ON CERTAIN PAIRS OF MATRICES WHICH GENERATE FREE GROUPS

BOMSHIK CHANG, S. A. JENNINGS AND RIMHAK REE

1. Introduction. Denote by $F_{\alpha,\beta}$ the multiplicative group generated by the two matrices

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

where α and β are complex numbers. Sanov **(3)** proved that $F_{2,2}$ is free, and Brenner **(1)** showed that $F_{m,m}$ is free if $m \geqslant 2$.

In this note we extend these results, proving that $F_{\alpha,\beta}$ is free if $\alpha\beta$ satisfies all three of the conditions

$$|\alpha\beta| \geqslant 2, \; |\alpha\beta - 2| \geqslant 2 \quad \text{and} \quad |\alpha\beta + 2| \geqslant 2$$

(Theorem 2). In § 3, we prove that the set of algebraic numbers $\alpha\beta$ for which $F_{\alpha,\beta}$ is free is dense in the whole complex plane, and exhibit some values of $\alpha\beta$ for which $F_{\alpha,\beta}$ is not free. In the last section we show that the main idea used in the proof of Theorem 2 can be applied to a more general case.

2. Main theorems.

THEOREM 1. *If* $\alpha\beta = \gamma\delta \neq 0$ *then* $F_{\alpha,\beta}$ *and* $F_{\gamma,\delta}$ *are isomorphic.*

Proof. It suffices to prove that $F_{\alpha,\beta} \cong F_{\alpha\beta,1}$. We have

$$\begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} = P^{-1}\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}P, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = P^{-1}\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}P, \quad \text{where } P = \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}.$$

Hence the mapping $X \rightarrow P^{-1}XP$ gives the required isomorphism.

By Theorem 1, the consideration of the general group $F_{\alpha,\beta}$ is reduced to that of $F_\lambda = F_{2,\lambda}$ where $\alpha\beta = 2\lambda$. We shall say that a complex number λ is *free* if the group F_λ is free.

THEOREM 2. *Any complex number* λ *which satisfies*

$$(2.1) \qquad |\lambda| \geqslant 1, \; |\lambda - 1| \geqslant 1, \; |\lambda + 1| \geqslant 1$$

is free.

In order to prove Theorem 2, we adopt the following notation: for a complex variable z and a matrix

Received December 30, 1956. This research was in part supported by National Research Council of Canada grant G. 489.

https://doi.org/10.4153/CJM-1958-029-2 Published online by Cambridge University Press

$$P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad ad - bc = 1,$$

with complex entries, we denote by $P(z)$ the number $(az + b)/(cz + d)$. Then, as is well known, $(QP)\ (z) = Q(P(z))$ where Q is another such matrix.

In the rest of this section, we set

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix},$$

and define point sets $\mathscr{D}$ and $\mathscr{D}'$ in the complex plane as follows:

$$\mathscr{D} = \{z|\ |\Re z| \leqslant 1\}, \quad \mathscr{D}' = \{z|\ |\Re z| \geqslant 1\},$$

where $\Re z$ denotes the real part of z.

The following lemma is well known:

LEMMA 1. *If $z \in \mathscr{D}'$ then*

$$|z^{-1} - \tfrac{1}{2}| \leqslant \tfrac{1}{2} \quad \textit{or} \quad |z^{-1} + \tfrac{1}{2}| \leqslant \tfrac{1}{2}.$$

If, on the other hand,

$$|z - \tfrac{1}{2}| \geqslant \tfrac{1}{2} \quad \textit{and} \quad |z + \tfrac{1}{2}| \geqslant \tfrac{1}{2},$$

then $z^{-1} \in \mathscr{D}$.

LEMMA 2. *If λ satisfies* (2.1), *then $z \in \mathscr{D}'$ implies $B^n(z) \in \mathscr{D}$ for any non-zero integer n.*

Proof. Since

$$B^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & n\lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

we may write

$$z_1 = z^{-1}, z_2 = z_1 + \mu, B^n(z) = z_2^{-1},$$

where $\mu = n\lambda$, which clearly satisfies (2.1). By Lemma 1, $z \in \mathscr{D}'$ implies

$$|z_1 - \tfrac{1}{2}| \leqslant \tfrac{1}{2} \quad \text{or} \quad |z_1 + \tfrac{1}{2}| \leqslant \tfrac{1}{2}.$$

If $|z_1 - \frac{1}{2}| \leqslant \frac{1}{2}$, then

$$|z_2 - \tfrac{1}{2}| = |z_1 + \mu - \tfrac{1}{2}| \geqslant |\mu| - |z_1 - \tfrac{1}{2}| \geqslant 1 - \tfrac{1}{2} = \tfrac{1}{2},$$

and

$$|z_2 + \tfrac{1}{2}| = |z_1 + \mu + \tfrac{1}{2}| \geqslant |\mu + 1| - |z_1 - \tfrac{1}{2}| \geqslant 1 - \tfrac{1}{2} = \tfrac{1}{2}.$$

Similarly, if $|z_1 + \frac{1}{2}| \leqslant \frac{1}{2}$, then we have

$$|z_2 - \tfrac{1}{2}| \geqslant \tfrac{1}{2} \quad \text{and} \quad |z_2 + \tfrac{1}{2}| \geqslant \tfrac{1}{2}.$$

Then again by Lemma 1, we have $B^n(z) \in \mathscr{D}$ as required.

https://doi.org/10.4153/CJM-1958-029-2 Published online by Cambridge University Press

Proof of Theorem 2. We shall derive a contradiction by assuming that F_λ is not free. If F_λ is not free there must exist a non-trivial word G of F_λ such that

$$G = B^{n_r}A^{m_r}\ldots B^{n_1}A^{m_1} = E \tag{2.2}$$

where we can always assume that the integers $m_1, n_1, \ldots, m_r$ are all not zero. Define

$$\begin{aligned} &(2.3) \qquad & z_1 &= A^{m_1}(0), & z_1' &= B^{n_1}(z_1), & & \\ & & z_k &= A^{mk}(z_{k-1}'), & z_k' &= B^{nk}(z_k), & &(k \leqslant r-1), \\ &\text{and} & z_r &= A^{-m_r}B^{-n_r}(0). & & & & \end{aligned}$$

Then (2.2) implies

$$z_{r-1}{}' = z_r. \tag{2.4}$$

Since $z_1 = 2m_1$, $|\Re z_1| \geqslant 1$, $z_1 \in \mathscr{D}'$. By Lemma 2, we have

$$z_1' = B^{n_1}(z_1) \in \mathscr{D}.$$

Then, by (2.3), $z_2 = z_1 + 2m_m$, and hence

$$|Rz_2| \geqslant |2m_2| - |\Re z_1{}'| \geqslant 1.$$

Thus, $z_2 \in \mathscr{D}'$. Again, using Lemma 2, we have

$$z_2' = B^{n_2}z_2 \in \mathscr{D}.$$

Repeating this argument, we find $z_{r-1}{}' \in \mathscr{D}$. On the other hand, $z_r = -2m_r$, and $|\Re z_r| \geqslant 2$. Therefore $z_r \notin \mathscr{D}$ and $z_{r-1}{}' \neq z_r$, which contradicts (2.4). Thus Theorem 2 is proved.

3. Distribution of free and non-free points. First we note that *any transcendental number is free.* This is seen as follows. Let

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix},$$

where x is an indeterminate. Then any word G generated by A and B is of the form

$$G = \begin{pmatrix} p_1(x) & p_2(x) \\ p_3(x) & p_4(x) \end{pmatrix},$$

where $p_1(x), \ldots, p_4(x)$ are polynomials in x with integral coefficients. In the course of proving Theorem 2 we have shown that if G is of the form given in (2.2) and if λ is a number satisfying (2.1), then $G(0) = p_2(\lambda)/\mathrm{p}_4(\lambda) \neq 0$. Hence, for such an element G, the polynomial $p_2(x)$ is always not identically zero. Therefore $G \neq E$ for any transcendental value of x. From this it follows that any transcendental number is free.

The following theorem, however, shows that there are also many free algebraic numbers in the domain excluded by Theorem 2.

THEOREM 3. *Any point in the complex plane is a limit of algebraic free points.*

https://doi.org/10.4153/CJM-1958-029-2 Published online by Cambridge University Press

In order to prove Theorem 3, we need the following well-known result (**4**, p. 122).

LEMMA 3. *Let p be a prime and c a rational number. Then the polynomial $x^p - c$ is reducible over the rational field, if and only if, c is a* p*th power of a rational number.*

Proof of Theorem 3. Let w be a given complex number. Because of Theorem 2, we may assume that w lies in the domain excluded by Theorem 2. For any positive number ϵ there exist a prime p, an integer q, and a rational number a such that $|w - \lambda_1| > \epsilon$ and $\lambda_2 > 4$, where

$$\lambda_1 = a + 2^{2+1/p}e^{2q\pi i/p},\ \lambda_2 = a + 2^{2+1/p}.$$

We shall show that λ_1 is free. Assume the contrary. Then there must be a non-trivial word G of $F_{2,x}$

$$G = \begin{pmatrix} p_1(x) & p_2(x) \\ p_3(x) & p_4(x) \end{pmatrix}$$

which becomes the identity matrix when $x = \lambda_1$. Hence, we have

$$p_1(\lambda_1) - 1 = p_2(\lambda_1) = p_3(\lambda_1) = p_4(\lambda_1) - 1 = 0.$$

Since the polynomials $p_1(x) - 1$, $p_2(x)$, $p_3(x)$ and $p_4(x) - 1$ have integral coefficients uniquely determined by G and since λ_1, λ_2 are roots of a polynomial $(x - a)^p - 2^{2p+1}$, which, by Lemma 3, are irreducible over the rational field, it follows that

$$p_1(\lambda_2) - 1 = p_2(\lambda_2) = p_3(\lambda_2) = p_4(\lambda_2) - 1 = 0,$$

and consequently that $\lambda_2 > 4$ is not free. This is a contradiction by Theorem 2. Thus λ_1 is shown to be free. Since λ_1 is algebraic and since ϵ is an arbitrary positive number, w is a limit of free algebraic numbers. Thus, Theorem 3 is proved.

THEOREM 4. *Let a, b, c, d, k and h be non-zero integers such that $k > 2$, $(k, h) = 1$. Then*

$$\lambda = \frac{-(a+c)(b+d) \pm [(a+c)^2(b+d)^2 - 16abcd\sin^2(h\pi/k)]^{\frac{1}{2}}}{4abcd}$$

is not free.

Proof. By an elementary computation we see that the trace of the matrix $M = A^aB^bA^cB^d$ is

$$2 + 2(a + c)(b + d)\lambda + 4abcd\lambda^2 = e^{2h\pi i/k} + e^{-2h\pi i/k}.$$

Since det $(M) = 1$, it follows that $r_1 = e^{2h\pi i/k}$ and $r_2 = e^{-2h\pi i/k}$ are characteristic roots of M. Moreover, $k > 2$, $(k,h) = 1$ implies $r_1 \neq r_2$. Therefore M can be diagonalized with diagonal elements r_1 and r_2, and hence $M^k = E$. Thus F_λ is not free.

https://doi.org/10.4153/CJM-1958-029-2 Published online by Cambridge University Press

COROLLARY 1. *Every number λ on the segment $[-2,2]$ of the real axis is a limit of non-free real numbers.*

Proof. Set $a = b = c = d = \pm 1$ in Theorem 4, and note that the numbers of the form $\cos(h\pi/k)$ are densely distributed in the segment $[0, 1]$.

COROLLARY 2. *Every number of the form λi, where $-1 \leqslant \lambda \leqslant 1$, is a limit of non-free pure imaginary numbers.*

Proof. Set $a = b = -c = -d = \pm 1$ in Theorem 4.

The authors have been unable to decide whether the domain $\{\lambda| \ |\lambda| < 1$ or $|\lambda - 1| < 1$ or $|\lambda + 1| < 1\}$ contains an open set consisting of free numbers only.

4. An example of free products. We have seen that in certain cases $F_{\alpha,\beta}$ is the free product of cyclic groups $\{A\}$ and $\{B\}$. Using similar methods we may also construct an example of free products of two abelian groups, each of which is a free abelian group of rank 2.

THEOREM 5. *Let*

$$A_1 = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & \alpha i \\ 0 & 1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 \\ \beta i & 1 \end{pmatrix},$$

where $|\alpha| \geqslant 2$ and $|\beta| \geqslant 2$. Then the group $F = \{A_1, A_2, B_1, B_2\}$ is the free product of two free abelian groups $F_A = \{A_1, A_2\}$ and $F_B = \{B_1, B_2\}$.

The proof of Theorem 5 is essentially the same as that of Theorem 2. The following lemma is useful.

LEMMA 4. *If*

$$z' = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}^n (z)$$

with $|\lambda| \geqslant 2$ and $|z| \geqslant 1$, then $|z'| \leqslant 1$.

Proof. Since $z' = z/(n\lambda z + 1)$, we have $z'^{-1} = n\lambda + z^{-1}$. Therefore $|z'^{-1}| \geqslant 1$ or $|z'| \leqslant 1$.

Proof of Theorem 5. Suppose F is not the free product of F_A and F_B, so that there exists an element G of F such that

$$G = B_{n_r} A_{m_r} \ldots B_{n_1} A_{m_1} = E,$$

where

$$A_{m_i} = A_1^{m_{1i}} A_2^{m_{2i}}, B_{n_j} = B_1^{n_{1j}} B_2^{n_{2j}}$$

We may always assume that none of

$$A_{m_i} \quad \text{and} \quad B_{n} \cdot \qquad (1 \leqslant j \leqslant n-1)$$

https://doi.org/10.4153/CJM-1958-029-2 Published online by Cambridge University Press

are the identity elements of F_A and F_B respectively. Then each

$$A_{m_j} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

with $|a| \geqslant 2$ and each

$$B_{n_j} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \qquad (1 \leqslant j \leqslant n-1)$$

with $|b| \geqslant 2$. Using Lemma 4, it is easy to show, as in the proof of Theorem 2, that

$$|B_{n_{r-1}}A_{m_{r-1}} \dots B_{n_1}A_{m_1}(0)| \leqslant 1,$$
$$|A_{m_r}^{-1}B_{n_r}^{-1}(0)| \geqslant 1.$$

This gives the necessary contradiction, and Theorem 5 is proved.

Let $H_m = \{A_1{}^mB_1A_1{}^{-m}\}, m = 1, 2, 3, \dots$ and $K_n = \{A_2{}^nB_1A_2{}^{-n}, A_2{}^nB_2A_2{}^{-n}\}$, $n = 1, 2, 3, \dots$. Each H_m is a free abelian group of rank 1 and each K_n is a free abelian group of rank 2 all contained in F. It is not hard to verify that F contains the free product of all H_m and all K_n. Therefore we can obtain a representation of the free product of any finite or countable number of free abelian groups each of which has rank 1 or 2.

The authors, however, have been unable to obtain matric representations of free products of free abelian groups whose ranks are greater than 2.

We show, as an example, that the matrices

$$C_1 = \begin{pmatrix} 1 & m & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & 0 & 0 \\ m & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ m & 0 & 1 \end{pmatrix}$$

do not generate a free product. The groups $F_C = \{C_1, C_2\}$ and $F_D = \{D_1, D_2\}$ are free abelian and of rank 2, and the groups $\{C_i, D_j\}$ $(i = 1, 2; j = 1, 2)$ are all free groups of rank 2. But the group $F = \{C_1, C_2, D_1, D_2\}$ is not a free product of F_C and F_D, since the relation

$$C_1C_2D_1{}^{-1}D_2C_1{}^{-1}C_2{}^{-1}D_1D_2{}^{-1}C_1C_2D_1D_2{}^{-1}C_1{}^{-1}C_2{}^{-1}D_1{}^{-1}D_2 = E$$

always holds.

References

1. J. L. Brenner, *Quelques groupes libres de matrices*, C. R. Acad. Sci. Paris *241* (1955), 1689–1691.
2. K. Goldberg and M. Newman, *Pairs of matrices of order two which generate free groups*, Ill. J. Math. *1* (1957), 446–448.
3. I. N. Sanov, *A property of a representation of a free group*, Doklady Akad. Nauk (N.S.) *57* (1947), 657–659.
4. B. L. van der Waerden, *Modern algebra*, vol. 1 (New York, 1949).

University of British Columbia

https://doi.org/10.4153/CJM-1958-029-2 Published online by Cambridge University Press