THE STRUCTURE OF SOME SUBGROUPS OF THE MODULAR GROUP[1]

BY
MORRIS NEWMAN

Introduction

Let Γ be the 2×2 modular group. In a recent article [7] the notion of the type of a subgroup Δ of Γ was introduced. If the exponents of

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

modulo Δ are r and s respectively, then Δ is said to be of type (r, s). It is trivial to verify that if Δ is of finite index in Γ, then $rs \neq 0$. In fact if G is any group and H a subgroup of finite index i, then there is an integer $e > 0$ such that $g^e \in H$ for all $g \in G$, since the $i + 1$ elements $1, g, \cdots, g^i$ of G cannot all be distinct modulo H.

Thus if Δ is of finite index in Γ, then $\Delta \supset \Gamma^m$, the fully invariant subgroup of Γ generated by the m^{th} powers of the elements of Γ, for some positive integer m. An obvious question to ask is whether Δ is of finite index in Γ if it contains such a subgroup. In this connection see [3], where certain necessary and sufficient conditions are given for this to occur. It is clearly sufficient to consider only $\Delta = \Gamma^m$. It turns out that the answer to this question is in the negative, but the proof requires the recent results of Novikov [9] on the Burnside problem.

The purpose of this paper is to elucidate the structure of the groups Γ^m, and incidentally to characterize Γ', the commutator subgroup of Γ, by the relationship $\Gamma' = \Gamma^2 \cap \Gamma^3$. This has a pleasing similarity to the formula $\Gamma = \Gamma^2\Gamma^3$. In addition certain related questions will be considered.

The problem is similar to the Burnside problem, the difference being that the modular group Γ is not a free group, but is instead the free product of a cyclic group of order 2 and a cyclic group of order 3.

The groups Γ^m

The modular group $\bar{\Gamma}$ is generated by the matrices $\bar{x}$, $\bar{y}$, where

$$(1) \qquad \bar{x} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \bar{y} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

with defining relationships $\bar{x}^2 = \bar{y}^3 = -I$, where I is the identity matrix. If $\bar{z}$ is any element of $\bar{\Gamma}$ and $\bar{z}$ is identified with $-\bar{z}$, the group so obtained

Received July 5, 1961.

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

(which is $\bar{\Gamma}$ modulo its center $\{I, -I\}$) is the modular group Γ, which may be regarded as the group generated by the symbols x, y with defining relationships $x^2 = y^3 = 1$, and we find it convenient to take this interpretation.

We shall write $\{x_1, x_2, \cdots\}$ for the group generated by $x_1, x_2, \cdots$. Thus

$$\Gamma = \{x, y\}, \qquad x^2 = y^3 = 1.$$

The fully invariant subgroups Γ^m of Γ are then defined by

$$\Gamma^m = \{x_1^m, x_2^m, \cdots\},$$

where $x_1, x_2, \cdots$ are the elements of Γ. It is clear that

$$\Gamma^m \supset \Gamma^{mn}, \tag{2}$$

$$(\Gamma^m)^n \supset \Gamma^{mn}. \tag{3}$$

It is also true that

$$\Gamma^m \Gamma^n = \Gamma^{(m,n)}, \tag{4}$$

where (m, n) is the greatest common divisor of m and n. To prove (4) we notice first that the product is well defined since the groups Γ^m are normal subgroups of Γ. We have $\Gamma^{(m,n)} \supset \Gamma^m$, $\Gamma^{(m,n)} \supset \Gamma^n$ (by (2)), so that $\Gamma^{(m,n)} \supset \Gamma^m\Gamma^n$. Also let z be any element of Γ. Determine integers m_1, n_1 so that $m_1 m + n_1 n = (m, n)$. Then $z^{m_1 m} \epsilon \Gamma^m$, $z^{n_1 n} \epsilon \Gamma^n$, $z^{m_1 m + n_1 n} \epsilon \Gamma^m\Gamma^n$, $z^{(m,n)} \epsilon \Gamma^m\Gamma^n$. This implies that $\Gamma^m\Gamma^n \supset \Gamma^{(m,n)}$, and so $\Gamma^m\Gamma^n = \Gamma^{(m,n)}$, completing the proof of (4).

In particular

$$\Gamma^2\Gamma^3 = \Gamma. \tag{5}$$

We first work out the structure of Γ^2 and Γ^3.

THEOREM 1. *The group Γ^2 is the free product of two cyclic groups of order 3, and*

$$(\Gamma : \Gamma^2) = 2, \qquad \Gamma = \Gamma^2 + x\Gamma^2, \qquad \Gamma^2 = \{y, xyx\}.$$

The elements of Γ^2 may be characterized by the requirement that the sum of the exponents of x be divisible by 2.

THEOREM 2. *The group Γ^3 is the free product of three cyclic groups of order 2, and*

$$(\Gamma : \Gamma^3) = 3, \qquad \Gamma = \Gamma^3 + y\Gamma^3 + y^2\Gamma^3, \qquad \Gamma^3 = \{x, yxy^2, y^2xy\}.$$

The elements of Γ^3 may be characterized by the requirement that the sum of the exponents of y be divisible by 3.

Proof of Theorem 1. Set $H = \{y, xyx\}$. Then, as is easily verified, H is a normal subgroup of Γ contained in Γ^2, and the elements of H satisfy the requirements of Theorem 1; that is, the sum of the exponents of x is even.

Let z be any element of Γ. Then we can write

$$z = y^{c_1}xy^{c_2}x \cdots y^{c_n}xy^{c_{n+1}}, \tag{6}$$

where the c_i's are integers which may be 0. Thus

$$z = y^{c_1}(xyx)^{c_2}y^{c_3} \cdots (xyx)^{c_n}y^{c_{n+1}} \quad \text{for } n \text{ even},$$

$$z = y^{c_1}(xyx)^{c_2}y^{c_3} \cdots y^{c_n}(xyx)^{c_{n+1}}x \quad \text{for } n \text{ odd}.$$

Hence $z \in H$ or $zx \in H$. Since x is not in H, this implies that $\Gamma = H + Hx = H + xH$. Now $\Gamma \supset \Gamma^2 \supset H$ and $(\Gamma:H) = 2$, which implies that $(\Gamma:\Gamma^2) = 1$ or 2. But $\Gamma \neq \Gamma^2$ (x is not in Γ^2), and so $(\Gamma:\Gamma^2) = 2$. Thus $\Gamma^2 = H$. It is also clear that H is the free product of two cyclic groups of order 3 since the defining relations for H are $y^3 = (xyx)^3 = 1$. The proof of Theorem 1 is complete.

Proof of Theorem 2. Set $K = \{x, yxy^2, y^2xy\}$. Then K is a normal subgroup of Γ contained in Γ^3, and the elements of K satisfy the requirements of Theorem 2; that is, the sum of the exponents of y is a multiple of 3. Let w_n be any word of the form $y^{c_1}xy^{c_2}x \cdots y^{c_n}x$. We have $y^{c_1}x = y^{c_1}xy^{2c_1} \cdot y^{-2c_1}$, so that

$$w_n = y^{c_1}xy^{2c_1}w_{n-1},$$

where $w_{n-1} = y^{c_2-2c_1}x \cdots y^{c_n}x$. But $y^{c_1}xy^{2c_1} = x$, yxy^2 or y^2xy. This implies by induction on n that $w_n = ky^{c_0}$, where $k \in K$ and c_0 is an integer. Hence for z as given by (6) we have that $z = w_n y^{c_{n+1}} = ky^c$ where c is an integer. Since neither y nor y^2 belongs to K, this implies that $\Gamma = K + Ky + Ky^2 = K + yK + y^2K$.

Now $\Gamma \supset \Gamma^3 \supset K$ and $(\Gamma:K) = 3$, which implies that $(\Gamma:\Gamma^3) = 1$ or 3. But $\Gamma \neq \Gamma^3$ (y is not in Γ^3), and so $(\Gamma:\Gamma^3) = 3$. Thus $\Gamma^3 = K$.

To prove that K is the free product of three cyclic groups of order 2, we need only show that no generator belongs to the group generated by the other two, so that K has defining relations $x^2 = (yxy^2)^2 = (y^2xy)^2 = 1$. This is easy to verify since the generators are all of period 2. Thus setting $yxy^2 = z$, the elements of $\{x, z\}$ are of the form $(xz)^n$, $(zx)^n$, $(xz)^n x$, $(zx)^n z$; and that none of these can equal y^2xy may be seen from the matrix representation of x and y given in (1). This completes the proof of Theorem 2.

For the case when m is not divisible by 6, Theorems 1 and 2 determine Γ^m completely. In fact we have

THEOREM 3. *The groups* Γ^m *satisfy*

$$\begin{aligned} \Gamma^m &= \Gamma, & (m, 6) &= 1, \\ \Gamma^{2m} &= \Gamma^2, & (m, 3) &= 1, \\ \Gamma^{3m} &= \Gamma^3, & (m, 2) &= 1. \end{aligned} \tag{7}$$

Proof. When $(m, 6) = 1$, Γ^m contains both x and y since $x = x^m$, $y = y^{\pm m}$, so that $\Gamma^m = \Gamma$. Suppose that $(m, 3) = 1$. Then $y = y^{\pm 2m}$, $xyx = (xyx)^{\pm 2m}$, so that $\Gamma^2 \subset \Gamma^{2m}$. Since in addition $\Gamma^2 \supset \Gamma^{2m}$ (by (2)), we have that $\Gamma^2 = \Gamma^{2m}$. Finally suppose that $(m, 2) = 1$. Then $x = x^{3m}$, $yxy^2 = (yxy^2)^{3m}$, $y^2xy = (y^2xy)^{3m}$, so that $\Gamma^3 \subset \Gamma^{3m}$. Since in addition $\Gamma^3 \supset \Gamma^{3m}$ (by (2)), we have that $\Gamma^3 = \Gamma^{3m}$. The proof of the theorem is complete.

We also require the structure of Γ'. This is well known, and we have

Lemma 1. *The commutator subgroup Γ' of Γ is a free group of rank* 2, *and*

$$(8)\qquad (\Gamma:\Gamma') = 6, \qquad \Gamma = \sum_{r=0}^{5} (xy)^r \Gamma', \qquad \Gamma' = \{xyxy^2,\ xy^2xy\}.$$

In fact J. Nielsen has shown [8] that the commutator subgroup of the free product of a finite number of cyclic groups of finite order is a free group of finite rank.

We set

$$(9)\qquad a = xyxy^2, \qquad b = xy^2xy.$$

Then a and b have the matrix representations

$$(10)\qquad \bar{a} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \bar{b} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

We note that the quotient groups Γ/Γ^2, Γ/Γ^3 are cyclic and therefore abelian, so that $\Gamma^2 \supset \Gamma'$, $\Gamma^3 \supset \Gamma'$. Hence $\Gamma^2 \cap \Gamma^3 \supset \Gamma'$. By one of the isomorphism theorems (Γ^2 and Γ^3 being normal subgroups of Γ),

$$\Gamma^2\Gamma^3/\Gamma^3 \cong \Gamma^2/\Gamma^2 \cap \Gamma^3.$$

By (5) this becomes

$$\Gamma/\Gamma^3 \cong \Gamma^2/\Gamma^2 \cap \Gamma^3.$$

Hence

$$(\Gamma^2:\Gamma^2 \cap \Gamma^3) = (\Gamma:\Gamma^3) = 3.$$

But

$$(\Gamma:\Gamma^2 \cap \Gamma^3) = (\Gamma:\Gamma^2)(\Gamma^2:\Gamma^2 \cap \Gamma^3) = 2\cdot 3 = 6.$$

Since $\Gamma \supset \Gamma^2 \cap \Gamma^3 \supset \Gamma'$ and $(\Gamma:\Gamma') = (\Gamma:\Gamma^2 \cap \Gamma^3) = 6$, it follows that $\Gamma' = \Gamma^2 \cap \Gamma^3$. Thus we have proved

Theorem 4. *The commutator subgroup Γ' of Γ satisfies*

$$(11)\qquad \Gamma' = \Gamma^2 \cap \Gamma^3.$$

Because of Theorem 3 we have left only the groups Γ^{6m} to consider. Since $\Gamma^2 \supset \Gamma^6$ and $\Gamma^3 \supset \Gamma^6$, (11) implies that

$$(12)\qquad \Gamma' \supset \Gamma^6.$$

Then because Γ' is a free group and $\Gamma^6 \supset \Gamma^{6m}$, we have by Schreier's theorem [10]

Theorem 5. *The groups Γ^{6m} are free groups.*

We can say something more about the groups Γ^{6m}. In the first place, $\Gamma^{6m} \supset (\Gamma')^{6m}$ since $\Gamma \supset \Gamma'$. Hence if $(\Gamma':(\Gamma')^{6m}) < \infty$, then the same holds for $(\Gamma:\Gamma^{6m})$. In particular M. Hall's solution of the Burnside problem for 6 (see [2] for an account of this) implies that $(\Gamma':(\Gamma')^{6}) < \infty$, so that $(\Gamma:\Gamma^{6}) < \infty$. Secondly, we have from (3) and (12) that

$$(\Gamma')^m \supset (\Gamma^6)^m \supset \Gamma^{6m}.$$

Then the results of Novikov on the Burnside problem [9] imply that $(\Gamma':(\Gamma')^m) = \infty$ for $m \geqq 72$, so that $(\Gamma:\Gamma^{6m}) = \infty$ for $m \geqq 72$. There are left therefore the 70 cases

$$\Gamma^{6m}, \quad 2 \leqq m \leqq 71 \tag{13}$$

in which the index $(\Gamma:\Gamma^{6m})$ is unknown.

We are going to determine the structure of Γ^6. We have

LEMMA 2. *Let G be a group generated by two elements α, β. Let N be a normal subgroup of G containing*

$$[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}. \tag{14}$$

Then N contains G', the commutator subgroup of G.

Proof. G is abelian modulo N, which implies that $N \supset G'$.

COROLLARY 1. $\Gamma^6 \supset \Gamma''$, *the second commutator subgroup of* Γ.

For $\Gamma' \supset \Gamma^6$, Γ' is generated by the two elements a, b given in (9), Γ^6 is a normal subgroup of Γ', and

$$[a, b] = (xyxyx)^6 \in \Gamma^6.$$

COROLLARY 2. *The quotient group* Γ'/Γ^6 *is abelian.*

We remark that Γ'' is of infinite index in Γ and is countably infinitely generated, being the commutator subgroup of a free group of finite rank [5]. Hence $\Gamma^6 \neq \Gamma''$.

Let p, q be positive integers. We define a class of normal subgroups $\Gamma'(p, q)$ of Γ' as follows: The element

$$w = a^{r_1}b^{s_1} \cdots a^{r_n}b^{s_n}$$

of Γ' belongs to $\Gamma'(p, q)$ if and only if

$$\textstyle\sum_{i=1}^{n} r_i \equiv 0 \pmod{p}, \qquad \sum_{i=1}^{n} s_i \equiv 0 \pmod{q}.$$

It is clear that

$$\Gamma'(p, q) \supset \Gamma'', \tag{15}$$

(16) $$(\Gamma':\Gamma'(p, q)) = pq, \qquad \Gamma' = \sum_{r=0}^{p-1} \sum_{s=0}^{q-1} a^r b^s \Gamma'(p, q),$$

and that $\Gamma'(p, q)$ is a free group of rank $1 + pq$. The latter fact follows from Schreier's formula

$$R = 1 + i(r - 1)$$

for the rank R of a subgroup of index i in a free group of rank r (see [10]), since Γ' is of rank 2 and $(\Gamma':\Gamma'(p, q)) = pq$. Formula (15) follows from the fact that the word w belongs to Γ'' if and only if

$$\sum_{i=1}^{n} r_i = \sum_{i=1}^{n} s_i = 0.$$

We are going to prove

THEOREM 6. *The group* Γ^6 *is just* $\Gamma'(6, 6)$. *Hence* Γ^6 *is of index* 216 *in* Γ *and is the free group on* 37 *generators. We have*

(17) $$(\Gamma':\Gamma^6) = 36, \qquad \Gamma' = \sum a^r b^s \Gamma^6, \qquad 0 \leqq r, s \leqq 5.$$

Proof. Let $w = a^{r_1}b^{s_1} \cdots a^{r_n}b^{s_n} \in \Gamma'(6, 6)$. Then because Γ' is abelian modulo Γ'' we may write

$$w = a^{r_1+\cdots+r_n} b^{s_1+\cdots+s_n} w_1,$$

where $w_1 \in \Gamma''$. Since $\Gamma'' \subset \Gamma^6$ (Corollary 1) and

$$\sum_{i=1}^{n} r_i \equiv \sum_{i=1}^{n} s_i \equiv 0 \pmod 6,$$

it follows that $w \in \Gamma^6$. Hence $\Gamma'(6, 6) \subset \Gamma^6$.

Now let u be an arbitrary element of Γ. By Lemma 1 there is an integer r, $0 \leqq r \leqq 5$ such that $u = (xy)^r u'$, where $u' \in \Gamma'$. Then

$$\begin{aligned} u^6 &= \{(xy)^r u'\}^6 \\ &= \{(xy)^r u'(xy)^{-r}\}\{(xy)^{2r} u'(xy)^{-2r}\} \cdots \{(xy)^{6r} u'(xy)^{-6r}\}(xy)^{6r}. \end{aligned}$$

A simple calculation shows that

(18) $$(xy)^6 = ab^{-1}a^{-1}b \in \Gamma'' \subset \Gamma'(6, 6).$$

Now if w is any element of Γ, define $S(w) = (xy)w(xy)^{-1}$. Thus

(19) $$u^6 = S^r(u')\ S^{2r}(u') \cdots S^{6r}(u')(xy)^{6r}.$$

We note that $S^k(u') \in \Gamma'$ for every integer k, and that $S^k(gh) = S^k(g)S^k(h)$ for arbitrary elements g, h of Γ. This implies that integers α, β exist such that

(20) $$u^6 = \{S^r(a)S^{2r}(a) \cdots S^{6r}(a)\}^{\alpha}\{S^r(b)S^{2r}(b) \cdots S^{6r}(b)\}^{\beta} u_1,$$

where $u_1 \in \Gamma'' \subset \Gamma'(6, 6)$.

$$
(21)\qquad
\begin{aligned}
S(a) &= ab^{-1}, & S(b) &= a,\\
S^2(a) &= ab^{-1}a^{-1}, & S^2(b) &= ab^{-1},\\
S^3(a) &= ab^{-1}a^{-1}ba^{-1}, & S^3(b) &= ab^{-1}a^{-1},\\
S^4(a) &= ab^{-1}a^{-1}b^2a^{-1}, & S^4(b) &= ab^{-1}a^{-1}ba^{-1},\\
S^5(a) &= ab^{-1}a^{-1}baba^{-1}, & S^5(b) &= ab^{-1}a^{-1}b^2a^{-1},\\
S^6(a) &= ab^{-1}a^{-1}bab^{-1}aba^{-1}, & S^6(b) &= ab^{-1}a^{-1}baba^{-1}.
\end{aligned}
$$

If we examine the exponent sums of a and of b in table (21) and take formula (20) into account, we find that if $r \neq 0$, then $u^6 \in \Gamma'' \subset \Gamma'(6, 6)$; while if $r = 0$, then $u^6 \in \Gamma'(6, 6)$. Hence $u^6 \in \Gamma'(6, 6)$ always, implying that $\Gamma^6 \subset \Gamma'(6, 6)$. Together with the previous inclusion this implies that $\Gamma^6 = \Gamma'(6, 6)$ and completes the proof of the theorem.

A noteworthy result implied by the previous discussion is that the decomposition of Γ^6 modulo Γ'' is given by

$$\Gamma^6 = \sum_{r=0}^{\infty} \sum_{s=0}^{\infty} a^{6r}b^{6s}\Gamma''.$$

Going to the matrix representation of Γ, we define $\Gamma(n)$, the principal congruence subgroup of Γ of level n, as the totality of 2×2 rational integral matrices A of determinant 1 satisfying $A \equiv \pm I \pmod{n}$; and $\bar{\Gamma}(n)$ as the totality of 2×2 rational integral matrices A of determinant 1 satisfying $A \equiv I \pmod{n}$.

It is easy to prove

THEOREM 7. $\Gamma' \supset \Gamma(6) \supset \Gamma^6$.

The proof of the latter inclusion consists of showing that

$$A^6 \equiv \pm I \pmod{6} \qquad \text{for matrices } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \bar{\Gamma}.$$

This is best done from the relationship $A^2 = tA - I$, $t = a + d$, by considering t modulo 2 and modulo 3 separately. Furthermore, it is not difficult to show that $\Gamma(2)$ is generated by elements of Γ^2 and $\Gamma(3)$ by elements of Γ^3, so that $\Gamma^2 \supset \Gamma(2)$, $\Gamma^3 \supset \Gamma(3)$. Since $\Gamma(2) \cap \Gamma(3) = \Gamma(6)$, it follows from (11) that $\Gamma' \supset \Gamma(6)$.

Theorem 7 is in agreement with some recent work of van Lint on the commutator subgroup $\bar{\Gamma}'$ of $\bar{\Gamma}$ (see [6]). In particular van Lint shows that $\bar{\Gamma}' \supset \bar{\Gamma}(12)$. The observation that $\Gamma' \supset \Gamma(6)$ was communicated to the author independently by J. R. Smart.

The remaining subgroups (13), if not of infinite index, are of high index in Γ.

For example we have that

$$\Gamma^6 \supset (\Gamma^6)^2 \supset \Gamma^{12}, \qquad \Gamma^6 \supset (\Gamma^6)^3 \supset \Gamma^{18};$$

and on the basis of Theorem 6 we have that

$$(\Gamma^6 : (\Gamma^6)^2) = 2^{37}, \qquad (\Gamma^6 : (\Gamma^6)^3) = 3^{8473},$$

since Γ^6 is the free group on 37 generators (see [2]). Hence

$$(\Gamma : \Gamma^{12}) \geqq 6^3 \cdot 2^{37}, \qquad (\Gamma : \Gamma^{18}) \geqq 6^3 \cdot 3^{8473}.$$

In conclusion we mention that each of the groups Γ^2 and Γ^3 is of genus 0 (see [1]).

REFERENCES

1. L. R. FORD, *Automorphic functions*, 2nd ed., New York, 1951.
2. M. HALL, JR., *The theory of groups*, New York, 1959.
3. A. KARRASS AND D. SOLITAR, *Note on a theorem of Schreier*, Proc. Amer. Math. Soc., vol. 8 (1957), pp. 696–697.
4. F. KLEIN, *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, Leipzig, 1890.
5. A. G. KUROSH, *The theory of groups*, New York, 1955, 1956.
6. J. H. VAN LINT, *On the multiplier system of the Riemann-Dedekind function η*, Nederl. Akad. Wetensch. Proc. Ser. A, vol. 61 (= Indag. Math., vol. 20) (1958), pp. 522–527.
7. M. NEWMAN, *Subgroups of the modular group and sums of squares*, Amer. J. Math., vol. 82 (1960), pp. 761–778.
8. J. NIELSEN, *The commutator subgroup of the free product of cyclic groups*, Mat. Tidsskr. B., 1948, pp. 49–56 (in Danish).
9. P. S. NOVIKOV, *On periodic groups*, Dokl. Akad. Nauk SSSR, vol. 127 (1959), pp. 749–752 (in Russian).
10. O. SCHREIER, *Die Untergruppen der freien Gruppen*, Abh. Math. Sem. Univ. Hamburg, vol. 5 (1927), pp. 161–183.

NATIONAL BUREAU OF STANDARDS
WASHINGTON, D. C.