Bull. Austral. Math. Soc. 20E05
Vol. 61 (2000) [27–32]

APPLICATIONS OF FOX'S DERIVATION IN DETERMINING THE GENERATORS OF A GROUP

Wan Lin

We give a necessary and sufficient condition for a set of elements to be a generating set of a quotient group F/N, where F is the free group of rank n and N is a normal subgroup of F. Birman's Inverse Function Theorem is a corollary of our criterion. As an application of this criterion, we give necessary and sufficient conditions for a set of elements of the Burnside group $B(n,p)$ of exponent p and rank n to be a generating set.

For a group G, denote by $\mathbb{Z}G$ its integral group ring. Elements of $\mathbb{Z}G$ are of the form $\sum\limits_{g\in G} a_g g$, where $a_g \in \mathbb{Z}$ is equal to zero for all but a finite number of g. Addition and multiplication in $\mathbb{Z}G$ are defined by $\sum\limits_{g\in G} a_g g + \sum\limits_{g\in G} b_g g = \sum\limits_{g\in G}(a_g + b_g)g$ and $\Bigl(\sum\limits_{g\in G} a_g g\Bigr)\Bigl(\sum\limits_{g\in G} b_g g\Bigr) = \sum\limits_{g\in G}\Bigl(\sum\limits_{h\in G} a_{gh^{-1}} b_h\Bigr) g$. Let ε denote the augmentation homomorphism of $\mathbb{Z}G$ into itself, that is, $\left(\sum a_g g\right)^{\varepsilon} = \sum a_g$, for any element $\sum a_g g$ in $\mathbb{Z}G$. The kernel $\Delta = \operatorname{Ker}\varepsilon$ is called the augmentation ideal of $\mathbb{Z}G$ [**8**]. It is easily verified that $\Delta = \mathbb{Z}G(G-1)$. A mapping D of $\mathbb{Z}G$ into itself is called a (left) *derivation* if $D(u+v) = Du + Dv$ and $D(u\cdot v) = Du\cdot v^{\varepsilon} + u\cdot Dv$, for any u, v in $\mathbb{Z}G$. Derivation in $\mathbb{Z}G$ has the following elementary properties:

(i) $Da = 0$, for any $a \in \mathbb{Z}$;

(ii) $D(u_1\cdot u_2\cdots u_k) = \sum\limits_{i=1}^{k} u_1\cdot u_2\cdots u_{i-1}\cdot Du_i$, for any elements $u_1, u_2, \ldots, u_k \in G$, $k \geq 1$;

(iii) $D(u^{-1}) = -u^{-1}\cdot Du$, for any element $u \in G$.

Let F be the free group with basis $x_1, x_2, \ldots, x_n$. We let $\dfrac{\partial}{\partial x_j}$, $j = 1, 2, \ldots, n$, be the Fox free partial derivative with respect to x_j in $\mathbb{Z}F$ [**6, 8**], that is, $\dfrac{\partial x_i}{\partial x_j} = \delta_{ij}$, where δ_{ij} is the Kroneker delta. If $y_1, y_2, \ldots, y_n$ is a set of elements of F, let

Received 23rd March, 1999
I would like to thank my supervisor Professor C.K. Gupta for suggesting this topic to me.

$\left\|\frac{\partial y_i}{\partial x_j}\right\| = \left\|\frac{\partial(y_1, y_2, \dots, y_n)}{\partial(x_1, x_2, \dots, x_n)}\right\|$ denote the Jacobian matrix. In 1973, Birman [4] proved that y_1, $y_2, \dots, y_n$ generate F if and only if $\left\|\frac{\partial y_i}{\partial x_j}\right\|$ has a right inverse.

In the current paper, we shall establish a necessary and sufficient condition for a set of elements $\overline{y_1}$, $\overline{y_2}, \dots, \overline{y_n}$ to be a generating set for $G = F/N$, where N is a normal subgroup of F. As an application of our criterion, we give necessary and sufficient conditions for a set of elements of the Burnside group $B(n,p)$ of exponent p and rank n to be a generating set.

THEOREM 1. *Let F be the free group with basis $x_1, x_2, \dots, x_n$ and N a normal subgroup of F. Suppose y_1, $y_2, \dots, y_n$ is a set of elements of F. Then $\overline{y_1}$, $\overline{y_2}$, $\dots$, $\overline{y_n}$ is a generating set for F/N if and only if there exist an $n \times n$ matrix $A = (a_{ij})$ over $\mathbb{Z}F$, elements g_1, g_2, $\dots$, g_n in $\mathbb{Z}F$ and h_1, h_2, $\dots$, h_n in N such that*

$$(a_{ij})\left\|\frac{\partial y_i}{\partial x_j}\right\| + \operatorname{diag}(g_1, g_2, \dots, g_n)\left\|\frac{\partial h_i}{\partial x_j}\right\| = E,$$

where E is the $n \times n$ identity matrix and $\operatorname{diag}(g_1, g_2, \dots, g_n)$ is the $n \times n$ diagonal matrix with main diagonal entries $g_1, g_2, \dots, g_n$.

PROOF: If $\overline{y_1}$, $\overline{y_2}, \dots, \overline{y_n}$ is a generating set of F/N, then $\overline{x_i} = X_i(\overline{y_1}, \overline{y_2}, \dots, \overline{y_n})$ is a word in $\overline{y_1}$, $\overline{y_2}$, $\dots$, $\overline{y_n}$. Thus $x_i = W_i(y_1, y_2, \dots, y_n)h_i$, where $h_i \in N$. In $\mathbb{Z}F$, we have that

$$\delta_{ij} = \frac{\partial x_i}{\partial x_j} = \frac{\partial}{\partial x_j}\{W_i(y_1, y_2, \dots, y_n)h_i\} = \frac{\partial W_i}{\partial x_j} + W_i\frac{\partial h_i}{\partial x_j}.$$

By property (ii), we may write $\frac{\partial W_i}{\partial x_j}$ as

$$\frac{\partial W_i}{\partial x_j} = \sum_{k=1}^{n} a_{ik}\frac{\partial y_k}{\partial x_j},$$

where a_{ik}, $1 \le k \le n$, are elements in $\mathbb{Z}F$.

Let $A = (a_{ij})$ and $g_i = W_i$, $i = 1, 2, \dots, n$, then

$$(a_{ij})\left\|\frac{\partial y_i}{\partial x_j}\right\| \operatorname{diag}(g_1, g_2, \dots, g_n)\left\|\frac{\partial h_i}{\partial x_j}\right\| = E.$$

Conversely, suppose that

$$(a_{ij})\left\|\frac{\partial y_i}{\partial x_j}\right\| + \operatorname{diag}(g_1, g_2, \dots, g_n)\left\|\frac{\partial h_i}{\partial x_j}\right\| = E,$$

where $g_1, g_2, \dots, g_n \in \mathbb{Z}F$ and $h_1, h_2, \dots, h_n \in N$. Then

$$\sum_{k=1}^{n} a_{ik}\frac{\partial y_k}{\partial x_j} + g_i\frac{\partial h_i}{\partial x_j} = \delta_{ij}.$$

Multiplying both sides of the above equation by $x_j - 1$ and summing over j, we have

$$\sum_{j=1}^{n}\sum_{k=1}^{n} a_{ik}\frac{\partial y_k}{\partial x_j}(x_j - 1) + \sum_{j=1}^{n} g_i\frac{\partial h_i}{\partial x_j}(x_j - 1) = \sum_{j=1}^{n}\delta_{ij}(x_j - 1).$$

By Fox's fundamental formula [6], we have that $\sum_{j=1}^{n}\frac{\partial y_k}{\partial x_j}(x_j - 1) = y_k - 1$ and $\sum_{j=1}^{n}\frac{\partial h_i}{\partial x_j}(x_j - 1) = h_i - 1$. Thus

$$\sum_{k=1}^{n} a_{ik}(y_k - 1) + g_i(h_i - 1) = x_i - 1.$$

Hence

$$\sum_{k=1}^{n} a_{ik}(y_k - 1) = x_i - 1 \mod \mathbb{Z}F(N - 1).$$

It follows, by [5, Lemma 4.1], that $\overline{y_1}, \overline{y_2}, \dots, \overline{y_n}$ is a generating set for F/N. □

REMARK.

(i) The proof of the necessity actually gives an algorithm for finding the matrix A, elements $g_1, g_2, \dots, g_n$ and $h_1, h_2, \dots, h_n$. The elements $g_1, g_2, \dots, g_n$ are actually in the free group F.

(ii) When $N = 1$, Theorem 1 says that a set of elements $y_1, y_2, \dots, y_n$ of F is a basis for F if and only if the Jacobian matrix $\left\|\frac{\partial y_i}{\partial x_j}\right\|$ has an inverse in $\mathbb{Z}F$. Thus Birman's Inverse Function Theorem [4] is a corollary of our Theorem 1.

As an application of Theorem 1, we shall prove the following result regarding the generating set of the Burnside group $B(n,p)$ of exponent p and rank n. Let p be a prime and F^p the subgroup of F generated by the pth power of the elements of F. Then $B(n,p) = F/F^p$ is the Burnside group of exponent p and rank n. We let I_p denote the ideal of $\mathbb{Z}F$ generated by all elements of the form $1 + w + w^2 + \cdots + w^{p-1}$, $w \in F$.

Corollary 2. *Let $y_1, y_2, \ldots, y_n$ be a set of elements of F. Then we have the following:*

(i) *If $\overline{y_1}, \overline{y_2}, \ldots, \overline{y_n}$ is a generating set of $B(n,p)$, then $\overline{\left\| \frac{\partial y_i}{\partial x_j} \right\|}$ is invertible over $\mathbb{Z}F/I_p$.*

(ii) *If $\overline{\left\| \frac{\partial y_i}{\partial x_j} \right\|}$ has a left inverse over $\mathbb{Z}F/\mathbb{Z}F(F^p - 1)$, then $\overline{y_1}, \overline{y_2}, \ldots, \overline{y_n}$ is a generating set of $B(n,p)$.*

(iii) *If $\overline{\left\| \frac{\partial y_i}{\partial x_j} \right\|}$ has a left inverse over $\mathbb{Z}F/I_p$, then $\overline{y_1}, \overline{y_2}, \ldots, \overline{y_n}$ is a generating set of F/N, where N is the normal subgroup of F corresponding to I_p, that is, $I_p = \mathbb{Z}F(N-1)$.*

Proof: (i) If $\overline{y_1}, \overline{y_2}, \ldots, \overline{y_n}$ is a generating set of $B(n,p)$, then, by Theorem 1, there exist an $n \times n$ matrix $A = (a_{ij})$, elements $g_1, g_2, \ldots, g_n$ in F and elements $h_1, h_2, \ldots, h_n$ in F^p such that

$$(a_{ij}) \left\| \frac{\partial y_i}{\partial x_j} \right\| + \operatorname{diag}(g_1, g_2, \ldots, g_n) \left\| \frac{\partial h_i}{\partial x_j} \right\| = E.$$

Since $h_i \in F^p$, $1 \le i \le n$, we have that $\frac{\partial h_i}{\partial x_j} \in I_p$ for all i and j. Thus

$$(a_{ij}) \left\| \frac{\partial y_i}{\partial x_j} \right\| = E$$

over $\mathbb{Z}F/I_p$. Hence (a_{ij}) is a left inverse of $\overline{\left\| \frac{\partial y_i}{\partial x_j} \right\|}$ over $\mathbb{Z}F/I_p$. By a theorem of Montgomery [9], (a_{ij}) is also a right inverse of $\overline{\left\| \frac{\partial y_i}{\partial x_j} \right\|}$. Therefore (a_{ij}) is the inverse of $\overline{\left\| \frac{\partial y_i}{\partial x_j} \right\|}$.

(ii) Suppose that

$$(a_{ij}) \left\| \frac{\partial y_i}{\partial x_j} \right\| = E$$

over $\mathbb{Z}F/\mathbb{Z}F(F^p - 1)$. Then we can find u_{ij} in $\mathbb{Z}F(F^p - 1)$ such that

$$(a_{ij}) \left\| \frac{\partial y_i}{\partial x_j} \right\| + (u_{ij}) = E$$

over $\mathbb{Z}F$. Thus, for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n$,

$$\sum_{k=1}^{n} a_{ik} \frac{\partial y_k}{\partial x_j} + u_{ij} = \delta_{ij}.$$

Multiplying both sides of this equation by $x_j - 1$ and summing over j, we have

$$\sum_{j=1}^{n}\sum_{k=1}^{n} a_{ik}\frac{\partial y_k}{\partial x_j}(x_j - 1) + \sum_{j=1}^{n} u_{ij}(x_j - 1) = \sum_{j=1}^{n} \delta_{ij}(x_j - 1).$$

By Fox's fundamental formula, we have that

$$\sum_{k=1}^{n} a_{ik}(y_k - 1) + \sum_{j=1}^{n} u_{ij}(x_j - 1) = x_i - 1.$$

Thus

$$\sum_{k=1}^{n} a_{ik}(y_k - 1) = x_i - 1 \mod \mathbb{Z}F(F^p - 1).$$

Therefore, by [**5**, Lemma 4.1], $\overline{y_1}, \overline{y_2}, \dots, \overline{y_n}$ is a generating set for $B(n,p)$.

(iii) If

$$(a_{ij})\left\|\frac{\partial y_i}{\partial x_j}\right\| = E$$

over $\mathbb{Z}F/I_p$, then we can find u_{ij} in I_p such that

$$(a_{ij})\left\|\frac{\partial y_i}{\partial x_j}\right\| + (u_{ij}) = E$$

over $\mathbb{Z}F$. Thus, for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, n$,

$$\sum_{k=1}^{n} a_{ik}\frac{\partial y_k}{\partial x_j} + u_{ij} = \delta_{ij}.$$

Multiplying both sides of this equation by $x_j - 1$ and summing over j, we have

$$\sum_{j=1}^{n}\sum_{k=1}^{n} a_{ik}\frac{\partial y_k}{\partial x_j}(x_j - 1) + \sum_{j=1}^{n} u_{ij}(x_j - 1) = \sum_{j=1}^{n} \delta_{ij}(x_j - 1).$$

By Fox's fundamental formula, we have

$$\sum_{k=1}^{n} a_{ik}(y_k - 1) + \sum_{j=1}^{n} u_{ij}(x_j - 1) = x_i - 1.$$

Thus

$$\sum_{k=1}^{n} a_{ik}(y_k - 1) = x_i - 1 \mod I_p.$$

Let N be the normal subgroup of F such that $I_p = \mathbb{Z}F(N - 1)$, then $N \supseteq F^p$. Thus, by [**5**, Lemma 4.1], $\overline{y_1}, \overline{y_2}, \dots, \overline{y_n}$ is a generating set for F/N.

https://doi.org/10.1017/S0004972700021985 Published online by Cambridge University Press

REFERENCES

[1] S. Bachmuth, 'Automorphisms of free metabelian groups', *Trans. Amer. Math. Soc.* **118** (1965), 93–104.

[2] S. Bachmuth, 'Automorphisms of a class of metabelian groups', *Trans. Amer. Math. Soc.* **127** (1967), 284–293.

[3] S. Bachmuth and H.Y. Mochizuki, 'Automorphisms of a class of metabelian groups II', *Trans. Amer. Math. Soc.* **127** (1967), 294–301.

[4] J.S. Birman, 'An inverse function theorem for free groups', *Proc. Amer. Math. Soc.* **41** (1973), 634–638.

[5] D.E. Cohen, *Groups of cohomological dimension one*, Lecture Notes in Math. **245** (Springer-Verlag, Berlin, Heidelberg, New York, 1972).

[6] R.H. Fox, 'Free differential calculus I, Derivation in the free group ring', *Ann. of Math.* **57** (1953), 547–560.

[7] R.H. Fox, 'Free differential calculus II, The isomorphism problem of groups', *Ann. of Math.* **59** (1954), 196–210.

[8] N.D. Gupta, *Free group rings*, Contemporary Mathematics **66** (Amer. Math. Soc., Providence, RI, 1987).

[9] M.S. Montgomery, 'Left and right inverses in group algebras', *Bull. Amer. Math. Soc.* **75** (1969), 539–540.

Department of Mathematics
University of Manitoba
Winnipeg
Manitoba R3T 2N2
Canada
e-mail: umlin010@cc.umanitoba.ca