PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 39, Number 2, July 1973

COMMUTATORS AS PRODUCTS OF SQUARES

ROGER C. LYNDON[1] AND MORRIS NEWMAN

ABSTRACT. It is shown that if G is the free group of rank 2 freely generated by x and y, then $xyx^{-1}y^{-1}$ is never the product of two squares in G, although it is always the product of three squares in G. It is also shown that if G is the free group of rank n freely generated by $x_1, x_2, \cdots, x_n$, then $x_1^2x_2^2 \cdots x_n^2$ is never the product of fewer than n squares in G.

Let G be a group, G' its commutator subgroup, and G^2 the fully invariant subgroup generated by the squares of the elements of G. It is well known that $G^2 \supset G'$; indeed, if x, y are any element of G, then

$$[x, y] = xyx^{-1}y^{-1} = (xy)^2(y^{-1}x^{-1}y)^2(y^{-1})^2,$$

so that $[x, y]$ is the product of three squares in G. The question naturally arises as to whether this number is minimal. That is, we ask if the equation

$$[x, y] = xyx^{-1}y^{-1} = a^2b^2 \tag{1}$$

has solutions in G. In many cases the answer is in the affirmative; for example, if either x or y is of odd order or of order 2. In general, however, the answer is in the negative, and the purpose of this note is to prove the following:

THEOREM 1. *Let $G=\{x, y\}$ be the free group of rank 2 freely generated by x and y. Then the equation* (1) *has no solutions in G.*

Two proofs of this theorem will be given. The first (which is due to the second author) will be by representing G as a suitable transformation group and then showing the impossibility by matrix arguments. The second (which is due to the first author, who acted as referee for the original version of the paper) is both simpler and provides a proof of a related result, and will be by considering suitable homomorphic images of free groups of finite rank. No doubt a proof by a word argument alone is possible (in this connection see [3]) but seems difficult.

Received by the editors June 9, 1972 and, in revised form, June 30, 1972.
AMS (MOS) subject classifications (1970). Primary 20F05, 20F10, 20H05.
[1] The first author wants to acknowledge support from the National Science Foundation.

The result referred to above is the following:

THEOREM 2. *Let G be the free group of rank n freely generated by $x_1, x_2, \cdots, x_n$. Then $x_1^2 x_2^2 \cdots x_n^2$ is never the product of fewer than n squares in G.*

For the first proof of Theorem 1 we start with the classical modular group

$$\Gamma = \mathrm{PSL}(2, Z) = \mathrm{SL}(2, Z)/\{\pm I\}.$$

The elements of Γ will be written as matrices instead of cosets. We shall be careful to make plain when elements of $\mathrm{SL}(2, Z)$ are being discussed and when elements of Γ are being discussed.

The group Γ is generated by

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and is the free product of the cyclic group $\{T\}$ of order 2 and the cyclic group $\{ST\}$ of order 3. The commutator subgroup Γ' of Γ is a free group of rank 2 and index 6, and is freely generated by

$$X = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \qquad Y = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}.$$

Then (as a matrix product)

$$[X, Y] = XYX^{-1}Y^{-1} = \begin{pmatrix} -1 & -6 \\ 0 & -1 \end{pmatrix} = -S^6.$$

The exponent of S modulo Γ' is 6. An easy consequence of the Kurosh subgroup theorem (or of simple matrix calculation) is that two commuting elements of Γ are necessarily powers of the same element of Γ (see [1] and [2]).

We first state and prove two lemmas.

LEMMA 1. *All solutions of the equation*

$$A^2B^2 = -S^6 \tag{2}$$

in $\mathrm{SL}(2, Z)$ *are given by* $A = S^3M^{-1}$, $B = MS^{-3}N$, *where* M, N *are any elements of* $\mathrm{SL}(2, Z)$ *such that* $MN = NM$, $(NS^{-3})^2 = -I$.

LEMMA 2. *Let* V *belong to* $\mathrm{SL}(2, Z)$, $V^2 = -I$. *Then neither of the congruences* $W^2 \equiv \pm V \bmod 3$ *has a solution* W *in* $\mathrm{SL}(2, Z)$.

In fact, although this is not relevant to the proof of the theorem, the congruence

$$W^2 \equiv V \bmod p, \qquad p \text{ prime}, p \text{ odd},$$

has a solution W in SL(2, Z) if and only if $(2/p)=1$, where $(2/p)=(-1)^{(p^2-1)/8}$ is the Legendre symbol.

PROOF OF LEMMA 1. We have

$$A^2B^2 - I = -S^6 - I = -2S^3.$$

Multiplying on the left by A^{-1} and on the right by B^{-1} we have

$$AB - (BA)^{-1} = -2A^{-1}S^3B^{-1}.$$

Since $\operatorname{tr}(AB)=\operatorname{tr}(BA)^{-1}$, this implies that $\operatorname{tr}(A^{-1}S^3B^{-1})=0$. But $A^{-1}S^3B^{-1}$ belongs to SL(2, Z). Thus $(A^{-1}S^3B^{-1})^2=-I$, which we rewrite as

$$(ABS^{-3})^2 = -I, \tag{3}$$

as well as

$$-S^3B^{-1} = ABS^{-3}A. \tag{4}$$

Rewriting (2) as

$$AB = A^{-1}S^3(-S^3B^{-1}), \tag{5}$$

we find on substitution of (4) into (5) that $AB=(A^{-1}S^3)(AB)(S^{-3}A)$, so that AB commutes with $A^{-1}S^2$. Put $A^{-1}S^3=M$, $AB=N$. Then $A=S^3M^{-1}$, $B=MS^{-3}N$, where $MN=NM$. Furthermore, $ABS^{-3}=NS^{-3}$, so that $(NS^{-3})^2=-I$, by (3). Thus

$$NS^{-3}N = -S^3. \tag{6}$$

But now

$$\begin{aligned} A^2B^2 &= S^3M^{-1}S^3M^{-1}MS^{-3}NMS^{-3}N \\ &= S^3NS^{-3}N = S^3(-S^3) = -S^6, \end{aligned}$$

by (6). Hence all solutions are of the form indicated by Lemma 1, and the proof is complete.

PROOF OF LEMMA 2. Since $V^2=-I$, $\operatorname{tr}(V)=\operatorname{tr}(-V)=0$. Also, the trace of W^2 is t^2-2, where t is the trace of W. Hence $t^2-2\equiv 0 \bmod 3$, an impossibility. This concludes the proof.

We now turn to the proof of the theorem. For this purpose it is only necessary to show that equation (2), considered as an equation over Γ', has no solutions in Γ'. Suppose the contrary. Then $A\in\Gamma'$, $B\in\Gamma'$, so that $N=AB\in\Gamma'$, $MS^{-3}=A^{-1}\in\Gamma'$. Since M and N commute, we must have $M=U^a$, $N=U^b$, $U\in\Gamma$. Since $(NS^{-3})^2=I$ (as an element of Γ), we have $N=VS^3$, $V^2=I$, $V\in\Gamma$. Since $MS^{-3}=U^aS^{-3}\in\Gamma'$, we also have $M^bS^{-3b}=U^{ab}S^{-3b}\in\Gamma'$ (generally, if x, y are elements of a group G such that xy belongs to a normal subgroup H, and n is any integer, then x^ny^n also belongs to H). It follows that $S^{3b}\in\Gamma'$, since $U^b=N\in\Gamma'$. Since the exponent of S modulo Γ is 6, b must be even. Thus $N=W^2$ for some matrix

W of Γ, and $W^2=VS^3$. As an element of SL(2, Z), V satisfies $V^2=-I$. But then Lemma 2 implies that this has no solutions. This completes the proof.

We now turn to the second proof of Theorem 1 and the proof of Theorem 2. We prove

THEOREM 3. *Let F be free of rank $n\geqq 1$ with a basis $X=\{x_1, x_2, \cdots, x_n\}$. Let N be the normal subgroup of F generated by all triple commutators $[x, y, z]=[[x, y], z]$ together with all squares $[x, y]^2$ of double commutators. Let $G=F/N$, so that G is generated by the images $\bar{x}_i$ of the x_i. Then if $k<n$, there do not exist elements $u_1, u_2, \cdots, u_k$ of G such that*

$$\bar{x}_1^2\bar{x}_2^2\cdots\bar{x}_n^2 = u_1^2u_2^2\cdots u_k^2. \tag{7}$$

Furthermore, there do not exist elements u_1, u_2 of G such that

$$\bar{x}_1\bar{x}_2\bar{x}_1^{-1}\bar{x}_2^{-1} = u_1^2u_2^2. \tag{8}$$

PROOF. We drop bars and set $k_{ij}=[x_i, x_j]$. Then G is the group generated by the x_i together with the R_{ij} with defining relations

$$\begin{aligned} x_ix_j &= k_{ij}x_jx_i, && i<j,\\ x_hk_{ij} &= k_{ij}x_h, && i<j, \quad \text{all } h,\\ k_{ij}^2 &= 1, && i<j. \end{aligned}$$

We note that it follows that $k_{ij}=[x_i, x_j]=[x_j, x_i]$, and that x_i^2 lies in the center of G.

Suppose now that (7) holds. Then every element u_h has a representation of the form

$$u_h = \prod_i x_i^{a_{ih}} \prod_{i<j} k_{ij}^{b_{ijh}}$$

where the a_{ih} are unique elements of Z and the $b_{ijh}\in\{0, 1\}$. An easy calculation gives

$$u_h^2 = \prod_i x_i^{2a_{ih}} \prod_{i<j} k_{ij}^{a_{ih}a_{jh}},$$

whence

$$u_1^2u_2^2\cdots u_k^2 = \prod_i x_i^{2\sum_{h=1}^k a_{ih}} \prod_{i<j} k_{ij}^{\sum_{h=1}^k a_{ih}a_{jh}}.$$

Hence we may conclude from (7) that

$$\sum_{h=1}^k a_{ih} = 1 \quad \text{for all } i, \tag{9}$$

$$\sum_{h=1}^k a_{ih}a_{jh} \equiv 0 \bmod 2, \quad \text{for all } i, j \text{ with } i\neq j. \tag{10}$$

Let α_{ih} be the image of a_{ih} in Z_2 (the ring of integers modulo 2). For $1 \leqq i \leqq n$, let $v_i=(\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{ik})$, a vector in the vector space V of dimension k over Z_2. Then (9) implies that $\sum_{h=1}^{k} \alpha_{ih}^2=1$ for all i; that is, that

$$|v_i| = 1 \quad \text{for all } i. \tag{11}$$

Similarly, (10) implies that

$$v_i \cdot v_j = 0 \quad \text{for all } i, j \text{ with } i \neq j. \tag{12}$$

Thus (11) and (12) assert the existence of an orthonormal set of n vectors in V, impossible since $n>k=\dim(V)$.

Suppose now that (8) holds. Clearly, we may assume that $n=2$. Then retaining the notation for u_h introduced previously, we have

$$k_{12} = x_1^{2(a_{11}+a_{12})} x_2^{2(a_{21}+a_{22})} k_{12}^{a_{11}a_{21}+a_{12}a_{22}}, \tag{13}$$

whence

$$a_{11} + a_{12} = 0, \quad a_{21} + a_{22} = 0, \quad a_{11}a_{21} + a_{12}a_{22} \equiv 1 \bmod 2.$$

The first two equations give

$$a_{11} \equiv a_{12} \bmod 2, \qquad a_{21} \equiv a_{22} \bmod 2,$$

which when substituted into the last gives $2a_{11}a_{22} \equiv 1 \bmod 2$, an impossibility. This completes the proof.

In conclusion, we note that Theorem 1 may also be proved by means of a finite group of order 64: namely, the group G of all 3×3 matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

where a, b, c run over all of Z_4. Here

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

are generators of G, and

$$xyx^{-1}y^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

References

1. K. Goldberg, *Unimodular matrices of order* 2 *that commute*, J. Washington Acad. Sci. **46** (1956), 337–338. MR **19**, 123.

2. A. Karrass and D. Solitar, *On free products*, Proc. Amer. Math. Soc. **9** (1958), 217–221. MR **20** #2373.

3. P. E. Schupp, *On the substitution problem for free groups*, Proc. Amer. Math. Soc. **23** (1969), 421–423. MR **39** #6963.

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48104 (Current address of R. C. Lyndon)

Institut des Mathématiques, Université de Montpellier, Montpellier, France

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