PAIRS OF MATRICES GENERATING DISCRETE FREE GROUPS AND FREE PRODUCTS

Morris Newman

The purpose of this note is to prove that certain pairs of real 2×2 matrices of determinant 1 generate discrete free groups, and to indicate extensions to pairs of real linear fractional transformations generating discrete free products. The conditions are formulated in terms of the signs of the elements of the matrices, and they may be regarded as a generalization of the situation that exists in the classical modular group Γ and the Hecke groups (see [4], [5], [9], and [10]). Some work along these lines has been done by various authors (see [1], [2], [3], [7], [8], and [11]), but the conditions previously imposed were of a different type, and there is very little intersection with the present work. In addition, it is worth noticing that $\Gamma(2)$ and Γ', the only free normal 2-generator subgroups of Γ, are not covered by the present discussion. Reasonably simple conditions for deciding when an arbitrary pair of elements of SL(2, R) (where R denotes the real field) generates a free group are probably not to be found, and partial answers of the type given here may be the most that can be expected.

Let $G = \{A, B\}$ denote the group generated by the elements A and B of SL(2, R). Then each element W of G has the form

$$W = A^{r_1} B^{s_1} \cdots A^{r_n} B^{s_n}, \tag{1}$$

where the exponents are different from 0 except possibly for r_1 and s_n. If all the exponents are different from 0, we say that W is *of type* (AB). A simple argument shows that

(a) G is free and freely generated by A and B if and only if A and B are not of finite period and no word of type (AB) with $n > 0$ represents the identity,

(b) G is discrete if and only if there is no convergent infinite sequence $W_1, W_2, \cdots$ of distinct words W_i of type (AB).

Our method will consist of deriving inequalities for the elements of the matrices $A^r B^s$ $(rs \neq 0)$. The inequalities carry over on multiplication, and they imply the desired results.

THEOREM 1. *Let* A, B *be elements of* SL(2, R). *Suppose that*

$$A = \begin{pmatrix} -a & b \\ -c & d \end{pmatrix}, \quad B = \begin{pmatrix} -\alpha & -\beta \\ \gamma & \delta \end{pmatrix},$$

where $a, b, c, d, \alpha, \beta, \gamma, \delta \geq 0$ *and* $t = d - a \geq 2$, $\tau = \delta - \alpha \geq 2$. *Then the group* $G = \{A, B\}$ *is a free discrete subgroup of* SL(2, R) *and is freely generated by* A, B.

Before embarking on the proof, we should make the following observation: Let us regard A, B as elements of LF(2, R), and add the further restriction that

Received July 10, 1967.

$$\frac{a-1}{c} > \frac{1-\alpha}{\gamma}.$$

Then the isometric circles of A, A^{-1}, B, B^{-1} are pairwise disjoint, and the result (in this case) follows by the methods used in [2] and [4].

We now turn to the proof.

LEMMA 1. *There is a conjugacy over* GL(2, R) *that takes* A *into* $\begin{pmatrix} 0 & 1 \\ -1 & t \end{pmatrix}$ *and* B *into a matrix with the same sign pattern as* B.

Proof. Since $bc = 1 + ad \geq 1$, c cannot vanish. Put

$$M = \begin{pmatrix} c & -a \\ 0 & 1 \end{pmatrix} \in GL(2, R).$$

Then

$$MAM^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & t \end{pmatrix}, \quad MBM^{-1} = \frac{1}{c}\begin{pmatrix} -\alpha c - \gamma a & -\beta c^2 - \gamma a^2 - (\alpha + \delta)ac \\ \gamma & \gamma a + \delta c \end{pmatrix}.$$

Since MBM^{-1} and B obviously have the same sign pattern, the lemma follows.

Because of this lemma, we lose no generality in assuming that $A = \begin{pmatrix} 0 & 1 \\ -1 & t \end{pmatrix}$, and this will be done in what follows.

As usual, we define sgn(x) by

$$\operatorname{sgn}(x) = \begin{cases} 1 & (x \geq 0), \\ -1 & (x < 0). \end{cases}$$

Let X, Y be any elements of SL(2, R). We write $X \gg Y$ to mean that every element of X is nonnegative and exceeds or equals the absolute value of the corresponding element of Y. Notice that if $X_1 \gg Y_1$ and $X_2 \gg Y_2$, then $X_1 X_2 \gg Y_1 Y_2$.

We now prove

LEMMA 2. *Let* r *and* s *be nonzero integers. Then*

$$\operatorname{sgn}(rs)\, A^r B^s \gg |rs| \begin{pmatrix} \gamma & 0 \\ 0 & \beta \end{pmatrix}. \tag{2}$$

Furthermore, if $\alpha = 0$, $\beta = 1$, $\gamma = 1$ $\left(\text{so that } B = \begin{pmatrix} 0 & -1 \\ 1 & \tau \end{pmatrix}\right)$, *then*

$$\operatorname{sgn}(rs)\, A^r B^s \gg |rs|\, C(r, s), \tag{3}$$

where C(r, s) *is one of the matrices*

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Proof. Since A has trace t and determinant 1, A satisfies its characteristic equation $A^2 = tA - I$. Hence for each integer r, A^r must be a linear combination of A and I. In fact,

$$A^r = t_r A - t_{r-1} I,$$

where $t_0 = 0$, $t_1 = 1$, $t_{r+1} = tt_r - t_{r-1}$. It is readily seen that

$$t_{-r} = -t_r, \tag{4}$$

and (because $t \geq 2$)

$$t_r \geq r \qquad (r \geq 0). \tag{5}$$

Similarly, for each integer s,

$$B^s = \tau_s B - \tau_{s-1} I,$$

where $\tau_0 = 0$, $\tau_1 = 1$, $\tau_{s+1} = \tau\tau_s - \tau_{s-1}$, and where

$$\tau_{-s} = -\tau_s, \tag{6}$$

$$\tau_s \geq s \qquad (s \geq 0). \tag{7}$$

Direct computation now shows that

$$A^r B^s = \begin{pmatrix} a_{r,s} & b_{r,s} \\ c_{r,s} & d_{r,s} \end{pmatrix},$$

where

$$a_{r,s} = t_{r-1}\tau_{s-1} + \alpha t_{r-1}\tau_s + \gamma t_r \tau_s,$$

$$b_{r,s} = \beta t_{r-1}\tau_s + \alpha t_r \tau_s + t_r \tau_{s+1},$$

$$c_{r,s} = t_r \tau_{s-1} + \alpha t_r \tau_s + \gamma t_{r+1}\tau_s,$$

$$d_{r,s} = \beta t_r \tau_s + \alpha t_{r+1}\tau_s + t_{r+1}\tau_{s+1}.$$

Observe that if $rs > 0$, then all the elements of $A^r B^s$ are nonnegative, and that if $rs < 0$, then all the elements of $-A^r B^s$ are nonnegative. In fact, using (4), (5), (6), and (7), we obtain the relations

$$A^r B^s \gg rs\begin{pmatrix} \gamma & \alpha + 1 \\ \alpha + \gamma & \alpha + \beta + 1 \end{pmatrix} \qquad (r > 0,\ s > 0),$$

$$-A^r B^s \gg -rs\begin{pmatrix} \gamma & \alpha \\ \alpha + \gamma + 1 & \alpha + \beta \end{pmatrix} \qquad (r > 0,\ s < 0),$$

$$-A^r B^s \gg -rs\begin{pmatrix}\alpha+\gamma & \alpha+\beta+1\\ \alpha & \beta\end{pmatrix} \qquad (r<0,\ s>0),$$

$$A^r B^s \gg rs\begin{pmatrix}\alpha+\gamma+1 & \alpha+\beta\\ \alpha+1 & \beta\end{pmatrix} \qquad (r<0,\ s<0),$$

from which both (2) and (3) follow. This completes the proof of the lemma.

We now turn to the proof of Theorem 1. If W is of type (AB), define $h(W)$ as the absolute value of the product of the exponents of W. We note first that neither A nor B is of finite period. Let W, given by (1), be any word of type (AB), and put

$$\varepsilon = \operatorname{sgn}(r_1 s_1)\cdots\operatorname{sgn}(r_n s_n).$$

Then Lemma 2 implies that

$$\varepsilon W \gg h(W)\begin{pmatrix}\gamma^n & 0\\ 0 & \beta^n\end{pmatrix}, \tag{8}$$

and also that if $B = \begin{pmatrix}0 & -1\\ 1 & \tau\end{pmatrix}$, then

$$\varepsilon W \gg h(W)\,C(r_1, s_1)\cdots C(r_n, s_n). \tag{9}$$

If $B \neq \begin{pmatrix}0 & -1\\ 1 & \tau\end{pmatrix}$, then $\beta > 1$ or $\gamma > 1$, and (8) implies that W can never be the identity. If $B = \begin{pmatrix}0 & -1\\ 1 & \tau\end{pmatrix}$, then (9) implies that W can never be the identity. Hence we have proved the first part of the theorem; namely, the group G is free.

Now suppose that

$$W_i = a^{r_{i1}} B^{s_{i1}} \cdots A^{r_{ik_i}} B^{s_{ik_i}} \qquad (i = 1, 2, 3, \cdots)$$

is any infinite sequence of distinct elements of type (AB). Then certainly

$$\sum_{j=1}^{k_i} \{|r_{ij}| + |s_{ij}|\} \to \infty \quad \text{as } i \to \infty, \tag{10}$$

which implies that either $h(W_i) \to \infty$ as $i \to \infty$, or $k_i \to \infty$ as $i \to \infty$, or both. Put

$$\varepsilon_i = \operatorname{sgn}(r_{i1} s_{i1})\cdots\operatorname{sgn}(r_{ik_i} s_{ik_i}).$$

We see again that

$$\varepsilon_i W_i \gg h(W_i)\cdot\begin{pmatrix}\gamma^{k_i} & 0\\ 0 & \beta^{k_i}\end{pmatrix}, \tag{11}$$

and also that if $B = \begin{pmatrix} 0 & -1 \\ 1 & \tau \end{pmatrix}$, then

$$\varepsilon_i W_i \gg h(W_i) \cdot C(r_{i1}, s_{i1}) \cdots C(r_{ik_i}, s_{ik_i}). \tag{12}$$

A little reflection shows that because of (10), (11), and (12), some of the elements of $\varepsilon_i W_i$ become arbitrarily large as $i \to \infty$. Hence no such sequence converges, and we have proved the second part of the theorem; namely, the group G is discrete. This completes the proof of Theorem 1.

Essentially the same method allows us to prove the following generalization of Theorem 1 (we omit the proof):

THEOREM 2. *Let* A, B *be elements of* LF(2, R) *and let* p *and* q *be integers* (p, q $\geq$ 2). *Suppose that*

$$A = \begin{pmatrix} -a & b \\ -c & d \end{pmatrix}, \quad B = \begin{pmatrix} -\alpha & -\beta \\ \gamma & \delta \end{pmatrix},$$

where a, b, c, d, α, β, γ, $\delta \geq 0$. *Put* $t = d - a$, $\tau = \delta - \alpha$. *Then the group* $G = \{A, B\}$ *generated by* A, B *is discrete and equal to* $\{A\} * \{B\}$ *(the free product of the indicated cyclic groups) in each of the following four cases:*

$$t \geq 2, \quad \tau \geq 2, \tag{13}$$

$$t = 2\cos\frac{\pi}{p}, \quad \tau \geq 2, \tag{14}$$

$$t \geq 2, \quad \tau = 2\cos\frac{\pi}{q}, \tag{15}$$

$$t = 2\cos\frac{\pi}{p}, \quad \tau = 2\cos\frac{\pi}{q}. \tag{16}$$

The presentation of this paper was materially improved by the referee's comments, which we gratefully acknowledge.

REFERENCES

1. J. L. Brenner, *Quelques groupes libres de matrices.* C.R. Acad. Sci. Paris 241 (1955), 1689-1691.
2. L. R. Ford, *Automorphic functions*, Second Ed. Chelsea, New York, 1951.
3. K. Goldberg and M. Newman, *Pairs of matrices of order two which generate free groups.* Illinois J. Math. 1 (1957), 446-448.
4. E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung.* Math. Ann. 112 (1936), 664-699.
5. K. A. Hirsch, Appendix B to vol. 2 of his translation of *The Theory of Groups* by A. G. Kurosh. Chelsea, New York, 1955.

6. J. Lehner, *Representations of a class of infinite groups*. Michigan Math. J. 7 (1960), 233-236.

7. A. M. Macbeath, *Packing, free products and residually finite groups*. Proc. Cambridge Phil. Soc. 59 (1963), 555-558.

8. B. Maskit, *Construction of Kleinian groups*. Proc. Conf. Complex Analysis (Minneapolis, 1964), 281-296. Springer, Berlin (1965).

9. M. Newman, *Some free products of cyclic groups*. Michigan Math. J. 9 (1962), 369-373.

10. H. Rademacher, *Zur Theorie der Dedekindschen Summen*. Math. Z. 63 (1955/56), 445-463.

11. I. N. Sanov, *A property of a representation of a free group*. Doklady Akad. Nauk SSSR (N.S.) 57 (1947), 657-659 (Russian).

National Bureau of Standards
Washington, D. C. 20234