

# NOTE ON NORMAL SUBGROUPS OF THE MODULAR GROUP

L. GREENBERG

Let  $\Gamma$  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

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

generate  $\Gamma$ , 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  $\Gamma$  is conjugate to a power of  $Z$ .

Let  $N$  be a normal subgroup of finite index  $\mu$  in  $\Gamma$ . The level  $n$  of  $N$  is defined as the least positive integer such that  $Z^n \in N$ . The conjugacy class of  $Z$  in  $\Gamma$  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  $\mu, n, t$  satisfy the relation

$$(1) \quad \mu = nt.$$

One way of seeing this relation is the following.  $\Gamma$  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  $\Gamma$ , we have a normal (branched) covering  $\phi: S_N \rightarrow S_\Gamma$ .  $S_N$  is a closed surface with  $t$  punctures, and  $S_\Gamma$  is the sphere with one puncture. If we compactify  $S_\Gamma$  and  $S_N$  by adding a point  $p$  at the puncture in  $S_\Gamma$ , and points  $p_1, p_2, \dots, p_t$  at the punctures in  $S_N$ , we obtain surfaces  $\bar{S}_\Gamma, \bar{S}_N$  and a normal covering  $\bar{\phi}: \bar{S}_N \rightarrow \bar{S}_\Gamma$ . The covering has  $\mu$  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  $\mu$ . It is also known that there are infinitely many normal subgroups of level  $n$ , for all integers  $n \geq 6$ . (There are only finitely many for  $1 \leq n \leq 5$ .) To find such groups, one might as well add the relation  $Z^n = 1$  to the relations for  $\Gamma$ . We then obtain the triangle group  $\Delta(2, 3, n)$ . It is known that this is finite for  $n \leq 5$ , and infinite for  $n \geq 6$ . 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  $n \pmod N$ .

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  $\Gamma$  with  $t$  parabolic classes, for any integer  $t \geq 1$ . He also showed that there are only finitely many normal subgroups with  $t \leq 11$ . In this paper we shall show that for any  $t \geq 1$ , there is only a finite number of normal subgroups with  $t$  parabolic classes.

Let  $H$  be a finite homomorphic image of  $\Gamma$ , 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

$$(2) \quad f_{uv, w} f_{u, v} = f_{u, v} f_{v, w},$$

$$(3) \quad f_{u, 1} = f_{1, u} = 1.$$

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

$$(4) \quad (g_u f_1)(g_v f_2) = g_{uv} f_u v f_1 f_2,$$

(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:*

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

$$(b) \quad f_{z,z} f_{z,z^2} \cdots f_{z,z^{k-1}} f_{z,u}^k = f,$$

where  $f$  generates  $F$ . Then  $G$  is a homomorphic image of  $\Gamma$ .

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

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

LEMMA 2. Let  $G$  be a finite homomorphic image of  $\Gamma$ , 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  $\bar{x}, \bar{y}, \bar{y}^2, \bar{z}, \bar{z}^2, \dots, \bar{z}^{k-1}$  to be the coset representatives of their  $F$ -cosets. It will then follow that

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

and

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

q.e.d.

LEMMA 3. Let  $N$  be a normal subgroup of finite index in  $\Gamma$ , 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)  $[G:F] \leq t^2$ .

PROOF. Let  $F = U \cap x U x^{-1}$ . Since  $F$  is normalized by  $x$  and  $z$ , it is a normal subgroup of  $G$ . For  $g \in G$ , let  $\alpha_g: F \rightarrow F$  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  $[G:U] = [G:x U x^{-1}] = t$ , it follows that  $[G:F] \leq t^2$ . q.e.d.

THEOREM 1. Let  $N$  be a normal subgroup of  $\Gamma$  with  $t$  parabolic classes and index  $\mu$ . Then  $\mu \leq 6t^4$ .

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  $s \leq t^2$ .

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  $\{f_{u,v}^s\}$  splits. Since  $F$  is central, this means that  $G' \approx F \times H$ .

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

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

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

**COROLLARY.** *There are only a finite number of normal subgroups of  $\Gamma$  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  $\Gamma$  with  $p$  parabolic classes.<sup>1</sup>*

**PROOF.** Suppose  $N$  is a normal subgroup with  $p$  parabolic classes, level  $n$  and index  $\mu$ . By Lemma 3,  $G = \Gamma/N$  contains a central subgroup  $F$ , generated by  $z^k$  (where  $k$  divides  $n$ ) such that  $[G:F] \leq p^2$ .  $H = G/F$  is a quotient group of  $\Gamma: H = \Gamma/M$ . Since  $z$  has order  $k$  in  $H$ ,  $M$  has level  $k$ , and index  $\nu \leq p^2$ . Since  $|F| = n/k$ ,  $\nu = k\mu/n = kp$ , so that  $M$  also has  $p$  parabolic classes. The new level  $k$  satisfies  $k \leq p$ . If  $k = p$  then  $H$  is a group of order  $\nu = p^2$ , and therefore  $H$  is abelian. But all abelian quotient groups of  $\Gamma$  have order  $\leq 6$ , 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  $\Gamma$ . Since  $K$  is abelian, the order  $k \leq 6$ . Thus  $k = 1, 2, 3$  or  $6$ . However,  $6 | \nu = kp$ , since  $x$  and  $y$  are non-trivial in  $H$  (if  $x = 1$  or  $y = 1$  then  $\nu \leq 3$ ). 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  $\Gamma$ , 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

<sup>1</sup> This theorem was proved simultaneously and independently by M. Newman.