JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematical Sciences
Vol. 78B, No. 2, April–June 1974

A Conjecture on a Matrix Group With Two Generators

Morris Newman

Institute for Basic Standards, National Bureau of Standards, Washington, D.C. 20234

(January 3, 1973)

Let ζ be a primitive qth root of unity. It is conjectured that the group generated by

$$A=\begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix} \quad \text{and} \quad B=\begin{pmatrix}1 & 0\\ \zeta & 1\end{pmatrix}$$

is never free. The conjecture is proved when q is an even prime power, or an odd prime power having 2 as a primitive root.

Key words: Free groups; matrix groups; roots of unity.

Let $G=\{A, B\}$ be the group generated by the matrices

$$A=\begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix}, \qquad B=A^T=\begin{pmatrix}1 & 0\\ \zeta & 1\end{pmatrix},$$

where ζ is an arbitrary complex number. It has been known for some time that G is free when $|\zeta|\geqslant 2$ (see [1], [3]); and it is also true that G is free if ζ is transcendental, or if ζ is algebraic and has a conjugate which is greater than or equal to 2 in absolute value. (See the references at the end of this note for further results of this kind.) The only values in question therefore are those algebraic ζ all of whose conjugates are less than 2 in absolute value. This remark prompts the conjecture that if ζ is a root of unity, then G is not free. Although we do not have a proof of this, the following result provides evidence that it is correct:

THEOREM: *Suppose that ζ is a primitive* q*th root of unity, where* q *is a prime power. Then* G *is not free when* q *is even, and also when* q *is odd and* 2 *is a primitive root of* q.

PROOF: We define a sequence of elements of G as follows:

$$(1) \qquad K_1=B=\begin{pmatrix}1 & 0\\ \zeta & 1\end{pmatrix}, \qquad K_{m+1}=K_mA^{-1}K_m^{-1}=K_m\begin{pmatrix}1 & -\zeta\\ 0 & 1\end{pmatrix}K_m^{-1}, \qquad m\geqslant 1.$$

We note first that as a formal word in A and B no cancellation occurs, and that K_m is of length 2^m-1, beginning and ending with B. Next, set

$$K_m=\begin{pmatrix}a_m & b_m\\ c_m & d_m\end{pmatrix}, \qquad m\geqslant 1.$$

Then (1) implies readily that for $m\geqslant 1$,

$$a_{m+1}=1+\zeta a_mc_m, \qquad b_{m+1}=-\zeta a_m^2$$

$$c_{m+1}=\zeta c_m^2, \qquad d_{m+1}=1-\zeta a_mc_m,$$

AMS Subject Classification: 20F05; 20H10.

from which we deduce that for $m \geqslant 1$,

$$(2) \qquad a_m = \sum_{k=0}^{m-1} \zeta^{2^m - 2^k + 1}, \qquad b_m = -\zeta a_{m-1}^2,$$
$$c_m = \zeta^{2^m - 1}, \qquad d_m = 2 - a_m,$$

where a_0 is understood to be 0.

Suppose first that $q = 2^r$, so that $\zeta^{2^r} = 1$, $\zeta^{2^{r-1}} = -1$. Choose $m = r - 1$. Then $\operatorname{tr}(AK_m) = a_m + \zeta c_m + d_m = 2 + \zeta^{2^m} = 1$, and so $(AK_m)^6 = \mathrm{I}$. This is a genuine relation, so that G is not free in this case.

Next suppose that $q = p^r$, where p is an odd prime and 2 is a primitive root of q. Then the numbers 2^k, $0 \leqslant k \leqslant \varphi(q) - 1$, form a reduced set of residues modulo q. Choose $m = 1 + \varphi(q)$. Then it follows easily that

$$a_m = \sum_{k=0}^{\varphi(q)} \zeta^{2^m - 2^k + 1} = 1 + \zeta^2 \mu(q),$$

where $\mu(q)$ is the Möbius function, since the numbers

$$\zeta^{-2^k + 1}, \qquad 0 \leqslant k \leqslant \varphi(q) - 1,$$

are the $\varphi(q)$ primitive qth roots of unity, and the sum of the primitive qth roots of unity is $\mu(q)$. There are now two subcases to consider.

I. $r > 1$. Then $\mu(q) = 0$, and $a_m = 1$.

It follows from (2) that $K_m = \begin{pmatrix} 1 & 0 \\ \zeta & 1 \end{pmatrix} = B$, which is a genuine relation.

II. $r = 1$. Then $\mu(q) = -1$, $\quad a_m = 1 - \zeta^2$,

$$K_m = \begin{pmatrix} 1 - \zeta^2 & -\zeta^3 \\ \zeta & 1 + \zeta^2 \end{pmatrix}. \text{ Thus}$$

$$AK_m = \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix} K_m = \begin{pmatrix} 1 & \zeta \\ \zeta & 1 + \zeta^2 \end{pmatrix} = BA,$$

$K_m = A^{-1}BA$. Again, this is a genuine relation.

This completes the proof.

References

[1] Brenner, J. L., Quelques groupes libres de matrices, C. R. Acad. Sci. Paris 241, 1689–1691 (1955).

[2] Chang, B., Jennings, S. A., and Ree, R., On certain pairs of matrices which generate free groups. Canad. J. Math. **10**, 279–284 (1958).

[3] Lyndon, R. C., and Ullman, J. L., Pairs of real 2-by-2 matrices that generate free products, Mich. Math. J. **15**, 161–166 (1968).

[4] Newman, M., Pairs of matrices generating discrete free groups and free products, Michigan Math. J. **15**, 155–160 (1968).

(Paper 78B2–400)