

THE FOX MODULES OF A FINITE GROUP

N. D. GUPTA*

University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

AND

I. B. S. PASSI

Centre for Advanced Study in Mathematics, Panjab University,
Chandigarh 160014, India

(Received 4 September 1980)

Let F be a free group of finite rank > 1 and let R be a normal subgroup of F . Then the quotient $\overline{F(k, R)} = F(k, R)/F(k + 1, R)$, where $F(n, R)$ denotes the n th Fox subgroup of F relative to R , can be regarded as a right F/R -module via conjugation in F . This paper determines, for finite F/R , the structure of the module $U_k = \overline{F(k, R)} \otimes_{\mathbb{Z}} \mathbb{Q}$ as a right $\mathbb{Q}(F/R)$ -module, where \mathbb{Q} is the field of rational numbers.

1. INTRODUCTION

Let $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ be a free presentation of a finite group G with F free of finite rank exceeding one. For each $k \geq 0$, let $F(k, R) = F \cap (1 + \mathfrak{f}^k \mathfrak{r})$ be the k th Fox subgroup of F relative to R , where $\mathfrak{f} = (F - 1)\mathbb{Z}F$ and $\mathfrak{r} = (R - 1)\mathbb{Z}R$. The quotient $\overline{F(k, R)} = F(k, R)/F(k + 1, R)$ can be regarded as a right G -module via conjugation in F . We call these modules the Fox modules of G (the case $k = 0$ is the relation module R/R'). The purpose of this paper is to determine the structure of the module $U_k = \overline{F(k, R)} \otimes_{\mathbb{Z}} \mathbb{Q}$ as a right $\mathbb{Q}G$ -module, where \mathbb{Q} is the field of rational numbers. This is achieved by finding a character formula for U_k . As an application we are able to determine the behaviour of the upper central series of $F/F(k, R)$. Our main results are as follows :

Theorem A -- For $k \geq 0$, let χ_k denote the character of the Fox module

$$U_k = \overline{F(k, R)} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Then

$$\chi_k(g) = \begin{cases} \rho(k + 1) + m^k(1 - m) & \text{for } g \neq 1 \\ \rho(k + 1) + m^k(t - m) & \text{for } g = 1 \end{cases}$$

*Research supported by NSERC, Canada.

where m is the rank of F , $\rho(n) = \frac{1}{n} \sum_{d|n} \mu(d) m^{n/d}$ (= the rank of the n th lower central factor $\gamma_n(F)/\gamma_{n+1}(F)$) and $t = 1 + (m - 1) |G|$ is the rank of R .

Theorem B — For $k \geq 0$,

$$U_k = \mathbb{Q} \oplus \mathbb{Q} \oplus \dots \oplus \mathbb{Q} \oplus \mathfrak{g} \oplus \mathfrak{g} \oplus \dots \oplus \mathfrak{g}$$

$$\leftarrow \rho(k + 1) \rightarrow \leftarrow m^k(m - 1) \rightarrow$$

where $\mathfrak{g} = (G - 1) \mathbb{Q}G$ is the augmentation ideal of $\mathbb{Q}G$.

Theorem C — For $k \geq 0$, the centre of $F/F(k + 1, R)$ is the isolator of

$$\gamma_{k+1}(C) F(k + 1, R)/F(k + 1, R),$$

where C/R' is the centre of F/R' .

Theorem D — For $k \geq 0$, the second centre of $F/F(k + 1, R)$ coincides with the centre of $F/F(k + 1, R)$.

2. SOME PRELIMINARY RESULTS

Let $1 \rightarrow R \rightarrow F \xrightarrow{\theta} G \rightarrow 1$ be a free presentation of a finite group G with F free of finite rank $m \geq 2$. Then by (Magnus *et al.* 1966, Theorem 3.5, p. 140) we can choose a set of free generators x_1, x_2, \dots, x_m of F and a set of generators of R such that

$$r_i = x_i^{d_i} \xi_i \quad \text{for } 1 \leq i \leq m$$

and $r_i = \xi_i \quad \text{for } m + 1 \leq i \leq s$

where d_i 's are integers > 0 (since G is finite) and ξ_i 's are in F' , the derived group of F . Let

$$V = \frac{R}{R'} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Then, as a \mathbb{Q} -vector space, V is spanned by $(r_i R') \otimes 1 (1 \leq i \leq s)$. Clearly

$$(r_i R') \otimes 1 (1 \leq i \leq m)$$

are linearly independent. Without loss of generality we may, therefore, assume that $(r_i R') \otimes 1 (1 \leq i \leq t)$ is a basis of V for some t with $m \leq t \leq s$. Since $t = \dim V = \text{rank of } R/R' = \text{rank of } R$, the Schreier formula gives

$$t = 1 + (m - 1) |G|.$$

For each $i = 1, 2, \dots, m$, let

$$r_i^* R' = \sum_{g \in G} (r_i R') \cdot g.$$

Then

$$r_i^* = r_i^{|G|} \zeta_i$$

with $\zeta_i \in R \cap F'$. Therefore,

$$(r_i^* R') \otimes 1 = |G| ((r_i R') \otimes 1) + (\zeta_i R') \otimes 1$$

Since $\zeta_i \in R \cap F'$, $(\zeta_i R') \otimes 1$ lies in the subspace spanned by

$$r_j R' \otimes 1 \quad (m + 1 \leq j \leq t).$$

We can thus conclude that

$$\{(r_1^* R' \otimes 1, \dots, (r_m^* R') \otimes 1, (r_{m+1} R') \otimes 1, \dots, (r_t R') \otimes 1\}$$

is a basis for V where now each $(r_i^* R') \otimes 1$ is left fixed by all elements of G . Hence we have a decomposition of V as

$$V = V_1 \oplus V_2 \oplus \dots \oplus V_m \oplus W$$

where V_i is the 1-dimensional subspace spanned by $(r_i^* R') \otimes 1$ on which G acts as identity and W is $(t - m)$ -dimensional subspace spanned by $(r_j R') \otimes 1$ $(m + 1 \leq j \leq t)$ which is easily seen to be G -invariant. Let χ_0 denote the character of V as a G -module. Then we have the following well-known result :

Lemma 1 (Gaschütz 1954) —

$$\chi_0(g) = \begin{cases} 1 & \text{for } g \neq 1 \\ t & \text{for } g = 1. \end{cases}$$

As an immediate consequence of Lemma 1 we have the following :

Lemma 2 — Let φ denote the character of W as a G -module. Then

$$\varphi(g) = \begin{cases} 1 - m & \text{for } g \neq 1 \\ t - m & \text{for } g = 1. \end{cases}$$

It has been shown by Gupta (1977) that (for F/R finite)

$$F(k, R) = \sqrt{\{[R \cap \gamma_k(F), R \cap \gamma_k(F)] \gamma_{k+1}(R)\}}.$$

(For $H \leq G$, \sqrt{H} denotes the isolator $\{x \in G \mid x^m \in H \text{ for some } m > 0\}$)

Lemma 3 — $U_k = (\gamma_{k+1}(R) F(k + 1, R))/F(k + 1, R) \otimes_{\mathbb{Z}} \mathbb{Q}$.

PROOF : For $r_{i(t)} \in \{r_1, r_2, \dots, r_m\}$, $k \geq 2$,

the left-normed commutator

$$[r_{i(1)}, r_{i(2)}, \dots, r_{i(k)}]$$

is equal, mod $\gamma_{k+1}(F)$, to the left-normed commutator

$$[x_{i(1)}, x_{i(2)}, \dots, x_{i(k)}]^{d_{i(1)}d_{i(2)}\dots d_{i(k)}}.$$

Consequently

$$R \cap \gamma_k(F) \leq \sqrt{\{(R \cap \gamma_{k+1}(F)) \gamma_k(R)\}}$$

and hence the commutator subgroup

$$[R \cap \gamma_k(F), R \cap \gamma_k(F)]$$

is contained in

$$\sqrt{\{[R \cap \gamma_{k+1}(F), R \cap \gamma_{k+1}(F)] \gamma_{k+1}(R)\}}.$$

and the Lemma follows.

We next describe for U_k a basis which is essentially contained in Gupta (1977). We, however, give full details for the sake of completeness.

Lemma 4 — For $k \geq 0$, a basis for U_k consists of all elements of the form

$$\overline{b_{k+1}(r_1^*, r_2^*, \dots, r_m^*)} \otimes 1$$

where $b_{k+1}(r_1^*, r_2^*, \dots, r_m^*)$ is a basic commutator of weight $k + 1$ in $r_1^*, r_2^*, \dots, r_m^*$ (bar denotes the coset mod $F(k + 1, R)$) and all elements of the form

$$[r_j, r_{i(1)}^*, r_{i(2)}^*, \dots, r_{i(k)}^*] \otimes 1$$

with $r_j \in \{r_{m+1}, r_{m+2}, \dots, r_l\}$ and $r_{i(l)}^* \in \{r_1^*, r_2^*, \dots, r_m^*\}$ for $1 \leq l \leq k$.

PROOF : By Lemma 3, U_k is generated by

$$\overline{[s_{i(1)}, s_{i(2)}, \dots, s_{i(k+1)}]} \otimes 1$$

where $s_{i(j)} \in \{r_1^*, r_2^*, \dots, r_m^*, r_{m+1}, \dots, r_l\}$.

Since every commutator of weight $k + 1$ in R with two of its entries in $R \cap F'$ is contained in $F(k + 1, R)$, we may assume that in each of the above generators at most one of the entries $s_{i(j)}$ is in the set $\{r_{m+1}, r_{m+2}, \dots, r_l\}$. It, therefore, follows that U_k is spanned by all elements of the form

$$\overline{b_{k+1}(r_1^*, r_2^*, \dots, r_m^*)} \otimes 1 \quad (\text{Type I})$$

where $b_{k+1}(r_1^*, r_2^*, \dots, r_m^*)$ is a basic commutator of weight $k + 1$ in $r_1^*, r_2^*, \dots, r_m^*$ and (using Jacobi identity) by all element of the form

$$[r_i, r_{i(1)}^*, r_{i(2)}^*, \dots, r_{i(k)}^*] \otimes 1 \quad (\text{Type II}).$$

Working modulo $\gamma_{k+2}(F)$ alone shows that the generators of Type I are linearly independent and

$$U_k = U_k^{(1)} \oplus U_k^{(2)}$$

where $U_k^{(1)}$ is the subspace with basis consisting of elements of Type I and $U_k^{(2)}$ is the subspace spanned by elements of Type II. To prove the linear independence of elements of Type II it clearly suffices to prove that for $u_i = u_{i(i(1), i(2), \dots, i(k))} \in R \cap F'$,

$$\prod_{i=1}^{m^k} [u_i, r_{i(1)}^*, r_{i(2)}^*, \dots, r_{i(k)}^*] \otimes 1 = 0$$

if and only if each $u_i \in R'$. To see this observe that if

$$\prod_i [u_i, r_{i(1)}^*, r_{i(2)}^*, \dots, r_{i(k)}^*]$$

belongs to $F(k + 1, R)$, then

$$\sum_i (-1)^k (r_{i(k)}^* - 1) (r_{i(k-1)}^* - 1) \dots (r_{i(1)}^* - 1) (u_i - 1) \in \mathfrak{f}^{k+1}\mathfrak{r}$$

which in turn implies that

$$\begin{aligned} &\sum_i (-1)^k |G|^k d_{i(k)} d_{i(k-1)} \dots d_{i(1)} (x_{i(k)} - 1) (x_{i(k-1)} - 1) \dots (x_{i(1)} - 1) \\ &\times (u_i - 1) \in \mathfrak{f}^{k+1}\mathfrak{r}. \end{aligned}$$

This is possible if and only if, for all $i, u_i - 1 \in \mathfrak{f}\mathfrak{r}$ i.e. $u_i \in R'$ [see Gupta and Passi (1976), section 2].

We can now compute the dimension of U_k . By Witt's formula (Magnus *et al.* 1966, p. 330), the number of elements of Type I is

$$\rho(k + 1) = \frac{1}{k + 1} \sum_{d | k+1} \mu(d) m^{(k+1)/d}$$

where
$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ 0 & \text{if } p^2 | d \text{ for some prime } p \\ (-1)^t & \text{if } d = p_1 p_2 \dots p_t, p_i\text{'s distinct primes} \end{cases}$$

is the Mobius function. On the other hand, the number of elements of Type II is clearly $m^k(t - m)$. Thus we have the following :

Lemma 5 — For $k \geq 0$, the dimension of U_k is $\rho(k + 1) + m^k(t - m)$.

3. PROOFS OF THEOREMS

Proof of Theorem A

The case $k = 0$ is Lemma 1. Let $k \geq 1$. If

$\overline{b_{k+1}(r_1^*, r_2^*, \dots, r_m^*)} \otimes 1$ is an element of Type I, then for $g = \theta(j) \in G$,

$$\begin{aligned} & (\overline{b_{k+1}(r_1^*, r_2^*, \dots, r_m^*)} \otimes 1) \cdot g \\ &= \overline{b_{k+1}(r_1^{*j}, r_2^{*j}, \dots, r_m^{*j})} \otimes 1 \\ &= \overline{b_{k+1}(r_1^*, r_2^*, \dots, r_m^*)} \otimes 1 \end{aligned}$$

since $r_i^{*j} \equiv r_i \pmod{R'}$. Further, the action of g on elements of Type II is given by

$$\begin{aligned} & (\overline{[r_j, r_{i(1)}^*, r_{i(2)}^*, \dots, r_{i(k)}^*]} \otimes 1) \cdot g \\ &= \overline{[r_j^j, r_{i(1)}^{*j}, r_{i(2)}^{*j}, \dots, r_{i(k)}^{*j}]} \otimes 1. \end{aligned}$$

It follows that for each k -tuple

$(r_{i(1)}^*, r_{i(2)}^*, \dots, r_{i(k)}^*)$, the subspace spanned by the Type II elements

$$[r_j, r_{i(1)}^*, r_{i(2)}^*, \dots, r_{i(k)}^*] \otimes 1 \quad (m + 1 \leq j \leq t)$$

is isomorphic to the right G -module W (= the subspace of U_0 spanned by the elements $(r_i R') \otimes 1$ ($m + 1 \leq j \leq t$)) under the map induced by

$$(r_i R') \otimes 1 \rightarrow \overline{[r_j, r_{i(1)}^*, r_{i(2)}^*, \dots, r_{i(k)}^*]} \otimes 1$$

(see proof of Lemma 4). Hence U_k is a direct sum of $\rho(k + 1)$ copies of the trivial G -module \mathbb{Q} and m^k copies of W . The result therefore follows from Lemma 2.

Proof of Theorem B

Since the equivalence class of a representation is determined by its character, Theorem B follows by comparing the characters of the two sides and observing that the character χ of g as a right $\mathbb{Q} G$ -module is given by

$$\chi(g) = \begin{cases} -1 & \text{if } g \neq 1 \\ |G| - 1 & \text{if } g = 1. \end{cases}$$

Proof of Theorem C

By Theorem 3.3 of Gupta and Passi (1976), the centre of $F/F(k + 1, R)$ is contained in $\overline{F(k, R)}$ and hence is equal to $\overline{F(k, R)}^0$, the fixed submodule of $\overline{F(k, R)}$. Clearly the fixed submodule U_k^0 of U_k is $\overline{F(k, R)}^0 \otimes \mathbb{Q}$. Therefore, by Theorem B,

$$\begin{aligned} \text{rank of } \overline{F(k, R)}^0 &= \text{dimension of } U_k^0 \\ &= \rho(k + 1). \end{aligned}$$

Let C^* be the subgroup of R generated by $r_1^*, r_2^*, \dots, r_m^*$. Then

$$\gamma_{k+1}(C^*) F(k + 1, R)/F(k + 1, R)$$

is a subgroup of $\overline{F(k, R)}^0$ of rank $\rho(k + 1)$ (Lemma 4). Hence

$$\overline{F(k, R)}^0 \leq \sqrt{\{\gamma_{k+1}(C^*) F(k + 1, R)\}/F(k + 1, R)}.$$

If C/R' is the centre of F/R' , then clearly $C^* \leq C$. It is easy to see that

$$\sqrt{\{\gamma_{k+1}(C) F(k + 1, R)\}/F(k + 1, R)} \leq \overline{F(k, R)}^0.$$

Hence it follows that

$$\text{centre of } F/F(k + 1, R) = \overline{F(k, R)}^0 = \sqrt{\{\gamma_{k+1}(C) F(k + 1, R)\}/F(k + 1, R)}.$$

Proof of Theorem D

Let $wF(k + 1, R)$ be in the second centre of $F/F(k + 1, R)$. Then

$$[w, x] F(k + 1, R) \in \overline{F(k, R)}^0 \quad \text{and} \quad wF(k, R) \in \overline{F(k - 1, R)}^0.$$

Therefore, for some $a \geq 1$,

$$w^a \in \gamma_k(C^*) F(k, R) \text{ and, for some } b \geq 1,$$

$$[w^a, x]^b \in \gamma_{k+1}(C^*) F(k + 1, R) \quad (\text{see the proof of Theorem C}).$$

Let $w^a = uv$, where

$$u = \prod_i b_{k,i}^{a_i} (r_1^*, r_2^*, \dots, r_m^*) \in \gamma_k(C^*)$$

and $v \in F(k, R)$. Then taking $x = r_i$

$$[w^a, r_i]^b = [uv, r_i]^b \equiv [u, r_i]^b \pmod{F(k + 1, R)}.$$

Thus

$$[u, r_i]^b \in \gamma_{k+1}(C^*) F(k + 1, R).$$

Since

$$U_k = U_k^{(1)} \oplus U_k^{(2)}$$

(see proof of Lemma 4)

$$\gamma_{k+1}(C^*) F(k + 1, R)/F(k + 1, R) \leq U_k^{(1)}$$

and

$$[u, r_i]^b F(k + 1, R) \in U_k^{(2)}$$

it follows that

$[u, r_i]^b$ and, therefore $[u, r_i]$ belongs to $F(k + 1, R)$. This implies that

$$(u - 1)(r_i - 1) - (r_i - 1)(u - 1) \in \mathfrak{f}^{k+1}\mathfrak{r}.$$

Now observe that $(r_i - 1)(u - 1) \in \mathfrak{f}^{k+1}\mathfrak{r}$ because $r_i - 1 \in \mathfrak{f}^2$ and $u - 1 \in \mathfrak{f}^{k-1}\mathfrak{r}$. Therefore, $(u - 1)(r_i - 1) \in \mathfrak{f}^{k+1}\mathfrak{r}$ and consequently $u - 1 \in \mathfrak{f}^{k+1}$. Substituting for u gives that $|G|^k \sum_i a_i(b_{k,i}(x_1, x_2, \dots, x_k) - 1) \in \mathfrak{f}^{k+1}$ which is possible only if each $a_i = 0$, i.e. $u = 1$.

Thus $w^a \in F(k, R)$ and so $w \in F(k, R)$. The fact that $wF(k + 1, R)$ is in the second centre therefore gives

$$(wF(k + 1, R)) \cdot (g - 1)(h - 1) = 0 \text{ for all } g, h \in G.$$

From this it follows that

$$wF(k + 1, R) \cdot (g - 1) = 0 \text{ for all } g \in G$$

i.e. $wF(k + 1, R)$ is in the centre of $F/F(k + 1, R)$. This completes the proof.

4. CONCLUDING REMARKS

Remark 1

It may be pointed out that in Theorem C the radical sign is essential as can be seen from the following simple example :

Consider the presentation

$$G = \langle x, y; x^2, y^2, [x, y] \rangle$$

of the Klein four-group. Let F be the free group on x, y and R the normal closure of $x^2, y^2, [x, y]$. Then R is freely generated by

$$\{r_1, r_2, r_3, r_4, r_5\}$$

where

$$r_1 = x^2, r_2 = y^2, r_3 = [x, y], r_4 = [x^2, y], r_5 = [y^2, x].$$

Let k be an integer ≥ 1 . A straightforward verification shows that if

$$u = [r_1, r_2, r_2, \dots, r_2]_{\leftarrow k \rightarrow}^2 [r_4, r_2, r_2, \dots, r_2]_{\leftarrow k \rightarrow} \prod_i w_i$$

where

$$w_i = [r_1, r_2, r_2, \dots, r_2, r_5, r_2, r_2, \dots, r_2]_{\leftarrow i-1 \rightarrow} \leftarrow k-i \rightarrow$$

then

$$u \notin \gamma_{k+1}(C) F(k+1, R)$$

whereas $u^{2^{k-1}} \equiv [r_1^2 r_4, r_2^2 r_5, r_2^2 r_5, \dots, r_2^2 r_5]_{\leftarrow l \rightarrow} \in \gamma_{k+1}(C) F(k+1, R)$.

Remark 2

The exact sequence

$$0 \rightarrow (F(k+1, R) \cap \gamma_{k+1}(R))/\gamma_{k+2}(R) \rightarrow \gamma_{k+1}(R)/\gamma_{k+2}(R) \rightarrow \gamma_{k+1}(R) F(k+1, R)/F(k+1, R) \rightarrow 0$$

and Lemma 3 imply that we have a G -module decomposition of the higher relation module

$$\gamma_{k+1}(R)/\gamma_{k+2}(R) \otimes_{\mathbb{Z}} \mathbb{Q}$$

as

$$\gamma_{k+1}(R)/\gamma_{k+2}(R) \otimes_{\mathbb{Z}} \mathbb{Q} \cong U_k \oplus (F(k+1, R) \cap \gamma_{k+1}(R))/\gamma_{k+2}(R) \otimes_{\mathbb{Z}} \mathbb{Q}$$

The results of Gupta-Laffey-Thomson (1979) indicate that the structure of

$$\gamma_{k+1}(R)/\gamma_{k+2}(R) \otimes_{\mathbb{Z}} \mathbb{Q}$$

depends on $\gcd(k+1, |G|)$; whereas the structure of U_k is independent of $\gcd(k+1, |G|)$. It would, therefore, be of interest to investigate the dependence of the structure of $(F(k+1, R) \cap \gamma_{k+1}(R))/\gamma_{k+2}(R) \otimes_{\mathbb{Z}} \mathbb{Q}$ on $\gcd(k+1, |G|)$.

Remark 3

For $R \trianglelefteq F$ the series

$$G_1 = R \geq G_2 \geq \dots \geq G_i \geq \dots,$$

where

$$G_i = R \cap (1 + \mathfrak{f}^{i-1}\mathfrak{r})$$

is an N -series in R and we have a Lie ring

$$\mathcal{L} = \sum_{i \geq 1} G_i/G_{i+1}.$$

On the other hand we have a filtration $\{A_n\}_{n \geq 0}$ of $\mathbb{Z}R$ given by

$$A_0 = \mathbb{Z}R, A_1 = \mathfrak{r} \quad \text{and} \quad A_n = \mathbb{Z}R \cap \mathfrak{f}^{n-1}\mathfrak{r} \quad \text{for} \quad n \geq 2.$$

This leads to an epimorphism

$$\theta : \mathcal{U}(\mathcal{L}) \rightarrow \sum_{n \geq 0} A_n/A_{n+1}$$

where $\mathcal{U}(\mathcal{L})$ is the universal envelope of \mathcal{L} (see Passi (1979), Chapter VIII). If $R = F$, then θ is an isomorphism. In view of this, the investigation for $\text{Ker } \theta$, in the general case, seems to be of interest.

ACKNOWLEDGEMENT

This work was completed during the visit of the first author to the Centre for Advanced Study, Panjab University, Chandigarh. He thanks the Centre for its warm hospitality.

REFERENCES

- Gaschütz, W. (1954). Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden. *Math. Z.*, **60**, 274–86.
- Gupta, N. D. (1977). Fox subgroups of free groups. *J. Pure Appl. Algebra*, **11**, 1–7.
- Gupta, N. D., Laffey, T. J., and Thomson, M. W. (1979). On the higher relation modules of a finite group. *J. Algebra*, **59**, 172–87.
- Gupta, N. D., and Passi, I. B. S. (1976). Some properties of Fox subgroups of free groups. *J. Algebra*, **43**, 198–211.
- Magnus, W., Karrass, A., and Solitar, D. (1966). *Combinatorial Group Theory*. Interscience Publs., New York.
- Passi, I. B. S. (1979). *Group Rings and Their Augmentation Ideals*. Lecture Notes in Mathematics, Vol. 715. Springer-Verlag, Berlin.