FREE SUBGROUPS AND NORMAL SUBGROUPS OF THE MODULAR GROUP[1]

BY

MORRIS NEWMAN

In this note we wish to point out some easy consequences of the Kuroš subgroup theorem applied to the modular group Γ, which yield information of interest about free subgroups and normal subgroups of Γ. Here Γ is the group of 2×2 rational integral matrices of determinant 1 in which a matrix and its negative are identified. It is known that Γ is the free product of a cyclic group of order 2 and a cyclic group of order 3, and we write $\Gamma = \{x\} * \{y\}$, where $x^2 = y^3 = 1$ and $\{x_1, x_2, \cdots\}$ stands for the group generated by $x_1, x_2, \cdots$. Define Γ^m as the subgroup of Γ generated by the m^{th} powers of all elements of Γ. Then in a recent article [3] the structure of these groups was investigated, and it was shown that

$$\begin{aligned} \Gamma^2 &= \{y\} * \{xyx\} = \{y, xyx\}, \\ \Gamma^3 &= \{x\} * \{yxy^2\} * \{y^2xy\} = \{x, yxy^2, y^2xy\}, \end{aligned} \tag{1}$$

so that Γ^2 is the free product of two cyclic groups of order 3, and Γ^3 the free product of three cyclic groups of order 2. The groups Γ^m are fully invariant, and therefore normal, subgroups of Γ. The principal result we wish to prove is the theorem that follows:

THEOREM 1. *Let H be a nontrivial normal subgroup of Γ different from Γ, Γ^2, Γ^3. Then H is a free group.*

The proof of this theorem depends on the lemmas that follow.

LEMMA 1. *Let H be a nontrivial subgroup of Γ. Then H is free if and only if it contains no elements of finite period.*

LEMMA 2. *The only normal subgroups of Γ containing elements of finite period are Γ, Γ^2, Γ^3.*

Proof of Lemma 1. The Kuroš subgroup theorem (see [2]) states that a subgroup $H \neq \{1\}$ of a free product G is itself a free product, $H = F * \Pi * G_i$, where F is either free or $\{1\}$ and each G_i is the conjugate of a subgroup of one of the free factors of G. Thus if H is a subgroup of Γ, it follows that

$$H = F * \Pi * G_i, \tag{2}$$

where F is either free or $\{1\}$ and each G_i is conjugate to $\{x\}$ or to $\{y\}$. Thus if H contains no elements of finite period, then the free product $\Pi * G_i$ is

Received October 11, 1962.

[1] The preparation of this paper was supported by the Office of Naval Research.

vacuous, and so $H = F$. Since H is nontrivial, it follows that H is free. The converse is clear.

Proof of Lemma 2. Let H be a normal subgroup of Γ containing an element of finite period. Then (2) implies that H contains an element of period 2 or an element of period 3: Since every element of Γ of period 2 is conjugate to x and every element of Γ of period 3 is conjugate to y or y^{-1}, it follows that H contains x or y, since H is normal. There are then three possibilities:

(i) H contains x and y. Then $H \supset \Gamma$ and so $H = \Gamma$.

(ii) H contains y but not x. Then $H \neq \Gamma$ and $H \supset \Gamma^2$, by (1) and the fact that H is normal. Since $(\Gamma:\Gamma^2) = 2$ (see [3]) it follows that $H = \Gamma^2$.

(iii) H contains x but not y. Then $H \neq \Gamma$ and $H \supset \Gamma^3$, by (1) and the fact that H is normal. Since $(\Gamma:\Gamma^3) = 3$ (see [3]) it follows that $H = \Gamma^3$.

The proofs of the lemmas are completed, and the proof of the theorem is an immediate consequence of the lemmas. It is worthwhile noting that (2) implies the known result that an element of Γ of finite period is necessarily of period 2 or 3.

We now go on to a theorem proved by Gunning in his book on modular forms [1] by other methods. The theorem is

THEOREM 2. *Let H be a normal subgroup of Γ different from Γ, Γ^2, Γ^3 such that $(\Gamma:H) = \mu < \infty$. Then μ is divisible by* 6.

Proof. Theorem 1 implies that H is free, and so H cannot contain x or y. Further, if $xy^{-1} \in H$, then $y^{-1}x \in H$, since H is normal, and so $y = y^{-1}xxy^{-1} \in H$, a contradiction. Therefore the cosets xH, yH are different from H and distinct, and so Γ/H contains cyclic subgroups of orders 2 and 3, which implies the theorem.

Going over to the matrix representation of Γ as the totality of rational integral matrices

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

of determinant 1 in which A and $-A$ are identified, let $\Gamma_0(n)$ be the subgroup of Γ defined by $c \equiv 0 \pmod{n}$, n a positive integer. Then $\Gamma_0(n)$ is a nonnormal subgroup of Γ for $n > 1$. Suppose that $A \neq \pm I$. Then A is of period 2 if and only if $A^2 + I = 0$, and of period 3 if and only if $A^2 \pm A + I = 0$. It follows that if A is of period 2 and $A \in \Gamma_0(n)$, then

$$a^2 + 1 \equiv 0 \pmod{n}; \tag{3}$$

and if A is of period 3 and $A \in \Gamma_0(n)$, then

$$a^2 \pm a + 1 \equiv 0 \pmod{n}. \tag{4}$$

Congruence (3) has no solutions if and only if n is divisible by 4 or by a prime of the form $4t + 3$, and congruence (4) has no solutions if and only if n is divisible by 2, 9, or by a prime of the form $3t + 2$. In these cases

$\Gamma_0(n)$ can have no elements of finite period. Furthermore, the existence of solutions of the congruences implies the existence of elements of $\Gamma_0(n)$ of finite period. Thus if $a^2 + 1 = nt$, then $\begin{pmatrix} a & -t \\ n & -a \end{pmatrix} \epsilon \Gamma_0(n)$ and is of period 2, and if $a^2 \pm a + 1 = nt$, then $\begin{pmatrix} -a & -t \\ n & a \pm 1 \end{pmatrix} \epsilon \Gamma_0(n)$ and is of period 3. Hence Lemma 1 implies

THEOREM 3. *If n is odd, then the group $\Gamma_0(n)$ is free if and only if n is divisible by a prime of the form $4t + 3$, and by 9 or by a prime of the form $3t + 2$. If n is even, then $\Gamma_0(n)$ is free if and only if n is divisible by 4 or by a prime of the form $4t + 3$.*

In particular $\Gamma_0(n)$ is free if n is of the form $12t - 1$. The usual proofs in this area depend heavily on the fundamental region of a group and ideas from geometry. (But see [4] by H. Rademacher, in which the Reidemeister-Schreier method is applied to the case when n is prime.)

An interesting generalization of Theorem 3 can be obtained for a more inclusive class of groups. Let m, n be positive integers, and let $\Gamma(m, n)$ be the subgroup of Γ defined by $b \equiv 0 \pmod m$, $c \equiv 0 \pmod n$, so that $\Gamma_0(n) = \Gamma(1, n)$. Then we have

THEOREM 4. *If mn is odd, then the group $\Gamma(m, n)$ is free if and only if mn is divisible by a prime of the form $4t + 3$, and by 9 or by a prime of the form $3t + 2$. If mn is even, then $\Gamma(m, n)$ is free if and only if mn is divisible by 4 or by a prime of the form $4t + 3$.*

Proof. Put

$$D = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $D^{-1}\Gamma(m, n)D = \Gamma(1, mn) = \Gamma_0(mn)$, so that $\Gamma(m, n)$ and $\Gamma_0(mn)$ are conjugate subgroups in the group of rational 2×2 matrices of determinant 1, in which a matrix and its negative are identified. The result now follows from Theorem 3.

It is of interest to note that $\Gamma(m, n)$ and $\Gamma_0(mn)$ are conjugate subgroups in Γ if and only if m and n are coprime. We omit the proof, which is not difficult.

We remark that if $G(n)$ is the principal congruence subgroup of G, G a subgroup of Γ (that is, the totality of elements $A \epsilon G$ such that $A \equiv \pm I \pmod n$), then $G(n)$ is always free for $n > 1$, since $G(n)$ is a subgroup of $\Gamma(n)$, and $\Gamma(n)$ is a normal subgroup of Γ different from Γ, Γ^2, Γ^3, and therefore free, by Theorem 1.

REFERENCES

1. R. C. GUNNING, *Lectures on modular forms*, Princeton, 1962.
2. A. G. KUROSH, *The theory of groups*, New York, 1955, 1956.

3. M. NEWMAN, *The structure of some subgroups of the modular group*, Illinois J. Math., vol. 6 (1962), pp. 480–487.
4. H. RADEMACHER, *Über die Erzeugenden von Kongruenzuntergruppen der Modulgruppe*, Abh. Math. Sem. Univ. Hamburg, vol. 7 (1930), pp. 134–148.

NATIONAL BUREAU OF STANDARDS
WASHINGTON, D. C.