On monomorphisms of free groups

Vladimir Shpilrain

1 Introduction

Let F be the free group of a finite or countable infinite rank with a system $X = \{x_i\}$, $i \in I$, of free generators. When we consider the free group of a finite rank $n \geqslant 2$, we usually write F_n for F.

Let ϕ be an endomorphism of the group F_n given by $\phi\colon x_i \to y_i$, $1 \leqslant i \leqslant n$. Birman [3] has given a matrix characterization of automorphisms among arbitrary endomorphisms (the "inverse function theorem") as follows. Define the matrix $J_\phi = \|d_j(y_i)\|_{1\leqslant i,j\leqslant n}$ (the "Jacobian matrix" of ϕ), where d_j denotes Fox derivation in the free group ring $\mathbb{Z}F$ (see [6]). Then ϕ is an automorphism if and only if the matrix J_ϕ is invertible. This result has been later generalized by Krasnikov [8]. He has proved the following: let R be an arbitrary normal subgroup of F_n, and let $\sigma_R\colon F_n \to F_n/R$ be the natural homomorphisms; it can be linearly extended to a homomorphism of group rings $\sigma_R\colon \mathbb{Z}F_n \to \mathbb{Z}(F_n/R)$. Then elements $y_1, \ldots, y_n$ generate the group F_n modulo R' if and only if the matrix $\|\sigma_R(d_j(y_i))\|_{1\leqslant i,j\leqslant n}$ is invertible over the ring $\mathbb{Z}(F_n/R)$.

The proofs of these results amount to showing a given map to be *onto*, i.e. to be an *epimorphism*. Here we give a matrix characterization of *monomorphisms* of free groups. More generally, we give a necessary and sufficient condition (in the matrix form) for an arbitrary finite set of elements of a free group to freely generate a free subgroup. Namely, we prove the following.

Theorem 1.1. *Let $Y = \{y_1, \ldots, y_m\}$ be an arbitrary finite set of elements of a free group F_n, and $R \leqslant F_n$ — the subgroup generated by Y. Define the matrix $J_Y = \|d_j(y_i)\|_{1\leqslant j\leqslant n,\, 1\leqslant i\leqslant m}$. Then the elements $y_1, \ldots, y_m$ freely generate the group R if and only if the rows of the matrix J_Y are left independent over $\mathbb{Z}F_n$.*

Since $\mathbb{Z}F$ is a free ideal ring (fir), there is an effective procedure for detecting linear independence over $\mathbb{Z}F$ based on P. M. Cohn's "weak algorithm" — see [4, p. 101–102]. Thus our Theorem 1.1 provides an alternative to known combinatorial algorithms for detecting Nielsen irreducible systems of elements in F — see e.g. [10, Theorem 3.1].

As a by-product, we also have a simple proof of an important result of J. Lewin [9] which says that if $y_1, \ldots, y_m$ freely generate a subgroup of F, then $(y_1 - 1), \ldots, (y_m - 1)$ freely generate a left ideal of $\mathbb{Z}F$ as a free left module over this ring (Remark 3.2).

As an immediate corollary, we have what may be called "the inverse function cotheorem":

Corollary 1.2. *Let ϕ be an endomorphism of the group F_n given by $\phi\colon x_i \to y_i$, $1 \leqslant j \leqslant n$. It is a monomorphism if and only if the rows of the matrix J_ϕ are left independent over $\mathbb{Z}F_n$.*

This corollary motivates the following definition: if M is a matrix over $\mathbb{Z}F$, we define the (left) rank of M ($\operatorname{rank} M$) as the maximal number of (left) independent rows. Right rank can be defined similarly; for an arbitrary matrix over $\mathbb{Z}F$ left and right ranks may not coincide.

Our Corollary 1.2 now says that ϕ is a monomorphism of F_n if and only if $\operatorname{rank} J_\phi = \operatorname{rank} \phi(F_n) = n$ (by $\operatorname{rank} \phi(F_n)$ we mean as usual the minimal number of generators of the free group $\phi(F_n)$).

Corollary 1.3. *For an arbitrary finite set $Y \subseteq F_n$, one has rank J_Y equal to the rank of the subgroup generated by Y. In particular, if ϕ is an endomorphism of F_n, then* $\operatorname{rank} J_\phi = \operatorname{rank} \phi(F_n)$.

We note that if k is the minimal number of elements generating $\operatorname{Ker} \phi$ as a *normal* subgroup of F_n (if $\operatorname{Ker} \phi = \{1\}$, put $k = 0$), then $k + \operatorname{rank} \phi(F_n)$ — this follows from Theorem 3.3 of [10].

The "only if" and the *if* parts of Theorem 1.1 can be generalized to some other groups of the form F/R' (Theorem 3.1 and 3.3). This implies, in particular, a well-known result on subgroups of free solvable groups (Corollary 3.4) independently obtained by Baumslag [2] and Shmel'kin [12].

In the end of Section 3, we give an application of our method to the study of the Hopf property of F/R' groups.

2 Preliminaries

For all unexplained notation and proofs of technical results concerning Fox calculus, we refer to [7].

Let $\mathbb{Z}F$ be the integral group ring of the group F and Δ_F its augmentation ideal, that is, the kernel of the natural homomorphism $\sigma_F\colon \mathbb{Z}F \to \mathbb{Z}$. More generally, when $R \leqslant F$ is a normal subgroup of F, we denote by Δ_R the ideal of $\mathbb{Z}F$ generated by all elements of the form $(r-1)$, $r \in R$. It is the kernel of the natural homomorphism $\sigma_R\colon \mathbb{Z}F \to \mathbb{Z}(F/R)$.

The ideal Δ_F is a free left $\mathbb{Z}F$-module with a free basis $\{(x_i - 1)\}$, $i \in I$, and Fox derivations d_i are projections to the corresponding free cyclic direct summands. Thus any element $u \in \Delta_F$ can be uniquely written in the form $u = \sum_i d_i(u)(x_i - 1)$.

One can extend these derivations linearly to the whole $\mathbb{Z}F$ defining $d_i(1) = 0$.

The next lemma is an immediate consequence of the definitions.

Lemma 2.1. *Let J be an arbitrary right ideal of $\mathbb{Z}F$ and let $u \in \Delta_F$. Then $u \in J\Delta_F$ if and only if $d_i(u) \in J$ for each $i \in I$.*

Proof of the next lemma can be found in [6] and [7].

Lemma 2.2. *Let R be a normal subgroup of F, and let $y \in F$. Then $y - 1 \in \Delta_R \Delta_F$ if and only if $y \in R'$.*

We also need the "chain rule" for Fox derivations (see [6], [7]):

Lemma 2.3. *Let $v = v(x_1, \ldots, x_m)$ be an element of $\mathbb{Z}F$, and $y_1, \ldots, y_m$ — elements of F. Denote $u_k(x_1, \ldots, x_m) = d_k(v)$. Then:*

$$d_j(v(y_1, \ldots, y_m)) = \sum_{1 \leqslant k \leqslant m} u_k(y_1, \ldots, y_m) d_j(y_k).$$

Now comes the key technical lemma.

Lemma 2.4. *Let G be an arbitrary group, $\mathbb{Z}G$ — its integral group ring. Let H be a subgroup of G, and suppose one has $\sum_{1 \leqslant k \leqslant m} (h_k - 1)u_k = 0$ for some $h_k \in H$, $u_k \in \mathbb{Z}G$, and some of u_i is not equal to zero. Then there are $v_k \in \mathbb{Z}H$ (some of them non-zero) with $\sum_{1 \leqslant k \leqslant m} (h_k - 1)v_k = 0$.*

Proof. Before we proceed with the proof of this lemma, we have to introduce one special mapping of a group ring. Given a group ring KG of a group G over an arbitrary commutative ring K with the unit, and a subgroup H of G, we can define a mapping $\pi_H \colon KG \to KH$ as follows: if $v = \sum_{g \in G} n_g g$, $n_g \in K$, then $\pi_H(v) = \sum_{g \in H} n_g g$. This mapping has one property we are going to use (see [11] for more details): if $v \in KH$ and $w \in KG$, then $\pi_H(vw) = v\pi_H(w)$.

Now multiplying both sides of the equality

$$\sum_{1 \leqslant k \leqslant m} (h_k - 1)u_k = 0 \tag{1}$$

by an element of the group G on the right (if necessary), we can assume that at least for one u_i, we have $\pi_H(u_i) \neq 0$. Apply the mapping π_H to both sides of (1); this gives $\sum_{1 \leqslant k \leqslant m} (h_k - 1)\pi_H(u_k) = 0$, and the result follows by setting $v_k = \pi_H(u_k)$. □

Finally, we make the following trivial but useful observation:

Lemma 2.5. *Let R be an arbitrary normal subgroup of F, and $y_1, \ldots, y_m$ — arbitrary elements of F. If there exists an element $u = u(x_1, \ldots, x_m) \in \mathbb{Z}F$, $u \notin \Delta_R$, such that $u(y_1, \ldots, y_m) \in \Delta_R$, then there also exists an element $g = g(x_1, \ldots, x_m) \in F$, $g \notin R$, such that $g(y_1, \ldots, y_m) \in R$.*

We need the following notational agreement to be used in Section 3: if u is an element of $\mathbb{Z}F$, we write $u(X)$ for $u(x_1, \ldots, x_m)$ and $u(Y)$ for $u(y_1, \ldots, y_m)$ when it does not lead to any confusion.

3 Proof of main results

We begin by proving the following Theorem 3.1 which will imply the "only if" part of Theorem 1.1.

Theorem 3.1. *Let R be a fully invariant subgroup of F_n, and $Y = \{y_1, \dots, y_m\}$ — a finite system of elements of F_n. If the rows of the matrix $\sigma_R(J_Y)$ are left dependent over the ring $\mathbb{Z}(F_n/R)$, then at least one of the following possibilities occurs:*

(i) *there exists an element $g = g(x_1, \dots, x_m) \in F_n$, $g \notin R'$, such that $g(y_1, \dots, y_m) \in R'$;*

(ii) *there exists an element $h = h(x_1, \dots, x_m) \in F_n$, $h \notin R$, and an element $r \in R$, such that $[h, r] \notin R'$ but $[h(y_1, \dots, y_m), r] \in R'$.*
(When $m = n$, the second possibility is just included in the first one.)

Proof. By embedding F_n in F_N with $N > n$ if necessary, we can assume that $m \leqslant n$. This will result in adding some zero columns to the matrix $\sigma_R(J_Y)$, so it won't change left dependence of its rows.

If the rows of the matrix $\sigma_R(J_Y)$ are left dependent over the ring $\mathbb{Z}(F_n/R)$, this means that we have a congruence

$$AJ_Y \equiv 0 \pmod{\Delta_R}, \tag{2}$$

where A is a row matrix $(u_1, \dots, u_m)$ with $u_i \in \mathbb{Z}F_n$, and some of these u_i don't belong to Δ_R. Multiply now both sides of (2) on the right by the column matrix $(x_1 - 1, \dots, x_n - 1)$; this yields $\sum_{1 \leqslant k \leqslant m} u_k(y_k - 1) = 0$ in $\mathbb{Z}(F_n/R)$. Applying Lemma 2.4 gives $\sum_{1 \leqslant k \leqslant m} v_k(y_1, \dots, y_m)(y_k - 1) = 0$ in $\mathbb{Z}(F_n/R)$, and some $v_k(y_1, \dots, y_m) \neq 0$. Let now $w = w(x_1, \dots, x_m) = \sum_{1 \leqslant k \leqslant m} v_k(x_1, \dots, x_m)(x_k - 1)$. It is clear that some $v_k(x_1, \dots, x_m) \neq 0$ in $\mathbb{Z}(F_n/R)$ because R is a fully invariant subgroup of F. Hence $w \notin \Delta_R\Delta_F$. Now we have to consider 2 cases:

(1) $w \notin \Delta_R$. Since $w(y_1, \dots, y_m) \in \Delta_R$, we can apply Lemma 2.5 to find an element $h = h(x_1, \dots, x_m) \in F$, $h \notin R$, such that $h(y_1, \dots, y_m) \in R$.

If $R = \{1\}$, then $R = R'$, and we are done. If $R \neq \{1\}$, there exists an element $r \in R$ such that $[h, r] \notin R'$ — see [1]. But $[h(y_1, \dots, y_m), r] \in R'$, and the result follows.

(2) $w \in \Delta_R$. Then we can write $w \equiv \sum_i c_i(r_i - 1)h_i \pmod{\Delta_R\Delta_F}$ for some $r_i \in R$, $h_i \in F$, $c_i \in \mathbb{Z}$. It follows that $w \equiv g \equiv \prod_i r_i^{c_i h_i} \pmod{\Delta_R\Delta_F}$. We are going to show that this element g is a one we need. First of all, $g \notin R'$ since $g - 1 \equiv w \pmod{\Delta_R\Delta_F}$, and $w \notin \Delta_R\Delta_F$ as it was shown before. Hence $g - 1 \notin \Delta_R\Delta_F$, so $g \notin R'$ by Lemma 2.2. Now prove that $g(y_1, \dots, y_m) \in R'$. Applying Lemma 2.3 gives $J_{g(Y)} \equiv BJ_Y \equiv 0 \pmod{\Delta_R}$ with $B = (v_1(y_1, \dots, y_m), \dots, v_m(y_1, \dots, y_m))$, which means that $g(y_1, \dots, y_m) - 1 \in \Delta_R\Delta_F$ by Lemma 2.1, and this completes the proof. □

Proof of Theorem 1.1. (1) The "only if" part follows from Theorem 3.1 upon taking $R = \{1\}$.

(2) In order to prove the "if" part, suppose there is an element $g(x_1, \dots, x_m) \in F$, $g \neq 1$, but $g(y_1, \dots, y_m) = 1$. Take an element g of minimal length with this property. Applying Lemma 2.3 gives $D_{g(Y)} = AJ_Y = 0$, where A is the row matrix $(u_1(Y), \dots, u_m(Y))$ with $u_k(x_1, \dots, x_m) = d_k(g)$. If some $u_1(Y) \neq 0$, then the rows of the matrix J_Y appear to be left dependent, and the result follows. Suppose all $u_i(Y) = 0$. Taking into account the "combinatorial" definition of Fox derivatives (see [6], [7]), we deduce that $g_1(Y) = g_2(Y)$, where g_1 and g_2 are distinct initial segments of the word g, and at least one of them is a proper initial segment, i.e., it is not equal to g and to 1. It follows that $g_1^{-1}g_2(X) \neq 1$, but $g_1^{-1}g_2(Y) = 1$, and $g_1^{-1}g_2$ has smaller length than g. This contradiction completes the proof of Theorem 1.1. □

Remark 3.2. Our method also yields a simple proof of J. Lewin's result cited in the Introduction. Indeed, suppose that elements $y_1, \dots, y_m$ freely generate a free subgroup of F_n, but $\sum_{1 \leqslant k \leqslant m} u_k(y_k - 1) = 0$ for some $u_k \in \mathbb{Z}F_n$, at least one of them non-zero. Applying Fox derivations d_i, $1 \leqslant i \leqslant n$, to both sides of this equality, we see that the rows of the matrix J_Y are left dependent, so $y_1, \dots, y_m$ don't freely generate a free subgroup of J_Y by Theorem 1.1, hence a contradiction.

Proof of Corollary 1.3. If the subset $Y = \{y_1, \dots, y_m\}$ is Nielsen reduced, then the rank of the group $gp\langle Y\rangle$ equals m, and so is rank J_Y by Theorem 1.1. If Y is not Nielsen reduced, we can reduce it to some $\{z_1, \dots, z_k, 1, \dots, 1\}$, $k < m$, with $\{z_1, \dots, z_k\}$ Nielsen reduced, after applying a finite number of Nielsen transformations (see e.g. [10]). Every elementary Nielsen transformation is mimiced by an elementary transformation of the rows which does not change the rank of a matrix. The result follows. □

Theorem 3.3. *Let R be a normal subgroup of F_n, and $Y = \{y_1, \dots, y_m\}$ — a finite system of elements of F_n such that the rows of the matrix $\sigma_R(J_Y)$ are left independent over $\mathbb{Z}(F/R)$. If there is an element $g \in F_n$ such that $g(x_1, \dots, x_m) \notin R'$, but $g(y_1, \dots, y_m) \in R'$, then there is an element h such that $h(x_1, \dots, x_m) \notin R$, but $h(y_1, \dots, y_m) \in R$. If $m = n$, the converse is also true.*

Proof. (1) Suppose there is no element $g \in F_n$ such that $g(X) \notin R$, $g(Y) \in R$, but there is an element g such that $g(X) \notin R'$, but $g(Y) \in R'$. Applying Fox derivations d_i, $1 \leqslant i \leqslant n$, to both sides of the inclusion $g(Y) \in R'$, we get a system of inclusions which can be written in the matrix form as

$$AJ_Y \equiv 0 \pmod{\Delta_R}, \tag{3}$$

where A is a row matrix $(u_1(Y), \dots, u_m(Y))$ with $u_k(x_1, \dots, x_m) = d_k(g)$. Since $g(X) \notin R'$, we must have at least one $u_k(x_1, \dots, x_m) \notin \Delta_R$; then by the conditions of the theorem, we also have $u_k(y_1, \dots, y_m) \notin \Delta_R$. Hence (3) implies that the rows of the matrix J_Y are left dependent over $\mathbb{Z}(F/R)$, and this contradiction completes the proof in one direction.

(2) Suppose there is an element $g \in F_n$ such that $g(X) \notin R$, $g(Y) \in R$. If $R \neq \{1\}$, there is an element $r \in R$ such that $[g, r] \notin R'$ by a result of [1]. Let

$h = [g, r]$; then $h(X) \notin R'$, but $h(Y) \in R'$, and the result follows. If $R = \{1\}$, the situation is reduced to that of Theorem 1.1. □

Now we can use Theorem 3.3 to prove the following result on subgroups of free solvable groups (by $F^{(c)}$ we denote the c^{th} term of the derived series of the group F so that $F^{(0)} = F$; $F^{(1)} = F'$ etc.):

Corollary 3.4 (cf. [2], [12]). *Let $Y = \{y_1, \dots, y_m\}$, $m \geqslant 2$, be an arbitrary finite set of elements of a free group $F = F_n$, $n \geqslant 2$, and let $S_c = F/F^{(c)}$ be a free solvable group of the derived length $c \geqslant 1$. The elements $y_1F^{(c)}, \dots, y_mF^{(c)}$ freely generate a free solvable subgroup of S_c (of the same derived length) if and only if the elements $y_1, \dots, y_m$ are independent modulo F'.*

Proof. (1) We proceed by induction on c. Let $R = F^{(c-1)}$, and suppose the elements $y_1F^{(c-1)}, \dots, y_mF^{(c-1)}$ don't freely generate a free solvable subgroup of S_{c-1}, so that there is $g = g(x_1, \dots, x_m)$, $g \notin R$, but $g(y_1, \dots, y_m) \in R$. Denote by S the subgroup of F generated by $Y = y_1, \dots, y_m$. Consider the intersection of S with R; if it is contained in R', then we are done. Let now $s \in S \cap R$, $s = s(Y)$; $s \notin R'$. Take $h(X) = [g(X), s(X)]$; we may clearly assume that $g(X)$ and $s(X)$ are not in the same cyclic subgroup modulo R', so they don't commute modulo R' (see [7]), hence $h(X) \notin R'$ whereas $h(Y) \in R'$, and this completes the proof.

(2) If $y_1, \dots, y_m$ are independent modulo F', then, in particular, none of y_i belongs to F'. Hence condition "the rows of the matrix $\sigma_F(J_Y)$ are independent over $\mathbb{Z}$" implies that the rows of the matrix $\sigma_R(J_Y)$ are left independent over $\mathbb{Z}(F/R)$. The result follows after applying Theorem 3.3. □

In conclusion, we give an application of our method to the study of the Hopf property of F/R' groups. A group G is called *hopfian* if every homomorphism of G *onto* itself has trivial kernel, i.e. is actually an automorphism. First of all, we notice that our Corollary 1.2 immediately implies the hopficity of F_n: if an endomorphism ϕ is *onto*, then by Lemma 2.3 the Jacobian matrix J_ϕ is invertible, in particular its rows are left independent, hence by Corollary 1.2, ϕ is a monomorphism. Also, we have the following

Corollary 3.5 (cf. [5]). *If a group F/R is hopfian, then so is F/R'.*

Proof. Let ϕ be an *onto* endomorphism of the group F/R'. Then the matrix $\sigma_R(J_\phi)$ is invertible over $\mathbb{Z}(F/R)$ by [8]; in particular, its rows are left independent over $\mathbb{Z}(F/R)$. Applying Theorem 3.3 now yields the result. □

Acknowledgement. I am grateful to A. A. Mikhalev for useful discussions, in particular for pointing out Corollary 1.3.

References

[1] M. Auslander and R. C. Lyndon, Commutator subgroups of free groups, *Amer. J. Math.*, **77** (1955), 929–931.

[2] G. Baumslag, Some subgroups theorems for free v-groups, *Trans. Amer. Math. Soc.*, **108** (1963), 516–525.

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

[4] P. M. Cohn, *Free Rings and Their Relations*, Academic Press, London, second edition edition (1985).

[5] M. Dunwoody, The hopficity of F/R', *Bull. London Math. Soc.*, **3** (1971), 18–20.

[6] R. H. Fox, Free differential calculus. I. Derivation in the free group ring, *Ann. Math. (2)*, **57** (1953), 547–560.

[7] N. Gupta, Free group rings, *Contemp. Math.*, **66** (1987), American Math. Society, R.I.

[8] A. F. Krasnikov, Generators of the group $F/[N, N]$, *Math. Notes*, **24** (1979), 591–594.

[9] J. Lewin, Free modules over free algebras and free group algebras: the Schreier technique, *Trans. Amer. Math. Soc.*, **145** (1969), 455–465.

[10] W. Magnus, J. Karras, and D. Solitar, *Combinatorial Group Theory*, New York–London–Sydney (1966).

[11] D. S. Passman, *The algebraic structure of group rings*, John Wiley and Sons, New York (1977).

[12] A. L. Shmel'kin, Free polynilpotent groups, *Soviet Math. Dokl.*, **4** (1963), 950–953.