NOTE ON NORMAL SUBGROUPS OF THE MODULAR GROUP

L. GREENBERG

Let Γ denote the modular group, namely the group of linear fractional transformations

$$T(z) = \frac{az + b}{cz + d},$$

where a, b, c, d are integers and $ad-bc=1$. It is well known that the transformations

$$X(z) = -\frac{1}{z}, \qquad Y(z) = -\frac{1}{1+z}$$

generate Γ, with defining relations

$$X^2 = Y^3 = 1.$$

We shall often need to consider the element $Z=XY$, which is a parabolic transformation. Any parabolic transformation in Γ is conjugate to a power of Z.

Let N be a normal subgroup of finite index μ in Γ. The level n of N is defined as the least positive integer such that $Z^n \in N$. The conjugacy class of Z in Γ splits up into a finite number of equivalence classes under conjugacy by N. The number t of equivalence classes is called the parabolic class number of N. It is known that the integers μ, n, t satisfy the relation

$$\mu = nt. \tag{1}$$

One way of seeing this relation is the following. Γ operates discontinuously in the upper half-plane D. We obtain quotient surfaces $S_\Gamma = D/\Gamma$ and $S_N = D/N$. Since N is a normal subgroup of Γ, we have a normal (branched) covering $\phi: S_N \to S_\Gamma$. S_N is a closed surface with t punctures, and S_Γ is the sphere with one puncture. If we compactify S_Γ and S_N by adding a point p at the puncture in S_Γ, and points $p_1, p_2, \cdots, p_t$ at the punctures in S_N, we obtain surfaces $\overline{S}_\Gamma$, $\overline{S}_N$ and a normal covering $\bar{\phi}: \overline{S}_N \to \overline{S}_\Gamma$. The covering has μ sheets and there are exactly t points lying over p, each of which has branching order $n-1$ (i.e. n sheets meet at each p_i). By counting the sheets over p, we find $\mu = nt$.

Received by the editors February 17, 1966.

It is clear that there is only a finite number of subgroups N of index μ. It is also known that there are infinitely many normal subgroups of level n, for all integers $n \geqq 6$. (There are only finitely many for $1 \leqq n \leqq 5$.) To find such groups, one might as well add the relation $Z^n = 1$ to the relations for Γ. We then obtain the triangle group $\Delta(2, 3, n)$. It is known that this is finite for $n \leqq 5$, and infinite for $n \geqq 6$. In the last case it is known (cf. Fox [1]) that $\Delta(2, 3, n)$ contains subgroups of finite index without elements of finite order. It therefore contains infinitely many normal subgroups N, such that Z has order n mod N.

We now ask the analogous question for the parabolic class number t. M. Newman [3] has shown that there are infinitely many non-normal subgroups of finite index in Γ with t parabolic classes, for any integer $t \geqq 1$. He also showed that there are only finitely many normal subgroups with $t \leqq 11$. In this paper we shall show that for any $t \geqq 1$, there is only a finite number of normal subgroups with t parabolic classes.

Let H be a finite homomorphic image of Γ, and let F be a finite cyclic group. We wish to study extensions G of F by H such that F is contained in the center of G ($H \approx G/F$). One obtains such extensions from factor sets $\{f_{u,v}\}$, where $u, v \in H$, $f_{u,v} \in F$ and

$$f_{uv,w} f_{u,v} = f_{u,vw} f_{v,w}, \tag{2}$$

$$f_{u,1} = f_{1,u} = 1. \tag{3}$$

The extension G then consists of elements $g_u f$ ($u \in H$, $f \in F$) with multiplication:

$$(g_u f_1)(g_v f_2) = g_{uv} f_{u,v} f_1 f_2, \tag{4}$$

(cf. Hall [2]).

LEMMA 1. *Let x, y, z be the images of X, Y, Z in H, and let z have order k. Suppose that the factor set $\{f_{u,v}\}$ satisfies:*

(a) $f_{x,x} = f_{y,y} f_{y,y^2} = 1$,

(b) $f_{z,z} f_{z,z^2} \cdots f_{z,z^{k-1}} f^k_{x,y} = f$,

where f generates F. Then G is a homomorphic image of Γ.

PROOF. Let $\bar{x} = g_x$, $\bar{y} = g_y$. Then

$$\bar{x}^2 = g_x^2 = g_{x^2} f_{x,x} = 1,$$
$$\bar{y}^3 = g_y^3 = g_{y^3} f_{y,y} f_{y,y^2} = 1.$$

Therefore the subgroup $\overline{G}$ generated by $\bar{x}$ and $\bar{y}$ is a homomorphic image of Γ. If we can show that $\overline{G} \supset F$, it will follow that $\overline{G} = G$.

Let $\bar{z}=\bar{x}\bar{y}=g_x g_y=g_z f_{x,y}$. By induction, we can show that $\bar{z}^r=g_{z^r}f_{z,z}f_{z,z^2}\cdots f_{z,z^{r-1}}f^r_{x,y}$. In particular $\bar{z}^k=g_{z^k}f_{z,z}f_{z,z^2}\cdots f_{z,z^{k-1}}f^k_{x,y}=f$. Therefore $\overline{G}\supset F$ and $\overline{G}=G$. q.e.d.

LEMMA 2. *Let G be a finite homomorphic image of Γ, and let $\bar{x}$, $\bar{y}$, $\bar{z}$ be the images of X, Y, Z in G. Let k divide the order of $\bar{z}$, and suppose that the subgroup F generated by $\bar{z}^k$ is central in G. Let $H=G/F$, and let x, y, z be the images of $\bar{x}$, $\bar{y}$, $\bar{z}$ in H. Then there exists a factor set $\{f_{u,v}\}$ for G, relative to F and H, which satisfies conditions* (a), (b) *of Lemma* 1.

PROOF. Choose $\bar{x}$, $\bar{y}$, $\bar{y}^2$, $\bar{z}$, $\bar{z}^2$, $\cdots$, $\bar{z}^{k-1}$ to be the coset representatives of their F-cosets. It will then follow that

$$f_{x,y}=f_{x,x}=f_{y,y}=f_{y,y^2}=f_{z,z}=f_{z,z^2}=\cdots=f_{z,z^{k-2}}=1,$$

and

$$f_{z,z^{k-1}}=\bar{z}^k.$$

q.e.d.

LEMMA 3. *Let N be a normal subgroup of finite index in Γ, with t parabolic classes. Let $G=\Gamma/N$ and let x, y, z be the images of X, Y, Z in G. Let U be the subgroup generated by z. Then U contains a subgroup F such that*

(a) *F is contained in the center of G,*
(b) $[G:F]\leqq t^2$.

PROOF. Let $F=U\cap xUx^{-1}$. Since F is normalized by x and z, it is a normal subgroup of G. For $g\in G$, let α_g: $F\rightarrow F$ be the automorphism $\alpha_g(f)=g^{-1}fg$. We then have: $\alpha_x^2=\alpha_y^3=1$, $\alpha_x\alpha_y=\alpha_z=1$. Therefore $\alpha_x=\alpha_y=1$, so F is central in G. Since $[G:U]=[G:xUx^{-1}]=t$, it follows that $[G:F]\leqq t^2$. q.e.d.

THEOREM 1. *Let N be a normal subgroup of Γ with t parabolic classes and index μ. Then $\mu\leqq 6t^4$.*

PROOF. Let $G=\Gamma/N$ and let $\bar{x}$, $\bar{y}$, $\bar{z}$ be the images of X, Y, Z in G. Let F be the central subgroup from Lemma 3. F is generated by $\bar{z}^k$ (where k divides the order of $\bar{z}$). Let $H=G/F$, $r=\text{order}(F)$, $s=\text{order}(H)$. Then $\mu=rs$ and $s\leqq t^2$.

Let x, y, z be the images of $\bar{x}$, $\bar{y}$, $\bar{z}$ in H. By Lemma 2, there is a factor set $\{f_{u,v}\}$ for G, relative to F and H, which satisfies conditions (a), (b) of Lemma 1. By a theorem in extension theory (Hall [2], p. 223) the extension G' corresponding to the factor set $\{f^s_{u,v}\}$ splits. Since F is central, this means that $G'\approx F\times H$.

Let F^s denote the subgroup of F consisting of all sth powers, and let $G''=\{g_u f\in G' \mid f\in F^s\}$. G'' is a subgroup of G', since the factors

$f^s_{u,v} \in F^s$. G'' is the extension of F^s by H, corresponding to the factor set $\{f^s_{u,v}\}$. Since the factors $f^s_{u,v}$ satisfy conditions (a) and (b) of Lemma 1 (with F replaced by F^s), it follows that G'' is a homomorphic image of Γ.

Since $G' \approx F \times H$, there is a projection $\pi: G' \to F$. Let $F' = \pi(G'')$. F' is a homomorphic image of Γ, which contains F^s. Since an abelian homomorphic image of Γ has order $\leqq 6$, we have $|F^s| \leqq |F'| \leqq 6$. But $r/s \leqq r/(r, s) = |F^s|$. Therefore $r \leqq 6s$, $s \leqq t^2$ and $\mu = rs \leqq 6t^4$. q.e.d.

COROLLARY. *There are only a finite number of normal subgroups of* Γ *with t parabolic classes.*

THEOREM 2. *Let p be a prime such that* $p \equiv -1 \pmod 3$. *Then there is no normal subgroup of finite index in* Γ *with p parabolic classes.*[1]

PROOF. Suppose N is a normal subgroup with p parabolic classes, level n and index μ. By Lemma 3, $G = \Gamma/N$ contains a central subgroup F, generated by z^k (where k divides n) such that $[G:F] \leqq p^2$. $H = G/F$ is a quotient group of Γ: $H = \Gamma/M$. Since z has order k in H, M has level k, and index $\nu \leqq p^2$. Since $|F| = n/k$, $\nu = k\mu/n = kp$, so that M also has p parabolic classes. The new level k satisfies $k \leqq p$. If $k = p$ then H is a group of order $\nu = p^2$, and therefore H is abelian. But all abelian quotient groups of Γ have order $\leqq 6$, therefore $\nu < p^2$ and $k < p$.

Let S be a Sylow p-subgroup of H and let m be the number of conjugates of S in H. Then m is of the form $m = 1 + pr$ and $m | kp$. Since $k < p$, it follows that $m = 1$ and S is normal in H.

Let K be the subgroup generated by $z \in H$. $K \cap S$ has order dividing $|K| = k$ and $|S| = p$. Since these are relatively prime, $K \cap S = \{1\}$. Therefore H is the semidirect product $H = S \cdot K$. Thus K is a homomorphic image of H, and therefore of Γ. Since K is abelian, the order $k \leqq 6$. Thus $k = 1$, 2, 3 or 6. However, $6 | \nu = kp$, since x and y are nontrivial in H (if $x = 1$ or $y = 1$ then $\nu \leqq 3$). Thus $6 | k$, $k = 6$ and $\nu = 6p$. But M. Newman [3] showed that $6p$ does not occur as the index of a normal subgroup of Γ, when $p \equiv -1 \pmod 3$ and p is prime. q.e.d.

REFERENCES

1. R. Fox, *On Fenchel's conjecture about F-groups*, Mat. Tids. B (1952), 61–65.
2. M. Hall, *The theory of groups*, Macmillan, New York, 1959.
3. M. Newman, *Classification of normal subgroups of the modular group* (to appear).

UNIVERSITY OF MARYLAND AND
NATIONAL BUREAU OF STANDARDS

---

[1] This theorem was proved simultaneously and independently by M. Newman.