Canad. Math. Bull. Vol. 17 (5), 1975

A NOTE ON TORSION FREE GROUPS GENERATED BY PAIRS OF MATRICES

BY
A. CHARNOW

Let $A=\left[\begin{smallmatrix}1 & m\\ 0 & 1\end{smallmatrix}\right]$ and let G_m be the group generated by A and the transpose of A. The problem of determining complex numbers m such that G_m is a free group had been studied by several authors [1, 2, 3]. In this note we characterize those rational values of m for which G_m is torsion free.

We shall need the fact that every element of G_m is of the form:

$$\begin{bmatrix} 1+m^2f_1(m) & mf_2(m) \\ mf_3(m) & 1+m^2f_4(m) \end{bmatrix},$$

where the f_i are polynomials with integral coefficients. This is easily proved by induction on the length of a word in G_m.

THEOREM. *Let m be rational. Then G_m has an element of finite order (other than the identity) if and only if m is the reciprocal of an integer.*

Proof. Suppose $m=1/n$, where n is an integer. Let B=the transpose of A and let

$$C=\begin{bmatrix} -2 & -3m \\ 1/m & 1 \end{bmatrix}.$$

Then $A^{-3}B^{n^2}=\left[\begin{smallmatrix}1 & -3m\\ 0 & 1\end{smallmatrix}\right]\left[\begin{smallmatrix}1 & 0\\ n^2m & 1\end{smallmatrix}\right]=C$, hence C is in G_m. We have $C^3=\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$ and hence C has order 3. Conversely, assume that G_m has some element (other than the identity) of finite order. Then clearly G_m will have an element of prime order. Hence there exists C in G_m with

$$C^p=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad C\neq\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and p prime.

Then the minimal polynomial of C must divide x^p-1 and hence has no multiple roots. Thus C is diagonalizable over the complex field. Hence

$$QCQ^{-1}=\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$

for some Q. Since every element of G has determinant 1, we must have $\lambda_2=1/\lambda_1$. Since

$$C^p=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

it follows that $\lambda_1^p=1$. Since C is not the identity, $\lambda_1\neq 1$. Thus λ_1 is a primitive pth root of 1. Thus the degree of λ_1 over the rationals is $p-1$. But λ_1 is a root of a quadratic with rational coefficients, namely the characteristic polynomial of C. Hence $p-1\leq 2$. Thus either $\lambda_1=-1$ or λ_1 is a primitive cube root of 1. Let $m=a/b$, $a>0$, a, b integers with $(a, b)=1$. We have

$$C=\begin{bmatrix}1+m^2f_1(m) & mf_2(m)\\ mf_3(m) & 1+m^2f_4(m)\end{bmatrix},$$

where the f_i are polynomials with integral coefficients.

Case 1. $\lambda_1=-1$. Then

$$C=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$$

and $1+m^2f_1(m)=-1$. Thus there exists integers a_i such that $a_tm^t+\cdots+a_2m^2+2=0$. It follows that $a\mid 2$. If $a=2$ then $a_t2^t+a_{t-1}2^{t-1}b+\cdots+a_22^2b^{t-2}+2b^t=0$ and this implies $2\mid b$, a contradiction. Thus $a=1$ and $m=1/b$.

Case 2. λ_1 is a primitive cube root of 1. Then trace $C=\lambda_1+(1/\lambda_1)=-1$. Hence $2+m^2[f_1(m)+f_2(m)]=-1$. Hence there exist integers a_i with $a_tm^t+\cdots+a_2m^2+3=0$. It follows that $a\mid 3$. If $a=3$ then $a_t3^t+a_{t-1}3^{t-1}b+\cdots+a_23^2b^{t-2}+3b^t=0$ and this implies $3\mid b$, a contradiction. Thus $a=1$, $m=1/b$.

References

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

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

3. R. C. Lyndon and J. L. Ullman, *Groups generated by two parabolic linear fractional transformations*, Can. J. Math. **21** (1969), 1388–1403.

Department of Mathematics
California State University
Hayward, California 94542