EQUATIONS IN FREE METABELIAN GROUPS

Gilbert Baumslag and Kurt Mahler

from the

MICHIGAN MATHEMATICAL JOURNAL

vol. 12 (1965)
pp. 417-420

EQUATIONS IN FREE METABELIAN GROUPS

Gilbert Baumslag and Kurt Mahler

Introduction. Equations in free groups have recently attracted considerable attention (see, for example, R. C. Lyndon and M. P. Schützenberger [3], G. Baumslag [1]). Free metabelian groups share many properties with free groups, and we now prove an analogue of a theorem about equations in free groups.

THEOREM. *If* a *and* b *are elements of a free metabelian group that are linearly independent modulo the derived group, and if* n *is any integer greater than* 1, *then* $a^n b^n$ *is not an* n*-th power.*

This theorem leaves unanswered a host of related questions. For example, if ℓ, m, and n are integers greater than 1, can $a^\ell b^m$ be an n-th power? This certainly seems unlikely. Of course, a and b must be linearly independent modulo the derived group; for if u and v are elements of a metabelian group and v lies in the derived group, then

$$(u^{-1})^2 (uv^2)^2 = (u^{-1} vu \cdot v)^2 .$$

We effect the proof of our theorem by first reducing it in a standard way to a problem in the group ring over the integers of a free abelian group (see G. Baumslag, Bernhard H. Neumann, Hanna Neumann, and Peter M. Neumann [2]) and then solving this problem with the help of elementary algebraic number theory.

The reduction to the group ring. Suppose that a and b are elements of a free metabelian group M and that they are linearly independent modulo M', the derived group of M. By a theorem of Nielsen [4] it follows that we can find an automorphism θ of M and a free set of generators x, y, z, $\cdots$ such that

$$a\theta \equiv x^\alpha \ (M'), \quad b\theta \equiv y^\beta \ (M') \qquad (\alpha > 0,\ \beta > 0).$$

We may therefore assume

$$a \equiv x^\alpha \ (M'), \quad b \equiv y^\beta \ (M') \qquad (\alpha > 0,\ \beta > 0). \tag{1}$$

The homomorphism η of M into M defined by

$$x\eta = x, \quad y\eta = y, \quad z\eta = 1, \quad \cdots$$

maps M into a free metabelian group of rank 2 in which $a\eta$ and $b\eta$ are themselves linearly independent modulo the derived group. Thus it suffices to settle the theorem for a free metabelian group M of rank 2 on x and y with a and b given by (1).

As usual, we put

Received March 23, 1965.

This paper was written at the Institute for Advanced Studies in Canberra. The first author gratefully acknowledges a grant from the National Science Foundation and the hospitality of the Australian National University.

$$(u^{n_1})^{v_1}(u^{n_2})^{v_2}\cdots(u^{n_m})^{v_m} = u^{n_1v_1+n_2v_2+\cdots+n_mv_m},$$

where $u, v_1, \cdots, v_m$ are elements of M and $n_1, \cdots, n_m$ are integers.

Now let $k = x^{-1}y^{-1}xy$. It is well-known that then every element of M' can be uniquely represented in the form $k^{F(x,y)}$, where $F(x, y)$ is an element of the group ring R of the free abelian group M/M'. Thus $F(x, y)$ is a finite Laurent series of the form $\sum \gamma_{i,j}x^iy^j$, where $\gamma_{i,j}$, i, and j are integers. It follows that every element of M can be written uniquely in the form $x^\lambda y^\mu k^F$, where λ and μ are integers and F is in R.

Assume now that $a^nb^n = c^n$, where a and b are given by (1); we may clearly assume n is a prime. Thus $c \equiv x^\alpha y^\beta$ (M'). Therefore we have the relations

$$a = x^\alpha k^A, \quad b = y^\beta k^B, \quad c = x^\alpha y^\beta k^C \qquad (A, B, C \in R).$$

If we abbreviate $z^{t-1}+z^{t-2}+\cdots+1$ to $\frac{z^t-1}{z-1}$, then it is easy to show that

$$a^n = x^{\alpha n}k^{A\left(\frac{x^{\alpha n}-1}{x^\alpha - 1}\right)};$$

similarly for b^n and c^n. Thus $a^nb^n = c^n$ takes the form

$$x^{\alpha n}y^{\beta n}k^{A\left(\frac{x^{\alpha n}-1}{x^\alpha-1}\right)y^{\beta n}+B\frac{y^{\beta n}-1}{y^\beta-1}} = (x^\alpha y^\beta)^n k^{C\frac{(x^\alpha y^\beta)^n-1}{x^\alpha y^\beta-1}}. \tag{2}$$

Moreover, if u and v are elements of a metabelian group, then

$$(uv)^n = u^nv^n[v, u]^{\sum_{i=1}^{n-1} v^iu^{i-1}\frac{v^{n-i}}{v-1}}.$$

Now

$$[y^\beta, x^\alpha] = [x^\alpha, y^\beta]^{-1} = k^{-\frac{x^\alpha-1}{x-1}\frac{y^\beta-1}{y-1}}.$$

Therefore it follows that

$$(x^\alpha y^\beta)^n = x^{\alpha n}y^{\beta n}k^D,$$

where

$$D = -\left(\frac{x^\alpha - 1}{x-1}\right)\left(\frac{y^\beta-1}{y-1}\right)\sum_{i=1}^{n-1} y^{\beta i}x^{\alpha(i-1)}\frac{y^{\beta(n-i)}-1}{y^\beta-1}. \tag{3}$$

We see then from (2) that in the group ring R we have the relation

$$\begin{aligned} &A(1+x^\alpha+\cdots+x^{\alpha(n-1)})y^{\beta n} + B(1+y^\beta+\cdots+y^{\beta(n-1)}) \\ &\qquad = D + C(1+x^\alpha y^\beta+\cdots+(x^\alpha y^\beta)^{n-1}). \end{aligned} \tag{4}$$

The analysis of (4). Let $A_1(x^\alpha, y^\beta)$ be the sum of all terms $\alpha_{i,j}\, x^i y^j$ in A in which i and j are multiples of α and β, respectively, and define B_1, C_1, D_1 similarly. If we now put $X = x^\alpha$, $Y = y^\beta$, then it follows from (3) and (4) that

$$(5)\quad \begin{aligned} &A_1(X, Y)(1 + X + \cdots + X^{n-1})Y^n + B_1(X, Y)(1 + Y + \cdots + Y^{n-1}) \\ &\qquad = D_1(X, Y) + C_1(X, Y)(1 + XY + \cdots + (XY)^{n-1}). \end{aligned}$$

Now, by (3),

$$(6)\quad D_1(X, Y) = -\sum_{i=1}^{n-1} Y^i X^{i-1}\left(\frac{Y^{n-i} - 1}{Y - 1}\right).$$

Put $X = z^{-1}$, $Y = z$ in (5), where z is a primitive n-th root of unity. Then (5) reduces to

$$0 = D_1(z^{-1}, z) + nC_1(z^{-1}, z).$$

Clearly, $d = D_1(z^{-1}, z)$ and $e = C_1(z^{-1}, z)$ are algebraic integers. However, by (6), we find that

$$d = -\sum_{i=1}^{n-1} z\left(\frac{z^{n-i} - 1}{z - 1}\right) = \frac{z[(z^{n-1} - 1) + \cdots + (z - 1) + (1 - 1)]}{z - 1}$$

$$= -\frac{z[(z^{n-1} + \cdots + z + 1) - n]}{z - 1} = \frac{nz}{z - 1}.$$

This means that $-e = \frac{z}{z - 1} = 1 + \frac{1}{z - 1}$. Hence

$$\frac{1}{z - 1} = -e - 1$$

is an algebraic integer. But z, and therefore also $w = z - 1$, is an algebraic integer of degree $n - 1$. However, $(w + 1)^n - 1 = 0$. Since $n > 1$, $w^n + nw^{n-1} + \cdots + nw = 0$, and so also

$$w^{n-1} + nw^{n-2} + \cdots + n = 0.$$

This polynomial in w is therefore irreducible. Thus we find that w^{-1} is a root of an irreducible polynomial of the form

$$f = n\xi^{n-1} + \cdots + n\xi + 1.$$

Therefore w^{-1} is *not* an integer. This contradiction completes the proof of the theorem.

Added in proof. R. C. Lyndon has recently shown that for any three relatively prime integers ℓ, m, and n ($\ell > 1$, $m > 1$, $n > 1$) and every free metabelian group M of rank at least 2, there exist elements a, b, c, with a and b independent modulo M', such that

$$a^{\ell} b^{m} = c^{n}.$$

REFERENCES

1. G. Baumslag, *Residual nilpotence and relations in free groups*, J. Algebra (to appear).

2. G. Baumslag, Bernhard H. Neumann, Hanna Neumann, and Peter M. Neumann, *On varieties generated by a finitely generated group*, Math. Z. 86 (1964), 93-122.

3. R. C. Lyndon and M. P. Schützenberger, *The equation* $a^M = b^N c^P$ *in a free group*, Michigan Math. J. 9 (1962), 289-298.

4. J. Nielsen, *Om regning med ikke-kommutative faktorer og dens anvendelse i gruppeteorien*, Mat. Tidsskr. B, (1921), 77-94.

The Graduate Center,
City University of New York

Research School of Physical Sciences,
The Australian National University