PACIFIC JOURNAL OF MATHEMATICS
Vol. 42, No. 3, 1972

COHOMOLOGY OF FINITELY PRESENTED GROUPS

P. M. CURRAN

Let G be a finitely presented group, G' a finite quotient of G and K a field. Let G act on the group algebra $V = K[G']$ in the natural way. For a suitable choice of G' we obtain estimates on the dimension of $H^1(G, V)$ in terms of the presentation and then use these estimates to derive information about G.

If G is generated by n elements, of which m have finite orders $k_1, \cdots, k_m$, resp., and G has the presentation

$$\langle a_1, \cdots, a_n; a_1^{k_1}, \cdots, a_m^{k_m}, r_{m+1}, \cdots, r_{m+q}\rangle ,$$

then, in particular, we show that (a) the minimum number of generators of G is $\geqq n - q - \sum 1/k_i$; (b) if this lower bound is actually attained, then G is free, of this rank, and (c) G is infinite if $\sum 1/k_i \leqq n - q - 1$. The latter, together with a result of R. Fox, yields an algebraic proof that the group

$$\langle a_1, \cdots, a_m; a_1^{k_1}, \cdots, a_m^{k_m}, a_1 \cdots a_m\rangle$$

is infinite if $\sum 1/k_i \leqq m - 2$.

1. An exact sequence. Let G be a group with the presentation $\langle a_1, \cdots, a_n; r_1, r_2, \cdots\rangle$, i.e., $G = F/N$, where F is the free group on $\{a_1, \cdots, a_n\}$ and N is the normal subgroup generated by $\mathscr{R} = \{r_1, r_2, \cdots\}$. We denote by φ the homomorphism of group rings $Z[F] \to Z[G]$ which extends the natutral map $F \to F/N$, and by A_i the element φa_i of G.

Let ρ be a representation of G in $\mathrm{Aut}(V)$, where V is a finite-dimensional vector space over a field K. We shall be concerned with the first cohomology group $H^1(G, V)$, which is also a vector space over K in an obvious way. One knows that an arbitrary map $f: \{A_1, \cdots, A_n\} \to V$ extends to a 1-cocycle of G in V if and only if the 1-cocycle of F determined by $a_i \mapsto f(A_i)$ vanishes on the relators. More precisely, the following sequence is exact:

$$(*) \qquad 0 \longrightarrow Z^1(G, V) \xrightarrow{E} V^n \xrightarrow{D} V_1 \oplus V_2 \oplus \cdots .$$

Here, $Z^1(G, V)$ is the space of 1-cocycles, V^n is the direct sum of n copies of V, $V_i = V$ for each i, E is the map $f \mapsto (f(A_1), \cdots, f(A_n))$, D is the map

$$(u_1, \cdots, u_n) \longmapsto \left(\sum_j (\partial r_1/\partial a_j)u_j, \sum_j (\partial r_2/\partial a_j)u_j, \cdots\right) ,$$

and in the last term of the sequence there is one copy of V for each member of $\mathscr{R}$. $\partial r/\partial a_j$ is the Fox derivative of r with respect to a_j [2, Chap. VII, § 2].

Now suppose $r_i = a_i^{k_i}$ for $i = 1, \cdots, m$, and that the characteristic of K does not divide any of the k_i. Then for $i = 1, \cdots, m$,

$$\sum_j (\partial r_i/\partial a_j)u_j = (1 + T_i + \cdots + T_i^{k_i-1})u_i ,$$

where $T_i = \rho\varphi a_i$, so, using the fact that

$$\mathrm{Ker}\,(1 + T_i + \cdots + T_i^{k_i-1}) = \mathrm{Im}\,(1 - T_i) ,$$

we may replace (*) by

$$(**) \qquad \begin{aligned} 0 \longrightarrow Z^1(G, V) &\xrightarrow{E} \mathrm{Im}\,(1 - T_1) \oplus \cdots \oplus \mathrm{Im}\,(1 - T_m) \\ &\oplus V^{n-m} \xrightarrow{D'} V_{m+1} \oplus V_{m+2} \oplus \cdots \end{aligned}$$

where D' is given by

$$(u_1, \cdots, u_n) \longmapsto \left(\sum_j (\partial r_{m+1}/\partial a_j)u_j, \sum_j (\partial r_{m+2}/\partial a_j)u_j, \cdots\right) .$$

2. Conditions for G to be a free product. The following lemma will be needed for the applications in the next section. In what follows, $[x, y, \cdots]$ denotes the subgroup of G generated by $\{x, y, \cdots\}$, $|x|$ is the order of x, $A = \varphi a$ and $G_1 * G_2$ is the free product of G_1 and G_2. Otherwise the notation is that of § 1.

LEMMA. *Let* $G = \langle a = a_1, a_2, \cdots, a_n; \mathscr{R}\rangle$. *Then*

(a) *The following statements are equivalent.*

(1) $\varphi(\partial r/\partial a(1 - a)) = 0$ *for all* $r \in \mathscr{R}$ *(and therefore for all* $r \in N$*).*

(2) $G = [A]*[A_2, \cdots, A_n]$.

(b) *If* (1) *is replaced by the stronger condition* $\varphi(\partial r/\partial a) = 0$ *for all* $r \in \mathscr{R}$, *then the condition* $|A| = \infty$ *may be added to* (2).

Proof. (a) If $A = 1$, then (1) and (2) are trivially true, so we may assume that $A \neq 1$ from now on.

(2) $\Rightarrow$ (1): Given $G = [A]*[A_2, \cdots, A_n]$, let $\langle a_2, \cdots, a_n; \mathscr{S}\rangle$ be a presentation for $[A_2, \cdots, A_n]$. Then $\varphi(\partial s/\partial a(1 - a)) = 0$ for all $s \in \mathscr{S}$, and if $|A| = k$, $\varphi(\partial a^k/\partial a(1 - a)) = \varphi(1 - a^k) = 0$. Thus $\varphi(\partial r/\partial a(1 - a)) = 0$ for all r in a system of defining relations for G. It follows easily that the same is true for all $r \in N$, hence, in particular, for all members of $\mathscr{R}$.

(1) $\Rightarrow$ (2): Suppose $\varphi(\partial r/\partial a(1-a)) = 0$ for all $r \in \mathscr{R}$. We may assume that no proper part of any member of $\mathscr{R}$ is in N, and if $|A| = k < \infty$, that $a^k \in \mathscr{R}$. Let $\mathscr{R}_1 = \mathscr{R} - \{a^k\}$ if $a^k \in \mathscr{R}$; otherwise, let $\mathscr{R}_1 = \mathscr{R}$. We claim that all members of $\mathscr{R}_1$ are free of a and a^{-1}. This will complete the proof.

Suppose some $r \in \mathscr{R}_1$ involves a or a^{-1}. We may assume that r has the form $r = aw_1a^{\pm 1}w_2 \cdots a^{\pm 1}w_r$, where w_1 is not the empty word. Applying condition (1) to r and multiplying the resulting equation on the left by $\varphi(a^{-1})$, we obtain

$$\begin{aligned}\varphi(a^{-1}) &\pm \varphi(w_1(a^{-1})) \pm \cdots \pm \varphi(w_1 \cdots w_{r-1}(a^{-1})) \\ &= 1 \pm \varphi(w_1(a)) \pm \cdots \pm \varphi(w_1 \cdots w_{r-1}(a)) ,\end{aligned}$$

where the parenthetical a^{-1} in the left hand member occurs precisely when the term has a minus sign and the parenthetical a on the right goes with the plus sign. But all terms except the first term on each side are images of proper parts of r, hence $\neq 1$, and $\varphi(a^{-1}) \neq 1$ by hypothesis, so the last equation is impossible in $Z[G]$. This contradiction completes the proof of (a).

As for (b), if $G = [A]*[A_2, \cdots, A_n]$ and $|A| = \infty$, then G has a presentation in which no relator involves a, so $\partial r/\partial a = 0$ for all r in N. Conversely, if $|A| = k < \infty$, then $\varphi(\partial a^k/\partial a) = 1 + A + \cdots A^{k-1} \neq 0$.

COROLLARY. *Let* $G = \langle a_1, \cdots, a_n; \mathscr{R}\rangle$. *Suppose that*

(1) *for* $j = 1, \cdots, m$, $\varphi(\partial r/\partial a_j(1-a_j)) = 0$, *all* $r \in \mathscr{R}$, *but there exists* $r_j \in N$ *such that* $\varphi(\partial r_j/\partial a_j) \neq 0$, *and*

(2) *for* $j = m+1, \cdots, m+p$, $\varphi(\partial r/\partial a_j) = 0$ *for all* $r \in \mathscr{R}$. *Then*

(a) $G = [A_1]* \cdots [A_{m+p}]*[A_{m+p+1}, \cdots A_n]$ *and*

(b) $|A_j| < \infty, j = 1, \cdots, m$ *and* $|A_j| = \infty, j = m+1, \cdots, m+p$.

3. The main theorem. We recall that a group G is *residually finite* if given $1 \neq g \in G$, there exists a finite quotient of G in which the image of g is $\neq 1$. By a theorem of Mal'cev [5], all finitely generated linear groups over a field are residually finite.

We note for future reference some easily deduced properties of residually finite groups. (R is any ring with unity.)

RF1. If G is residually finite and $\alpha_1, \cdots, \alpha_r$ are nonzero elements of the group ring $R[G]$, there exists a finite quotient G' of G such that the images of $\alpha_1, \cdots, \alpha_r$ in $R[G']$ are all nonzero.

RF2. Let g_i have finite order k_i, $i = 1, \cdots, m$, in a residually finite group G. Then there exists a finite quotient of G in which the image of g_i has order k_i for each i.

Now suppose G is a group, G' a finite quotient of G and K a field. Let an action of G on the group algebra $V = K[G']$ be defined as follows: If $g \in G$ and $v \in V$, gv is defined to be the product $g'v$ in $K[G']$ where g' is the image of g in G'. Then it is easy to show that $V^G = \{v \in V: gv = v, \text{ all } g \in G\}$ is the one-dimensional subspace generated by $s = \sum_{g' \in G'} g'$. We shall also need to know the "fixed point" space of an element $g \in G$, i.e. $\{v \in V: gv = v\}$. Let $G' = \{g'_1, \cdots, g'_d\}$. If π is the permutation of $\{1, \cdots, d\}$ such that $g'g'_i = g'_{\pi i}$ and g' has order k, then π is the product of d/k disjoint cycles: $\pi = (i_1, \cdots, i_k)(i_{k+1}, \cdots, i_{2k}) \cdots$. It follows easily that the fixed point space of g is the d/k-dimensional subspace of V generated by the elements

$$\sum_{j=1}^{k} g'_{i_j}, \ \sum_{j=k+1}^{2k} g'_{i_j}, \ \cdots .$$

The main results are consequences of the following theorem. The notation is that of § 2.

THEOREM. *Let G be a residually finite group with the presentation*

$$\langle a_1, \cdots, a_n; a_1^{k_1}, \cdots, a_m^{k_m}, r_{m+1}, r_{m+2}, \cdots \rangle$$

and let K be a field of characteristic 0. (*We assume the* $k_i > 1$.) *Then there exists a finite quotient G' of G such that if G acts on $V = K[G']$ as above, then, letting $d = |G'|$, $\sigma = \sum_{i=1}^{m} 1/|A_i|$ and $\tau = \sum_{i=1}^{m} 1/k_i$, we have*

(a) $\dim H^1(G, V) \leqq (n - \sigma - 1)d + 1 \leqq (n - \tau - 1)d + 1$

(b) *if equality holds throughout* (a), *then* $G = [A_1] * \cdots * [A_n]$, $|A_j| = k_j$, $j = 1, \cdots, m$ *and* $|A_j| = \infty$, $j = m + 1, \cdots, n$.

(c) *if the set of defining relations is finite, say*

$$\mathscr{R} = \{a_1^{k_1}, \cdots, a_m^{k_m}, r_{m+1}, \cdots, r_{m+q}\} ,$$

then $\dim H^1(G, V) \geqq (n - \sigma - q - 1)d + 1$.

REMARK. It will be clear from the proof that if a finite number of presentations of G are given, G' can be chosen so that (a) through (c) are simultaneously true for all the given presentations.

Proof. By RF2, choose G' so that the image of A_i in G' has order $|A_i|$, $i = 1, \cdots, m$. In the notation of (**), § 1,

$$\dim \operatorname{Im}(1 - T_i) = d - \dim \operatorname{Ker}(1 - T_i) = d(1 - 1/|A_i|)$$

by the remarks preceding the theorem. Hence, by (**)

$$(1) \qquad \dim Z^1(G, V) = (n - \sigma)d - \operatorname{rank}(D') .$$

Now the map of V onto the space $B^1(G, V)$ of coboundaries given by $v \mapsto f_v$, where $f_v(g) = gv - v$ for all $g \in G$, has kernel V^G, so

$\dim B^1 = d - 1$. Combining this with (1) yields the first inequality in (a). The second inequality is clear.

To prove (b), note first that if $|A_i| < k_i$ for some i, then the second inequality in (a) is strict. Therefore it with suffice to show that if $G \neq [A_1] * \cdots * [A_n]$ or if some A_j with $j > m$ has finite order, then G' can be chosen so that (in addition to the preservation of orders $|A_i|$, $i = 1, \cdots, m$) we have $D' \neq 0$. For then, (1) implies that the first inequality in (a) is strict.

Consider the following elements of $K[G]$:

$$\varphi(\partial r_i/\partial a_j), \quad i > m, j > m$$
$$\varphi(\partial r_i/\partial a_j(1 - a_j)), \quad i > m, j \leqq m \,.$$

One of these must be nonzero since otherwise, by the Corollary of § 2, $G = [A_1] * \cdots * [A_n]$ and $|A_i| = \infty$, $i > m$, contrary to hypothesis. Therefore by RF1 there exists a finite quotient G' such that the image in $K[G']$ of this nonzero element is also nonzero. One easily sees then that $D' \neq 0$. This proves (b).

Given the hypothesis of (c), we have rank $D' \leqq qd$. The conclusion then follows from (1) above.

COROLLARY 1. *Let G be a residually finite group with two presentations*

$$G = \langle a_1, \cdots, a_n; a_1^{k_1}, \cdots, a_m^{k_m}, r_{m+1}, \cdots, r_{m+q} \rangle$$
$$= \langle b_1, \cdots, b_N; b_1^{h_1}, \cdots, b_M^{h_M}, s_{M+1}, \cdots \rangle \,.$$

Then

$$n - \sum_{i=1}^{m} 1/|A_i| - q \leqq N - \sum_{j=1}^{M} 1/h_j \,,$$

and if equality holds, then $G = [B_1] * \cdots * [B_N]$, $|B_j| = h_j$ for $j = 1, \cdots, M$ and $|B_j| = \infty$ for $j > M$. (B_k is the image in G of the free generator b_k.)

Proof. Apply part (c) to the first presentation and parts (a) and (b) to the second. (See the remark preceding the proof of the theorem.)

Note that Corollary 1 implies for residually finite groups the well-known result [4, Cor. 5.14.2] that if a group G with n generators and q defining relations can be generated by $n - q$ elements, then G is free of rank $n - q$.

COROLLARY 2. *Let*

$$G = \langle a_1, \cdots, a_n; a_1^{k_1}, \cdots, a_m^{k_m}, r_{m+1}, \cdots, r_{m+q} \rangle \,.$$

Then G is infinite if

$$\sum_{i=1}^{m} 1/|A_i| \leqq n - q - 1 .$$

Proof. If $|G| = d < \infty$, we may take $G' = G$ in the proof of the Theorem. But then $dH^1(G, V) = 0$ [1, Chap. XII, Prop. 2.5] so $H^1(G, V) = 0$ since K has characteristic zero. The conclusion now follows from part (c) of the Theorem.

Finally, we apply Corollary 2 to a classical case. Let

$$G = \langle a_1, \cdots, a_m; a_1^{k_1}, \cdots, a_m^{k_m}, a_1 \cdots a_m \rangle .$$

From geometric considerations (e.g. [7, p. 28, Satz 8]) one knows that the group is infinite if $\sum 1/k_i \leqq m - 2$. In 1902, Miller [6] gave an algebraic proof of this fact for the case $m = 3$, but the argument involves consideration of many cases.

In [3] Fox shows that if k_1, k_2, k_3 are integers >1, then there exist permutations A and B of orders k_1 and k_2, resp., such that AB has order k_3. It follows easily from this that $k_i = |A_i|$ in the above group (assuming $m > 2$). Hence Corollary 2, together with this result, yields an algebraic proof that G is infinite when $\sum 1/k_i \leqq m - 2$.

References

1. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton, 1956.
2. R. H. Crowell and R. H. Fox, *Introduction to knot theory*, Ginn and Co., 1963.
3. R. Fox, *On Fenchel's conjecture about F-groups*, Mat. Tidsskr. B, (1952), 61-65.
4. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory*, Interscience, New York, 1966.
5. A. Mal'cev, *On isomorphic matrix representations of infinite groups*, Mat. Sb., **8** (50) (1940), 405-422. (Russian).
6. G. A. Miller, *Groups defined by the orders of two generators and the order of their product*, Amer. J. Math., **24** (1902), 96-100.
7. W. Threlfall, *Gruppenbilder*, Abh. sächs. Akad. Wiss. Math.-phys. Kl. 41, (1932), 1-59.

Received May 27, 1970 and in revised form July 21, 1972.

FORDHAM UNIVERSITY
AND
THE INSTITUTE FOR ADVANCED STUDY