (\lambda n_1 - 2, 2^\alpha)(\lambda n_1 - 2, n_1) \\ &= 1.\end{aligned}$$

We have

$$\begin{aligned}(k^2 - 1, n) &= (k^2 - 1, 2^\alpha n_1) \\ &= (k^2 - 1, 2^\alpha)(k^2 - 1, n_1) \\ &= ((\lambda n_1 - 1)(\lambda n_1 - 3), 2^\alpha)((\lambda n_1 - 1)(\lambda n_1 - 3), n_1) \\ &= (8, 2^\alpha)(3, n_1).\end{aligned}$$

But $\Delta | (k^2 - 1)$, $\Delta | n$ and so $\Delta | (k^2 - 1, n)$. Taking into account that also $\Delta | \sigma$, we see that $\Delta | 2^u \cdot 3$, and so Lemma 4 is proved.

To complete the proof of Theorem 1, we use Lemma 2 in the following way. Let

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

https://doi.org/10.4153/CJM-1956-005-5 Published online by Cambridge University Press

be any element of $G_0(n)$. If $n \equiv 0 \pmod 9$ then $3|\sigma$. Also $ad \equiv 1 \pmod 3$, which implies that $3|(d - a)$. Thus $3|\Delta$. If $n \not\equiv 0 \pmod 9$ then $\sigma \not\equiv 0 \pmod 3$ and so, by Lemma 1, $\Delta \not\equiv 0 \pmod 3$. Hence Δ contains the factor 3 if and only if n is divisible by 9.

If $n \equiv 0 \pmod{64}$ then $8|\sigma$. Also, $ad \equiv 1 \pmod 8$. Thus a and d are odd, and since the square of any odd number is congruent to 1 modulo 8, $8|(d - a)$. Thus $8|\Delta$. Coupled with Lemma 4, we see that Δ contains the factor 8 precisely if and only if n is divisible by 64.

The remaining cases (n divisible by 16 but not by 64, n divisible by 4 but not by 16, n not divisible by 4) are treated similarly.

The proof of Theorem 1 is thus completed.

Reference

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

National Bureau of Standards, Washington