TWO NOTES ON RANKIN'S BOOK ON THE MODULAR GROUP

Dedicated to the memory of Hanna Neumann

ROGER LYNDON

(Received 27 June 1972)

Communicated by M. F. Newman

We supply proofs that are simple, and possibly partly new, for two theorems that appear in Rankin's book [6].

1.

The first concerns subgroups of the inhomogeneous modular group. Let $\Gamma = SL(2, Z)$, the group of all 2 by 2 matrices with integer coefficients and with determinant 1. For each positive integer n, let $\Gamma(n)$ consist of those T in Γ such that $T \equiv I$ modulo n. Let $\Delta(n)$ be the least normal subgroup of Γ that contains the element $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

THEOREM 1. (a) *If* $1 \leqq n \leqq 5$, *then* $\Gamma(n) = \Delta(n)$.
(b) *For all* n, *the index of* $\Gamma(n)$ *in* Γ *is* $\eta(n) = n^3 \prod_{p/n} (1 - 1/p^2)$.
(c) *For* $n \geqq y$, *the index of* $\Delta(n)$ *in* Γ *is infinite.*

We first prove (b). Note that both $\Gamma(n)$ and $\Delta(n)$ are normal in Γ; thus we may write $\Gamma_n = \Gamma/\Gamma(n)$ and $\Delta_n = \Gamma/\Delta(n)$. Observe that both $|\Gamma_n|$ and $\eta(n)$ are multiplicative functions of n; therefore it suffices to treat the case that n is a power of a prime. The routine solution of a system of congruences shows that, under the natural map, $\Gamma_n \cong SL(2, Z_n)$. A standard argument gives the order of the latter group.

Clearly $\Delta(n) \subseteq \Gamma(n)$, whence $|\Gamma_n| \leqq |\Delta_n|$. Therefore, to establish (a) and (c) it suffices to show that, for $n \leqq 5$, $|\Delta_n| \leqq \eta(n)$ and that for $n \geqq 6$, $|\Delta_n| = \infty$. In the sequel we put aside the trivial case that $n = 1$.

Both Γ and Δ_n have center $Z = \{I, -I\}$. It is well known that $P = \Gamma/Z$ has the presentation

$$P\langle A, B \colon A^2 = 1, B^3 = 1\rangle,$$

where A and B are given by the matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Since $(AB)^n$ is given by $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, the group $G_n = \Delta_n/Z$ obtained from P by imposing the further relation $(AB)^n = 1$ has the presentation

$$G_n = \langle A, B;\, A^2 = 1, B^3 = 1, (AB)^n = 1 \rangle.$$

These groups are well known, especially from the work of Coxeter (see [1]). It remains to show that G_2 has order $\eta(2)$, that $2\,|G_n| = \eta(n)$ for $n = 3, 4, 5$, and that G_n is infinite for $n \geqq 6$.

For each $n \geqq 2$ we shall construct a graph T_n on the sphere (or better, for $n \geqq 6$, in the plane) such that each region is a triangle and that there are exactly n edges at each vertex. For $n = 2, 3, 4, 5$ we take T_n to be a triangle, the 1-skeleton of a tetrahedron, of an octahedron, of an icosahedron. This reflects the fact that the corresponding Δ_n are the symmetry groups of these figures.

Let $n \geqq 6$. We begin with a triangle ABC and enclose it it a circle K not touching it. Join A and B to a point C' on K, join B and C to a point A' on K, and join C and A to a point B' on K. Now join each of A, B, and C to additional points on K until there are n edges at each of these three vertices. Clearly this can be done so that each bounded region in the resulting figure is a (topological) triangle. We now enclose the figure obtained so far in a larger circle K' not touching it, and repeat the process. It is easy to see that this process can be iterated indefinitely and will yield an infinite graph T_n with the required properties.

We now modify T_n to obtain a new graph S_n. We draw small circles about the vertices of T_n (small enough that no two meet) and delete those parts of T_n interior to these circles. In S_n each vertex lies on exactly three edges: two that are arcs of the small circles and one that is 'straight', that is, the remnant of an edge from T_n.

Let Ω be the set of vertices of S_n. Define two permutations of Ω as follows. If P is any vertex, then $\alpha(P)$ is the other vertex on the straight edge at P, while $\gamma(P)$ is the other vertex on the circular arc proceeding counterclockwise out of P. It is immediate that $\alpha^2 = 1$ and $\gamma^n = 1$. Moreover, inspection shows that, if $\beta = \alpha\gamma$, then $\beta^3 = 1$. If π is the group of permutations of Ω generated by α and γ, it is immediate that setting $\phi(A) = \alpha$ and $\phi(B) = \beta$ define a homomorphism ϕ from G_n onto π. (In fact ϕ is an isomorphism, and S_n is a Cayley diagram for G_n; alternatively, that ϕ is an isomorphism follows by a method known to Poincaré (see Macbeath [3]).

Since π acts regularly on Ω, we have $|\pi| = |\Omega|$, whence $|G_n| \geqq |\Omega|$. This gives the desired inequality for $|\Delta_n|$ in both the finite and infinite cases.

2.

The second theorem is one of Nielsen [4]. We state it in a mildly modified form.

THEOREM 2. *Let $G_1, \cdots, G_n$ be arbitrary groups, and let N be the kernel* *of the natural map from the free product* $G = G_1 * \cdots * G_n$ *onto the direct product* $\bar{G} = G_1 \times \cdots \times G_n$. *Then* N *is free group with a basis* X *consisting of all non trivial elements of the form*

$$x = (a_1 \cdots a_{i-1} a_{i+1} \cdots a_n a_i)(a_1 \cdots a_n)^{-1}$$

where $a_1 \in G_1, \cdots, a_n \in G_n$.

We begin the proof by showing that X generates N. Let H be the subgroup generated by X. Clearly $H \subseteq N$. It will suffice to show that $G = HG_1 \cdots G_n$. For this it suffices to show that, for all $i = 1.2, \cdots, n$ one has $HG_1 \cdots G_n G_i = HG_1 \cdots G_n$. Now $Hx = H$ for all $x \in X$ implies that $HG_1 \cdots G_{i-1} G_{i+1} \cdots G_n G_i = HG_1 \cdots G_n$. Using this relation we find that $HG_1 \cdots G_n G_i = HG_1 \cdots G_{i-1} G_{i+1} \cdots G_n G_i G_i$ $HG_1 \cdots G_{i-1} G_{i+1} \cdots G_n G_i = HG_1 \cdots G_n$.

It remains to show that X is a basis for N. Note that an element x as above is not trivial just in case $a_i \neq 1$ and that $a_j \neq 1$ for some $j > i$. We write $x = UV^{-1}$ where $U = a_1 \cdots a_{i-1} a_{i+1} \cdots a_n a_i$ and $V = a_1 \cdots a_n$. Then U and V have the same length $|U| = |V| = m \leqq n$ and $|x| = 2m$. (Here m is the number of non-trivial factors a_i.) Let $x' = U'V'^{-1}$ denote analogously another element of X.

We make several observations.

(1) If x and x' have the initial segment U in common, then $x = x'$. This follows from the fact that a_i, as the first (non trivial) syllable of x with decreasing subscript, must match the first such syllable of x'. This implies that $U = U'$ whence also $V = V'$.

(2) If x^{-1} and x'^{-1} have an initial segment longer than V in common, then $x = x'$. Suppose they had such an initial segment in common, and hence the initial segment Va_i^{-1}. Since a_i^{-1} is the first syllable of x^{-1} with decreasing subscript, it must match the first such syllable of x'^{-1}, whence $Va_i^{-1} = V'a_{i'}^{-1}$. From $V = V'$ it follows that $a_1 = a_1', \cdots, a_n = a_n'$, and we have also that $a_i^{-1} = a_{i'}^{-1}$, whence $i = i'$. Thus $U = U'$ and $x = x'$.

(3) If x^{-1} and x' have the initial segment V in common, then they have no longer initial segment in common, and the segment V is less than half of x'. This follows from the facts that V, with increasing subscripts, must be a proper initial segment of U', and that Va_i^{-1}, containing two syllables a_i and a_i^{-1} from G_i, cannot be a segment of U'.

(4) In a product $xx'^e \neq 1$, with $e = \pm 1$, at most the right half V^{-1} of x cancels. If $e = +1$ this follows from (3), and if $e = -1$ from (2).

(5) In a product $x'^e x \neq 1$, with $e = \pm 1$, not all of the left half U of x cancels. If $e = +1$ this follows from (3), and if $e = -1$ from (1).

Now a classical argument of Nielsen [5] shows that in a product $w = x_1^{e_1} \cdots x_k^{e_k}$ where $k \geqq 1$ and no ${x_i}^{e_i} {x_{i+1}}^{e_{i+1}} = 1$, some part of each factor remains after cancellation, whence $w \neq 1$. This proves that X is a basis. (It is curious that Nielsen himself used at this point a different argument.)

We conclude with two remarks. The first is a minor point, that Nielsen used a slightly different basis consisting of elements of the form

$$x' = (a_1 \cdots a_{i-1}a_{i+1} \cdots a_{j-1})(a_i a_j a_i^{-1} a_j^{-1})(a_1 \cdots a_{i-1}a_{i+1} \cdots a_{j-1})^{-1}.$$

It is easy to pass from one basis to the other by Nielsen transformations. The second point is that Nielsen treated only the case that the G_i are all finite cyclic groups, and in this case gave a formula for the rank $r(N) = |X|$ of N. For the slightly more general case that all the groups G_i are arbitrary finite groups, and hence that $\bar{G}$ is finite and N again of finite rank, a formula for $r(N)$ can be recovered easily by counting how many n-tuples $a_1, \cdots, a_n$ yield non trivial elements $x \in X$. The result can be stated as a generalization of Schreier's index theorem. Assuming all the G_i finite, define the 'free rank' of G_i to be $r(G_i) = 1 - 1/|G_i|$ and $r(G) = r(G_1) + \cdots + r(G_n)$. Then one has

$$[G : N] = \frac{r(N) - 1}{r(G) - 1}.$$

In Nielsen's case this is indeed a case of a classical formula for surface groups, for which a combinatorial proof is given in [2]. One may conjecture that such a formula holds for a subgroup N, not neccesarily normal, in a free product G of some more extensive class of groups G_i for which a reasonable definition of $r(G_i)$ can be provided.

Postscript (August, 1972). Mr. I. Chiswell has established that for G and the function r as defined above, the formula stated above holds for any subgroup N of finite index in G, without the assumption that N is normal.

References

[1] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, 2nd ed., Ergebisse der Mathematik und ihrer Grenzegbiete, Band 14. (Springer-Verlag, Berlin, Göttingen, Heidleberg, New York, 1965).

[2] A. Howard M. Hoare, Abraham Karrass and Donald Solitar, 'Subgroups of finite index of Fuchsian groups', *Math. Z.* 120 (1971), 289–298.

[3] A. M. Macbeath, *Fuchsian Groups*, (Lectures at Queen's College, Dundee, 1961.)

[4] Jakob Nilsen, 'The commutator group of the free product of cyclic groups', (Danish), *Mat. Tidskr.* B 1948 (1948), 49–56.

[5] Jakob Nielsen, 'A basis for subgroups of free groups', *Math. Scand.* 3 (1955), 31–43.

[6] R. A. Rankin, *The Modular Group and its Subgroups*. (Ramanujan Institute, 1969),

Université de Montpellier
Montpellier, France.

Present address:
University of Michigan
Ann Arbor, Michigan, USA

https://doi.org/10.1017/S1446788700015433 Published online by Cambridge University Press