ON PRODUCTS OF POWERS IN GROUPS

ROGER LYNDON, 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

\[ x_1^N \cdots x_n^N = u_1^N \cdots u_m^N, \]

then $m \geq n$.

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 $m \geq n$.

Choose a prime $p$ dividing $N$ and write $N = qM$, where $q = p^e$ for some $e \geq 1$ 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 $\mathcal{I}$ be the ideal in $P$ generated by $X_1, \cdots, X_n$, and let $R = P[\mathcal{I}^{q+1}]$; 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 $x_i^{-1} = 1 - X_i + X_i^2 - \cdots + (-1)^qX_i^q$.

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

\[ x_1^N \cdots x_n^N = 1 + M \sum_{i=1}^nx_i^q. \]

Let $u_1, \cdots, u_m$ be in $G$. We may write $u_j = 1 + \sum \alpha_{ji}X_i + D_j$ where $D_j$ is in $\mathcal{I}^2$. Then

\[ u_j^q = (1 + \sum \alpha_{ji}X_i + D_j)^q = 1 + (\sum \alpha_{ji}X_i + D_j)^q = 1 + (\sum \alpha_{ji}X_i)^q = 1 + \sum \alpha_{ji}X_i \cdots \alpha_{ji}X_i \cdots X_i, \]

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 \( i_1, \ldots, i_q \) such that \( 1 \leq i_1, \ldots, i_q \leq n \). Therefore
\[
 u_j^M = 1 + M \sum_{i_1, \ldots, i_n} \sum_{j=1}^{m} \alpha_{j i_1} \cdots \alpha_{j i_q} X_{i_1} \cdots X_{i_q}.
\]
It follows that
\[
 u_1^N \cdots u_m^N = 1 + M \sum_{i_1, \ldots, i_n} \sum_{j=1}^{m} \alpha_{j i_1} \cdots \alpha_{j i_q} X_{i_1} \cdots X_{i_q}.
\]

Assume that (*) holds. Equating the coefficients of \( X_i^q \) for each \( i \) in (1) and (2) gives
\[
 M = M \sum_{j=1}^{m} \alpha_{j i_1}^q \quad (1 \leq i \leq n).
\]
Equating the coefficients of \( X_i^{q-1}X_h \) for \( i \neq h \) gives
\[
 0 = M \sum_{j=1}^{m} \alpha_{j i_1}^{q-1} \alpha_{j h} \quad (1 \leq i, h \leq n; i \neq h).
\]
Since \( p \) does not divide \( M \), we may divide (3) and (4) through by \( M \), obtaining
\[
 \sum_{j=1}^{m} \alpha_{j i_1}^q = 1 \quad (1 \leq i \leq n),
\]
\[
 \sum_{j=1}^{m} \alpha_{j i_1}^{q-1} \alpha_{j h} = 0 \quad (1 \leq i, h \leq n; i \neq h).
\]
Let \( A = (\alpha_{j i_1}^q) \) and \( B = (\alpha_{j i_1}) \), \( m \)-by-\( n \) matrices over \( GF(p) \). Then (3') and (4') assert that
\[
 A^T B = I_n
\]
where \( A^T \) is the transpose of \( A \) and \( I_n \) is the \( n \)-by-\( n \) identity matrix. It follows that \( n = \text{rank}(I_n) \leq \text{rank}(B) \leq m \).

**REFERENCE**