

ON ROOTS IN FREE GROUPS

Tekla Lewin

INTRODUCTION

Let R and S be disjoint subsets of a free group F such that $R \cup S$ is linearly independent modulo F' ; it is shown that the normal closure of R in F intersects $gp(S)$ trivially—this is the Proposition of Section 2. Since S is independent modulo F' , the subgroup generated by it is freely generated by it; thus we obtain

THEOREM 1. *Let R and S be disjoint subsets of a free group F such that $R \cup S$ is linearly independent modulo F' . In the group presented on F with defining relators R , the image of S freely generates a free group.*

This theorem is closely related to two theorems of Magnus that are concerned with presentations whose defining relators form part of a basis modulo the derived group: It generalizes his theorem which states that if a group with $n + r$ generators and r defining relators can be generated by n elements, then it is freely generated by them, and is related to his theorem which states that if G is a group with $n + r$ generators and r defining relators and G/G' is free abelian of rank n , then the generators of G may be chosen so that n of them freely generate a free group [7].

The proposition of Section 2 is applied here to the problem of finding the roots of an element in a free group. Let a and b be elements of a group G . If a is in the normal closure in G of b , then b is said to be a root of a in G , and we write $b \xrightarrow{G} a$. In 1930 [5] Wilhelm Magnus posed the problem of finding

all the roots of a given element of a free group F . For F free with a basis x, y, z, w, \dots he found all roots of x , $[x, y]$, and $x^2 y^p$ for p a prime, as well as of certain other elements. However, for example, the set of all roots of $x^k y^k$, for k not a prime, is not known. Nor is it known if the problem of finding all the roots of an arbitrary element of a free group is solvable. In view of the difficulty of finding all the roots of a given element in a free group, the following theorem of Arthur Steinberg [On equations in free groups. Michigan Math. J. 18(1971), 87-95] is very powerful; it can, for example, be combined with the results of Magnus to ascertain all the roots of $[[x, y], [z, w]]$.

THEOREM 2. *Let F be the free group with basis $x_1, \dots, x_n, y_1, \dots, y_m, \dots, z_1, \dots, z_r$. Let*

$$x = X(x_1, \dots, x_n), y = Y(y_1, \dots, y_m), \dots, z = Z(z_1, \dots, z_r)$$

be non-trivial elements, none of which is a proper power in F . Let E be the subgroup of F that has basis x, y, \dots, z . Let

Received February 10, 1978. Revision received April 10, 1979.

Michigan Math J. 27 (1980).

$$w = W(x, y, \dots, z)$$

be a non-trivial element of E . If $q \in F$ and $q \xrightarrow{F} w$, then either

- (i) $q \xrightarrow{F} u$ and $u \xrightarrow{E} w$, where u is one of the elements x, y, \dots, z , or
- (ii) q is conjugate in F to an element q' in E and $q' \xrightarrow{E} w$.

However, Roger Bryant, in a letter to the author, pointed out a gap in the proof of this theorem. (A shortening of length that is needed for an induction may not occur.) The Proposition of Section 2 fills this gap. To prove the theorem (Section 3), we then modify the construction used in Steinberg's proof. That proof was essentially correct in the case that the exponent sum on each of x, y, \dots, z in $W(x, y, \dots, z)$ is nonzero; the proposition removes this restriction.

The proof of the proposition uses, as do the proofs of the two theorems of Magnus mentioned above, the residual nilpotence of free groups. Also, it uses the embedding of a free nilpotent group in a free nilpotent \mathcal{D} -group. The question about free groups is first replaced by a question about free nilpotent groups: this can be viewed as a reduction to a question in the linear algebra of the integers. Then the question about free nilpotent groups is replaced by a question about free nilpotent \mathcal{D} -groups: this is a reduction to the much easier linear algebra of the rationals. (See A. Steinberg [8] for a similar use of free nilpotent \mathcal{D} -groups in investigating free groups; cf. also G. Baumslag [3]).

I would like to thank the referee for his helpful suggestions concerning the exposition of this paper. In particular, putting the statement and proof of the corollary of the proposition in a more general framework made it clear that I could prove more than I had stated (the proposition).

Notation. $H < G$ means H is a subgroup of the group G . If S is a subset of a group G , $gp(S)$ denotes the subgroup generated by S and $gp_G(S)$ denotes the normal closure of S in G . If T is a set, $gp\langle T \rangle$ denotes the free group with T as basis. If we write

$$G = gp\langle x_1, \dots, x_n; r_1, r_2, \dots \rangle,$$

then we mean that G is isomorphic to the factor group F/K of the free group $F = gp\langle x_1, \dots, x_n \rangle$ by $K = gp_F\langle r_1, r_2, \dots \rangle$.

Let x be an element of $F = gp\langle x_1, \dots, x_n \rangle$. Then x has an expression as a word $W(x_1, \dots, x_n)$ in the basis x_1, \dots, x_n . Corresponding to x there is a rule W which associates with an n -tuple (h_1, \dots, h_n) of elements from a group H the element $W(h_1, \dots, h_n)$ of H that is the image of x under the homomorphism of F that takes x_i into h_i for $i = 1, 2, \dots, n$. In particular, $W(x_1, \dots, x_n) = x$, so there is no conflict in the notation. In this paper we always distinguish between the element x and the associated rule W .

\mathcal{N}_c is the variety of groups that are nilpotent of class at most c .

If a and b are elements of a group, a^b denotes the element $b^{-1}ab$.

1. FREE NILPOTENT \mathcal{D} -GROUPS

We say that a group G is in the class \mathcal{D} or that G is a \mathcal{D} -group if for each $y \in G$ and natural number n there is a unique element $x \in G$ such that

$$x^n = y.$$

If for each natural number n we define the unary n th root extraction operation on the groups in \mathcal{D} , then \mathcal{D} together with these operations, the binary group operation, and the unary inverse extraction operation is a variety of algebras [1] in the sense of universal algebra. The groups free in the subvariety $\mathcal{D} \cap \mathfrak{N}_c$ have been studied by G. Baumslag [2]. We note the following: Let D be free in $\mathcal{D} \cap \mathfrak{N}_c$ with free \mathcal{D} -generating set a_1, a_2, \dots, a_k . Then the subgroup of D generated by a_1, a_2, \dots, a_k is free in the variety of groups \mathfrak{N}_c with a_1, a_2, \dots, a_k a free generating set. Also, D/D' is a vector space (written multiplicatively) over the rationals, with basis $a_1D', a_2D', \dots, a_kD'$. Further, if elements b_1, b_2, \dots, b_k in D are such that $b_1D', b_2D', \dots, b_kD'$ is a basis of D/D' , then b_1, b_2, \dots, b_k is a free \mathcal{D} -generating set of D . Thus any subset of D that is linearly independent modulo D' can be included in a free \mathcal{D} -generating set of D .

2. DEFINING RELATORS INDEPENDENT MODULO THE DERIVED GROUP

PROPOSITION. *Let F be a free group and let R and S be disjoint subsets of F such that the set $R \cup S$ is independent modulo F' . Then the normal closure of R in F intersects $gp(S)$ trivially.*

Proof. Let $w \in gp(S)$, $w \neq 1$. Then $w \notin \gamma_{c+1}(F)$ for some c [6]. Let $\bar{F} = F/\gamma_{c+1}(F)$, a group free in \mathfrak{N}_c . Embed \bar{F} in a group \bar{D} free in $\mathcal{D} \cap \mathfrak{N}_c$ so that a free generating set of \bar{F} is also a free \mathcal{D} -generating set of \bar{D} . If $a \in F$, its image in \bar{D} will be denoted by \bar{a} ; if A is a subset of F , its image will be denoted by \bar{A} . Since the set $R \cap S$ is linearly independent modulo F' , the set $\bar{R} \cup \bar{S}$ is linearly independent modulo \bar{F}' and hence also modulo \bar{D}' . Thus $\bar{R} \cup \bar{S}$ can be included in a set that freely \mathcal{D} -generates \bar{D} , say $\bar{R} \cup \bar{S} \cup X$, where \bar{R} , \bar{S} , and X are disjoint. Therefore, there is a retraction of \bar{D} onto the group free in $\mathcal{D} \cap \mathfrak{N}_c$ freely \mathcal{D} -generated by $\bar{S} \cup X$ having \bar{R} contained in its kernel. It maps the non-trivial element \bar{w} to itself.

It follows that w is not in the normal closure of R in F .

COROLLARY. *Let F be the free group with basis $x_1, \dots, x_n, y_1, \dots, y_m, \dots, z_1, \dots, z_r$, where $n \geq 2$. Let*

$$w = W(X(x_1, \dots, x_n), Y(y_1, \dots, y_m), \dots, Z(z_1, \dots, z_r)), \quad w \neq 1,$$

where $X(x_1, \dots, x_n) \notin F'$. If $X(x_1, \dots, x_n)$ has exponent sum zero on x_1 and $q \xrightarrow{F} w$, then q has exponent sum zero on x_1 .

Proof. Suppose $q \xrightarrow{F} w$, $x = X(x_1, \dots, x_n)$ has exponent sum zero on x_1 , but q has exponent sum nonzero on x_1 . Then $q, x, y_1, \dots, y_m, \dots, z_1, \dots, z_r$ is an independent set modulo F' . Therefore $gp_F(q)$ cannot contain the nontrivial element w of $gp(x, y_1, \dots, y_m, \dots, z_1, \dots, z_r)$.

3. ROOTS IN FREE GROUPS

The proof of Theorem 2 uses the techniques of the Freiheitssatz of Magnus [5], and we review certain material we will need.

Let F be a free group with basis x, y, \dots, z , and let N be the normal closure in F of $\{y, \dots, z\}$, consisting of all elements having exponent sum 0 on x . For u one of the elements y, \dots, z let $u_i = u^{x^i}$ for i an integer; the elements

$$(\#) \quad y_i, \dots, z_i, \quad i = \dots, -1, 0, 1, \dots,$$

form a basis of N . Let w be an element of N ; then it has an expression

$$(*) \quad w = R(y_{\mu(y)}, \dots, y_{M(y)}, \dots, z_{\mu(z)}, \dots, z_{M(z)})$$

as a word in this basis, where, for u one of the elements y, \dots, z , $\mu(u) = \mu(u, w)$ and $M(u) = M(u, w)$ denote respectively the least and greatest i such that u_i is involved in this expression. If u is involved in the expression for w in terms of x, y, \dots, z , then some u_i will be involved in the expression (*). The *span* on u in w is the number

$$\sigma(u, w) = M(u, w) - \mu(u, w) + 1$$

if u is involved in w and

$$\sigma(u, w) = 0$$

if u is not involved in w .

Now let $q \in N$ and suppose $q \xrightarrow{F} w$. Since $gp_F(q) = gp_N(\dots, q^{x^{-2}}, q^{x^{-1}}, q, q^x, q^{x^2}, \dots)$,

$$w \in gp_N(q^{x^j}, q^{x^{j+1}}, \dots, q^{x^{j+t}})$$

for some integers j and t , $t \geq 0$. The Hauptform of the Freiheitssatz tells us the following about choosing j and t .

THEOREM 3. (Magnus) *With the notation above, let q be an element of N cyclically reduced with respect to the basis (#) of N , and suppose $q \xrightarrow{F} w$. Then for each $u \in \{y, \dots, z\}$ the span on u in q is at most the span on u in w (w is in N , since q is in N). If u is involved in q , $t = \sigma(u, w) - \sigma(u, q)$, and $j = \mu(u, w) - \mu(u, q)$, then*

$$w \in gp_N(q^{x^j}, q^{x^{j+1}}, \dots, q^{x^{j+t}}).$$

Thus, if the span on u in w is 1, then so also is the span on u in q , provided u is involved in q ; in this case we obtain the following information about roots of w that lie in N .

COROLLARY. *With the notation above, let w be an element of N for which the expression (*) involves only a single u_i , where u is one of the elements y, \dots, z . If $q \xrightarrow{F} w$, q lies in N , and q is cyclically reduced with respect to the basis (#) of N , then either u is not involved in q or for some j*

$$q^{x^j} \xrightarrow{N} w.$$

LEMMA. (Magnus) *Let \bar{F} be the free group with basis v_1, v_2, \dots, v_r and F be the subgroup of \bar{F} with basis v_1^t, v_2, \dots, v_r for some $t \geq 1$. If $p, q \in F$, then $p \xrightarrow{\bar{F}} q$ if and only if $p \xrightarrow{F} q$.*

We are now ready to prove the theorem.

THEOREM 2. *Let F be the free group with basis $x_1, \dots, x_n, y_1, \dots, y_m, \dots, z_1, \dots, z_r$. Let*

$$x = X(x_1, \dots, x_n), y = Y(y_1, \dots, y_m), \dots, z = Z(z_1, \dots, z_r)$$

be non-trivial elements, none of which is a proper power in F . Let E be the subgroup of F that has basis x, y, \dots, z . Let $w = W(x, y, \dots, z)$ be a non-trivial element of E . If $q \in F$ and $q \xrightarrow{F} w$, then either

- (i) $q \xrightarrow{F} u$ and $u \xrightarrow{E} w$, where u is one of the elements x, y, \dots, z , or
- (ii) q is conjugate in F to an element q' in E and $q' \xrightarrow{E} w$.

Proof. We may assume that q is cyclically reduced and that w involves each letter x_1, \dots, z_r .

Suppose that q involves only one of the sets of generators, say $q \in gp(x_1, \dots, x_n)$. Then since $w \in gp_F(q) < gp_F(x_1, \dots, x_n)$,

$$W(1, Y(y_1, \dots, y_m), \dots, Z(z_1, \dots, z_r)) = 1;$$

i.e., $x \xrightarrow{E} w$.

If $K = gp_F(q)$, then

$$F/K = gp \langle x_1, \dots, x_n; q \rangle^* gp \langle y_1, \dots, z_r \rangle.$$

Since $W(xK, yK, \dots, zK) = wK = 1$ in this free product, it must be that $x^t \in K$ for some positive integer t . Hence either $x \in K$, so $q \xrightarrow{F} x$, and condition (i) is satisfied, or else x is an element of finite order in the one-relator group F/K . In the latter case the defining relator q is conjugate to a power of x [Karass, Magnus, and Solitar, 4], say x^s . Now, the image of E in the free product F/K is

$$gp(xK, yK, \dots, zK) = gp(xK)^* gp(yK, \dots, zK);$$

and we see these factors have presentations

$$gp(xK) = gp\langle x; x^s \rangle, \quad gp(yK, \dots, zK) = gp\langle y, \dots, z \rangle.$$

Thus

$$gp(xK, yK, \dots, zK) = gp\langle x, y, \dots, z; x^s \rangle.$$

Since $W(xK, yK, \dots, zK) = 1$, $x^s \xrightarrow{E} w$, and condition (ii) is satisfied.

From here on the number of sets of generators is fixed and by the foregoing may be taken to be at least two, and the proof proceeds by induction on the sum of the lengths of $X(x_1, \dots, x_n)$, $Y(y_1, \dots, y_m)$, ..., $Z(z_1, \dots, z_r)$. The initial case occurs when each of these lengths is 1, which happens if and only if $n = m = \dots = r = 1$, and then $F = E$, so condition (ii) is satisfied. We now assume that one of these lengths, say the length of $X(x_1, \dots, x_n)$, is greater than 1. Since x is not a proper power, this implies that $n \geq 2$. We also assume that q involves at least two sets of generators, so it involves a generator different from all of x_1, \dots, x_n , say it involves y_1 .

We now will embed F in a free group \bar{F} freely generated by $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n, y_1, y_2, \dots, z_r$ in such a way that both x and q have exponent sum 0 on \bar{x}_1 , and hence lie in the normal closure N of $\bar{x}_2, \dots, \bar{x}_n, y_1, y_2, \dots, z_r$. We will treat separately the cases a) $x \notin F'$ and b) $x \in F'$.

a) Suppose $x \notin F'$. If for some x_j the exponent sum in x on x_j is 0, then let $\bar{x}_1 = x_j$ and let $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$ be a reordering of x_1, x_2, \dots, x_n . In this case $\bar{F} = F$.

If the exponent sum in x is nonzero on each of x_1, x_2, \dots, x_n , then let s be the exponent sum in x on x_1 and t be the exponent sum in x on x_2 . Embed F in a free group \bar{F} with basis $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n, y_1, \dots, z_r$ by setting $\bar{x}_1^t = x_1$. Then \bar{F} also has a basis $\bar{x}_1, \bar{x}_2 = x_2 \bar{x}_1^s, \bar{x}_3 = x_3, \dots, \bar{x}_n = x_n, y_1, \dots, z_r$. With respect to this basis $x = X(\bar{x}_1^t, \bar{x}_2 \bar{x}_1^{-s}, \bar{x}_3, \dots, \bar{x}_n)$ has exponent sum 0 on \bar{x}_1 . Since x has exponent sum $t \neq 0$ on \bar{x}_2 , $x \notin \bar{F}'$.

The corollary to the Proposition of Section 2 applies in each of these subcases of a) and assures that q also has exponent sum 0 on \bar{x}_1 .

b) Suppose $x \in F'$. Applying the procedure above to q instead of to x , we arrange that q has exponent sum 0 on \bar{x}_1 , relative to the basis $\bar{x}_1, \dots, \bar{x}_n, y_1, \dots, z_r$ of \bar{F} . Since $x \in F' < \bar{F}'$, x also has exponent sum 0 on \bar{x}_1 .

This completes the embedding of F in \bar{F} ; observe that in all cases F is related to \bar{F} as in the Lemma of this section (with respect to some pair of bases). Moreover, as desired, both x and q lie in

$$N = \text{gp}_{\bar{F}}(\bar{x}_2, \dots, \bar{x}_n, y_1, \dots, z_{\ell}).$$

N has a basis consisting of the elements

$$(\#) \quad \bar{x}_2^{\bar{x}_1^i}, \dots, \bar{x}_n^{\bar{x}_1^i}, y_1^{\bar{x}_1^i}, \dots, z_{\ell}^{\bar{x}_1^i}, \quad i = \dots, -1, 0, 1, \dots$$

Now, x has shorter length relative to the basis (#) of N than relative to the original basis x_1, \dots, z_{ℓ} of F . (If \bar{x}_1 was chosen to be x_j , then the length is shorter by the number of occurrences of x_j in $X(x_1, \dots, x_n)$; otherwise, it is shorter by the number of occurrences of x_1 in $X(x_1, \dots, x_n)$; by assumption each x_i is involved in $W(X(x_1, \dots, x_n), \dots, Z(z_1, \dots, z_{\ell}))$, so this number is not 0.) Let the expression for x as a word in the basis (#) for N be

$$x = S(\bar{x}_2^{\bar{x}_1^{\mu_2}}, \dots, \bar{x}_2^{\bar{x}_1^{M_2}}, \dots, \bar{x}_n^{\bar{x}_1^{\mu_n}}, \dots, \bar{x}_n^{\bar{x}_1^{M_n}}).$$

Then the expression for w as a word in the basis (#) for N is

$$w = W(S(\bar{x}_2^{\bar{x}_1^{\mu_2}}, \dots, \bar{x}_n^{\bar{x}_1^{M_n}}), Y(y_1, \dots, y_m), \dots, Z(z_1, \dots, z_{\ell})).$$

The only generator $y_1^{\bar{x}_1^i}$ occurring in this expression is for $i = 0$. It is not difficult to check that since q is cyclically reduced with respect to the basis x_1, \dots, z_{ℓ} of F , it is also cyclically reduced with respect to the basis (#) of N . Also $q \xrightarrow{\bar{F}} w$, q lies in N , and y_1 is involved in q . So by the corollary to Theorem 3, for some j

$$q^{\bar{x}_1^j} \xrightarrow{N} w.$$

It is not difficult to see that x, y, \dots, z are not proper powers in \bar{F} , and so they are a fortiori not proper in N . Thus $q^{\bar{x}_1^j}$ and w satisfy the hypotheses of the theorem with respect to the free group N and its basis (#), with the subgroup E unchanged. (That this basis is infinite causes no trouble—we could restrict our attention to the group generated by the subset involved in w .) Furthermore, the sum of the lengths of x, y, \dots, z with respect to this basis of N is less than the sum of their lengths with respect to the basis x_1, \dots, z_{ℓ} of F . Therefore, by induction, either (i) $q^{\bar{x}_1^j} \xrightarrow{N} u$ and $u \xrightarrow{E} w$, where u is one of the elements x, y, \dots, z , or (ii) $q^{\bar{x}_1^j}$ is conjugate in N to an element q' in E and $q' \xrightarrow{E} w$. If (i) obtains, then $q \xrightarrow{\bar{F}} u$ and $u \xrightarrow{E} w$, and so by the Lemma of this section $q \xrightarrow{\bar{F}} u$ and $u \xrightarrow{E} w$. If (ii) obtains, then q is conjugate in \bar{F} to q' and so by the same lemma, we

have $q \xrightarrow{F} q'$ and $q' \xrightarrow{F} q$; therefore q' is conjugate in F to q [5, Section 6], and $q' \xrightarrow{E} w$.

REFERENCES

1. G. Baumslag, *Some aspects of groups with unique roots*. Acta Math. 104 (1960), 217-303.
2. ———, *Some remarks on nilpotent groups with roots*. Proc. Amer. Math. Soc. 12 (1961), 262-267.
3. ———, *Residual nilpotence and relations in free groups*. J. Algebra 2 (1965), 271-282.
4. A. Karrass, W. Magnus, and D. Solitar, *Elements of finite order in groups with a single defining relation*. Comm. Pure Appl. Math. 13 (1960), 57-66.
5. W. Magnus, *Über diskontinuierliche Gruppen mit einer definierenden Relation. (Der Freiheitssatz)*. J. Reine Angew. Math. 163 (1930), 141-165.
6. ———, *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring*. Math. Ann. 111 (1935), 259-280.
7. ———, *Über freie Faktorgruppen und freie Untergruppen gegebener Gruppen*. Mh. Math. Physik. 47 (1939), 307-313.
8. A. Steinberg, *On free nilpotent quotient groups*. Math. Z. 85 (1964), 185-196.
9. ———, *On equations in free groups*. Michigan Math. J. 18 (1971), 87-95.

Department of Mathematics
Syracuse University
Syracuse, New York 13210