PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 40, Number 2, October 1973

ON PRODUCTS OF POWERS IN GROUPS

ROGER LYNDON,[1] THOMAS McDONOUGH AND MORRIS NEWMAN

ABSTRACT. In this note we show that a product of Nth powers in a group cannot in general be expressed as a product of fewer Nth powers. This extends a result of Lyndon and Newman [1].

THEOREM. *Let F be a free group of rank n with basis $x_1, \cdots, x_n$, let $u_1, \cdots, u_m$ be elements of F, and let N be an integer greater than* 1. *If*

$$(*) \qquad x_1^N \cdots x_n^N = u_1^N \cdots u_m^N,$$

then $m \geqq n$.

For the proof it will suffice to exhibit a group G and elements $x_1, \cdots, x_n$ in G such that, if $u_1, \cdots, u_m$ are any elements of G satisfying $(*)$, then $m \geqq n$.

Choose a prime p dividing N and write $N=qM$, where $q=p^e$ for some $e \geqq 1$ and p does not divide M. Let P be the ring of polynomials over $GF(p)$ in noncommuting indeterminates $X_1, \cdots, X_n$. Let $\mathscr{J}$ be the ideal in P generated by $X_1, \cdots, X_n$, and let $R=P/\mathscr{J}^{q+1}$; we shall write X_i also for the image of X_i in R. Let G be the group of units in R. (Thus G is a finite group of exponent pq.) The elements $x_i=1+X_i$ belong to G, since they have inverses $x_i^{-1}=1-X_i+X_i^2-\cdots+(-1)^q X_i^q$.

Now $x_i^q=(1+X_i)^q=1+X_i^q$, whence $x_i^N=x_i^{qM}=(1+X_i^q)^M=1+Mx_i^q$. It follows that

$$(1) \qquad x_1^N \cdots x_n^N = 1 + M \sum_{i=1}^{n} x_i^q.$$

Let $u_1, \cdots, u_m$ be in G. We may write $u_j=1+\sum_i \alpha_{ji}x_i+D_j$ where D_j is in $\mathscr{J}^2$. Then

$$\begin{aligned} u_j^q &= (1 + \sum \alpha_{ji}X_i + D_j)^q = 1 + (\sum \alpha_{ji}X_i + D_j)^q \\ &= 1 + (\sum \alpha_{ji}X_i)^q = 1 + \sum \alpha_{ji_1} \cdots \alpha_{ji_q} X_{i_1} \cdots X_{i_q}, \end{aligned}$$

Received by the editors January 15, 1973.

AMS (MOS) subject classifications (1970). Primary 20F10, 20E05.

[1] The author wishes to acknowledge the support of the National Science Foundation, and also the hospitality of the University of Birmingham.

summed over all $i_1, \cdots, i_q$ such that $1 \leqq i_1, \cdots, i_q \leqq n$. Therefore $u_j^{qM} = 1 + M \sum \alpha_{ji_1} \cdots \alpha_{ji_q} X_{i_1} \cdots X_{i_q}$. It follows that

$$(2) \qquad u_1^N \cdots u_m^N = 1 + M \sum_{i_1, \cdots, i_n} \sum_{j=1}^{m} \alpha_{ji_1} \cdots \alpha_{ji_q} X_{i_1} \cdots X_{i_q}.$$

Assume that (*) holds. Equating the coefficients of X_i^q for each i in (1) and (2) gives

$$(3) \qquad M = M \sum_{j=1}^{m} \alpha_{ji}^q \qquad (1 \leqq i \leqq n).$$

Equating the coefficients of $X_i^{q-1} X_h$ for $i \neq h$ gives

$$(4) \qquad 0 = M \sum_{j=1}^{m} \alpha_{ji}^{q-1} \alpha_{jh} \qquad (1 \leqq i, h \leqq n; i \neq h).$$

Since p does not divide M, we may divide (3) and (4) through by M, obtaining

$$(3') \qquad \sum_j \alpha_{ji}^q = 1 \qquad (1 \leqq i \leqq n),$$

$$(4') \qquad \sum_j \alpha_{ji}^{q-1} \alpha_{jh} = 0 \qquad (1 \leqq i, h \leqq n; i \neq h).$$

Let $A = (\alpha_{ji}^{q-1})$ and $B = (\alpha_{ji})$, m-by-n matrices over $GF(p)$. Then (3′) and (4′) assert that

$$(5) \qquad A^T B = I_n$$

where A^T is the transpose of A and I_n is the n-by-n identity matrix. It follows that $n = \operatorname{rank}(I_n) \leqq \operatorname{rank}(B) \leqq m$.

Reference

1. Roger C. Lyndon and Morris Newman, *Commutators as products of squares*, Proc. Amer. Math. Soc. **39** (1973), 267–272.

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48104 (Current address of Roger Lyndon)

Département de Mathematiques, Université de Montpellier, 34 Montpellier, France

Department of Mathematics, University College of Wales, Aberystwyth, Cardiganshire, Wales (Current address of Thomas McDonough)

National Bureau of Standards, Washington, D.C. 20234 (Current address of Morris Newman)