University of Alberta

Groups generated by two parabolic linear fractional transformations

by

Quan Zhou ©

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of **Master of Science**.

Department of Mathematical and Statistical Sciences

Edmonton, Alberta
Fall 2006

Your file Votre référence
ISBN: 978-0-494-22418-2
Our file Notre référence
ISBN: 978-0-494-22418-2

Abstract

Structure of the group generated by two parabolic linear fractional transformations is studied. For the set of 2-free points, several classical results and the corresponding methods are reviewed and a new method is given. The set of nonfree points is described and analyzed. Farbman's results about rational 1-nonfree set is presented. A new set of torsion-free points is given.

Acknowledgements

I thank my supervisor, Dr. Mazi Shirvani, for his guidance, advice, and patience.

Thanks to Andrew and Jeremy for providing a stimulating work environment.

Contents

List of Figures

Chapter 1

Introduction and background

1.1 Introduction

Define $\langle A_\alpha, B_\beta \rangle$ to be the multiplicative group generated by two noncommuting parabolic linear fractional transformations:

$$A_\alpha = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \text{ and } B_\beta = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$$

where α and β are complex numbers.

The topic of this thesis is the study of the structure of the group $\langle A_\alpha, B_\beta \rangle$. We are interested in whether it is free or not. As there is a direct relation between the freeness of $\langle A_\alpha, B_\beta \rangle$ and the complex number $\tau = \alpha\beta$, people are trying to find the domain of $\lambda = \tau/2$ for which the group $\langle A_\alpha, B_\beta \rangle$ is free and call such a λ *2-free.* (We will also use the notation *free* for $u = \sqrt{\tau}$ and the notation *1-free* for τ.) Most of the complex plane is then proved to give 2-free points. However, there is still an eye-shaped area unknown. We will review these results and give a new method to find 2-free points in Chapter 2.

Another way to solve this problem is to find all *2-nonfree* points. We will discuss the density of 2-nonfree points and show some specific *nonfree* sets in the eye-shaped area in Chapter 3. In Section 3.3, we will review Farbman [11]'s result about nonfree rational set and will give the complete proof of the nonfreeness of rational numbers with numerators 1 to 12.

It is also a major question to determine the *torsion-freeness* of group $\langle A_\alpha, B_\beta \rangle$. Charnow discuss the rational case in [8]. We propose a more general result in Chapter 4. This is one of the most important original results of the thesis.

The remainder of this chapter consists of background material we will be needing later on.

1.2 Basics

We use mark "$\doteq$" to denote "*represent*". For example, $(a_1x + a_2)x \doteq f(x)$ means we use $f(x)$ to represent the polynomial $(a_1x + a_2)x$. We also fix the following notations.

Definition 1.1 *The* FLOOR FUNCTION $\lfloor x \rfloor$, *gives the largest integer less than or equal to* x.

Definition 1.2 *The* CEILING FUNCTION $\lceil x \rceil$, *gives the smallest integer greater than or equal to* x.

Definition 1.3 *The* INTEGER PART FUNCTION $[x]$ *gives the integer part of* x.

Definition 1.4 *The* GREATEST COMMON DIVISOR $(a_1, a_2, \cdots, a_n)$ *of* n *integers* a_1, a_2, $\cdots$, a_n, *where at least one of them is nonzero, is the largest positive divisor shared by all the nonzero integers of them. For example,* $(2, 6, -22) = 2$ *and* $(1, 0, 15, -3) = 1$.

Definition 1.5 *If* a *and* $b \neq 0$ *are integers, it can be proved that there exist unique integers* q *and* r, *such that* $a = qb + r$ *and* $-a/2 < r \leq a/2$. *The number* r *is called the* MODIFIED REMAINDER.

Here we give some definitions about polynomials.

Definition 1.6 *The* ROOTS *of a polynomial* $f(x)$ *are the values of* x *for which the equation* $f(x) = 0$ *is satisfied.*

Definition 1.7 *The highest power in a univariate polynomial is known as its* DEGREE, *or sometimes* ORDER. *For example, the polynomial* $P(x) = a_nx^n + \ldots + a_2x^2 + a_1x + a_0$, *where* $a_n \neq 0$, *is of degree* n, *denoted* $\deg P(x) = n$.

Definition 1.8 *A polynomial is said to be* IRREDUCIBLE *if it cannot be factored into nontrivial polynomials over the same field.*

Definition 1.9 *The* MINIMAL POLYNOMIAL *of an algebraic number ζ is the unique irreducible monic polynomial of smallest degree $f(x)$ with rational coefficients such that $f(\zeta) = 0$ and whose leading coefficient is 1.*

Note that for an algebraic number ζ, it can have lots of irreducible polynomials but it can have only one minimal polynomial. Those polynomials have the same degree.

Definition 1.10 *The characteristic polynomial of a square matrix A is the polynomial left-hand side of the characteristic equation*

$$\det(A - \xi I) = 0$$

where I is the identity matrix and ξ is the variate of the polynomial.

We give some group theory basics here.

Definition 1.11 *If G is a group, then the* TORSION ELEMENTS *Tor(G) of G (also called the* TORSION *of G) are defined to be the set of elements g in G such that $g^n = 1$ for some natural number n, where 1 is the identity element of the group G.*

Definition 1.12 *If Tor(G) consists only of the identity element, the group G is called* TORSION-FREE.

Definition 1.13 *A $\mathbb{Q}$-*AUTOMORPHISM *σ of a field $\mathbb{Q}(\zeta)$ is a bijective map $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ fixing $\mathbb{Q}$ that preserves all of $\mathbb{Q}(\zeta)$'s algebraic properties, more precisely, it is a field isomorphism fixing $\mathbb{Q}$.*

Definition 1.14 *A group G is called* FREE *if no relation exists between one of its group generators other than the relationship between an element and its inverse required as one of the defining properties of a group.*

Definition 1.15 *Let G be a free group. Then a word W in G is called* REDUCED *if it contains no part aa^{-1} for any $a \in G$.*

Definition 1.16 *The* FREE PRODUCT *$G * H$ of groups G and H is the set of elements of the form $g_1h_1g_2h_2...g_rh_r$, where $g_i \in G$ and $h_j \in H$. Here G and H have the same identity and no other relations exist between g_i and h_j.*

1.3 Background

Our group $\langle A_\alpha, B_\beta \rangle$ contains two generators. To study its structure, we need to discuss the value of α and β. To simplify this question, Chang *et al.* [7] proved the following lemma.

Lemma 1.17 *If $\alpha\beta = \gamma\delta \neq 0$, then $\langle A_\alpha, B_\beta \rangle$ and $\langle A_\gamma, B_\delta \rangle$ are isomorphic.*

Proof. It suffices to prove that $\langle A_\alpha, B_\beta \rangle \cong \langle A_\gamma, B_\delta \rangle$. We have

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

where $P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \beta \end{smallmatrix}\right)$. Hence the mapping $X \longrightarrow P^{-1}XP$ gives the required isomorphism.

□

By Lemma 1.17, two groups generated by such elements are conjugate to each other as long as they have the same value of $\tau = Trace(A_\alpha B_\beta) - 2 = \alpha\beta$.

We can easily get the trivial case,

Lemma 1.18 $\tau = Trace(A_\alpha B_\beta) - 2 = 0$ *if and only if the group $\langle A_\alpha, B_\beta \rangle$ is abelian.*

Proof. If $\tau = Trace(A_\alpha B_\beta) - 2 = \alpha\beta = 0$, we have either $\alpha = 0$ or $\beta = 0$. Now if $\alpha = 0$, then A_α is the identity matrix, group $\langle A_\alpha, B_\beta \rangle$ is $\langle B_\beta \rangle$ with only one generator. Hence, group $\langle A_\alpha, B_\beta \rangle$ is abelian. Similarly, if $\beta = 0$, we can also obtain the same result.

If the group $\langle A_\alpha, B_\beta \rangle$ is abelian, then the two words $A_\alpha B_\beta = \left(\begin{smallmatrix} 1+\alpha\beta & \alpha \\ \beta & 1 \end{smallmatrix}\right)$ and $B_\beta A_\alpha = \left(\begin{smallmatrix} 1 & \alpha \\ \beta & 1+\alpha\beta \end{smallmatrix}\right)$ are equal. Therefore, $\tau = Trace(A_\alpha B_\beta) - 2 = 0$.

□

Putting aside the trivial case, most of the work done to date on this problem has put the two generators in one of the following forms

$$A_u = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, B_u = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \tag{1.1}$$

or

$$A_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, B_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \tag{1.2}$$

or

$$A_\tau = \begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}, B_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{1.3}$$

Let $G_u = \langle A_u, B_u \rangle$, $H_\lambda = \langle A_\lambda, B_2 \rangle$ and $\Psi_\tau = \langle A_\tau, B_1 \rangle$, where people usually use G_u in the study of the non-free groups and H_λ in the study of the free groups. Now we can give the following definitions:

Definition 1.19 *A complex number u is said to be* FREE *if the multiplicative group $\langle \left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ u & 1 \end{smallmatrix}\right) \rangle$ is a free group, and* NONFREE, *otherwise.*

Definition 1.20 *A complex number λ is said to be* 2-FREE *if the multiplicative group $\langle \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right) \rangle$ is a free group, and* 2-NONFREE, *otherwise.*

Definition 1.21 *A complex number τ is said to be* 1-FREE *if the multiplicative group $\langle \left(\begin{smallmatrix} 1 & \tau \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \rangle$ is a free group, and* 1-NONFREE, *otherwise.*

Since these parameters are connected by the relations $\tau = u^2 = 2\lambda$, we conclude that α is free is equivalent to $\frac{\alpha^2}{2}$ is 2-free and α^2 is 1-free.

We can also obtain:

Lemma 1.22 *The set of u for which G_u is free is symmetric with respect to the real axis, the imaginary axis and the origin.*

Proof. Given $u \in \mathbb{C}$, such that G_u is free. Now if $G_{\bar{u}}$ is not free, we can obtain an element $W_1 \in G_{\bar{u}}$, such that

$$W_1 = B_{\bar{u}}^{m_r} A_{\bar{u}}^{n_r} \cdots B_{\bar{u}}^{m_1} A_{\bar{u}}^{n_1} = I$$

$$W_1 = B_{\bar{u}}^{m_r} A_{\bar{u}}^{n_r} \cdots B_{\bar{u}}^{m_1} A_{\bar{u}}^{n_1} = I \tag{1.4}$$

where $n_1, m_1, \cdots, n_r, m_r \in \mathbb{Z}$ and $n_1 \neq 0, m_1 \neq 0, \cdots, n_r \neq 0, m_r \neq 0$.

Since

$$B_{\bar{u}} = \begin{pmatrix} 1 & \bar{u} \\ 0 & 1 \end{pmatrix} = \overline{B_u} \qquad \text{and} \qquad A_{\bar{u}} = \begin{pmatrix} 1 & \bar{u} \\ 0 & 1 \end{pmatrix} = \overline{A_u},$$

then

$$W_1 = \overline{B_u^{m_r}} \cdot \overline{A_u^{n_r}} \cdots \overline{B_u^{m_1}} \cdot \overline{A_u^{n_1}} = \overline{B_u^{m_r} A_u^{n_r} \cdots B_u^{m_1} A_u^{n_1}}$$

From (1.4), we have

$$B_u^{m_r} A_u^{n_r} \cdots B_u^{m_1} A_u^{n_1} = \overline{W_1} = I$$

which contradicts our assumption that u is free.

Similarly, we can prove that $G_{-\bar{u}}$ is free given a free u.

Now if G_{-u} is not free, there is a word $W_2 \in G_{-u}$, such that

$$W_2 = B_{-u}^{m_r} A_{-u}^{n_r} \cdots B_{-u}^{m_1} A_{-u}^{n_1} = I \tag{1.5}$$

where $n_1, m_1, \cdots, n_r, m_r \in \mathbb{Z}$ and $n_1 \neq 0, m_1 \neq 0, \cdots, n_r \neq 0, m_r \neq 0$.

Since

$$B_{-u} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} B_u \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad A_{-u} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} A_u \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

It follows

$$\begin{aligned} W_2 &= [\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} B_u \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}]^{m_r} \cdots [\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} A_u \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}]^{n_1} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} B_u^{m_r} A_u^{n_r} \cdots B_u^{m_1} A_u^{n_1} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

By (1.5), we have

$$B_u^{m_r} A_u^{n_r} \cdots B_u^{m_1} A_u^{n_1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which contradicts the freeness of u.

□

Lemma 1.23 *The set of λ for which H_λ is free is symmetric with respect to the real axis, the imaginary axis and the origin.*

Proof. Given $\lambda \in \mathbb{C}$, such that H_λ is free. Suppose $H_{\bar{\lambda}}$ is not free, then as in the proof of Lemma 1.22, we can obtain an element $W_3 \in H_{\bar{\lambda}}$, such that

$$W_3 = B_2^{m_r} A_{\bar{\lambda}}^{n_r} \cdots B_2^{m_1} A_{\bar{\lambda}}^{n_1} = I \tag{1.6}$$

where $n_1, m_1, \cdots, n_r, m_r \in \mathbb{Z}$ and $n_1 \neq 0, m_1 \neq 0, \cdots, n_r \neq 0, m_r \neq 0$.

Then

$$B_2^{m_r} A_{\lambda}^{n_r} \cdots B_2^{m_1} A_{\lambda}^{n_1} = \overline{W_3} = I$$

contradicts our assumption of 2-free λ.

Similarly, we can prove that $H_{-\bar{\lambda}}$ and $H_{-\lambda}$ are free given a 2-free λ.

□

The following lemmas are well known:

Lemma 1.24 *If u is nonfree, then u/k is also nonfree for any nonzero integer k.*

Proof. Since u is nonfree, there must be a reduced word

$$W(u) = B_u^{m_r} A_u^{n_r} \cdots B_u^{m_1} A_u^{n_1},$$

such that $W(u) = I$. Then replace A_u by $A_{u/k}^k$ and replace B_u by $B_{u/k}^k$, we could rewrite $W(u)$ to the form $W(u) = A_{u/k}^{ka_n} B_{u/k}^{kb_n} \cdots A_{u/k}^{ka_1} B_{u/k}^{kb_1}$. Hence $W(u)$ is a reduced word of $G_{u/k}$ and $W(u) = I$. Therefore, u/k is also nonfree.

□

Lemma 1.25 *For any non-trivial $W(u) \in G_u$, by conjugation, it has only one reduced form. We can write it as $W(u) = A_u^{a_1} B_u^{b_1} \cdots A_u^{a_n} B_u^{b_n}$, where $n > 0$ and all $a_i, b_j \neq 0$. Also, the entries of $W(u)$ are polynomials in u with integer coefficients.* □

Chapter 2

Free sets

The purpose of this chapter is to find when λ is 2-free, i.e. $\sqrt{2\lambda}$ is free.

Brenner [6] showed that H_λ is free for $|\lambda| \geq 2$.

Chang, Jennings and Ree [7] derived the freeness of H_λ for λ lying outside three open discs of radius 1 with centers $(-1, 0)$, $(0, 0)$ and $(1, 0)$ respectively (See Figure 2.1, page 14). In [7], it is proved that free algebraic numbers and 2-free algebraic numbers are dense in the complex plane.

Lyndon and Ullman [27] extend the results by showing that H_λ is free for $\lambda \notin K$, where K is the interior of the convex hull of the set consisting of the unit circle together with the points $z = \pm 2$ (See Figure 2.2, page 17). They also showed the freeness of H_λ for λ satisfying $|\lambda \pm \frac{1}{2}i| \geq \frac{1}{2}$ and $|\lambda \pm 1| \geq 1$ (See Figure 2.3, page 20) and the density of algebraic 2-free points in the complex plane.

Ignatov showed in [20] the freeness of H_λ for λ lying above the arc of the circle $|z-1| = \frac{1}{2}$ when $1 \leq \Re(\lambda) < \frac{5}{4}$ and λ lying above a line passing through the point $1 + i/2$ perpendicular to a line segment joining $1 + i/2$ to the origin when $\Re(\lambda) < 1$ (See Figure 2.5, page 27). In [16], he showed that H_λ is free for $|\lambda| \geq 1$ and $|\Im(\lambda)| \geq \frac{1}{2}$ (See Figure 2.6, page 27).

We will review all of these results in this chapter. Putting them together, we finally reach an eye-shaped non-decided area. With the help of valuation theory we will give a new method to further explore the eye-shaped area.

We note that

Lemma 2.1 *Any transcendental number is 2-free.*

Proof. Suppose H_λ is not free, so there must be a non-trivial word C_r of H_λ such that

$$C_r = A_\lambda^{n_1} B_2^{m_1} \ldots A_\lambda^{n_r} B_2^{m_r} = I_2$$

where I_2 is the 2-by-2 identity matrix and the integers $n_1, \ldots, n_r$, $m_1, \ldots, m_r$ are nonzero.

Set

$$C_r = \begin{pmatrix} p_{1,r}(\lambda) & p_{2,r}(\lambda) \\ p_{3,r}(\lambda) & p_{4,r}(\lambda) \end{pmatrix}$$

where $p_{1,r}(\lambda), \ldots, p_{4,r}(\lambda)$ are polynomials with integral coefficients. While calculating $A_\lambda^{n_1} B_2^{m_1}$, we have $p_{1,1}(\lambda) = 1 + 2m_1 n_1 \lambda$, the leading term of it is $2m_1 n_1$. The entries of matrix $A_\lambda^{n_i} B_2^{m_i}$ only contain λ with the highest power 1. Therefore, for entries of C_r, the highest possible power of λ is r.

Now suppose that for some $k \in \mathbb{Z}^+$, the leading term of $p_{1,k}(\lambda)$ is $2^k m_1 \cdots m_k n_1 \cdots n_k \lambda^k$, then

$$C_{k+1} = C_k \cdot A_\lambda^{n_{k+1}} B_2^{m_{k+1}} = \begin{pmatrix} p_{1,k}(\lambda) & p_{2,k}(\lambda) \\ * & * \end{pmatrix} \cdot \begin{pmatrix} 1 + 2m_{k+1}n_{k+1}\lambda & * \\ 2m_{k+1} & * \end{pmatrix}$$

Hence, $p_{1,k+1}(\lambda) = (1 + 2m_{k+1}n_{k+1}\lambda) \cdot p_{1,k}(\lambda) + 2m_{k+1}p_{2,k}(\lambda)$. Since the highest power of λ is $k+1$ and the highest possible power of $p_{2,k}(\lambda)$ is k, the leading term is

$$\begin{aligned} &(2m_{k+1}n_{k+1}\lambda) \cdot (2^r m_1 \cdots 2^k m_1 \cdots m_k n_1 \cdots n_k \lambda^k) \\ =&2^{k+1} m_1 \cdots m_{k+1} n_1 \cdots n_{k+1} \lambda^{k+1}. \end{aligned}$$

Now we can get the conclusion that the leading term of $p_{1,r}(\lambda)$ is

$$2^r m_1 \cdots m_r n_1 \cdots n_r \lambda^r.$$

Since the integers $n_1, \ldots, n_r$, $m_1, \ldots, m_r$ are nonzero, the leading coefficient of $p_{1,r}(\lambda)$ is not zero. As λ is transcendental, nonzero polynomial of λ can not equal zero. Therefore, $p_{1,k+1}(\lambda) - 1 \neq 0$. Thus, $C_r \neq I$. From this contradiction, it follows that any transcendental number is 2-free.

□

Since λ is transcendental is equivalent to $\sqrt{2\lambda}$ being transcendental, we find that both free points and 2-free points are dense in the complex plane, since transcendental numbers are dense in the complex plane.

Hirsch in his review of [24] asked the question of which algebraic numbers u yield free groups G_u. In 1947, Sanov[36] first answered this question by showing that G_u is free for $u = 2$, and explicitly characterized the matrices representing elements of G_u. Although this answer is far from complete, Sanov provided a new way to study the free points.

In proving his result, Sanov applied a classical method formalized by Macbeath[30] directly to the action of the matrices as linear fractional transformations. This method, which has been widely used by Sanov's successors, is sometimes called "the method of combination" and is more commonly known as the "Ping-Pong" Lemma. It is stated as follows:

Lemma 2.2 *(Macbeath[30]) Let $\mathbb{A}$ and $\mathbb{B}$ be subgroups of the permutation group on an infinite set Ω, such that at least one of them has order greater than 2. Let G be the group generated by $\mathbb{A}$ and $\mathbb{B}$. Suppose that Ω contains two disjoint non-empty sets Γ and Δ such that $1 \neq A \in \mathbb{A}$ implies $A\Gamma \subseteq \Delta$ and $1 \neq B \in \mathbb{B}$ implies $B\Delta \subseteq \Gamma$. Then G is a free product of the subgroups $\mathbb{A}$ and $\mathbb{B}$.*

Proof. Suppose that $\mathbb{B}$ has order greater than 2. Assuming that G is not a free product of $\mathbb{A}$ and $\mathbb{B}$, then there must exist a $W \in G$, s.t.

$$W = A_n B_n \ldots A_1 B_1 = 1$$

where $n \geq 1$, and $1 \neq A_i \in \mathbb{A}$ and $1 \neq B_i \in \mathbb{B}$ for all i between 1 and n.

Then since $1 \neq B \in \mathbb{B}$ implies $B\Delta \subseteq \Gamma$, we have $B_1\Delta \subseteq \Gamma$. Now we want to prove $B_1\Delta \subset \Gamma$. Suppose $B_1\Delta = \Gamma$. Then

$$B_1\Gamma \cap \Gamma = B_1\Gamma \cap B_1\Delta = B_1(\Gamma \cap \Delta) = \emptyset. \tag{2.1}$$

We also know that the order of $\mathbb{B}$ is greater than 2, which means that there exists a nontrivial $B_1' \in \mathbb{B}$, such that $B_1 B_1' \neq 1$. Then

$$\emptyset \neq (B_1 B_1')\Delta \subseteq \Gamma$$

and

$$(B_1 B_1')\Delta = B_1(B_1'\Delta) \subseteq B_1\Gamma$$

Therefore

$$B_1\Gamma \cap \Gamma \supseteq (B_1 B_1')\Delta \neq \emptyset$$

which contradicts (2.1). Hence

$$B_1\Delta \subset \Gamma$$

Then since $1 \neq A \in \mathbb{A}$ implies $A\Gamma \subseteq \Delta$, we have $A_1(B_1\Delta) \subset \Delta$. By a continuation of this argument, we finally obtain $W\Delta \subset \Delta$, which implies $W \neq 1$. Therefore, G is a free product of its subgroups $\mathbb{A}$ and $\mathbb{B}$.

□

Now we can use this lemma to derive Sanov's theorem.

Theorem 2.3 *The matrices* $A_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ *and* $B_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ *over* $\mathbb{Z}$ *are a basis for a free group.*

Proof. The group $G_2 = \langle A_2, B_2 \rangle$ is a subgroup of $H = \langle A_2, J \rangle$, where $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $B_2 = JA_2J$. To show that G_2 is free, we must show that $A_2^{n_1} B_2^{m_1} \ldots A_2^{n_r} B_2^{m_r} \neq I$ provided that $r \geq 1$ and all $n_i, m_i \neq 0$. This comes to showing that $A_2^{p_1} J A_2^{p_2} \cdots J A_2^{p_n} \neq 1$ provided that $n \geq 1$ and all $p_i \neq 0$. Let H act as a group of linear fractional transformations on the Riemann sphere $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ with $A_2 z = z + 2$ and $Jz = 1/z$. Let $\Gamma = \{z : |z| < 1\}$ and $\Delta = \{z : |z| > 1\}$. Then $A_2^p \Gamma \subseteq \Delta$ for $p \neq 0$, and $J\Delta \subseteq \Gamma$. By Lemma 2.2, H is the free product of the infinite cyclic group $\langle A_2 \rangle$ and $\langle J \rangle$. The conclusion follows.

□

Beginning with the result of Sanov, arguments of this sort were refined successively by many people to show that the same conclusion holds for u in larger regions in $\bar{\mathbb{C}}$.

Brenner [6], using the same argument as Sanov's, showed that G_u is free provided that $|u| \geq 2$. However, when studying the free group, it is easier to work with the group H_λ than G_u in most of the cases. Several other people, like Chang, Jennings and Ree [7], Lyndon and Ullman [27], and Ignatov [20], using the group H_λ, gave approaches to the region of 2-free points.

In this chapter we will use the group H_λ. By using this notation, we can restate Sanov and Brenner's results in the following form

Theorem 2.4 *H_λ is free if $|\lambda| \geq 2$.* □

We will now review the works of Chang, Jennings and Ree [7], Lyndon and Ullman [27], and Ignatov [20] [21]. At the end, the author will give a new method for finding free and 2-free points.

2.1 Chang, Jennings and Ree

We adopt the following notation: For a complex number z and a matrix

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

with complex entries, we denote by $P(z)$ the number $\frac{az+b}{cz+d}$, which is a linear fractional transformation. As is well known, given another such matrix Q, we have $(QP)(z) = Q(P(z))$. If we regard a line to be a circle passing through infinity, then it can be shown that:

Lemma 2.5 *A linear fractional transformation maps circles to circles.* □

We denote by D_1 and D_2 the following subsets of the complex planes:

$$D_1 = \{z|\ |\Re(z)| < 1\}, \qquad D_2 = \{z|\ |\Re(z)| > 1\}$$

We have the following well known lemma:

Lemma 2.6 *For any $z \in D_2$, we have either*

$$|z^{-1} - \frac{1}{2}| < \frac{1}{2} \qquad or \qquad |z^{-1} + \frac{1}{2}| < \frac{1}{2}.$$

If, on the other hand,

$$|z - \frac{1}{2}| > \frac{1}{2} \qquad and \qquad |z + \frac{1}{2}| > \frac{1}{2},$$

then $z^{-1} \in D_1$. □

Then we have,

Lemma 2.7 *If a complex number λ satisfies*

$$|\lambda| \geq 1, \qquad |\lambda - 1| \geq 1, \qquad |\lambda + 1| \geq 1, \tag{2.2}$$

then $z \in D_2$ implies that $(A_\lambda^T)^n(z) \in D_1$ for all non-zero $n \in \mathbb{Z}$.

Proof. Let $z' = z^{-1} + n\lambda$. From

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

we have

$$(A_\lambda^T)^n(z) = \frac{z}{n\lambda z + 1} = (z^{-1} + n\lambda)^{-1} = (z')^{-1}$$

By Lemma 2.6, $z \in D_2$ implies that

$$|z^{-1} - \frac{1}{2}| < \frac{1}{2} \qquad \text{or} \qquad |z^{-1} + \frac{1}{2}| < \frac{1}{2}.$$

Since by (2.2), $|n\lambda| \geq 1$ and $|n\lambda + 1| \geq 1$, then from $|z^{-1} - \frac{1}{2}| < \frac{1}{2}$ we have:

$$|z' - \frac{1}{2}| = |z^{-1} + n\lambda - \frac{1}{2}| \geq |n\lambda| - |z^{-1} - \frac{1}{2}| > 1 - \frac{1}{2} = \frac{1}{2}$$

and

$$|z' + \frac{1}{2}| = |z^{-1} + n\lambda + \frac{1}{2}| \geq |n\lambda + 1| - |z^{-1} - \frac{1}{2}| > 1 - \frac{1}{2} = \frac{1}{2}.$$

Similarly, if $|z^{-1} + \frac{1}{2}| < \frac{1}{2}$, then from $|n\lambda - 1| \geq 1$, we obtain

$$|z' - \frac{1}{2}| > \frac{1}{2} \qquad \text{and} \qquad |z' + \frac{1}{2}| > \frac{1}{2}$$

Therefore by Lemma 2.6, $(A_\lambda^T)^n(z) = (z')^{-1} \in D_1$.

□

With these two lemmas, we can prove the following theorem:

Theorem 2.8 *(Chang, Jennings and Ree[7]) Let λ be a complex number lying in none of the open discs of radius 1 with centres (-1,0), (0,0), (+1,0). (See Figure 2.1) Then the group H_λ generated by*

$$A_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \textit{and} \quad B_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

is a free group, freely generated by A_λ and B_2.

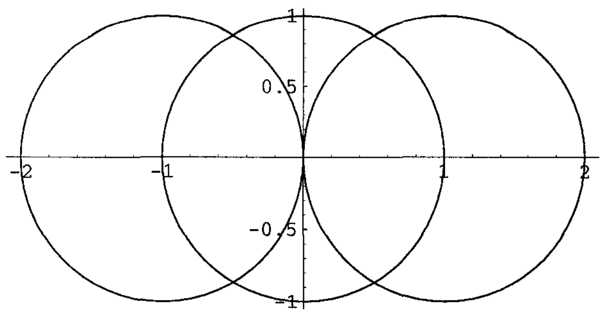

Figure 2.1: Chang, Jennings and Ree

Proof. Assume that the group H_λ with λ satisfying (2.2) is not free. Then there must be a non-trivial word C of H_λ such that

$$C = B_2^{m_1} A_\lambda^{n_1} \dots B_2^{m_r} A_\lambda^{n_r} = I_2$$

where I_2 is 2-by-2 identity matrix and $n_1, \dots, n_r$, $m_1, \dots, m_r$ are nonzero integers. Hence,

$$C = C^T = (A_\lambda^T)^{n_r} (B_2^T)^{m_r} \dots (A_\lambda^T)^{n_1} (B_2^T)^{m_1} = I_2 \tag{2.3}$$

Define the following sequences:

$$\begin{array}{ll} z_1 = (B_2^T)^{m_1}(0) = 2m_1 & z_k = (B_2^T)^{m_k}(z'_{k-1}) \\ z'_1 = (A_\lambda^T)^{n_1}(z_1) & z'_k = (A_\lambda^T)^{n_k}(z_k) \end{array} \tag{2.4}$$

for any $k \leq r-1$. Since $z_1 = 2m_1$, $|\Re(z_1)| > 1$, which means that $z_1 \in D_2$. Thus, by Lemma 2.7, we have

$$z'_1 = (A_\lambda^T)^{n_1}(z_1) \in D_1$$

By (2.4),

$$z_2 = \frac{\frac{2m_1}{2m_1 n_1 \lambda + 1} + 2m_2}{1} = z'_1 + 2m_2$$

Hence,

$$|\Re(z_2)| \geq |2m_2| - |\Re(z'_1)| > 2 - 1 = 1$$

which implies that $z_2 \in D_2$. Again by Lemma 2.7, we have

$$z'_2 = (A_\lambda^T)^{n_2}(z_2) \in D_1.$$

By repeatedly doing this, we finally obtain

$$z'_{r-1} \in D_1. \tag{2.5}$$

Define

$$y_r = (B_2^T)^{-m_r}(A_\lambda^T)^{-n_r}(0)$$

Then, by (2.3), we have

$$z'_{r-1} = y_r \tag{2.6}$$

However, on the other hand, $y_r = -2m_r$, then $|\Re(y_r)| > 2$. Thus $y_r \in D_2$, which contradicts (2.5) and (2.6). Therefore, we have proved the theorem.

□

With the result of Theorem 2.8 and the following lemma from [25]:

Lemma 2.9 *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 pth power of a rational number.* □

We can prove the following important theorem:

Theorem 2.10 *Algebraic 2-free points are dense in the complex plane.*

Proof. The theorem is equivalent to proving that for any w in the complex plane, there is a sequence of algebraic 2-free points having w as a limit.

Because of Theorem 2.8, we may assume that $w = b + ci$ (where $b, c \in \mathbb{R}$) lies in the domain excluded by Theorem 2.8. Then $|c| < 1$. Without loss of generality, we assume $b > 0$. For any positive number ε, there exist a prime number $p > 16/\varepsilon$ and an integer q such that

$$\left|\frac{q}{p} - \frac{1}{2} + \frac{\arcsin(c/4)}{2\pi}\right| < \frac{\varepsilon}{16\pi}.$$

Therefore

Therefore

$$\left|\pi - \frac{2q\pi}{p} - \arcsin(c/4)\right| < \frac{\varepsilon}{8}. \tag{2.7}$$

Since the derivative of $\sin(x)$ is a most 1, we obtain

$$\left|\sin(\frac{2q\pi}{p}) - \frac{c}{4}\right| = \left|\sin(\pi - \frac{2q\pi}{p}) - \frac{c}{4}\right| < \frac{\varepsilon}{8}$$

Then

$$\left|4\sin(\frac{2q\pi}{p}) - c\right| < \frac{\varepsilon}{2} \tag{2.8}$$

At the same time, since the derivative of 2^x in the domain $[0,1]$ is less than 1, from $p > 16/\varepsilon$, we have

$$|2^{1/p} - 1| < \frac{\varepsilon}{8}$$

Thus

$$\left|(2^{1/p} - 1)\cdot 4\sin(\frac{2q\pi}{p})\right| < \frac{\varepsilon}{2}. \tag{2.9}$$

Combining (2.8) with (2.9), we obtain

$$\left|2^{2+1/p}\sin(\frac{2q\pi}{p}) - c\right| < \left|4\sin(\frac{2q\pi}{p}) - c\right| + \left|(2^{1/p} - 1)\cdot 4\sin(\frac{2q\pi}{p})\right| < \varepsilon \tag{2.10}$$

Define

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

Then

$$\begin{aligned} |\lambda_1 - w| &= \left|b - 2^{2+1/p}\cos(\tfrac{2q\pi}{p}) + 2^{2+1/p}cos(\tfrac{2q\pi}{p}) + i2^{2+1/p}\sin(\tfrac{2q\pi}{p}) - b - ci\right| \\ &= \left|i2^{2+1/p}\sin(\tfrac{2q\pi}{p}) - ci\right| = \left|2^{2+1/p}\sin(\tfrac{2q\pi}{p}) - c\right| < \varepsilon \end{aligned} \tag{2.11}$$

Set $a = b - 2^{2+1/p}\cos(\frac{2q\pi}{p})$ and $\lambda_2 = a + 2^{2+1/p}$. Since the range of $\arcsin(x)$ is $[-\pi/2, \pi/2]$, from (2.7) we obtain that $2q\pi/p \in [\pi/2, 3\pi/2]$. Hence $\cos(2q\pi/p) < 0$ and $a = b - 2^{2+1/p}\cos(2q\pi/p) > b > 0$. Therefore $\lambda_2 > 4$, which implies that λ_2 is 2-free.

Now assume λ_1 is not 2-free. Then there must be a non-trivial word C of group H_λ which becomes the identity matrix when $\lambda = \lambda_1$. Denote our C as:

$$C = \begin{pmatrix} p_1(\lambda) & p_2(\lambda) \\ p_3(\lambda) & p_4(\lambda) \end{pmatrix}$$

then, we have

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

Since the polynomials $p_1(\lambda_1) - 1$, $p_2(\lambda_1)$, $p_3(\lambda_1)$ and $p_4(\lambda_1) - 1$ have integral coefficients uniquely determined by C and since λ_1 and λ_2 are roots of the polynomial $(x-a)^p - 2^{2p+1}$, which, by Lemma 2.9, is 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 2-free. However, this is a contradiction by Theorem 2.8. Thus, λ_1 is shown to be 2-free. Since λ_1 is algebraic and ε is an arbitrary positive numbers, w is a limit of 2-free algebraic numbers. Hence, algebraic 2-free points are dense in the complex plane.

□

2.2 Lyndon and Ullman

With the help of Lemma 2.2, Lyndon and Ullman improved Chang, Jennings and Ree's results to

Theorem 2.11 *Let K be the convex hull of the set consisting of the unit circle together with the points $z = \pm 2$. If the complex number λ is not in the interior of K, then the group H_λ is freely generated by A_λ and B_2. (See Figure 2.2)*

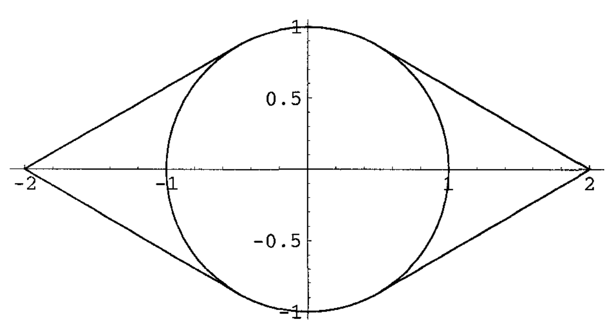

Figure 2.2: Lyndon and Ullman

Proof. Let Γ be the region bounded by the two circles C_1 and C_2 of radius $\frac{1}{2}$ with centers $\pm\frac{1}{2}$,

$$C_1 = \{z : |z - \frac{1}{2}| \leq \frac{1}{2}\} \quad \text{and} \quad C_2 = \{z : |z + \frac{1}{2}| \leq \frac{1}{2}\}, \tag{2.12}$$

and let Δ be the set of all $z \in \mathbb{C}$ such that

$$|z^{-1} - \frac{1}{2}| \geq \frac{1}{2} \qquad \text{and} \qquad |z^{-1} + \frac{1}{2}| \geq \frac{1}{2}.$$

Let λ satisfy

$$|\lambda| \geq 1, \qquad |\lambda - 1| \geq 1, \qquad |\lambda + 1| \geq 1.$$

as in (2.2). Then pick any $z \in \Gamma$ and any nonzero $n \in \mathbb{Z}$. As in the proof of Lemma 2.7, we obtain

$$|A_\lambda^n z - \frac{1}{2}| = |z + n\lambda - \frac{1}{2}| \geq |n\lambda| - |z - \frac{1}{2}| \geq 1 - \frac{1}{2} = \frac{1}{2}$$

and

$$|A_\lambda^n z + \frac{1}{2}| = |z + n\lambda + \frac{1}{2}| \geq |n\lambda + 1| - |z - \frac{1}{2}| \geq 1 - \frac{1}{2} = \frac{1}{2}$$

Therefore, $JA_\lambda^n\Gamma \subseteq \Delta$, where $J = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and

$$A_\lambda^n \Gamma \cap \Gamma = \emptyset \tag{2.13}$$

for all $n \neq 0$. For arbitrary $u \neq 0$, define

$$U = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}$$

and let

$$\Gamma^* = U\Gamma \qquad \text{and} \qquad A_\lambda^* = UA_\lambda U^{-1} = \begin{pmatrix} 1 & u\lambda \\ 0 & 1 \end{pmatrix}$$

It follows from (2.13) that

$$(A_\lambda^*)^n \Gamma^* \cap \Gamma^* = \emptyset \text{ for all } n \neq 0. \tag{2.14}$$

Now let Δ^* be the interior of the complement of $J\Gamma^*$. As in the proof of Lemma 2.2, we obtain

$$(A_\lambda^*)^n \Gamma^* \subset J\Delta^* \tag{2.15}$$

Therefore Δ^* is the region

$$|(z/u)^{-1} - \frac{1}{2}| \geq \frac{1}{2} \qquad \text{and} \qquad |(z/u)^{-1} + \frac{1}{2}| \geq \frac{1}{2} \tag{2.16}$$

bounded by $L_1 = JUC_1$ and $L_2 = JUC_2$. By Lemma 2.5, we know that L_1 and L_2 are two lines. Let L be the line $\Re(z) = 1$, so $C_1 = JL$. Hence,

$L_1 = JUJ \cdot JC_1 = \left(\begin{smallmatrix} 1/u & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot JC_1$ is the line perpendicular to the line from the origin to $1/u$, and crosses that line at the point $1/u$. Similarly, L_2 is the line perpendicular to the line from the origin to $-1/u$, and crosses that line at the point $-1/u$. It follows that the two lines L_1 and L_2 are parallel.

If now we have $\Re(u) = 1$, then u is on the line JC_1. Then $JUJ \cdot u = 1$ is on the line L_1. Similarly, -1 is on the line L_2. Then since L_1 and L_2 are the boundary of Δ^*, for arbitrary $z \in \Delta^*$, we have $(B_2^T)^n z = z + 2n \notin \Delta^*$.

Therefore

$$(B_2^T)^n \Delta^* \cap \Delta^* = \{z + 2n | z \in \Delta^*\} \cap \Delta^* = \emptyset, \tag{2.17}$$

so, as in (2.15), we obtain

$$B_2^n J\Delta^* \subset \Gamma^*. \tag{2.18}$$

We claim that $\langle A_\lambda^*, B_2 \rangle$ is a free group. This is because any nonzero word W in A_λ^* and B_2 is of the form

$$W = B_2^{m_r}(A_\lambda^*)^{n_r} \dots B_2^{m_1}(A_\lambda^*)^{n_1}$$

where $n_1, m_1, \dots n_r, m_r \in \mathbb{Z}$ and $n_1 \neq 0, m_1 \neq 0, \dots n_r \neq 0, m_r \neq 0$. From (2.15) and (2.18), we have the following sequence:

$$\begin{array}{lcl} (A_\lambda^*)^{n_1}\Gamma^* & \subset & J\Delta^* \\ B_2^{m_1} J\Delta^* & \subset & \Gamma^* \\ & \dots & \\ (A_\lambda^*)^{n_r}\Gamma^* & \subset & J\Delta^* \\ B_2^{m_r} J\Delta^* & \subset & \Gamma^* \end{array}$$

Finally we have $W\Gamma^* \subset \Gamma^*$, which means W is not identity. Hence, $\langle A_\lambda^*, B_2 \rangle$ is free.

This shows that if λ satisfies (2.2), then $G_{\lambda'}$ is free for all $\lambda' = u\lambda$, where u satisfies $\Re(u) = 1$. Geometrically, this means $G_{\lambda'}$ is free for all λ' lying on the line through λ which is perpendicular to the line from the origin to λ. Hence, we complete the proof of Theorem 2.11.

□

Before Theorem 2.14, we introduce the following lemmas.

Lemma 2.12 *For $h > 0$, the circle $|z-a| = h|z-b|$ has diameter*

$$d = \left|\frac{2h(a-b)}{h^2-1}\right|. \qquad \square$$

Lemma 2.13 *Let $W = \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix}$ and p be its fixed point. Let E be a disc with p on its boundary. If for a disc D with the same center of E we have $WD \cap D = \emptyset$ and $p \notin D$, then $WE \cap E = \emptyset$.* $\square$

Then comes Theorem 2.14, which is a further improvement of Theorem 2.8.

Theorem 2.14 *Let $\lambda \in \mathbb{C}$ satisfy $|\lambda \pm \frac{1}{2}i| \geq \frac{1}{2}$ and $|\lambda \pm 1| \geq 1$. (See Figure 2.3)*

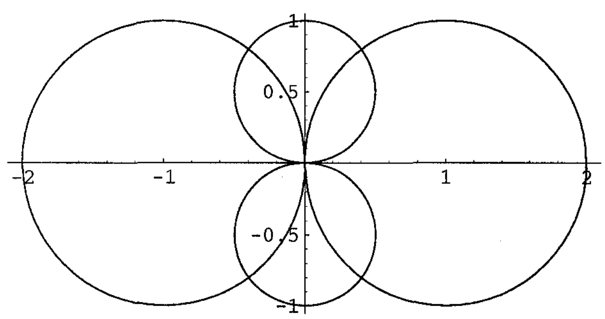

Figure 2.3: Lyndon and Ullman II

Then the group H_λ is freely generated by A_λ and B_2.

Proof. In proof of the theorem, we will use the following notation: we use A^c to denote the *interior of complement* of a set A and $\bar{A}$ to denote the *closure* of the set A.

By Lemma 1.22, the set of λ for which H_λ is free is symmetric with respect to reflection in both the real and imaginary axes. If H_λ is free, then $-\lambda$ and the conjugate of λ are also 2-free. Furthermore, the conjugate of $-\lambda$ is 2-free. Therefore we only need to discuss the situation in the first quadrant. What is more, from Theorem 2.8, we know if λ is in the area outside the circles $|\lambda \pm 1| = 1$ and $|\lambda| = 1$, then H_λ is free. Therefore, we only need to discuss

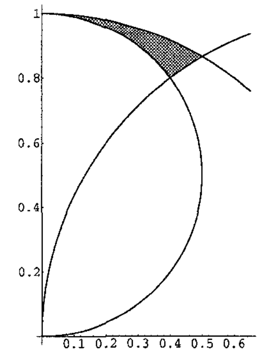

Figure 2.4: Lyndon and Ullman II(2)

the situation when λ lies inside the open curvilinear triangular region between the circle $|\lambda - 1| = 1$, $|\lambda| = 1$ and $|\lambda - \frac{1}{2}i| = 1$.

In the proof we call the shaded open curvilinear triangular region in Figure 2.4 the region F and assume that λ lies in this region. From the graph, the minimum $|\lambda|$ on $\bar{F}$ is at the point $\frac{2+4i}{5}$, which is the intersection of the circles $|\lambda| = 1$ and $|\lambda - \frac{1}{2}i| = 1$.

Let Δ be the set of z such that $|\Re(z)| < 1$. As in the proof of Theorem 2.11, we have

$$(B_2^T)^n \Delta \cap \Delta = \emptyset. \tag{2.19}$$

Therefore

$$B_2^n J\Delta \subset \Gamma = J\Delta^c. \tag{2.20}$$

Here, $\Gamma = J\Delta^c$ is the union of the open discs Γ_1 and Γ_2 of radius $\frac{1}{2}$ with centers at $-\frac{1}{2}$ and $+\frac{1}{2}$ respectively.

Since the minimum $|\lambda|$ on $\bar{F}$ is at the point $\frac{2+4i}{5}$ and our region F is inside the unit disc, we have

$$1 > |\lambda| > \frac{2\sqrt{5}}{5} > \frac{1}{2}$$

which means that if $|k| \geq 2$, then the distance between the centers of the two open discs $A_\lambda^k \Gamma_i$ and Γ_i is $|k\lambda| > 1$. Thus

$$A_\lambda^k \Gamma_1 \cap \Gamma_1 = \emptyset \qquad \text{and} \qquad A_\lambda^k \Gamma_2 \cap \Gamma_2 = \emptyset \tag{2.21}$$

for $|k| \geq 2$.

Now $\lambda \in F$ implies that $|\lambda - 1| > 1$. We also note that the imaginary part of λ is greater than 4/5 and the real part of λ is greater than 0. Hence, if $|k| \geq 2$, then $|k\lambda - 1| \geq |\Im(k\lambda)| \geq 8/5 > 1$. If $k = -1$, then $|k\lambda - 1| = |-\Re(\lambda) - i\Im(\lambda) - 1| > |\Re(\lambda) + i\Im(\lambda) - 1| = |\lambda - 1| > 1$. Therefore, $|k\lambda - 1| > 1$ for all $k \neq 0$, which means that for $k \neq 0$, the distance between the centers of the two open discs $A_\lambda^k \Gamma_1$ and Γ_2 is $|k\lambda - 1| > 1$. Similarly, the distance between centers of the other two open discs $A_\lambda^k \Gamma_2$ and Γ_1 is also $|k\lambda - 1| > 1$. Hence

$$A_\lambda^k \Gamma_1 \cap \Gamma_2 = \emptyset \qquad \text{and} \qquad A_\lambda^k \Gamma_2 \cap \Gamma_1 = \emptyset \tag{2.22}$$

for $k \neq 0$.

Hence, from (2.21) and (2.22), if we delete the closures of $\Gamma_1 \cap A_\lambda^{-1}\Gamma_1$ and $\Gamma_2 \cap A_\lambda \Gamma_2$ from Γ, the remaining set, say Γ', satisfies

$$(A_\lambda)^n \Gamma' \cap \Gamma = \emptyset \tag{2.23}$$

for all $n \neq 0$, which implies

$$(A_\lambda)^n \Gamma' \subset J\Delta. \tag{2.24}$$

Define $\Delta' = J(\Gamma')^c$, so

$$\Delta' = J(\Gamma')^c = \Delta \cup JA_\lambda^{-1}\Gamma_1 \cup JA_\lambda \Gamma_2.$$

Since $\lambda \in F$, then $A_\lambda \Gamma_2$ lies in the first quadrant, hence $JA_\lambda\Gamma_2$ lies in the fourth quadrant. Similarly, $JA_\lambda^{-1}\Gamma_1$ lies in the second quadrant. Therefore, $JA_\lambda^{-1}\Gamma_1$ and $JA_\lambda\Gamma_2$ are symmetric with respect to the origin and

$$JA_\lambda^{-1}\Gamma_1 \cap JA_\lambda\Gamma_2 = \emptyset.$$

We set $v = \lambda + \frac{1}{2}$, so the boundary of the disc $A_\lambda\Gamma_2$ is the circle C: $|z - v| = \frac{1}{2}$. Then the boundary of $JA_\lambda\Gamma_2$ is JC, which is $|z^{-1} - v| = \frac{1}{2}$. We can simplify JC to the form $|z| = 2|v| \cdot |z - \frac{1}{v}|$. Hence, by Lemma 2.12, the diameter of JC is

$$d = \left| \frac{4}{4|v^2| - 1} \right|. \tag{2.25}$$

By assumption, $\Re(\lambda) > 0$, so from $v = \lambda + \frac{1}{2}$, we have $|v| > \frac{1}{2}$. Therefore, the denominator of (2.25) is positive. We know that $|\lambda| > \frac{2\sqrt{5}}{5}$, so $|\lambda|^2 > \frac{4}{5}$ and it follows that

$$|v^2| = |\lambda|^2 + \Re(\lambda) + \frac{1}{4} > \frac{4}{5} + \frac{1}{4} = \frac{21}{20}.$$

Then from (2.25), the diameter of JC, i.e. the diameter of $JA_\lambda\Gamma_2$, is less than $\frac{5}{4}$. The real part of the center of JC, i.e. the real part of $1/v$, is

$$\begin{aligned} \Re(\tfrac{1}{v}) &= \cos(\arg(\tfrac{1}{v})) \cdot |\tfrac{1}{v}| \\ &< \max_{\lambda \in F} \cos(\arg(\lambda + \tfrac{1}{2})) \cdot \sqrt{\tfrac{20}{21}} \\ &< \cos(\arg(1 + \tfrac{\sqrt{3}}{2}i) \cdot 1 \\ &= \tfrac{4}{7} < \tfrac{3}{4}. \end{aligned}$$

Therefore, the disc $JA_\lambda\Gamma_2$ lies in the region $\{z : |z| < 2\}$. Similarly, the disc $JA_\lambda^{-1}\Gamma_1$ also lies in the region $\{z : |z| < 2\}$. Therefore, for $|k| \geq 2$,

$$(B_2^T)^k JA_\lambda^{-1}\Gamma_1 \cap JA_\lambda^{-1}\Gamma_1 = \emptyset$$

and

$$(B_2^T)^k JA_\lambda\Gamma_2 \cap JA_\lambda\Gamma_2 = \emptyset.$$

Since $JA_\lambda^{-1}\Gamma_1$ and $JA_\lambda\Gamma_2$ lie in the second and the fourth quadrants respectively, we find that

$$(B_2^T)^k(JA_\lambda^{-1}\Gamma_1 \cup JA_\lambda\Gamma_2) \cap (JA_\lambda^{-1}\Gamma_1 \cup JA_\lambda\Gamma_2) = \emptyset.$$

Hence, it follows that

$$(B_2^T)^k\Delta' \cap \Delta' = \emptyset$$

for $|k| \geq 2$. Define,

$$P_1 = \Delta' \cap (B_2^T)^{-1}JA_\lambda\Gamma_2 = \Delta' \cap (B_2^T)^{-1}\Delta'$$

and

$$P_2 = \Delta' \cap B_2^T JA_\lambda^{-1}\Gamma_1 = \Delta' \cap B_2^T\Delta'.$$

Also let $\Delta'' = \Delta' - (\bar{P}_1 \cup \bar{P}_2)$ and $\Gamma'' = J(\Delta'')^c$. Thus it is sufficient to show that Δ'' satisfies

$$(B_2^T)^n\Delta'' \cap \Delta'' = \emptyset$$

and hence

$$B_2^n J\Delta'' \subset \Gamma''.$$

Now we claim that Γ'' satisfies condition

$$(A_\lambda)^n \Gamma'' \cap \Gamma'' = \emptyset \text{ for all } n \neq 0 \tag{2.26}$$

then similarly to the proof of Theorem 2.11, we can prove Theorem 2.14.

We start from the definition of Δ''. Let $D_1 = J(B_2^T)^{-1} J A_\lambda \Gamma_2$ and $D_2 = J B_2^T J A_\lambda^{-1} \Gamma_1$, so

$$\Gamma'' = \Gamma' \cup D_1 \cup D_2.$$

Define $\Gamma_1'' = \Gamma_1' \cup D_1$ and $\Gamma_2'' = \Gamma_2' \cup D_2$, then

$$\Gamma'' = \Gamma_1'' \cup \Gamma_2''.$$

We know already that

$$A_\lambda^{-1} \Gamma' \cap \Gamma' = \emptyset$$

for $k \neq 0$, so to prove (2.26), it is sufficient to show that D_1 and D_2 are disjoint from $A_\lambda^k \Gamma''$ for $k \neq 0$. By symmetry, it is enough to show that D_1 is disjoint from $A_\lambda^k \Gamma''$ for $k \neq 0$. Since $A_\lambda^k \Gamma''$ lies in the lower half plane when $k < 0$ and D_1 lies in the upper half plane, then $A_\lambda^k \Gamma''$ and D_1 are disjoint in this case. It remains to show D_1 is disjoint from $A_\lambda^k \Gamma''$ for $k > 0$.

We have already proved that $J A_\lambda \Gamma_2$ lies in the intersection of the fourth quadrant and the region $\{z : |z| < 2\}$. Therefore $(B_2^T)^{-1} J A_\lambda \Gamma_2$ is in the third quadrant. Finally, $D_1 = J(B_2^T)^{-1} J A_\lambda \Gamma_2$ lies in the second quadrant. By symmetry, D_2 lies in the fourth quadrant. Since Γ_2', as a subset of Γ_2, lies in the right half plane, so does $\Gamma_2'' = \Gamma_2' \cup D_2$. Therefore, it is easily verified that $A_\lambda^k \Gamma_2''$ lies in the right half plane for all $k > 0$. Thus

$$D_1 \cap A_\lambda^k \Gamma_2'' = \emptyset$$

for all $k > 0$. Then the last thing we need to show is that

$$D_1 \cap A_\lambda^k \Gamma_1'' = \emptyset$$

for all $k > 0$. Since $\Gamma_1'' = \Gamma_1' \cup D_1$ and $\Gamma_1' \in \Gamma_1$, we can split the question into showing that $D_1 \cap A_\lambda^k \Gamma_1 = \emptyset$ and $D_1 \cap A_\lambda^k D_1 = \emptyset$ for all $k > 0$. We begin by showing that

$$D_1 \cap A_\lambda \Gamma_1 = \emptyset. \tag{2.27}$$

Setting

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad W = JU^{-2}JU = \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix},$$

We have $B_2^T = U^2$, $A_\lambda \Gamma_2 = U A_\lambda \Gamma_1$, and $D_1 = JU^{-2}JUA_\lambda\Gamma_1 = WA_\lambda\Gamma_1$. Then the equation (2.27) turns out to be

$$WA_\lambda \Gamma_1 \cap A_\lambda \Gamma_1 = \emptyset. \tag{2.28}$$

It is easy to check that the linear fractional transformation W has the two fixed points $p = \frac{-1+i}{2}$ and $p' = \frac{-1-i}{2}$. Then $\lambda \in F$ implies that $|\lambda - \frac{1}{2}i| > \frac{1}{2}$, so p does not lie in $A_\lambda\Gamma_1$ because $A_\lambda\Gamma_1$ has center $\lambda - \frac{1}{2}$ and radius $\frac{1}{2}$. Let E be the disc with center $\lambda - \frac{1}{2}$, the same center as $A_\lambda\Gamma_1$ and with p on its boundary B. Then by Lemma 2.13, it is sufficient to show that $WE \cap E = \emptyset$.

Since W is a non-Euclidean half turn about p, B and WB are externally tangent at p, from E finite region, it suffices to show that WE is the finite region bounded by WB. Since $\Im(\lambda) > \frac{1}{2}$, the center $\lambda - \frac{1}{2}$ of E lies above the horizontal line through p, and therefore is nearer to p, on its boundary, than to $-\frac{1}{2}$, Thus $-\frac{1}{2}$ is not in E, and $W(-\frac{1}{2}) = \infty$ is not in WE.

Thus, it suffices to observe that $A_\lambda\Gamma_1$ lies above the common tangent line H separating E from WE. Since $\Im(\lambda) > 0$, then $A_\lambda^k\Gamma_1$ lies above H for all $k \geq 1$, while $D_1 \subset WE$ lies below H. Therefore, we have

$$D_1 \cap A_\lambda^k \Gamma_1 = \emptyset$$

for $k > 1$.

Therefore, to complete the proof, we only need to show that $D_1 \cap A_\lambda^k D_1 = \emptyset$ for $k = 1$, which is equivalent to showing that D_1 has diameter $d < |\lambda|$. From the fact that $D_1 = J(B_2^T)^{-1}JA_\lambda\Gamma_2$ and our knowledge of $A_\lambda\Gamma_2$, we conclude that the boundary of D_1 has an equation of the form

$$|z + \frac{1}{2}| = 2|\lambda| \cdot |z + \frac{1}{2} + \frac{1}{4}\lambda|.$$

Now (2.25) shows that $d = \frac{1}{|4r^2-1|}$, where $r = |\lambda|$. Since $r > \frac{1}{2}$, we have $d = \frac{1}{4r^2-1}$, and the condition $d > r$ is equivalent to $1 < 4r^3 - r$, or that $f(r) = 4r^3 - r - 1$ be positive. Since $\frac{2\sqrt{5}}{5} < r < 1$, we can obtain this conclusion and so

$$D_1 \cap A_\lambda^k \Gamma_1 = \emptyset$$

for $k = 1$. Hence, we finally have proved that the two disjoint region Δ'' and $J\Gamma''$ satisfy

$$A_\lambda^k \Gamma'' \subseteq J\Delta'' \qquad \text{and} \qquad B_2^n J\Delta'' \subseteq \Gamma''$$

for any nonzero k and n and any $\lambda \in F$.

Therefore, by Lemma 2.2, H_λ is free for all λ in area F .

□

2.3 Ignatov

Since our 2-free points are symmetric in the complex plane, we only discuss the domain in the first quadrant. In Y.A.Ignatov's paper [15], he proves the following theorem:

Theorem 2.15 *Let λ be a complex number lying (considering the symmetry) above the arc of the circumference $|z-1| = \frac{1}{2}$ when $1 \leq \Re(\lambda) < \frac{5}{4}$, or lying above a line passing through the point $1 + i/2$ perpendicular to a line segment joining $1 + i/2$ to the origin when $\Re(\lambda) < 1$. Then λ is 2-free. (See Figure 2.5)* □

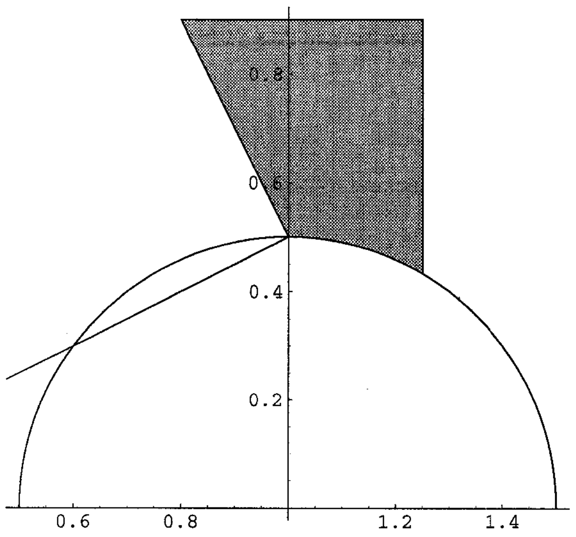

Figure 2.5: Ignatov I

In [16], he showed

Theorem 2.16 *Let λ be a complex number satisfying $|\lambda| \geq 1$ and $|\Im(\lambda)| \geq \frac{1}{2}$ Then λ is 2-free. (See Figure 2.6)* □

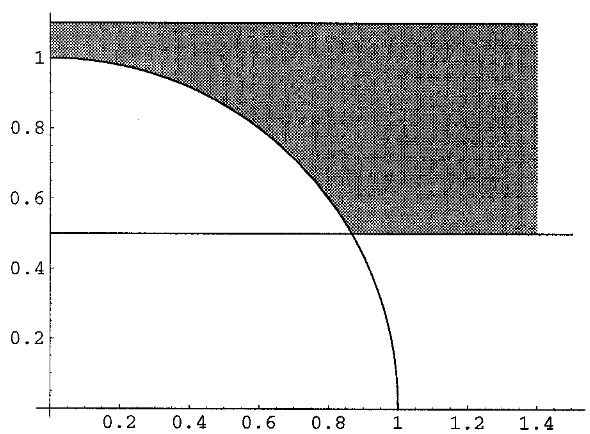

Figure 2.6: Ignatov II

2.4 New method to find free and 2-free points

By now, the shape of 2-nonfree area in the complex plane looks like an eye, so some author (Bamberg in [2], Ignatov in [29] and [19]) called this problem "the eye problem". We know from Theorem 2.10 that algebraic 2-free points are dense in the complex plane and found a set of 2-free points in the eye-shaped area of the form

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

where p is a prime number, q is an integer, a is a rational number such that $\lambda_2 = a + 2^{2+1/p}$ is greater than 4.

However, this may not be the only sets of 2-free points in the eye-shaped area and may not be the only way to find such points. In the rest of this chapter, we will provide another way to find 2-free points in the eye-shaped area.

Before we start, we should introduce several definitions:

Definition 2.17 *Let F be a field. An* ABSOLUTE VALUE *on F is a real-valued function $a \to |a|$ defined on F which satisfies the following conditions:*
i) $|a| \geq 0$ for all $a \in F$ and $|a| = 0$ iff $a = 0$;
ii) $|ab| = |a||b|$ for all $a, b \in F$;
iii) $|a + b| \leq |a| + |b|$ for all $a, b \in F$.

Definition 2.18 *An absolute value $|.|$ on F is called* NON-ARCHIMEDEAN *if*

$$|a + b| \leq max\{|a|, |b|\}$$

for all $a, b \in F$.

Definition 2.19 *Let $|.|$ be a non-Archimedean absolute value on F. We define an extended real-valued function V on F as follows: let $c \in \mathbb{R}$ and $c > 1$ and set*

$$V(a) = -log_c|a|$$

for all $a \in F$. Then V satisfies
i) $V(0) = \infty$ and $V(a) = \infty$ only if $a = 0$;

ii) $V(ab) = V(a) + V(b)$ *for all* $a, b \in F$*;*

iii) $V(a + b) \geq min\{V(a), V(b)\}|$ *for all* $a, b \in F$.

The function V *induces an isomorphism from* F *onto a subgroup of the additive group of real numbers. If the subgroup is discrete, we say* V *is a* DISCRETE VALUATION.

It follows that

Lemma 2.20 *Let* F *be a field. If* V *is a discrete valuation on* F *and if* $V(a) \neq V(b)$ *for* $a, b \in F$*, then*

$$V(a + b) = min\{V(a), V(b)\}$$

Proof. Without loss of generality, suppose

$$V(a) < V(b). \tag{2.29}$$

Then $V(a + b) \geq V(a)$, which implies that

$$V(a) = V(a + b - b) \geq min\{V(a + b), V(b)\}$$

If now we have $V(b) < V(a + b)$, then $V(a) \geq V(b)$, which contradicts (2.29). Therefore we must have $V(a + b) \leq V(b)$, so $V(a) \geq min\{V(a + b), V(b)\} = V(a + b)$. While at the same time $V(a + b) \geq V(a)$, we have $V(a + b) = min\{V(a), V(b)\}$.

□

To construct the method to find 2-free points in the eye-shaped area, we also require a number of preliminary lemmas. In the book by Weiss, the author proved the following lemma:

Lemma 2.21 *Let* V *be a discrete valuation on a field* F. *Let* $a_0, \cdots, a_n \in F$*, where* $a_0 a_n \neq 0$. *Put* $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. *Plot the points* $(i, V(a_i))$ *for* $i = 0, \cdots, n$ *and* $V(a_i) < \infty$ *on the complex plane. Then if the line segment joining* $(i, V(a_i))$ *to* $(j, V(a_j))$ *is an edge of* $G(f)$ *and has slope* $-m$*, then* f *has* $j - i$ *roots of valuation* m.

In [37], an important lemma is given by

Lemma 2.22 *Let F be a field and let $n \geq 2$ be an integer. Fix a set e_{ij} of n^2 matrix units in $R = F^{n\times n}$. Let v be a non-trivial discrete valuation on F. Consider the following subsets of R:*

$$V = V_v = \{diag(r_i) \in GL_n(F) : \text{ the set } \{v(r_i)\} \text{ has a unique minimum value } \}$$

and

$$T = T_v = \{\sum_{i,j} t_{ij}e_{ij} : \text{ the value } \{v(t_{ij})\} \text{ is finite and independent of } i \text{ and } j \}.$$

Then

(i) $TVT \subseteq T$

(ii) TV and VT are sub-semigroups of R, neither of which contains a scalar matrix.

Proof. For $w = diag(w_i) \in V$, write $v(w) = min\{v(w_i)\}$. For $t = \sum_{i,j} t_{ij}e_{ij} \in T$, write $v(t) = v(t_{ij})$. Similarly, for $t' = \sum_{i,j} t'_{ij}e_{ij} \in T$, we have $v(t') = v(t'_{ij})$. Then for any i, j, we have $(twt')_{ij} = \sum_{m,n} t_{im}w_{mn}t'_{nj} = \sum_m t_{im}w_m t'_{mj}$. Now, as every m occurs in the sum for $(twt')_{ij}$, we have

$$v((twt')_{ij}) = v(\sum_{m,n} t_{im}w_{mn}t'_{nj}) = v(\sum_{m} t_{im}w_m t'_{mj}).$$

Now for a fixed m, we have $v(t_{im}w_m t'_{mj}) = v(t) + v(w_m) + v(t')$. Then because the set $\{v(w_i)\}$ for $1 \leq i \leq t$ has a unique minimum value, from Lemma 2.20 it follows that

$$\begin{aligned} v((twt')_{ij}) &= \min_m\{v(t) + v(w_m) + v(t')\} = v(t) + \min_m\{v(w_m)\} + v(t') \\ &= v(t) + v(w) + v(t'). \end{aligned}$$

By definition, this means that $twt' \in T$. So (i) is established. It follows that $(TV)(TV) = (TVT)V \subseteq TV$ and $(VT)(VT) = V(TVT) \subseteq VT$, which means TV and VT are sub-semigroups of R. Since we have $(wt)_{ij} = \sum_m w_{im}t_{mj} = w_i t_{ij} \neq 0$ for any i, j, neither of TV and VT contains a scalar matrix. Hence, (ii) is proved.

□

By this lemma, it follows that $V * T$ is a free product of sets. This allow us to provide a way to find 2-free points in the eye-shaped area.

Theorem 2.23 *Given a set of generators* $\{C_1, C_2\}$ *of the multiplicative group of linear transformation* $H_\lambda = \langle A_\lambda, B_2 \rangle$*, construct matrices* P_1 *and* P_2 *that diagonalize* C_1 *and* C_2 *respectively:*

$$V_1 = P_1^{-1} C_1 P_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \quad V_2 = P_2^{-1} C_2 P_2 = \begin{pmatrix} \lambda_3 & 0 \\ 0 & \lambda_4 \end{pmatrix}$$

Let

$$T_0 = P_2^{-1} P_1 = \begin{pmatrix} \xi_1 & \xi_2 \\ \xi_3 & \xi_4 \end{pmatrix}$$

If now we have a discrete valuation v *such that* $v(Trace(C_1)) < 0$, $v(Trace(C_2)) < 0$ *and* $v(\xi_1) = v(\xi_2) = v(\xi_3) = v(\xi_4) = 0$*, then* H_λ *is freely generated by* A_λ *and* B_2.

Proof. Using the definition of V and T in Lemma 2.22, we have $T_0 \in T$. If we can show that $V_1, V_2 \in V$, then by Lemma 2.22, $\langle V_1, T_0^{-1} V_2 T_0 \rangle$ is a free set generated by a subgroup of V and T.

To show $V_1 \in V$, we need to prove the discrete valuation v separates λ_1 and λ_2. Since $v(Trace(C_1)) < 0$, we have $v(\lambda_1 + \lambda_2) = v(Trace(C_1)) < 0$. By definition of discrete valuation, we know $0 > v(\lambda_1 + \lambda_2) \geq min\{v(\lambda_1), v(\lambda_2)\}$. Therefore, a least one of the valuation of λ_1 and λ_2 has negative value. In the same time $H_\lambda \subset SL_2(\mathbb{C})$ implies $det(V_1) = 1$, which means $v(\lambda_1) + v(\lambda_2) = v(\lambda_1 \lambda_2) = v(1) = 0$. Hence, one of $v(\lambda_1)$ and $v(\lambda_2)$ is negative and the other one is positive. It follows that v separates λ_1 and λ_2. Similarly, v separates λ_3 and λ_4. Then, $V_1, V_2 \in V$. Therefore, $\langle V_1, T_0^{-1} V_2 T_0 \rangle$ is a free set generated by the subgroup of V and T. But $\langle V_1, T_0^{-1} V_2 T_0 \rangle = \langle V_1, P_1^{-1} P_2 V_2 P_2^{-1} P_1 \rangle$ is conjugate to $\langle P_1 V_1 P_1^{-1}, P_1 T_0^{-1} V_2 T_0 P_1^{-1} \rangle = \langle P_1 V_1 P_1^{-1}, P_2 V_2 P_2^{-1} \rangle = \langle C_1, C_2 \rangle$, which is the basis of H_λ. Therefore, H_λ is free.

□

Remark 2.24 *When using the above method, we can use Lemma 2.21 to get the valuation of* ξ_i *for* $i = 1, 2, 3, 4$*. We already know that* $v(Trace(C_1)) < 0$

implies $v(\lambda_1) \neq v(\lambda_2)$. *However, the two statements are actually equivalent. If* $v(\lambda_1) \neq v(\lambda_2)$ *is true, since* $v(\lambda_1)+v(\lambda_2) = 0$, *without loss of generality, we can suppose* $v(\lambda_1) < 0$. *Then* $v(Trace(C_1)) = v(\lambda_2 + \lambda_1) = min\{v(\lambda_2), v(\lambda_2)\} = v(\lambda_1) < 0$.

Remark 2.25 *This method can also be used to find free points.*

Although we have this method, to find a proper pair of C_1 and C_2 is still a big problem. Firstly, the original two matrices A_λ and B_2 are not suitable. Both matrices have trace 2, which makes the valuation greater than or equal to zero. Let us fix $n \in \mathbb{Z}^+$ and $A_\lambda B_2^n$ as C_1 and $A_\lambda B_2^{n+1}$ as C_2. Clearly, these two matrices constitute a basis of H_λ.

Now, we have $Trace(C_1) = 2(1+n\lambda)$ and $Trace(C_2) = 2(1+(n+1)\lambda)$. Use Mathematica to compute the matrix T_0, we obtain the minimal polynomial of ξ_1, ξ_2, ξ_3 and ξ_4 in $\mathbb{Q}(\lambda)$:

$$\frac{1}{2[2n + n(n+1)\lambda]}x^2 + x - 1. \tag{2.30}$$

By Lemma 2.21, if $v(\xi_1) = v(\xi_2) = v(\xi_3) = v(\xi_4) = 0$, the coefficient of (2.30) will have the same valuation, so the valuation of $2[2n+n(n+1)\lambda]$ will be zero.

Now if $v(Trace(C_1)) < 0$, since $v(2) \geq 0$, we have $v[2(1+n\lambda)] = min\{v(2), v(2n\lambda)\} = v(2n\lambda) < 0$, which means $v(2)+v(n)+v(\lambda) < 0$. If $v(Trace(C_2)) < 0$, similarly, we can get $v[2(1 + (n+1)\lambda)] = v[2(n+1)\lambda] < 0$, hence $v(2) + v(n+1) + v(\lambda) < 0$. Since $(n, n+1) = 1$, it follows that either $v(n) = 0$ or $v(n+1) = 0$. Without loss of generality, we say $v(n+1) = 0$, then it follows that

$$v[2n(n+1)\lambda] = v(n+1) + v(2n\lambda) = v(2n\lambda) < 0$$

However, we know $v(4n) > 0$

$$\begin{aligned} v(2[2n + n(n+1)\lambda]) &= v(4n + 2n(n+1)\lambda) \\ &\geq min\{v(4n), v[2n(n+1)\lambda]\} \\ &= v[2n(n+1)\lambda] < 0 \end{aligned}$$

Hence, we get the contradiction. Then the method does not work for the easiest form $C_1 = A_\lambda B_2^n$ and $C_2 = A_\lambda B_2^{n+1}$.

Chapter 3

NonFree sets

Now we know the region of some 2-free points. It is natural to ask whether the rest of the complex plane is 2-nonfree or not? In this chapter, we will discuss this question.

In general, a group $G = \langle A_\alpha, B_\beta \rangle$ is free of rank 2 if and only if there is no nontrivial word $A_\alpha^{a_1} B_\beta^{b_1} \cdots A_\alpha^{a_n} B_\beta^{b_n}$ in the reduced form which gives the value 1 in G. Therefore we have

Lemma 3.1 *For $\lambda \neq 0$, H_λ is nonfree if and only if here is some sequence of nonzero integers $b_1, a_1, \cdots, b_n, a_n$, where $n > 0$, such that $A_\lambda^{a_1} B_2^{b_1} \cdots A_\lambda^{a_n} B_2^{b_n}$ is the identity matrix.* □

We will discuss the density of nonfree and 2-nonfree points in Section 3.1. Then we will give several nonfree sets in Section 3.2. Finally, we will review Farbman[11]'s result about the 1-nonfreeness of rational numbers and show that Ψ_τ is free for $|\tau| = |a/b| \leq 4$ where $(a, b) = 1$ and $a = 1, 2, 3, \cdots, 16$.

3.1 Density

In Chapter 2, we proved that any transcendental number is 2-free. Chang *et al.* [7] deduced that algebraic 2-free points are dense in the complex plane. Then comes the question of how 2-nonfree points are distributed? We are also interested in the distribution of nonfree points.

3.1.1 Density of 2-nonfree points

Before we go further, we need the following well known lemma:

Lemma 3.2 *The non-identity matrix* $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2,\mathbb{C})$ *has finite order if and only if* $Trace(M) = 2cos\theta$, *where* $\theta \neq \pm\pi$ *and* θ *is a rational multiple of* π. □

Here we introduce the notation F to represent the closure of the set of 2-nonfree points in $\mathbb{C}$. Now look at the shape of the region F. For example, we know that F is contained in the circle of radius 2, center at the origin (Theorem 2.4), that F contains the circle of radius 1/2, center at the origin (Corollary 3.4), that F is connected (Theorem 3.5), and F contains various known line segment.

In Ree's paper [35], he proved the following theorem:

Theorem 3.3 *Given any* $T \in H_\lambda = \langle A_\lambda, B_2 \rangle$, *then* T *is of the form*

$$T = \begin{pmatrix} a(\lambda) & b(\lambda) \\ c(\lambda) & d(\lambda) \end{pmatrix}$$

where $a(\lambda), b(\lambda), c(\lambda), d(\lambda)$ *are polynomials in* λ. *If* $c(\lambda)$ *is not identically zero, then 2-nonfree points are densely distributed in the domain defined by* $|\lambda \cdot c(\lambda)| < 1$.

Proof. The proof consists in showing that, for a dense set of values of λ in the described domain, a certain group commutator has finite order. Let $T' = [A_\lambda, T] = A_\lambda T A_\lambda^{-1} T^{-1}$. Now we can calculate the entries of T'.

Firstly,

$$A_\lambda T = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a(\lambda) & b(\lambda) \\ c(\lambda) & d(\lambda) \end{pmatrix} = \begin{pmatrix} a(\lambda) + \lambda \cdot c(\lambda) & b(\lambda) + \lambda d(\lambda) \\ c(\lambda) & d(\lambda) \end{pmatrix}$$

and

$$A_\lambda^{-1} T^{-1} = \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} d(\lambda) & -b(\lambda) \\ -c(\lambda) & a(\lambda) \end{pmatrix} = \begin{pmatrix} d(\lambda) + \lambda \cdot c(\lambda) & -b(\lambda) - \lambda \cdot a(\lambda) \\ -c(\lambda) & a(\lambda) \end{pmatrix}.$$

Then, since $a(\lambda)d(\lambda) - b(\lambda)c(\lambda) = \det(T) = 1$, we can simplify T' to

$$T' = \begin{pmatrix} 1 + \lambda \cdot a(\lambda)c(\lambda) + \lambda^2 c^2(\lambda) & * \\ \lambda c^2(\lambda) & 1 - \lambda \cdot a(\lambda)c(\lambda) \end{pmatrix},$$

where $*$ is some complicated expression.

If we write

$$T' = \begin{pmatrix} a'(\lambda) & b'(\lambda) \\ c'(\lambda) & d'(\lambda) \end{pmatrix}$$

then

$$\lambda \cdot c'(\lambda) = \lambda^2 c^2(\lambda), \tag{3.1}$$

and the trace of T' is

$$t' = 2 + \lambda^2 c^2(\lambda) = 2 + \lambda \cdot c'(\lambda). \tag{3.2}$$

Define words $T_1, T_2, \cdots, T_n, \cdots$ inductively by $T_0 = T$ and $T_{n+1} = A_\lambda T_n A_\lambda^{-1} T_n^{-1}$. It follows from (3.1) and (3.2) that

$$t_n = Trace(T_n) = 2 + (\lambda \cdot c(\lambda))^{2^n} \tag{3.3}$$

Now take θ arbitrarily such that $0 < \theta < 2\pi$ and $\theta \neq \pi$, and let λ be any complex number satisfying

$$t_n = 2 + (\lambda \cdot c(\lambda))^{2^n} = e^{i\theta} + e^{-i\theta} = 2\cos\theta \tag{3.4}$$

for some fixed n.

Then since $\det T_n = 1$, the eigenvalues of T_n are $e^{i\theta}$ and $e^{-i\theta}$. Since $0 < \theta < 2\pi$ and $\theta \neq \pi$, we have $e^{i\theta} \neq e^{-i\theta}$. Then T_n can be diagonalized. If θ is a rational multiple of π, then T_n has finite order and hence λ is 2-nonfree.

Knowing that the rational multiples of π are densely distributed in the interval $[0, 2\pi]$, we can deduce from (3.4) that the value of $(\lambda \cdot c(\lambda))^{2^n} = t_n - 2 = 2\cos\theta - 2$ for which H_λ is not free are densely distributed in the interval $[-4, 0]$, especially in $[-1, 0]$. Since our n can be made arbitrarily large, the value of $\lambda \cdot c(\lambda)$ are dense in the region $\{x \mid x \in \mathbb{C}, |x| < 1\}$. Therefore 2-nonfree points are dense in the domain satisfying $|\lambda \cdot c(\lambda)| < 1$.

□

Now we obtain the following:

Corollary 3.4 *2-nonfree points are densely distributed in the circle* $|\lambda| < \frac{1}{2}$.

Proof. Taking $T_0 = B_2$, we have $\lambda \cdot c(\lambda) = 2\lambda$. Substituting in $|\lambda \cdot c(\lambda)| < 1$, the result follows.

□

Lyubich and Suvorov [29] give us a nice result about the 2-nonfree points:

Theorem 3.5 *The region F (the closure of the set of 2-nonfree points in $\mathbb{C}$) is a connected subset of $\mathbb{C}$.* □

In order to construct other regions where 2-nonfree points are densely distributed , we need the following set of 2-nonfree points.

Theorem 3.6 *([7], Theorem 4) Let a, b, c, d, k and h be non-zero integers such that $k > 2$ and $(k, h) = 1$. Then*

$$\lambda = \frac{-(a+c)(b+d) + [(a+c)^2(b+d)^2 - 16abcd\sin^2(h\pi/k)]^{1/2}}{4abcd} \tag{3.5}$$

is 2-nonfree.

Proof. Let $M = A_\lambda^d B_2^c A_\lambda^b B_2^a \in H_\lambda$. then direct calculation shows that:

$$\begin{aligned} Trace(M) &= 2 + 2(a+c)(b+d)\lambda \pm 4abcd\lambda^2 = 2 - 4\sin^2(h\pi/k) \\ &= 2\cos(2h\pi i/k) = e^{2h\pi i/k} + e^{-2h\pi i/k}. \end{aligned}$$

Since $\det M = 1$, it follows that the characteristic roots of M are $r_1 = e^{2h\pi i/k}$ and $r_2 = e^{-2h\pi i/k}$. Meanwhile, $k > 2$ and $(k, h) = 1$ imply that r_1 and r_2 are not equal, which implies M can be diagnoalized with diagonal elements r_1 and r_2. Therefore $M^k = I$, so H_λ is not free.

□

Corollary 3.7 *The open segment joining -2 and 2 is contained in F.*

Proof. Set $a = b = c = d = 1$ in (3.5), then $\lambda = -1 \pm \cos(h\pi/k)$. Set $a = c = 1$ and $b = d = -1$ in (3.5), we obtain $\lambda = 1 \pm \cos(h\pi/k)$. Since the numbers of the form $\cos(h\pi/k)$ are densely distributed in the segment $[-1, 1]$, it follows that 2-nonfree points are densely distributed in the segment $[-2, 0] \cup [0, 2] = [-2, 2]$.

□

Corollary 3.8 *The open segment joining $-i$ and i is contained in F.*

Proof. Set $a = b = 1$ and $c = d = -1$ in (3.5), so $\lambda = \pm i \sin(h\pi/k)$. Since the numbers of the form $\sin(h\pi/k)$ are densely distributed in the segment $[-1, 1]$, then 2-nonfree points are densely distributed in the segment $[-i, i]$.

□

3.1.2 Density of nonfree points

Now let us look at nonfree points. Let $T \in G_u = \langle A_u, B_u \rangle$ have the form

$$T = \begin{pmatrix} a(u) & b(u) \\ c(u) & d(u) \end{pmatrix}$$

where $a(u), b(u), c(u), d(u)$ are polynomials of u. Set $T' = \begin{pmatrix} a'(u) & b'(u) \\ c'(u) & d'(u) \end{pmatrix} = [A_u, T] = A_u T A_u^{-1} T^{-1}$. If $c(u)$ is not identically zero, then using the same method as in Theorem 3.3, we have:

$$u \cdot c'(u) = u^2 c^2(u) \tag{3.6}$$

and the trace of T' is

$$t' = 2 + u^2 c^2(u) = 2 + u \cdot c'(u) \tag{3.7}$$

We can extend Corollary 3.7 and Corollary 3.8 as follows:

Theorem 3.9 *([27], Theorem 5) Given a positive integer n, let u_0 be a complex number such that $u_0^{2^n} = -4$. Then the values of u that are nonfree are dense on the segment joining the origin to u_0.*

Proof. Define words $T_1, T_2, \cdots, T_n, \cdots$ inductively by $T_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T_{n+1} = [A_u, T_n] = A_u T_n A_u^{-1} T_n^{-1}$. Write $T_n = \begin{pmatrix} a_n(u) & b_n(u) \\ c_n(u) & d_n(u) \end{pmatrix}$. It follows from (3.6) and (3.7) that

$$t_n = Trace(T_n) = 2 + u c_n(u) = 2 + u^2 c_{n-1}^2(u) = 2 + (u \cdot c_0(u))^{2^n} = 2 + u^{2^n} \tag{3.8}$$

Although T_0 may not belong to G_u, our $T_1 = A_u T_0 A_u^{-1} T_0^{-1} = A_u B_u \in G_u$, so $T_n \in G_u$ for all $n \geq 1$. Now let $u = ru_0$, where $0 \leq r \leq 1$. Since $u_0^{2^n} = -4$, we have $t_n = 2 - 4r^{2^n}$. If $t_n = 2\cos\theta$, for θ a non-zero rational multiple of π between $-\pi$ and π, then as we showed before, T_n has finite order and hence u is nonfree.

Now the map carrying r into t_n maps $[0, 1]$ continuously onto $[-2, 2]$. Knowing that rational multiple of π are dense in the segment $[-\pi, \pi]$, we deduce that the values of $t_n = 2\cos\theta$ are dense in the interval $[-2, 2]$. It follows that the values of r for which G_u is not free are densely distributed in the interval $[0, 1]$, which completes the proof of the theorem.

□

Remark 3.10 *G_u is free for some extreme values of u satisfying $u^{2^n} = -4$, like $n = 1$ or $n = 2$. If $n = 1$, then $u^2 = -4$, hence $2\lambda = u^2 = -4$, so $\lambda = -2$. By Theorem 2.4, G_u is free. If $n = 2$, then $u^4 = -4$, hence $2\lambda = u^2 = \pm 2i$, so $\lambda = \pm i$. By Theorem 2.8, G_u is free. However, for larger n, this might not be true. For example, when $n = 3$, none of the 8 extreme values are nonfree. We will show this later in Theorem 3.18.*

Both Theorem 3.9 and Theorem 3.3 include Corollary 3.7 and Corollary 3.8 as a special case. We can restate the two corollaries in the u-form as follows:

Corollary 3.11 *Every number u on the segment $[-2, 2]$ and the segment $[-1-i, 1+i]$ is a limit of nonfree numbers.*

Corollary 3.12 *Let S be the set of u where G_u is not free. Then for any $u_0 \in S$, there is an open neighborhood of u_0 that lies in $\bar{S}$.*

Proof. Treat u as an indeterminate. Fix $u_0 \in S$. Then since G_u is not free, there exists a matrix $T = \begin{pmatrix} * & * \\ c_0(u) & * \end{pmatrix} \in G_u$ such that $c_0(u)$ is not identically equal to zero and $c_0(u_0) = 0$. Use this T as T_0 in Theorem 3.9. Then the trace of T_n is $t_n = 2 + (u \cdot c_0(u))^{2^n}$. Since $c_0(u_0) = 0$, it is clear that u_0 is contained in the open set $D = \{u \mid |uc_0(u)| < 1\}$.

Now we are going to show that $D \subset \bar{S}$. Pick any $u' \in D$. Then from the density of rational multiples of π, in every neighborhood of u', there is some value, say u'', and a value of n such that $t_n = 2 + (u'' \cdot c_0(u''))^{2^n} = 2\cos\theta$ for θ a rational multiples of π. Therefore, $T_n(u'')$ has finite order. Thus, $u'' \in S$ and $D \subset \bar{S}$. This completes the proof of the corollary.

□

Remark 3.13 *We note that F is the closure of 2-nonfree points and $\bar{S}$ is the closure of nonfree points. Since x is nonfree is equivalent to $x^2/2$ is 2-nonfree, we obtain $\bar{S} = \{x : x^2/2 \in F\}$.*

3.2 Nonfree Sets

We are more interested in some specific nonfree sets in the eye-shaped area. For this, we again view u as an indeterminate. By Lemma 1.25, any element of G_u is conjugate to a unique cyclically reduced form. Consider $W(u) = A_u^{a_1} B_u^{b_1} \cdots A_u^{a_n} B_u^{b_n}$, where $n > 0$ and all $a_i, b_j \neq 0$. The entries of $W(u)$ are polynomials in u with integer coefficients. Write

$$W(u) = \begin{pmatrix} 1 + f_{11}(u) & f_{12}(u) \\ f_{21}(u) & 1 + f_{22}(u) \end{pmatrix} \tag{3.9}$$

Then $A_u = I + uE_{12}$, $B_u = I + uE_{21}$, and

$$A_u^{a_1} B_u^{b_1} = \begin{pmatrix} 1 + a_1 b_1 u^2 & a_1 u \\ b_1 u & 1 \end{pmatrix}.$$

By induction, $f_{11}(u)$ and $f_{22}(u)$ are polynomials containing only even powers of u, while $f_{12}(u)$ and $f_{21}(u)$ are polynomials containg only odd powers of u. It is clear that the coefficients of $f_{ij}(u)$ (where $i, j = 1, 2$) depend on $b_1, a_1, \cdots, b_n, a_n$.

Write $f_{12}(u) = c_1 u + c_3 u^3 + \cdots + c_{2n-1} u^{2n-1}$, where each coefficient c_{2k+1} is a sum of $a_{i_1} b_{j_1} \cdots a_{i_k} b_{j_k} a_{i_{k+1}}$ for all

$$1 \leq i_1 \leq j_1 < i_2 \leq j_2 < \cdots < i_k \leq j_k < i_{k+1} \leq 2n - 1.$$

We note that the degree of $f_{12}(u)$ is $2n-1$ and its leading coefficient is $c_{2n-1} = a_1 b_1 \cdots a_{n-1} b_{n-1} a_n$. Similarly, the leading coefficients of $f_{11}(u)$ is $a_1 b_1 \cdots a_n b_n$, the leading coefficients of $f_{21}(u)$ is $b_1a_2b_2\cdots a_nb_n$ and the leading coefficients of $f_{22}(u)$ is $b_1a_2b_2\cdots a_{n-1}b_{n-1}a_n$. These are proved as in Lemma 2.1.

Theorem 3.14 *([27], Proposition 2) G_u is nonfree if and only if the complex number u is a root of some polynomial $f(x)$ in the following manner:*

$$f(x) = \sum_{k=0}^{n-1} c_{2k+1}x^{2k+1}$$

where $c_{k-1} = \sum a_{i1}b_{j1}\cdots a_{ik}b_{jk}a_{ik+1}$ and the factors are all the subsequences of the sequence $a_1, b_1, \ldots, a_n, b_n$.

Proof. Given any non-trivial reduced $W \in G_u$ which is not a power of B_u, if $f_{12}(u) = 0$ for some non-trivial $f_{12}(u)$, then we have

$$W(u) = \begin{pmatrix} a & 0 \\ c & \frac{1}{a} \end{pmatrix}$$

for some complex number a and c. Then since both $W(u)$ and B_u are lower triangular matrices, we can easily show by computation that

$$C_u = W(u)B_uW^{-1}(u) = \begin{pmatrix} a & 0 \\ c & \frac{1}{a} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{a} & 0 \\ -c & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{u}{a^2} & 1 \end{pmatrix}$$

is also a lower triangular matrix. It follows that $C_uB_u = \begin{pmatrix} 1 & 0 \\ u+\frac{u}{a^2} & 1 \end{pmatrix} = B_uC_u$, whence $[B_u, C_u] = I$. Therefore, G_u is nonfree.

If conversely G_u is nonfree, then there is a non-trivial reduced $W(u) \in G_u$ such that $W(u) = I$. It follows that u is the root of $f_{12}(u) = 0$.

We proved previously that $f_{12}(u)$ is of the form $f_{12}(u) = \sum_{k=0}^{n-1} c_{2k+1}u^{2k+1}$ where $c_{k-1} = \sum a_{i1}b_{j1}\cdots a_{ik}b_{jk}a_{ik+1}$ and the factors are all the subsequences of the sequence $a_1, b_1, \ldots, a_n, b_n$. This complete the proof.

□

We note that a zero-trace matrix $S \in G_u$ must be of the form $S = \begin{pmatrix} a & b(a^2+1) \\ -\frac{1}{b} & -a \end{pmatrix} \in G_u$, where $a, b \in \mathbb{C}$. Then $S^2 = \begin{pmatrix} -a^2+a^2+1 & 0 \\ 0 & -a^2+a^2+1 \end{pmatrix} = I$. Through this, applying the same method again, we can find the following set of nonfree points.

Corollary 3.15 *If $m \in \mathbb{Z}^+$ and u is one of the following: $\pm\sqrt{2/m}$, $\pm i\sqrt{2/m}$, $\pm\sqrt[4]{2/m}$, $\pm i\sqrt[4]{2/m}$, $\pm\frac{\sqrt{2}+i\sqrt{2}}{2}\sqrt[4]{2/m}$ or $\pm\frac{\sqrt{2}-i\sqrt{2}}{2}\sqrt[4]{2/m}$, then G_u is not free .*

Proof. Let $W = A_u^{a_1}B_u^{b_1}\cdots A_u^{a_n}B_u^{b_n}$ be a reduce non-trivial matrix as in Theorem 3.14. If $n = 1$, then $Trace(W) = 2 + a_1b_1u^2$. Then the root of $Trace(W) = 0$ is

$$u = \pm\sqrt{-\frac{2}{a_1b_1}}$$

Since a_1 and b_1 are arbitrary non-zero integers, G_u is nonfree if $u = \pm\sqrt{2/m}$ or $u = \pm i\sqrt{2/m}$. Let $n = 2$, so $Trace(W) = 2+(a_1+a_2)(b_1+b_2)u^2+a_1a_2b_1b_2u^4$. Now if $a_1 + a_2 = 0$, then the roots of $Trace(W) = 0$ are

$$u = \pm\sqrt[4]{\frac{2}{a_1^2b_1b_2}}.$$

Hence G_u is nonfree if $u = \pm i\sqrt[4]{2/m}$ or $u = \pm\sqrt[4]{2/m}$ or $u = \pm\frac{\sqrt{2}+i\sqrt{2}}{2}\sqrt[4]{2/m}$ or $u = \pm\frac{\sqrt{2}-i\sqrt{2}}{2}\sqrt[4]{2/m}$.

□

We can extend the first part of the above corollary to get a new result:

Corollary 3.16 *If u is nonfree, then so is $u' = u\sqrt{1/n}$ for any non-zero integer n.*

Proof. Let $\lambda = u^2/2$. If G_u is not free, then $H_\lambda = \langle A_\lambda, B_2\rangle = \langle A_{\lambda/n}^n, B_2\rangle$ is not free. Since H_λ is a subgroup of $H_{\lambda/n} = \langle A_{\lambda/n}, B_2\rangle$, then $H_{\lambda/n}$ is not free. Therefore, $u' = \sqrt{2\cdot(\lambda/n)} = u\sqrt{1/n}$ is not free.

□

For $W = A_u^{a_1}B_u^{b_1}A_u^{a_2}B_u^{b_3}A_u^{a_3}B_u^{b_3}$, we have the following result.

Corollary 3.17 *If $u^6 = 1$ then the points where $W = A_u^{-1}B_u^{-2}A_u^{-1}B_uA_u^2B_u$ has finite order are dense on the line segment from u to the origin. If $u^6 = -1$, then the points where $W = A_uB_u^{-2}A_uB_uA_u^{-2}B_u$ has finite order are dense on the line segment from w to the origin.*

Proof. For $W = A_u^{a_1}B_u^{b_1}A_u^{a_2}B_u^{b_3}A_u^{a_3}B_u^{b_3}$ with $a_1 + a_2 + a_3 = 0$, we have $Trace(W) = 2 - (a_2^2 b_1 b_2 + a_3^2 b_2 b_3 + a_1^2 b_1 b_2)u^4 + a_1 a_2 a_3 b_1 b_2 b_3 u^6$. To simplify this, let $a_1, a_2, b_2, b_3 = 1$ and then $a_3 = b_1 = -2$. Then, $Trace(W) = 2 + 4u^6$.

Now $Trace(W)$ ranges from -2 to 2 as u^6 ranges from -1 to the origin. Similarly, changing the sign of a_i's, we have $Trace(W) = 2 - 4u^6$, implying the density of u^6 from 1 to the origin.

□

The method indicated in Theorem 3.14 can be extended to produce additional groups G_u that are nonfree. For example, we already know (the remark after Theorem 3.9) that the values of u satisfying $u^{2^n} = -4$ are free when $n = 1$ and $n = 2$. We also mentioned that this may not be true for larger n but we did not give specific examples. Here, we use this method to prove G_u is not free for the case $n = 3$.

Theorem 3.18 *If $u = \pm\sqrt{\pm 1 \pm i}$ (i.e. $u^8 = -4$), then G_u is not free.*

Proof. First we note that the eight cases of u satisfying $u = \pm\sqrt{\pm 1 \pm i}$ are actually the eight roots of $u^8 = -4$, which is $u^{2^n} = -4$ for $n = 3$. Since $u^8 + 4 = (u^4 - 2u^2 + 2)(u^4 + 2u^2 + 2)$, four of its eight roots satisfy the equation $u^4 + 2u^2 + 2 = 0$. We show that G_u is not free for u satisfying this equation.

As in the proof of Theorem 3.9, set $T_1 = A_u B_u$, $T_2 = [A_u, T_1]$ and $T_3 = [A_u, T_2]$. Note that

$$\begin{aligned} T_3 &= [A_u, [A_u, T_1]] = [A_u, [A_u, A_u B_u]] \\ &= A_u^3 B_u A_u^{-1} B_u^{-1} A_u^{-1} B_u A_u B_u^{-1} A_u^{-2} \end{aligned}$$

is conjugate to

$$\begin{aligned} W &= A_u^{-2} T_3 A_u = A_u B_u A_u^{-1} B_u^{-1} A_u^{-1} B_u A_u B_u^{-1} = [A_u, B_u][A_u^{-1}, B_u] \\ &= \begin{pmatrix} 1 + u^2 + u^4 & -u^3 \\ u^3 & 1 - u^2 \end{pmatrix} \begin{pmatrix} 1 - u^2 + u^4 & -u^3 \\ -u^3 & 1 + u^2 \end{pmatrix} \\ &= \begin{pmatrix} * & -2u^3 - 2u^5 - u^7 \\ * & * \end{pmatrix} \end{aligned}$$

where $-2u^3 - 2u^5 - u^7 = -u^3(2 + 2u^2 + u^4) = 0$. If $W = B_u^n$ for some $n \in \mathbb{Z}^+$, then $B_u^{-n} W = I$ and G_u is nonfree. Otherwise, since both W and B_u are lower triangular, as before, we can show that $C_u = WB_uW^{-1}$ commutes with B_u, whence $[B_u, C_u] = I$. Therefore, G_u is not a free group for u satisfying $u^4 + 2u^2 + 2 = 0$.

Similarly, if u satisfies $u^4 - 2u^2 + 2 = 0$, then T_3 is conjugate to

$$\begin{aligned} W' &= (A_u^3 B_u A_u^{-1} B_u^{-1}) T_3 (A_u^3 B_u A_u^{-1} B_u^{-1}) = [A_u^{-1}, B_u][A_u, B_u] \\ &= \begin{pmatrix} 1 - u^2 + u^4 & -u^3 \\ -u^3 & 1 + u^2 \end{pmatrix} \begin{pmatrix} 1 + u^2 + u^4 & -u^3 \\ u^3 & 1 - u^2 \end{pmatrix} \\ &= \begin{pmatrix} * & -2u^3 + 2u^5 - u^7 \\ * & * \end{pmatrix} \end{aligned}$$

where $-2u^3 + 2u^5 - u^7 = -u^3(2 - 2u^2 + u^4) = 0$. Then $C'_u = W'B_uW'^{-1}$ commutes with B_u, whence G_u is not a free group for u satisfying $u^4 - 2u^2 + 2 = 0$. Therefore, none of the roots of $u^8 = -4$ is free.

□

Newman in [34] proved

Lemma 3.19 *G_u is not free if u is a q-th root of 1, for certain values of $q = 2^p$ for some $p \in \mathbb{Z}^+$.* □

After that Newman conjectured that G is not free for arbitrary values of q where u is a q-th root of 1 (i.e., $u^q = 1$), Evans in [10] proves Newman's conjecture.

Theorem 3.20 *Let u be the primitive q-th root of 1. Then G_u is nonfree.*

Proof. We define the matrices S_m recursively in the following manner. Let

$$S_1 = B_u, \qquad S_{m+1} = S_m A_u^{-1} S_m^{-1} \quad \text{for} \quad m \geq 1.$$

If we set

$$S_m = \begin{pmatrix} a_m & b_m \\ c_m & d_m \end{pmatrix}$$

then by computation

$$S_{m+1} = \begin{pmatrix} a_m & b_m \\ c_m & d_m \end{pmatrix} \begin{pmatrix} 1 & -u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d_m & -b_m \\ -c_m & a_m \end{pmatrix} = \begin{pmatrix} 1 + u a_m c_m & -u a_m^2 \\ u c_m^2 & 1 - u a_m c_m \end{pmatrix}$$

hence, by induction

$$a_m = \sum_{i=1}^{m} u^{2^m - 2^i}, \quad c_m = u^{2^m - 1}, \quad d_m = 2 - a_m \tag{3.10}$$

Now, fix m and define matrices $T_{m,n}$ recursively by:

$$T_{m,0} = S_m, \qquad T_{m,n+1} = T_{m,n} A_u T_{m,n}^{-1}$$

If we write

$$T_{m,n} = \begin{pmatrix} a_{m,n} & b_{m,n} \\ c_{m,n} & d_{m,n} \end{pmatrix},$$

then by computation, we obtain

$$a_{m,n+1} = 1 - u a_{m,n} c_{m,n}, \quad c_{m,n+1} = -u c_{m,n}^2.$$

Since we know $Trace(T_{m,n}) = Trace(A) = 2$, for $n \geq 1$, we have

$$\begin{aligned} a_{m,n} &= u^{2^{m+n}}(-\textstyle\sum_{i=1}^{m} u^{-2^i} + \sum_{i=m+1}^{m+n} u^{-2^i}) \\ &= u^{2^{m+n}}(-\textstyle\sum_{i=1}^{m} u^{-2^i} + \sum_{i=1}^{n} u^{-2^{m+i}}) \end{aligned} \tag{3.11}$$

and

$$c_{m,n} = -u^{2^{m+n}-1}, \quad d_{m,n} = 2 - a_{m,n}. \tag{3.12}$$

Now assume that u is a primitive q-th root of 1, We prove the theorem case by case.

Case 1. $q = 2^p$. Then by Lemma 3.19, G_u is not free.

Case 2. q is an odd number greater than 1. Pick $a \in \mathbb{C}$ such that $2^a = 1$ mod q. Then $u^{2^a} = u$ and $u^{2^{a+i}} = u^{2^i}$. Replace m with a and n with $a+1$, then by (3.11), we have

$$\begin{aligned} a_{m,n} &= u^{2^{2a+1}}(-\textstyle\sum_{i=1}^{a} u^{-2^i} + \sum_{i=1}^{a+1} u^{-2^{a+i}}) \\ &= u^2(-\textstyle\sum_{i=1}^{a} u^{-2^i} + \sum_{i=1}^{a+1} u^{-2^i}) \\ &= u^2(u^{-2^{a+1}}) = u^2(u^{-2}) = 1, \end{aligned}$$

and by (3.12),

$$c_{m,n} = -u^{2^{2a+1}-1} = -u^{2-1} = -u d_{m,n} = 2 - a_{m,n} = 1.$$

From $\det(T_{m,n}) = a_{m,n} d_{m,n} - b_{m,n} c_{m,n} = 1$, it is easy to obtain $b_{m,n} = 0$, whence

$$T_{m,n} = \begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix} = B_u^{-1},$$

which implies that G_u is not free.

Case 3. $q = 2^p r$ for some odd number r where $r > 1$ and $p > 1$. Pick $a \in \mathbb{C}$ such that $2^a = 1 \mod r$. Then, by (3.10), we have

$$a_p = u^{2^p} \sum_{i=1}^{p} u^{-2^i}, c_p = u^{2^p - 1}, d_p = 2 - a_p.$$

Therefore, by (3.11), we have

$$\begin{aligned} a_{p+a,a} &= u^{2^{p+2a}}(-\textstyle\sum_{i=1}^{p+a} u^{-2^i} + \sum_{i=1}^{a} u^{-2^{p+a+i}}) \\ &= u^{2^p}(-\textstyle\sum_{i=1}^{p} u^{-2^i} - \sum_{i=1}^{a} u^{-2^{p+i}} + \sum_{i=1}^{a} u^{-2^{p+i}}) \\ &= u^{2^p}(-\textstyle\sum_{i=1}^{p} u^{-2^i}) = -a_p, \end{aligned}$$

and by (3.12),

$$c_{p+a,a} = -u^{2^{p+2a}} = -u^{2^p} = -c_p d_{p+a,a} = 2 - a_{p+a,a} = d_p$$

whence

$$V = S_p^{-1} T_{p+a,a} = \begin{pmatrix} * & * \\ -c_p & a_p \end{pmatrix} \begin{pmatrix} -a_p & * \\ -c_p & * \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Then, as before, the matrix

$$W = V^{-1} A_u V = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

commutes with A_u. Therefore, G_u is not free.

□

3.3 Nonfree Rational sets

While seeking nonfree sets, many people have confined their attention to specific subsets of the complex or the real numbers. The most natural one of such subsets is the rational numbers. It is known that if $|u| \geq 2$, then u is free. By Corollary 3.7, we also know that nonfree points are dense on $(-2, 2)$.

Until now, several rational numbers have been proved to be nonfree. No rational numbers are known to be free. Hence it is quite natural to conjecture that all rational numbers within $(-2, 2)$ are nonfree.

People like Brenner *et al.*[5], Lyndon and Ullman[27] and Farbman[11] have done some work to support this conjecture. They have either found some specific nonfree rational sets, or given more general descriptions of nonfree rational sets. However, although we can not find a counterexample, the conjecture is still far from proved.

We will present some evidence supporting this conjecture. For convenience, in this section we will use the terms "1-free" and "1-nonfree". For $\tau \in \mathbb{C}$, we note that τ is 1-nonfree is equivalent to $\tau/2$ is 2-nonfree and $\sqrt{\tau}$ is nonfree. Then we can restate some previously proved results as follows:

Lemma 3.21 *The set of τ for which Ψ_τ is free is symmetric with respect to the reflection in both the real and the imaginary axes.* □

Lemma 3.22 *Any non-trivial $W(\tau) \in \Psi_\tau$ is conjugate to a unique word in reduced form. We can write $W(\tau) = A_\tau^{a_n} B_1^{b_n} \cdots A_\tau^{a_1} B_1^{b_1}$, where $n > 0$ and all $a_i, b_j \neq 0$. The entries of $W(\tau)$ are polynomials in τ with integer coefficients.* □

Lemma 3.23 *Ψ_τ is nonfree for some $\tau \neq 0$ if and only if there is some sequence of nonzero integers $b_1, a_1, \cdots, b_n, a_n$, where $n > 0$, such that*

$$A_\tau^{a_n} B_1^{b_n} \cdots A_\tau^{a_1} B_1^{b_1} = 1. \qquad \square$$

Lemma 3.24 *Ψ_τ is free if $|\tau| \geq 4$.* □

In Section 3.3.1, we will give some important results with which we can show the existence of good numerators. In Section 3.3.2, we will do some calculations to show such good numerators.

3.3.1 Good numerators

Now our conjecture turns out to be "All rational numbers in the interval $(-4, 4)$ are 1-nonfree." From now on, unless stated otherwise let $\tau = a/b$, where a and b are relatively prime nonzero integers and $|\tau| < 4$.

Definition 3.25 *An integer a is called a* GOOD NUMERATOR *if a/b is 1-nonfree for every b with $|a/b| < 4$.*

Before we start, we need to show the following lemma,

Lemma 3.26 *If τ is 1-nonfree, then τ/m is also 1-nonfree for any nonzero m.*

Proof. Since τ is 1-nonfree, there must be a reduced word $W(\tau) = A_\tau^{a_n} B_1^{b_n} \cdots A_\tau^{a_1} B_1^{b_1}$, such that $W(\tau) = I$. Substituting A_τ for $A_{\tau/m}^m$, we can rewrite $W(\tau)$ in the form $W(\tau) = A_{\tau/m}^{ma_n} B_1^{b_n} \cdots A_{\tau/m}^{ma_1} B_1^{b_1}$. Hence $W(\tau)$ is a reduced word of $\Psi_{\tau/m}$ and $W(\tau) = I$. Therefore, τ/m is also 1-nonfree.

□

There is another lemma which is particularly useful in the search for sequences as in Lemma 3.22.

Lemma 3.27 *τ is 1-nonfree if and only if there exists some $W(\tau) = A_\tau^{a_n} B_1^{b_n} \cdots A_\tau^{a_1} B_1^{b_1}$ in reduced form, where $n > 0$ and all $a_i, b_j \neq 0$, such that $W(\tau)$ is a lower triangular matrix.*

Proof. If τ is 1-nonfree, by Lemma 3.22, there is a non-identity word $W(\tau) \in \Psi_\tau$ which gives value I. This $W(\tau)$ is clearly a lower triangular matrix.

If $W(\tau)$ is a lower triangular matrix, we can write it in the form of

$$W(\tau) = \begin{pmatrix} a & 0 \\ c & \frac{1}{a} \end{pmatrix}$$

for some complex number a and c. Then since both $W(\tau)$ and B_1 are lower triangular matrices, we can easily show by computation that

$$C_\tau = W(\tau) B_1 W^{-1}(\tau) = \begin{pmatrix} a & 0 \\ c & \frac{1}{a} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & 0 \\ -c & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1}{a^2} & 1 \end{pmatrix}$$

is also a lower triangular matrix. It follows that $C_\tau B_1 = \begin{pmatrix} 1 & 0 \\ 1+\frac{1}{a^2} & 1 \end{pmatrix} = B_1 C_\tau$, whence $[B_1, C_\tau] = I$. Hence, τ is 1-nonfree. This completes the proof.

□

Using this lemma, we can now deal exclusively with one of the matrix entries. This significantly simplifies the complexity of the process. In the rest of this section, we will define an algorithm to find a sequence which will prove 1-nonfreeness.

In order to prove that Ψ_τ is free, one of the natural methods is to find a word with finite order. However, this method only works for some specific situations. For most cases, it does not work. The following theorem shows this result and the only condition where this method can work.

Theorem 3.28 *Let τ be a rational number such that $|\tau| < 4$ and $\tau = a/b$, where a, b are relatively prime integers. Then Ψ_τ has nontrivial elements of finite order if and only if $a = 1, 2$ or 3.*

Proof. Since

$$(B_1A_1^{-2})^4 = (B_1A_2^{-1})^4 = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}^4 = I_2$$

and

$$(B_1A_3^{-1})^3 = \begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}^3 = I_2,$$

we obtain that Ψ_τ has torsion if $\tau = 1, 2$ or 3. By Lemma 3.26, it immediately follows that Ψ_τ has torsion if the numerator $a = 1, 2$ or 3.

Conversely, if Ψ_τ has torsion, then there is a non-identity element $W(\tau) \in \Psi_\tau$ such that

$$W(\tau)^p = I_2 \tag{3.13}$$

for some prime number p. Then the minimum polynomial of $W(\tau)$ must divide $x^p - 1$ and hence has no multiple roots. Thus we can diagnoalize $W(\tau)$ over the complex field as

$$W(\tau) = P \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} P^{-1}$$

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

By

$$\lambda^2 - Trace(W(\tau))\lambda + det(W(\tau)) = 0,$$

we obtain

$$\begin{pmatrix} \lambda_1^2 & 0 \\ 0 & \lambda_2^2 \end{pmatrix} - Trace(W(\tau)) \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} + det(W(\tau)) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

and hence

$$P\begin{pmatrix}\lambda_1^2 & 0\\ 0 & \lambda_2^2\end{pmatrix}P^{-1} - Trace(W(\tau))P\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}P^{-1} + det(W(\tau))P\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}P^{-1} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

and finally,

$$W^2(\tau) - Trace(W(\tau)) \cdot W(\tau) + det(W(\tau)) \cdot I_2 = 0. \tag{3.14}$$

By (3.13), we have

$$W(\tau)^p = I_2 \Rightarrow (W(\tau) - I_2) \cdot \sum_{i=0}^{p-1} W(\tau)^i = 0$$

for $W(\tau)^0 = I_2$, where no factor of $W(\tau)^p - I_2$ is itself factorable.

Then by (3.14), we obtain either

$$W(\tau)^p - I_2 = W^2(\tau) - Trace(W(\tau)) \cdot W(\tau) + det(W(\tau)) \cdot I_2$$

or

$$\sum_{i=0}^{p-1} W(\tau)^i = W^2(\tau) - Trace(W(\tau)) \cdot W(\tau) + det(W(\tau)) \cdot I_2.$$

In the former case, $p = 2$ and hence $W(\tau) = -I_2$. In the latter case, $p = 3$ and then $Trace(W(\tau)) = -1$.

We can write $W(\tau)$ in the reduced form

$$W(\tau) = A_\tau^{a_n} B_1^{b_n} \cdots A_\tau^{a_1} B_1^{b_1}$$

where $n > 0$ and all $a_i, b_j \neq 0$. Then the entries of $W(\tau)$ are polynomials in τ with integer coefficients. As in (3.9), we can write

$$W(\tau) = \begin{pmatrix}1 + \tau p_{11}(\tau) & \tau p_{12}(\tau)\\ p_{21}(\tau) & 1 + \tau p_{22}(\tau)\end{pmatrix} \tag{3.15}$$

where the p_{ij}'s are elements of $\mathbb{Z}[\tau]$ dependent on the exponents a_k and b_k.

Now if $W(\tau) = -I_2$, we have $1 + \tau p_{11}(\tau) = -1$. Then τ is a rational root of a polynomial with integral coefficients whose constant term is 2, so τ has numerator 1 or 2. If, on the other hand, $Trace(W(\tau)) = -1$, then $2 + \tau(p_{11}(\tau) + p_{12}(\tau)) = -1$. Hence, τ is a rational root of a polynomial with integral coefficients whose constant term is 3, so τ has numerator 1 or 3.

□

In particular, the above theorem shows that 1, 2 and 3 are good numerators. Now we know that finding an element of finite order does not help too much in showing nonfreeness. We revert to looking for sequences as in Lemma 3.22.

Given a rational number $\tau = a/b$, where $a, b \in \mathbb{Z}$, and a sequence of nonzero integers $b_1, a_1, b_2, a_2, \cdots, b_m, a_m$, we can define the following sequence recursively:

$$\begin{aligned} x_0 &= 0 \\ y_1 &= 1 \\ &\cdots \\ y_n &= b_n x_{n-1} + y_{n-1} \\ x_n &= x_{n-1} + a_n \tau y_n. \end{aligned} \tag{3.16}$$

Then it follows that

$$h_0 = B_1^{b_1} = \begin{pmatrix} 1 & 0 \\ b_1 & 1 \end{pmatrix} = \begin{pmatrix} * & x_0 \\ * & y_1 \end{pmatrix}$$

and

$$g_n = A_\tau^{a_n} B_1^{b_n} \cdots A_\tau^{a_1} B_1^{b_1} = \begin{pmatrix} * & x_n \\ * & y_n \end{pmatrix} \tag{3.17}$$

$$h_n = B_1^{b_{n+1}} A_\tau^{a_n} B_1^{b_n} \cdots A_\tau^{a_1} B_1^{b_1} = \begin{pmatrix} * & x_n \\ * & y_{n+1} \end{pmatrix}. \tag{3.18}$$

From Lemma 3.27, to prove that τ is 1-nonfree we only need to show that there is a sequence $b_1, a_1, b_2, a_2, \cdots, b_m, a_m$ to make $x_m = 0$ for some $m \in \mathbb{Z}$.

To simplify the problem, we define

$$x'_n = b^n x_n \qquad \text{and} \qquad y'_{n+1} = b^n y_{n+1}. \tag{3.19}$$

The sequence (3.16) turns out to be:

$$\begin{aligned} x'_0 &= 0 \\ y'_1 &= 1 \\ x'_1 &= a_1 a \\ &\cdots \\ y'_n &= b_n x'_{n-1} + b y'_{n-1} \\ x'_n &= b x'_{n-1} + a a_n y'_n. \end{aligned} \tag{3.20}$$

Since $x_n = 0$ if and only if $x'_n = 0$, we still have the nonfreeness after converting the sequence. However, since x'_i and y'_j are integers, it is sufficient to concentrate on integers. The simplified sequence leads to

Theorem 3.29 *If the rational number* $\tau = \frac{a}{ar\pm 1}$, *where* $a, r \in \mathbb{Z}$ *and* $r \neq 0$, *then* τ *is 1-nonfree.*

Proof. Let $a_1 = r$ and $b_2 = -1$, then we have $x_1' = ra$ and $y_2' = a_1 b_2 a + b = -ra + ra \pm 1 = \pm 1$. Then let $a_2 = \mp \frac{bx_1'}{a} = \mp br = \mp ar^2 - r$, we obtain:

$$\begin{aligned} x_2' &= bx_1' + aa_2y_2' = ra(ra \pm 1) + a(\mp ar^2 - r)(\pm 1) \\ &= r^2a^2 \pm ra - r^2a^2 \mp ra = 0. \end{aligned}$$

Thus $x_2 = 0$ and g_2 is a lower triangular matrix. By Lemma 3.27, τ is 1-nonfree.

□

This theorem gives another way to show the 1-nonfreeness of 1, 2 and 3.

In general, given a rational number $\tau = a/b$, how can we find a proper sequence of nonzero integers $b_1, a_1, \cdots, b_n, a_n$ to make $x_n' = 0$? In the sequence (3.20), we have:

$$a|x_0' \qquad \text{and} \qquad a|x_1'.$$

Now if for some $k > 0$, we have $a|x_{k-1}'$, then since $a|aa_ky_k'$, it follows that

$$a|bx_{k-1}' + aa_ky_k' \Rightarrow a|x_k'.$$

By induction, we have $a|x_n'$ for $n \geq 0$. Now, if a and b are relatively prime, as $b|y_n'$, we have

$$(a, y_n') = 1$$

for $n > 0$. Thus

Lemma 3.30 *We can obtain* $y_n' = 0$ *only when* $a \neq \pm 1$.

We can extend the result of Theorem 3.29 to a more general form:

Lemma 3.31 *If a sequence yields* $y_n' = \pm 1$, *then* $\tau = a/b$ *is 1-nonfree.*

Proof. Since $a|x_n'$ for $n \geq 0$, then bx_{n-1}'/a is an integer. Pick $a_n = \mp bx_{n-1}'/a$, if $a_n \neq 0$, then $x_n' = bx_{n-1}' - bx_{n-1}' = 0$. If $a_n = 0$, we have $x_{n-1}' = 0$. Thus, by Lemma 3.27, $\tau = a/b$ is 1-nonfree.

□

Since our purpose is to find some $x'_i = 0$, or by Lemma 3.31, to find some $y'_j = \pm 1$, one way to construct the satisfactory sequence $b_1, a_1, \cdots, b_n, a_n$ is to choose nonzero numbers a_i and b_i that minimize the absolute values of y'_i and x'_i at each step until we get the desired number. In the rest of this paper, we call this method the "pure greedy" algorithm and the corresponding sequence $x'_0, y'_1, x'_1, \cdots$ the pure sequence.

One advantage of this method is that if $|by'_{i-1}| \geq |x'_{i-1}|/2$, in order to calculate smallest y'_i we are actually finding the modified remainder on division of by'_{i-1} by x'_{i-1}, whose absolute value is less than $|by'_{i-1}|$ and $|x'_{i-1}|$. Even if $|by'_{i-1}| < |x'_{i-1}|/2$, since we can not pick zero a_i and b_i, the element we obtain has the absolute value $|x'_{i-1}| - |by'_{i-1}|$. This value is greater than $|x'_{i-1}|/2$, whence greater than $|by'_{i-1}|$, but it is still less than $|x'_{i-1}|$. Therefore, small values of $|x'_{i-1}|$ provide small values of $|y'_i|$. Similarly, small values of $|y'_i|$ provide small values of $|x'_i|$, which is always less than $|ay'_i|$.

Thus, if $a = 1$, the absolute values of elements keep decreaseing at each step. By Lemma 3.30, we have $y'_i \neq 0$ for any $i \in \mathbb{Z}^+$. Since x'_i and y'_j are integers, we can finally reach some $x'_i = 0$ and prove that rational number $\tau = 1/b$ is 1-nonfree for nonzero integer b.

While using this algorithm, if for some $i \in \mathbb{Z}$, the adjacent elements y'_i and x'_i are not relatively prime, say $(y'_i, x'_i) = d_1 \neq 1$, we can improve the situation by substituting x'_i for $x''_i = x'_i/d_1$. By induction on the sequence (3.20), we obtain

Lemma 3.32 *$(y'_i, x'_i)|x'_j$ holds for $j \geq i$ and $(x'_i, y'_{i+1})|y'_j$ holds for $j \geq i+1$.* □

Thus x''_i is still a integer, but it is less than the original x'_i. If x'_{i-1} and y'_i are not relatively prime, say $(x'_{i-1}, y'_i) = d_2$, then similarly, replacing y'_i by $y''_i = y'_i/d_2$, we can obtain an integer y''_i which is less than the original y'_i.

Since our purpose is to find some $x'_k = 0$, we can define $x''_i = x'_i/(y'_i, x'_i)$ and $y''_i = y'_i/(x'_{i-1}, y'_i)$, then use the new sequence $x''_0, y''_1, x''_1, \cdots, y''_n, x''_n$ instead of the sequence (3.20). As $x''_k = 0$ if and only if $x'_k = 0$, the final conclusion does not change. To make a slight change of the relation in (3.20), we can define

Definition 3.33 *We call the sequence* $x''_0, y''_1, x''_1, \cdots, y''_n, x''_n$ *satisfying:*

$$\begin{aligned} x''_0 &= 0 \\ y''_1 &= 1 \\ &\cdots \\ y^*_n &= b_n x''_{n-1} + b y''_{n-1} \\ y''_n &= \frac{y^*_n}{(x''_{n-1}, y^*_n)} \\ x^*_n &= b x''_{n-1} + a a_n y''_n \\ x''_n &= \frac{x^*_n}{(y''_n, x^*_n)}. \end{aligned} \tag{3.21}$$

the MODIFIED PURE SEQUENCE *and the corresponding algorithm the* MODIFIED PURE GREEDY ALGORITHM.

In (3.21), the equation of y''_n will be the same as in (3.20) when $(x''_{n-1}, y^*_n) = 1$ and the equation of x''_n will be the same if $(y''_n, x^*_n) = 1$.

In the modified pure sequence $x''_0, y''_1, x''_1, \cdots, y''_n, x''_n$, any two adjacent elements are prime to each other. By fixing the algorithm in this way, we make the elements smaller, whence closer to our target, which speeds up the old algorithm to make it suitable for some larger a and b.

While building the new sequence, the b_i we pick to minimize y^*_i might not minimize x''_i. This is because some larger value for y^*_i might have the property that $(y''_i, x^*_i) = d_2 > 1$ and the new $x''_i = x^*_i / d_2$ might be smaller than value from the modified pure greedy algorithm. Similarly, the smallest value of y''_{i+1} might not come from the modified pure greedy algorithm, either.

To fix this problem, we further modify the modified pure greedy algorithm in the following way. Instead of using only b_i to determine the value of y^*_i, we use b_i and $b_i \pm 1$. Now we have three different values of y^*_i: $(b_i - 1)x''_{i-1} + b y''_{i-1}$, $b_i x''_{i-1} + b y''_{i-1}$ and $(b_i + 1)x''_{i-1} + b y''_{i-1}$. Let $y''_i = y^*_i / (x''_{i-1}, y^*_i)$. By (3.21), we can obtain three x^*_i's and their three corresponding x''_i's. For our new sequence, pick the y''_i that makes the absolute value of x''_i smallest and $y^*_i \neq b y''_{i-1}$. The reason why we can not have $y^*_i = b y''_{i-1}$ is that the sequence $b_1, a_1, \cdots, b_n, a_n$ is a nonzero sequence.

Definition 3.34 *We call this new sequence* RANGE-1 MODIFIED SEQUENCE *and the corresponding algorithm* RANGE-1 GREEDY ALGORITHM.

As in the modified pure sequence, the elements of range-1 modified sequence are all integers.

Similarly, if we use the $2n+1$ values $b_i, b_i \pm 1, \cdots, b_i \pm n$ to determine our y_i^*, we can extend the above "range-1 greedy" algorithm to "range-n greedy" algorithm. However, this extension is not unlimited as if n is too big, the algorithm becomes slow.

For convenience, "modified pure greedy algorithm" and "range-n greedy algorithm" will be called "*modified greedy algorithm*", "modified greedy algorithm" and "pure greedy algorithm" will be called "*greedy algorithm*". For the corresponding sequence, "modified pure sequence" and "range-n modified sequence" will be called "*modified sequence*", "pure sequence" and "modified sequence" will be called "*entry sequence*"

Then we can classify them in the following way.

<table>
<tr><td rowspan="3">greedy algorithm</td><td colspan="2">pure greedy algorithm</td></tr>
<tr><td rowspan="2">modified greedy algorithm</td><td>modified pure greedy algorithm</td></tr>
<tr><td>range-n greedy algorithm</td></tr>
<tr><td rowspan="3">entry sequence</td><td colspan="2">pure sequence</td></tr>
<tr><td rowspan="2">modified sequence</td><td>modified pure sequence</td></tr>
<tr><td>range-n modified sequence</td></tr>
</table>

In some cases, the range-n modified sequence converges even if the modified pure sequence does not. For example, for $\tau = 12/17$, the modified pure sequence repeats after step 2, but the range-1 modified sequence converges to 0 at step 4. There are also some cases in which the range-n modified sequence converges quicker than the modified one.

In some cases, even when the greedy algorithm does not end (i.e. it would never yield $x_i'' = 0$), we can still prove the 1-nonfreeness with the help of the following theorem:

Theorem 3.35 *Given $\tau = a/b \in \mathbb{Q}$, if there is some $N > 0$ and an infinite sequence of nonzero integers $b_1, a_1, \cdots, b_n, a_n$ such that in the corresponding modified sequence, $|x_i''| < N$ holds for all $i \in \mathbb{Z}^+$, then τ is 1-nonfree.*

Proof. By (3.21) we have $|y''_{i+1}| < |x''_i|$. Since $|x''_i| < N$ for all $i \in \mathbb{Z}^+$, all elements of the modified sequence $x''_0, y''_1, x''_1, \cdots, y''_n, x''_n, \cdots$ are bounded by N. Note that the modified sequence can be written in the form of $x'_0, y'_1, x'_1, \cdots,$ $\frac{x'_n}{(y'_n, x'_n)}, \frac{y'_{n+1}}{(x'_n, y'_{n+1})}, \cdots$. Then another sequence $x'_0, y'_1, x'_1, \cdots, \frac{x'_n}{(x'_n, y'_{n+1})}, \frac{y'_{n+1}}{(x'_n, y'_{n+1})},$ $\cdots$ is also bounded by N since all of its elements are less and equal to the corresponding elements in the modified sequence.

Since $\frac{x'_n}{(x'_n, y'_{n+1})}$ and $\frac{y'_{n+1}}{(x'_n, y'_{n+1})}$ are integers for all $i \in \mathbb{Z}^+$, there must be a repetition among pairs $(\frac{x'_n}{(x'_n, y'_{n+1})}, \frac{y'_{n+1}}{(x'_n, y'_{n+1})})$. Say there is a pair $(\frac{x'_i}{(x'_i, y'_{i+1})}, \frac{y'_{i+1}}{(x'_i, y'_{i+1})})$ and an integer $j > 0$ such that $\frac{x'_i}{(x'_i, y'_{i+1})} = \frac{x'_{i+j}}{(x'_{i+j}, y'_{i+j+1})}$ and $\frac{y'_{i+1}}{(x'_i, y'_{i+1})} = \frac{y'_{i+j+1}}{(x'_{i+j}, y'_{i+j+1})}$. By Lemma 3.32, we have $(x'_i, y'_{i+1}) | (x'_{i+j}, y'_{i+j+1})$, set $d = \frac{(x'_{i+j}, y'_{i+j+1})}{(x'_i, y'_{i+1})}$, then it follows

$$x'_{i+j} = dx'_i, \quad \text{and} \quad y'_{i+j+1} = dy'_{i+1}.$$

Pick $h_i = B_1^{b_{i+1}} A_\tau^{a_i} \cdots A_\tau^{a_1} B_1^{b_1}$ as in (3.18), and $h' = B_1^{b_{i+j+1}} A_\tau^{a_{i+j}} \cdots A_\tau^{a_{i+1}}$, then by (3.19), we have:

$$h_i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_i \\ y_{i+1} \end{pmatrix} = b^{-i} \begin{pmatrix} x'_i \\ y'_{i+1} \end{pmatrix},$$

$$h' h_i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_{i+j} \\ y_{i+j+1} \end{pmatrix} = db^{-i-j} \begin{pmatrix} x'_i \\ y'_{i+1} \end{pmatrix}.$$

Hence

$$h_i^{-1} h' h_i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = db^{-j} \cdot h_i^{-1} (b^{-i} \begin{pmatrix} x'_i \\ y'_{i+1} \end{pmatrix}) = db^{-j} \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{3.22}$$

It is clear that $h_i^{-1} h' h_i$ is neither of the form B_1^k nor the identity in Ψ_τ. Therefore, $h_i^{-1} h' h_i$ is a lower triangular matrix. By Lemma 3.27, τ is 1-nonfree.

□

Lemma 3.36 *If there is an infinite sequence of nonzero integers $b_1, a_1, \cdots, b_n,$ a_n such that the corresponding pure sequence is bounded for all $i \in \mathbb{Z}^+$, then τ is 1-nonfree.*

Proof. As the pure sequence is bounded, the corresponding modified pure sequence is also bounded. Then by Theorem 3.35, τ is 1-nonfree.

□

Now we have two ways to prove the 1-nonfreeness of the rational $\tau = a/b$. One is to find some $x'_i = 0$, the other one is to find the boundary of the entry sequence, then to find a pair (x'_i, y'_{i+1}) such that $x'_{i+j} = dx'_i$ and $y'_{i+j+1} = dy'_{i+1}$ for some integer d and j. The next theorem shows us the relation between the two methods and some other new 1-nonfree points, which also shows a way to extend the 1-nonfree set based on the former results.

Theorem 3.37 *Let $\tau = a/b \in \mathbb{Q}$. Given a sequence $a_1, b_2, \cdots, b_m, a_m, \cdots$ and its corresponding entry sequence $x_0, y_1, x_1, \cdots, y_m, x_m. \cdots$ such that either*

1) $x_i = 0$

or

2) $dx_i = dx_m$ and $dy_{i+1} = y_{m+1}$

holds for some integer d and some $i < m$. Let M be the integer such that $lcm\{y_i, x_i | i \leq m\} | M$. If for $r \in \mathbb{Z}$, we have $(Mr + b) \nmid M$, then $a/(Mr \pm b)$ is 1-nonfree.

Proof. Set $t = a/(Mr + b)$ and a sequence of nonzero integers $\hat{b}_1, \hat{a}_1, \cdots, \hat{b}_m, \hat{a}_m, \hat{b}_{m+1}$. Define the following sequence:

$$\begin{aligned} &\hat{x}_0 = 0 \\ &\hat{y}_1 = 1 \\ &\cdots \\ &\hat{y}_n = \hat{b}_n \hat{x}_{n-1} + (Mr + b)\hat{y}_{n-1} \\ &\hat{x}_n = (Mr + b)\hat{x}_{n-1} + a\hat{a}_n \hat{y}_n. \end{aligned} \tag{3.23}$$

If we can prove that for some i and j, $\hat{x}_i = 0$, or find a pair $(\hat{x}_i, \hat{y}_{i+1})$ such that $\hat{x}_{i+j} = d\hat{x}_i$ and $\hat{y}_{i+j+1} = d\hat{y}_{i+1}$, then the 1-nonfreeness of t follows.

By definition $\hat{x}_0 = x_0 = 0$ and $\hat{y}_1 = y_1 = 1$. Suppose for some n, we have $\hat{x}_n = x_n$ and $\hat{y}_{n+1} = y_{n+1}$. Let

$$\hat{a}_i = a_i - \frac{Mr\hat{x}_{i-1}}{a\hat{y}_i} \quad \text{and} \quad \hat{b}_{i+1} = b_{i+1} - \frac{Mr\hat{y}_i}{\hat{x}_i}.$$

Then

$$\begin{aligned} \hat{x}_{n+1} &= (Mr + b)\hat{x}_n + a\hat{a}_n \hat{y}_{n+1} \\ &= (Mr + b)x_n + a(a_{n+1} - \tfrac{Mrx_n}{ay_{n+1}})y_{n+1} \\ &= bx_n + aa_{n+1}y_{n+1} = x_{n+1} \end{aligned}$$

and

$$\begin{aligned}\hat{y}_{n+2} &= \hat{b}_{n+2}\hat{x}_{n+1} + (Mr+b)\hat{y}_{n+1} \\ &= (b_{n+2} - \tfrac{Mry_{n+1}}{x_{n+1}})x_{n+1} + (Mr+b)y_{n+1} \\ &= b_{n+2}x_{n+1} + by_{n+1} = y_{n+2}.\end{aligned}$$

Then the two sequence $\hat{x}_0, \hat{y}_1, \hat{x}_1, \cdots, \hat{y}_m, \hat{x}_m, \cdots$ and $x_0, y_1, x_1, \cdots, y_m, x_m, \cdots$ are exactly the same. Therefore t is 1-nonfree for the same reason that τ is.

Here $\hat{a}_i$ and $\hat{b}_{i+1}$ are both nonzero integers. As we showed before that $a|x_{i-1}$ for any i, so $\frac{x_{i-1}}{a}$ is a nonzero integer. By M's definition, we have $y_i|M$. Hence, $\hat{a}_i = a_i - \frac{Mr\hat{x}_{i-1}}{a\hat{y}_i}$ is a integer. If $\hat{a}_i = 0$,then $x_i = \hat{x}_i = (Mr+b)\hat{x}_{i-1} = (Mr+b)x_{i-1}$. Assume that x_{i-1} is nonzero, so from $M = lcm\{y_i, x_i | i \le m\}$, we have $x_i|M$, and hence $(Mr+b)|M$, which contradicts our hypothesis. Therefore $\hat{a}_i$ is a nonzero integer. Similarly, $\hat{b}_{i+1} = b_{i+1} - \frac{Mry_i}{x_i}$ is an integer and $\hat{b}_{i+1} \neq 0$.

From $(Mr+b) \nmid M$, it follows $(M(-r)+b) \nmid M$, then similarly, $t' = a/(M(-r)+b)$ is 1-nonfree. By Lemma 3.21, $t'' = -t' = a/(Mr-b)$ is also 1-nonfree. This completes the proof.

□

With the help of this new method, we find a way to restrict the range of range-1 modified sequence. Thus, by applying Theorem 3.35, we find a new way to show 1-nonfreeness.

Theorem 3.38 *Let $\tau = a/b$, where $b \neq \pm 1$. Define a finite set of integers $I \subset \{x \in \mathbb{Z},\ x|(b+1) \text{ or } x|(b-1)\}$. If for any positive integers k, we have $b^k \equiv i \mod a$ for some $i \in I$, then τ is 1-nonfree.*

Proof. Let $1 \in I$, then $y_1 = 1 \in I$. Choose $a_1 = 1$, we have $x_1 = a_1 a = a$. Thus, for nonzero sequence $a_1, b_2, a_2, \cdots$, we have

$$\begin{aligned}&1)\quad y_1 \equiv b^0 \mod a,\\ &2)\quad y_1 \in I,\\ &3)\quad x_1 = a.\end{aligned}$$

Now suppose for a positive integer n, we have

$$\begin{aligned}&1)\quad y_n \equiv b^k \mod a \text{ for some } k,\\ &2)\quad y_n \in I,\\ &3)\quad x_n = \pm a.\end{aligned} \tag{3.24}$$

Then by (3.20), we have

$$y_{n+1} = by_n + b_{n+1}x_n = by_n \pm ab_{n+1}.$$

Since $y_n \equiv b^k \mod a$, so $y_n b \equiv b^{k+1} \mod a$ and $y_n b \equiv i_{n+1} \mod a$ for some $i_{n+1} \in I$. Thus, we can choose b_{n+1} so that $y_{n+1} = i_{n+1} \in I$. Here $b_{n+1} \neq 0$, otherwise we will obtain $y_n b = i_{n+1}$. Then because $i_{n+1}|(b-1)$ or $i_{n+1}|(b+1)$, it follows $b|(b-1)$ or $b|(b+1)$. Therefore $b = 1$ or $b = -1$ which contradicts our assumption $b \neq \pm 1$. Thus $b_{n+1} \neq 0$.

Then,

$$x_{n+1} = bx_n + aa_{n+1}y_{n+1} = a(\pm b + a_{n+1}i_{n+1}).$$

As i_{n+1} divides one of $(b \pm 1)$, we can pick some $a_{n+1} \neq 0$ such that $a_{n+1}i_{n+1} = \mp(b \pm 1) \neq 0$, then $x_{n+1} = \pm a$ and (3.24) holds for y_{n+1} and x_{n+1}.

Now our sequence of x_i and y_i is bounded by $N = \max\{|a|, |i|(i \in I)\}$. By Theorem 3.35, τ is 1-nonfree.

□

Furthermore, if we choose M so that $i|M$ for all $i \in I$ and $b' = aM \pm b$. If $b' \nmid M$, then by Theorem 3.37, a/b' is also 1-nonfree.

3.3.2 Calculations

Now we can apply those methods to find new good numerators.

By Theorem 3.28, we have

Corollary 3.39 1, 2 *and* 3 *are good numerators.* □

By Theorem 3.29, we can show

Corollary 3.40 4 *and* 6 *are good numerators.*

Proof. By Theorem 3.29, we know that $4/(4r \pm 1)$ is 1-nonfree for any $r \neq 0$. By Theorem 3.28, we can obtain that $4/(4r \pm 2) = 2/(2r \pm 1)$ is 1-nonfree for any $r \neq 0$. Therefore, Ψ_τ is nonfree if $a = 4$, so 4 is a good numerator.

Similarly, by Theorem 3.29, we know the 1-nonfreeness of $6/(6r \pm 1)$, and by Theorem 3.28, we know the 1-nonfreeness of $6/(6r \pm 2) = 3/(3r \pm 1)$ and $6/(6r \pm 3)2/(2r \pm 1)$. Therefore, Ψ_τ is nonfree if $a = 6$, so 6 is a good numerator.

□

By Theorem 3.29 and above results, we obtain

Lemma 3.41 5 *is a good numerator.*

Proof. As $\frac{5}{10r\pm1} = \frac{5}{5(2r)\pm1}$, by Theorem 3.29, the rationals of this form are 1-nofree for $r \neq 0$. If $r = 0$, then $\left|\frac{5}{10r\pm1}\right| > 4$, they are still 1-nonfree. Similarly, $\frac{5}{5r\pm1}$ are 1-nonfree for $r \neq 0$, then $\frac{5}{10r\pm2}$ are 1-nonfree for $r \neq 0$ by Lemma 3.26. If $r = 0$, the greedy algorithm yields the following sequence $a_1 = 1, b_2 = -1, a_2 = 1, b_3 = -1, a_3 = -2$ and its corresponding sequence $x_0 = 1, y_1 = 1, x_1 = 5, y_2 = -3, x_2 = -5, y_3 = -1, x_3 = 0$. Hence, 5/2 is 1-nonfree.

Apply the greedy algorithm to 5/3, we obtain the sequence $a_1 = 1, b_2 = -1, a_2 = 1, b_3 = 1, a_3 = 3$ and $x_0 = 1, y_1 = 1, x_1 = 5, y_2 = -2, x_2 = 5, y_3 = -1, x_3 = 0$. Then the lease common multiple $M = lcm\{1, 5, 2\} = 10$. Since $3 \nmid 10$, for $b = 3$, we have $(Mr + b) \nmid M$ for any integer r. Hence all rationals of the form $\frac{5}{10r\pm3}$ are 1-nonfree.

Since $\frac{5}{10r+4} = \frac{5}{5(2r+1)-1}$ and $\frac{5}{10r-4} = \frac{5}{5(2r-1)+1}$, they are both 1-nonfree. As $\frac{5}{10r\pm5} = \frac{1}{2r\pm1}$, by Theorem 3.28, they are 1-nonfree. Therefore, 5 is a good numerator.

□

Lemma 3.42 *7, 8, 9, 10, 11 are good numerators.*

Proof. For $|\tau| = |a/b| < 4$, $(a, b) = 1$, assume that $a \geq 0$, $b > 0$. Firstly, we are going to show that $\frac{a}{6m\pm1}$ is 1-nonfree for any $a \in \{7, 8, 9, 10, 11\}$ and $m \in \mathbb{Z}$. Let $I = \{\pm1, \pm2, \pm3, \pm4, \pm6\}$. Since both $b = 6m + 1$ and $b = 6m - 1$ are odd, one of $b + 1$ and $b - 1$ is divisible by 4 for either b. It is clear that $\pm1, \pm2, \pm3, \pm6$ divide $6m = b \mp 1$. Therefore, for all $i \in I$, we have either $i|(b + 1)$ or $i|(b - 1)$. Since $(a, b) = 1$, it is never the case that $b^k \equiv 5 \mod a$ when $a = 10$. Note that I contains the complete set of residues modulo 10. Hence, for all positive integer k, we have $b^k \equiv i \mod a$ for some $i \in I$. Then, by Theorem 3.38, $\frac{10}{6m\pm1}$ are 1-nonfree. Since I also contains the complete set of residues modulo a for $a = 7, 8, 9$ and 11, similarly by Theorem 3.38, $\frac{7}{6m\pm1}$, $\frac{8}{6m\pm1}$, $\frac{9}{6m\pm1}$ and $\frac{11}{6m\pm1}$ are all 1-nonfree.

Now suppose a is not a good numerator, and b is the lowest denominator with $|a/b| < 4$ and $\tau = a/b$ 1-free. Then b must be in one of the forms $6m$, $6m \pm 2$ or $6m \pm 3$. Thus either form of b is divisible by 2 or 3. By Lemma 3.26, to show the 1-nonfreeness of a/b, we only need to discuss the 1-nonfreeness of $a/2$ and $a/3$. Since $(a, b) = 1$, we do not need to discuss the 1-nonfreeness of 8/2, 10/2 and 9/3. Furthermore, if we can show that $a/3$ is free, then because $3|6m$ and $3|(6m \pm 3)$, we obtain the 1-freeness of a/b for all $b = 6m$ and $b = 6m \pm 3$. That makes the discussion of 1-nonfreeness of $a/2$ only useful for $b = 6m \pm 2$. As $4|(6m \pm 2)$, in this case, the 1-nonfreeness of $a/4$ is equivalent to the 1-nonfreeness of $a/2$. Here, because both 9/2 and 11/2 are 1-free, we use 9/4 and 11/4 instead.

Therefore the last thing to show is the 1-nonfreeness of the following τ's:

$$\frac{7}{2}, \quad \frac{7}{3}, \quad \frac{8}{3}, \quad \frac{9}{4}, \quad \frac{10}{3}, \quad \frac{11}{4}, \quad \frac{11}{3}. \tag{3.25}$$

For $\tau = 7/3$, let $I = \{\pm1, \pm2, \pm4\}$, the complete set of residues modulo 7. Then, for all $i \in I$, it is clear that $i|(3-1)$ or $i|(3+1)$. Thus, by Theorem 3.38, 7/3 is 1-nonfree. The rest of (3.25) can be proved 1-nonfree by the pure and modified greedy algorithm as showed below:

τ	corresponding sequence
7/2	$a_1 = 1$, $b_2 = -1$, $a_2 = 1$, $b_3 = -1$, $a_3 = 1$, $b_4 = -1$, $a_4 = 1$, $b_5 = -1$, $a_5 = -1$, $b_6 = -1$, $a_6 = -1$, $b_7 = 1$, $a_7 = -2$.
	$x_1 = 7$, $y_2 = -5$, $x_2 = -21$, $y_3 = 11$, $x_3 = 35$, $y_4 = -13$, $x_4 = -21$, $y_5 = -5$, $x_5 = -7$, $y_6 = -3$, $x_6 = 7$, $y_7 = 1$, $x_7 = 0$.
7/3	$a_1 = 1$, $b_2 = -1$, $a_2 = 1$, $b_3 = -2$, $a_3 = 1$, $b_4 = 1$, $a_4 = -3$.
	$x_1 = 7$, $y_2 = -4$, $x_2 = -7$, $y_3 = 2$, $x_3 = -7$, $y_4 = -1$, $x_4 = 0$.
8/3	$a_1 = 1$, $b_2 = -1$, $a_2 = 1$, $b_3 = -1$, $a_3 = 6$.
	$x_1 = 8$, $y_2 = -5$, $x_2 = -16$, $y_3 = 1$, $x_3 = 0$.
9/4	$a_1 = 1$, $b_2 = -1$, $a_2 = 1$, $b_3 = -2$, $a_3 = -2$.
	$x_1 = 9$, $y_2 = -5$, $x_2 = -9$, $y_3 = -2$, $x_3 = 0$.
10/3	$a_1 = 1$, $b_2 = -1$, $a_2 = 1$, $b_3 = -1$, $a_3 = -2$.
	$x_1 = 10$, $y_2 = -6$, $x_2 = -20$, $y_3 = -4$, $x_3 = 0$.
11/4	$a_1 = 1$, $b_2 = -1$, $a_2 = 1$, $b_3 = -1$, $a_3 = 2$, $b_4 = 1$, $a_4 = -4$.
	$x_1 = 11$, $y_2 = -7$, $x_2 = -33$, $y_3 = 5$, $x_3 = -22$, $y_4 = -2$, $x_4 = 0$.
11/3	$a_1 = 1$, $b_2 = -1$, $a_2 = 1$, $b_3 = -1$, $a_3 = 1$, $b_4 = -1$, $a_4 = 1$, $b_5 = -1$, $a_5 = 1$, $b_6 = -1$, $a_6 = -1$, $b_7 = -1$, $a_7 = 1$, $b_8 = -3$, $a_8 = -1$, $b_9 = 6$, $a_9 = 1$, $b_{10} = -2$, $a_{10} = 1$, $b_{11} = -1$, $a_{11} = -3$.
	$x_1 = 11$, $y_2 = -8$, $x_2 = -55$, $y_3 = 31$, $x_3 = 176$, $y_4 = -83$, $x_4 = -385$, $y_5 = 136$, $x_5 = 341$, $y_6 = 67$, $x_6 = 286$, $y_7 = -85$, $x_7 = -77$, $y_8 = -24$, $x_8 = 11$, $y_9 = -6$, $x_9 = -11$, $y_{10} = 4$, $x_{10} = 11$, $y_{11} = 1$, $x_{11} = 0$.

Note here, we used the range-1 modified algorithm to calculate $\tau = 11/3$, otherwise the sequence will end at x_{12}.

□

We can apply the same methods to show the following lemma:

Lemma 3.43 *12 is a good numerator.*

Proof. Since we already know that a is a good numerator for $|a| \leq 11$, we only need to consider the b satisfying $(12, b) = 1$. Then $b \equiv \pm 5 \mod 12$. For $\tau = 12/5$, using the pure greedy algorithm, we have $a_1 = 1$, $b_2 = -1$, $a_2 = 1$, $b_3 = -1$, $a_3 = -1$, $b_4 = 5$, $a_4 = -1$, and hence $x_1 = 12$, $y_2 = -7$, $x_2 = -24$, $y_3 = -11$, $x_3 = 12$, $y_4 = 5$, $x_4 = 0$. Thus $12/5$ is 1-nonfree and by Lemma 3.26, b is 1-nonfree if $5|b$. If $b \equiv \pm 1 \mod 5$, taking $I = \{\pm 1, \pm 5\}$, by Theorem 3.38, b is 1-nonfree.

For $b \equiv \pm 2 \mod 5$, we discuss the following cases.

Case 1. $b \equiv \pm 5 \mod 24$, say $b = 24k \pm 5 = 5p \pm 2$, choose $a_1 = 2$, $b_2 = -k$, $a_2 = \mp 2p - 1$, $b_3 = 10k \pm 2$, $a_3 = \pm b$, and hence $x_1 = 24$, $y_2 = \pm 5$, $x_2 = \mp 12$, $y_3 = 1$, $x_3 = 0$.

Case 2. $b \equiv \pm 5 \mod 36$, say $b = 36k \pm 5 = 5p \pm 2$, choose $a_1 = 3$, $b_2 = -k$, $a_2 = \mp 3p - 1$, $b_3 = -15k \mp 2$, $a_3 = \pm b$, and hence $x_1 = 36$, $y_2 = \pm 5$, $x_2 = \pm 12$, $y_3 = 1$, $x_3 = 0$.

Case 3. $b \equiv \pm 7 \mod 36$, say $b = 36k \pm 7 = 5p \pm 2$, choose $a_1 = 1$, $b_2 = -3k \mp 1$, $a_2 = \pm p + 1$, $b_3 = -5k \mp 1$, $a_3 = \pm 3b$, and hence $x_1 = 12$, $y_2 = \mp 5$, $x_2 = \mp 36$, $y_3 = 1$, $x_3 = 0$.

In the above three cases, all values of x_i and y_i we got divide 360. Now pick $M = 2520 = 7 \times 360$, then by Theorem 3.37, $12/(2520r \pm b)$ is 1-nonfree for all $b \leq 1260$ except for 17, 127, 377, 487, 737, 847, 1097 and 1207. We can show the 1-nonfreeness of these 8 integers by the following table.

r	corresponding sequence
12/17	$a_1 = 2$, $b_2 = -1$, $a_2 = 5$, $b_3 = -10$, $a_3 = 17$.
	$x_1 = 24$, $y_2 = -7$, $x_2 = -12$, $y_3 = 1$, $x_3 = 0$.
12/127	$a_1 = 2$, $b_2 = -5$, $a_2 = -36$, $b_3 = -37$, $a_3 = -254$.
	$x_1 = 24$, $y_2 = 7$, $x_2 = 24$, $y_3 = 1$, $x_3 = 0$.
12/377	$a_1 = 2$, $b_2 = -16$, $a_2 = 108$, $b_3 = -110$, $a_3 = 754$.
	$x_1 = 24$, $y_2 = -7$, $x_2 = -24$, $y_3 = 1$, $x_3 = 0$.
12/487	$a_1 = 2$, $b_2 = -20$, $a_2 = -139$, $b_3 = -284$, $a_3 = -487$.
	$x_1 = 24$, $y_2 = 7$, $x_2 = 12$, $y_3 = 1$, $x_3 = 0$.
12/737	$a_1 = 2$, $b_2 = -31$, $a_2 = 212$, $b_3 = -43$, $a_3 = 7370$.
	$x_1 = 24$, $y_2 = -7$, $x_2 = -120$, $y_3 = 1$, $x_3 = 0$.
12/847	$a_1 = 2$, $b_2 = -35$, $a_2 = -242$.
	$x_1 = 24$, $y_2 = 7$, $x_2 = 0$.
12/1097	$a_1 = 2$, $b_2 = -46$, $a_2 = 312$, $b_3 = 64$, $a_3 = -10970$.
	$x_1 = 24$, $y_2 = -7$, $x_2 = 120$, $y_3 = 1$, $x_3 = 0$.
12/1207	$a_1 = 2$, $b_2 = -50$, $a_2 = -345$, $b_3 = 704$, $a_3 = 1207$.
	$x_1 = 24$, $y_2 = 7$, $x_2 = -12$, $y_3 = 1$, $x_3 = 0$.

Notice that the least common multiple of all the x_i and y_i in the table is $M = 2520$. Therefore, by Theorem 3.37, $12/(2520r \pm b)$ is 1-nonfree for all $b \leq 1260$. Hence, 12 is a good numerator.

□

Farbman also mentioned in his paper [11] without proof.

Lemma 3.44 *13, 14, 15, 16 are good numerators.* □

Chapter 4

Torsion-free groups

In this chapter, we will deal with torsion-free group. Charnow solved the rational case. In [8], he showed that G_u has an element of finite order (other than the identity) if and only if u is the reciprocal of an integer. We will extend his result with the help of Watkins and Zeitlin's work [39]. Before doing that, some definitions and a few facts about the degree and the conjugates of $2\cos(2\pi/n)$ over the rational numbers $\mathbb{Q}$ are needed.

Definition 4.1 *The* n-TH CHEBYSHEV POLYNOMIAL *is*

$$T_n(x) = \cos(n \cos^{-1} x) = \sum_{m=0}^{\lfloor n/2 \rfloor} \binom{n}{2m} x^{n-2m}(x^2-1)^m.$$

Then, the degree of n-th Chebyshev polynomial is $2\lfloor n/2 \rfloor$.

Let $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$ be primitive n-th root of unity. Since $2\cos(2\pi/n) = \zeta_n + \zeta_n^{-1}$, we have:

$$\mathbb{Q}(\zeta_n) \supseteq \mathbb{Q}(2\cos(2\pi/n)) \supseteq \mathbb{Q}.$$

Let $\phi(n)$ be the degree of ζ_n's minimal polynomial, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Lemma 4.2 *$\phi(n)$ is also the number of integers between 1 and n that are relatively prime to n and if $n = p_1^{r_1} \cdots p_t^{r_t}$, then $\phi(n) = \prod_{i=1}^{t} p_i^{r_i-1}(p_i-1)$.* □

Let $\psi_n(x)$ be the minimal polynomial of $2\cos(2\pi/n)$, then

Lemma 4.3 *If $n \geq 3$, then the roots of $\psi_n(x)$ are $2\cos(2k\pi/n)$, for $0 \leq k \leq [\frac{n}{2}] \doteq s$ and $(k,n) = 1$. The number of roots is $\phi(n)/2$.*

Proof. Given a $\mathbb{Q}$-automorphism σ_k of $\mathbb{Q}(\zeta_n)$ by $\sigma_k(\zeta_n) = \zeta_n^k$. For $n \geq 3$ and $(k, n) = 1$,

$$\begin{aligned}\sigma_k(2\cos(2\pi/n)) &= \sigma_k(\zeta_n + \zeta_n^{-1}) \\ &= \sigma_k(\zeta_n) + \sigma_k(\zeta_n^{-1}) \\ &= \zeta_n^k + \zeta_n^{-k} \\ &= 2\cos(2k\pi/n).\end{aligned}$$

Hence,

$$\psi_n(2\cos(2k\pi/n)) = \psi_n(\sigma_k(2\cos(2\pi/n))) = \sigma_k(\psi_n(2\cos(2\pi/n))) = \sigma_k(0) = 0.$$

Therefore, $2\cos(2k\pi/n)$ are the roots of $\psi_n(x)$ for $0 \leq k \leq [\frac{n}{2}] \doteq s$ and $(k, n) = 1$. Another important thing is to show those $2\cos(2k\pi/n)$'s are the only roots of $\psi_n(x)$.

If $(k, n) = g \neq 1$, say $k = k'g$ and $n = n'g$, then $\psi_n(x)$ will be the minimal polynomial of $2\cos(2k'\pi/n')$. Thus

$$\psi_n(2\cos(2\pi/n')) = \psi_n(\sigma_{1/k'}(2\cos(2k'\pi/n'))) = \sigma_{1/k'}(\psi_n(2\cos(2k'\pi/n'))) = 0.$$

Hence, $\psi_{n'}(x)$ (the minimal polynomial of $2\cos(2\pi/n')$) is a factor of $\psi_n(x)$. Note that $\psi_n(x) = \psi_{n'}(x) \cdot \frac{\psi_n(x)}{\psi_{n'}(x)}$, then $2\cos(2\pi/n)$ is the root of either $\psi_{n'}(x)$ or $\frac{\psi_n(x)}{\psi_{n'}(x)}$. Compared to $\psi_n(x)$, both of the two factors have the lower degree. This contradicts our assumption that $\psi_n(x)$ is the minimal polynomial of $2\cos(2\pi/n)$.

For $k \notin [0, s]$, the value of $2k\pi/n$ is not in the region $[0, 2\pi]$, so the corresponding $2\cos(2k\pi/n)$ are not new roots. Therefore, $2\cos(2k\pi/n)$ are the only roots of $\psi_n(x)$ for $0 \leq k \leq [\frac{n}{2}] \doteq s$ and $(k, n) = 1$.

Let $P(n)$ be the set of integers between 1 and n that are relatively prime to n. Since $(k, n) = 1$, then $(n - k, n) = 1$. Hence for each k such that $0 < k \leq s$ and $k \in P(n)$, there is an integer $n - k$ such that $s = [\frac{n}{2}] \leq n - k < n$ and $n - k \in P(n)$, and vice versa. Then we can divide $P(n)$ into two equal size subsets. We call them $P(n)_k$ and $P(n)_{n-k}$. Note that $\phi(n)$ is the size of $P(n)$, then the size of $P(n)_k$ is $\phi(n)/2$. Then the number of the corresponding $2\cos(2k\pi/n)$ is $\phi(n)/2$. Thus $\psi_n(x)$ has $\phi(n)/2$ roots.

□

4.1 Watkins and Zeitlin

We make a small change in Watkins and Zeitlin's theorem [39]:

Theorem 4.4 *Let* $\psi_n(x)$ *be the minimal polynomial of* $2\cos(2\pi/n)$ *and let* $T_s(x)$ *denote the s-th Chebyshev polynomial.*
a) If n=2s+1 is odd, then

$$2T_{s+1}(\frac{x}{2}) - 2T_s(\frac{x}{2}) = \prod_{d|n} \psi_d(x) \doteq \psi(n). \tag{4.1}$$

b) If n=2s is even, then

$$2T_{s+1}(\frac{x}{2}) - 2T_{s-1}(\frac{x}{2}) = \prod_{d|n} \psi_d(x) \doteq \psi(n). \tag{4.2}$$

Proof. Since ζ_n is a root of the quadratic polynomial $x^2-2\cos(2\pi/n)x+1$, we have $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(2\cos(2\pi/n))] = 1$ or 2. If $n = 1$, we have $2\cos(2\pi/n) = 2$. For $n = 2$, we have $2\cos(2\pi/n) = -2$. If $n \geq 3$, ζ_n is not real and therefore $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(2\cos(2\pi/n))] = 2$. Since $\phi(n)$ is the degree of ζ_n's minimal polynomial, we have:

$$\deg(\psi_n(x)) = \begin{cases} 1, & \text{if } n = 1, 2 \\ \phi(n)/2, & \text{if } n \geq 3 \end{cases} \tag{4.3}$$

To prove part a) of the theorem, it is sufficient to show that the roots and the leading coefficients of both sides of (4.1) are the same. Since $n = 2s + 1$ is odd, by Lemma 4.2, the degree of the right side of (4.1) is

$$\begin{aligned} \sum_{d|n} \deg(\psi_d(x)) &= \deg(\psi_1(x)) + \sum_{d|n, d\neq 1} \deg(\psi_d(x)) \\ &= \deg(\psi_1(x)) + \sum_{d|n, d\neq 1} \phi(d)/2 \\ &= 1 + \frac{1}{2}(n-1) \\ &= 1 + s. \end{aligned}$$

which equals the degree of the left side of (4.1).

Now we are going to prove that the roots of the left side and the right side of (4.1) are exactly the same.

For $0 \leq k \leq s$, let $g = (k, n)$, $k' = k/g$, $n' = n/g$, so that $(k', n') = 1$. Then $2\cos(2k\pi/n) = 2\cos(2k'\pi/n')$ is a root of $\psi_{n'}$, which is a factor of the right side of (4.1). On the left side,

$$\begin{aligned}
&2T_{s+1}(\frac{1}{2} \cdot 2\cos(2k\pi/n)) - 2T_s(\frac{1}{2} \cdot 2\cos(2k\pi/n)) \\
&= 2\cos(\frac{2k\pi(s+1)}{n}) - 2\cos(\frac{2k\pi s}{n}) \\
&= 2\cos(\frac{k\pi(n+1)}{n}) - 2\cos(\frac{k\pi(n-1)}{n}) \\
&= 2\cos(k\pi + \frac{k\pi}{n}) - 2\cos(k\pi - \frac{k\pi}{n}) \\
&= 0.
\end{aligned}$$

Therefore $2\cos(2k\pi/n)$ is also a root of the left side of (4.1). Hence, the roots of both sides are $2\cos(2k\pi/n)$ for $0 \leq k \leq s$, and these $s+1$ roots are all the roots of both sides.

The last thing is to check the leading coefficients of both sides of (4.1). Since

$$\begin{aligned}
T_s(\cos\theta) &= \cos(s\theta) \\
&= \Re((\cos\theta + i\sin\theta)^s) \\
&= \cos^s\theta - \binom{s}{2} \cdot \cos^{s-2}\theta(1-\cos^2\theta) + \binom{s}{4} \cdot \cos^{s-4}\theta(1-\cos^2\theta)^2 \\
&\quad - \cdots + (-1)^{[\frac{s}{2}]} \binom{s}{2[\frac{s}{2}]} \cdot \cos^{s-2[\frac{s}{2}]}\theta(1-\cos^2\theta)^{[\frac{s}{2}]} \\
&= (1 + \binom{s}{2} + \binom{s}{4} + \cdots + \binom{s}{2[\frac{s}{2}]}) \cdot \cos^s\theta + \cdots \\
&= 2^{s-1}\cos^s\theta + \cdots.
\end{aligned}$$

So $T_{s+1}(x/2) = 2^s \cdot (x/2)^{s+1} + \cdots$ and the leading coefficient of the left side is $2 \cdot 2^s \cdot (\frac{1}{2})^{s+1} = 1$, which equals the leading coefficient of the right side of (4.1). Hence, (4.1) is proved.

Similarly, we can prove part b) of the theorem. Since $n = 2s$ is even, the degree of the right side of (4.2) is

$$
\begin{aligned}
\sum_{d|n} \deg(\psi_d(x)) &= \deg(\psi_1(x)) + \deg(\psi_2(x)) + \sum_{d|n,d>2} \deg(\psi_d(x)) \\
&= \deg(\psi_1(x)) + \deg(\psi_2(x)) + \sum_{d|n,d>2} \phi(d)/2 \\
&= 2 + \frac{1}{2}(n-2) \\
&= 1 + s,
\end{aligned}
$$

which equals the degree of the left side of (4.2).

Again the roots of both sides of (4.2) are the same. They are $2\cos(2k\pi/n)$, where $0 \le k \le s$ and $(k,n) = 1$ and these $s+1$ roots are all the roots of both sides.

Let $g = (k,n)$, $k' = k/g$, $n' = n/g$, so that $(k',n') = 1$. Then $2\cos(2k\pi/n) = 2\cos(2k'\pi/n')$ is a root of $\psi_{n'}$, which is a factor of the right side of (4.2). On the left side,

$$
\begin{aligned}
&2T_{s+1}(\frac{1}{2}\cdot 2\cos(2k\pi/n)) - 2T_{s-1}(\frac{1}{2}\cdot 2\cos(2k\pi/n)) \\
&= 2\cos(\frac{2k\pi(s+1)}{n}) - 2\cos(\frac{2k\pi(s-1)}{n}) \\
&= 2\cos(\frac{k\pi(n+2)}{n}) - 2\cos(\frac{k\pi(n-2)}{n}) \\
&= 2\cos(k\pi + \frac{2k\pi}{n}) - 2\cos(k\pi - \frac{2k\pi}{n}) \\
&= 0.
\end{aligned}
$$

Therefore $2\cos(2k\pi/n)$ is also a root of the left side of (4.2). Since the leading coefficients of both sides of (4.2) are 1, thus (4.2) is proved.

□

4.2 Calculation of $\psi_n(2)$

Now we can use (4.1) and (4.2) to compute $\psi_n(x)$ using the following Lemma:

Lemma 4.5 *For $n = p_1^{r_1} \cdots p_t^{r_t}$, where $p_1, \cdots, p_t$ are different prime numbers.*

If $t = 2q+1$ *is odd, then*

$$\psi_n(x) = \frac{\psi(n) \cdot \prod_{j=1}^{q} \prod_{i_1<i_2<\cdots<i_{2j}, i_1, i_2, \cdots, i_{2j}=1}^{t} \psi(\frac{n}{p_{i_1} \cdot p_{i_2} \cdot \cdots \cdot p_{i_{2j}}})}{\prod_{j=1}^{q+1} \prod_{i_1<i_2<\cdots<i_{2j-1}, i_1, i_2, \cdots, i_{2j-1}=1}^{t} \psi(\frac{n}{p_{i_1} \cdot p_{i_2} \cdot \cdots \cdot p_{i_{2j-1}}})}. \tag{4.4}$$

If $t = 2q$ *is even, then*

$$\psi_n(x) = \frac{\psi(n) \cdot \prod_{j=1}^{q} \prod_{i_1<i_2<\cdots<i_{2j}, i_1, i_2, \cdots, i_{2j}=1}^{t} \psi(\frac{n}{p_{i_1} \cdot p_{i_2} \cdot \cdots \cdot p_{i_{2j}}})}{\prod_{j=1}^{q} \prod_{i_1<i_2<\cdots<i_{2j-1}, i_1, i_2, \cdots, i_{2j-1}=1}^{t} \psi(\frac{n}{p_{i_1} \cdot p_{i_2} \cdot \cdots \cdot p_{i_{2j-1}}})}. \tag{4.5}$$

□

For (4.4), the number of factors ($\psi(m)$ for some $m|n$) in its numerator is:

$$1 + \sum_{j=1}^{q} \binom{t}{2j} = \sum_{j=0}^{q} \binom{2q+1}{2j} = \sum_{j=0}^{q} \binom{2q+1}{2j+1} = 2^{2q} = 2^{t-1},$$

which is also the number of factors in its denominator.

It is similar to get the number of factors in (4.5)'s numerator:

$$1 + \sum_{j=1}^{q} \binom{2q}{2j} = \sum_{j=0}^{q} \binom{2q}{2j} = 2^{2q-1} = 2^{t-1} = \sum_{j=1}^{q} \binom{2q}{2j-1},$$

which equals the number of factors in its denominator. Then by Theorem 4.4, we can rewrite (4.4) and (4.5) in the form of:

$$\begin{aligned} \psi_n(x) &= \prod_{i=1}^{2^{t-1}} \frac{\psi(n_i)}{\psi(m_i)} \\ &= \prod_{i=1}^{2^{t-1}} \frac{2T_{\lceil \frac{n_i+1}{2} \rceil}(\frac{x}{2}) - 2T_{\lfloor \frac{n_i-1}{2} \rfloor}(\frac{x}{2})}{2T_{\lceil \frac{m_i+1}{2} \rceil}(\frac{x}{2}) - 2T_{\lfloor \frac{m_i-1}{2} \rfloor}(\frac{x}{2})} \\ &= \prod_{i=1}^{2^{t-1}} \frac{T_{\lceil \frac{n_i+1}{2} \rceil}(\frac{x}{2}) - T_{\lfloor \frac{n_i-1}{2} \rfloor}(\frac{x}{2})}{T_{\lceil \frac{m_i+1}{2} \rceil}(\frac{x}{2}) - T_{\lfloor \frac{m_i-1}{2} \rfloor}(\frac{x}{2})} \end{aligned} \tag{4.6}$$

for some $n_i|n$ and $m_i|n$.

If $x = 2$, for Chebyshev polynomials $T_s(\frac{x}{2})$, we have $T_s(1) = T_s(\cos 0) = \lim_{\theta\to 0}\cos(s\theta)$. Then after substitution, using l'Hôpital theorem, we have

$$\begin{aligned}
\psi_n(2) &= \lim_{x\to 2}\psi_n(x) \\
&= \lim_{x\to 1}\prod_{i=1}^{2^{t-1}}\frac{T_{\lceil\frac{n_i+1}{2}\rceil}(x) - T_{\lfloor\frac{n_i-1}{2}\rfloor}(x)}{T_{\lceil\frac{m_i+1}{2}\rceil}(x) - T_{\lfloor\frac{m_i-1}{2}\rfloor}(x)} \\
&= \lim_{\theta\to 0}\prod_{i=1}^{2^{t-1}}\frac{T_{\lceil\frac{n_i+1}{2}\rceil}(\cos\theta) - T_{\lfloor\frac{n_i-1}{2}\rfloor}(\cos\theta)}{T_{\lceil\frac{m_i+1}{2}\rceil}(\cos\theta) - T_{\lfloor\frac{m_i-1}{2}\rfloor}(\cos\theta)} \\
&= \lim_{\theta\to 0}\prod_{i=1}^{2^{t-1}}\frac{\cos(\lceil\frac{n_i+1}{2}\rceil\theta) - \cos(\lfloor\frac{n_i-1}{2}\rfloor\theta)}{\cos(\lceil\frac{m_i+1}{2}\rceil\theta) - \cos(\lfloor\frac{m_i-1}{2}\rfloor\theta)} \\
&= \lim_{\theta\to 0}\prod_{i=1}^{2^{t-1}}\frac{\lceil\frac{n_i+1}{2}\rceil\cdot\sin(\lceil\frac{n_i+1}{2}\rceil\theta) - \lfloor\frac{n_i-1}{2}\rfloor\cdot\sin(\lfloor\frac{n_i-1}{2}\rfloor\theta)}{\lceil\frac{m_i+1}{2}\rceil\cdot\sin(\lceil\frac{m_i+1}{2}\rceil\theta) - \lfloor\frac{m_i-1}{2}\rfloor\cdot\sin(\lfloor\frac{m_i-1}{2}\rfloor\theta)} \\
&= \prod_{i=1}^{2^{t-1}}\frac{(\lceil\frac{n_i+1}{2}\rceil)^2 - (\lfloor\frac{n_i-1}{2}\rfloor)^2}{(\lceil\frac{m_i+1}{2}\rceil)^2 - (\lfloor\frac{m_i-1}{2}\rfloor)^2} \\
&= \prod_{i=1}^{2^{t-1}}\frac{n_i}{m_i}.
\end{aligned} \tag{4.7}$$

Combine (4.7) with Lemma 4.5, if $t = 2q+1$ is odd, then:

$$\begin{aligned}
\psi_n(2) &= \frac{n\cdot\prod_{j=1}^{q}\prod_{i_1<i_2<\cdots<i_{2j},i_1,i_2,\cdots,i_{2j}=1}^{t}\frac{n}{p_{i_1}\cdot p_{i_2}\cdot\cdots\cdot p_{i_{2j}}}}{\prod_{j=1}^{q+1}\prod_{i_1<i_2<\cdots<i_{2j-1},i_1,i_2,\cdots,i_{2j-1}=1}^{t}\frac{n}{p_{i_1}\cdot p_{i_2}\cdot\cdots\cdot p_{i_{2j-1}}}} \\
&= \frac{\prod_{j=1}^{q+1}\prod_{i_1<i_2<\cdots<i_{2j-1},i_1,i_2,\cdots,i_{2j-1}=1}^{t}p_{i_1}\cdot p_{i_2}\cdot\cdots\cdot p_{i_{2j-1}}}{\prod_{j=1}^{q}\prod_{i_1<i_2<\cdots<i_{2j},i_1,i_2,\cdots,i_{2j}=1}^{t}p_{i_1}\cdot p_{i_2}\cdot\cdots\cdot p_{i_{2j}}} \\
&= \frac{(\prod_{i=1}^{t}p_i)^{\sum_{j=1}^{q}\binom{2q}{2j-1}}}{(\prod_{i=1}^{t}p_i)^{\sum_{j=1}^{q}\binom{2q}{2j-1}}} \\
&= 1.
\end{aligned}$$

Similarly, if $t = 2q+1$ is even, then:

$$\psi_n(2) = \frac{n\cdot\prod_{j=1}^{q}\prod_{i_1<i_2<\cdots<i_{2j},i_1,i_2,\cdots,i_{2j}=1}^{t}\frac{n}{p_{i_1}\cdot p_{i_2}\cdot\cdots\cdot p_{i_{2j}}}}{\prod_{j=1}^{q}\prod_{i_1<i_2<\cdots<i_{2j-1},i_1,i_2,\cdots,i_{2j-1}=1}^{t}\frac{n}{p_{i_1}\cdot p_{i_2}\cdot\cdots\cdot p_{i_{2j-1}}}} = 1.$$

Therefore, we have:

Lemma 4.6 $\psi_n(2) = 1$ *for any* $n \in \mathbb{Z}^+$. $\square$

4.3 New result

Let $G_u = \langle A_u, B_u \rangle$, then by induction, every element of G_u is of the form:

$$\begin{pmatrix} 1+u^2 f_1(u) & u f_2(u) \\ u f_3(u) & 1+u^2 f_4(u) \end{pmatrix}$$

where the f_i are polynomials with integral coefficients.

Theorem 4.7 *Let $u \in \mathbb{C}$ be an algebraic number over $\mathbb{Q}$ with an irreducible polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ of degree n, where $a_n, a_{n-1}, \cdots, a_1 \in \mathbb{Z}$, $a_0 \in \mathbb{Z}^+$ and $(a_n, a_{n-1}, \cdots, a_0) = 1$. If G_u has an element of finite order p (other than the identity), then,*
1) If $a_1 \neq 0$, then $a_0 = 1$;
2) $(p-1)|2n$.

Proof. If G_u is not torsion free, then there $\exists C \in G_u$, s.t.

$$C^p = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; C \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

where p is a prime number.

Then the minimal polynomial of C must divide $x^p - 1$ and C is diagonalizable over the complex field. Hence

$$QCQ^{-1} = \begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix}$$

for some invertible matrix Q. Since every element of G_u has determinant 1, we must have $\xi_2 = \frac{1}{\xi_1}$.

From

$$\begin{pmatrix} \xi_1^p & 0 \\ 0 & \xi_2^p \end{pmatrix} = \begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix}^p = (QCQ^{-1})^p = QC^pQ^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

it follows that $\xi_1^p = 1$. Thus if $p > 2$, $\xi_1^p = 1$ has only one real root, which is 1. Since C is not the identity and $\xi_1 \neq 1$, we obtain that ξ_1 is a primitive p-th root of 1 and the degree of ξ_1 over the rationals is $p-1$. Suppose $\xi_1 = \cos(\frac{2k\pi}{p}) + i\sin(\frac{2k\pi}{p})$ for $0 < k < [\frac{p}{2}]$ and $(k,p) = 1$, then $\xi_2 = \cos(\frac{2k\pi}{p}) - i\sin(\frac{2k\pi}{p})$. On the other hand, ξ_1 is a root of a quadratic polynomial with coefficients in $\mathbb{Q}(u)$, namely the characteristic polynomial of C. Hence $(p-1)|2n$.

From

$$C = \begin{pmatrix} 1+u^2 f_1(u) & u f_2(u) \\ u f_3(u) & 1+u^2 f_4(u) \end{pmatrix}$$

where the f_i are polynomials with integral coefficients, we have

$$\begin{aligned} Trace(C) &= \xi_1 + \xi_2 = 2\cos(\frac{2k\pi}{p}) \\ &= 1 + u^2 f_1(u) + 1 + u^2 f_4(u) = 2 + u^2 f_1(u) + u^2 f_4(u) \end{aligned} \tag{4.8}$$

Suppose the minimal polynomial of $2\cos(\frac{2k\pi}{p})$ is $\psi_p(x)$. Since the coefficients of the minimal polynomial of $\cos(\frac{2k\pi}{p})$ are all integers. Then $\psi_p(x)$ is also an irreducible polynomial with coprime integral coefficients. Then $\psi_p(\ 2 + u^2(f_1(u) + f_4(u))\ ) = \psi_p(2\cos(\frac{2k\pi}{p})) = 0$. By expansion, $\psi_p(\ 2 + x^2(f_1(x) + f_4(x))\ ) = x^2 f_5(x) + \psi_p(2)$, where $f_5(x)$ is a polynomial with integral coefficients. Thus, $u^2 f_5(u) = -\psi_p(2) \doteq p_0 \in \mathbb{Z}$. Therefore $f(x) - a_0$ is a factor of $x^2 f_5(x)$.

If the coefficient a_1 of the irreducible polynomial $f(x)$ of u is not zero, from $u \notin \mathbb{Q}$, there must be a factor $g(x)$ of $x f_5(x)$ with coprime integral coefficients, s.t. $g(u) * u \in \mathbb{Q}$. (We can pick $g(x) = \frac{f(x)-a_0}{x\cdot(a_1,a_2,\cdots,a_n)}$, it is a polynomial with coprime integral coefficients.) Since $a_1 \neq 0$ and $a_0 \neq 0$, we have $g(x)|x f_5(x) \Rightarrow g(x)|f_5(x)$, it follows $f_5(x) = g(x) * d(x)$. As both $f(x)$ and $g(x)$ are polynomials with coprime integral coefficients, $g(u) * u$ actually equals the remainder of the division of $x g(x)$ by $f(x)$, which is $\frac{a_0}{p_1}$ for some $p_1|(a_n, a_{n-1}, \cdots a_1)$. Therefore

$$u^2 f_5(u) = p_0 \Rightarrow u g(u) * u d(u) = p_0 \Rightarrow u d(u) = \frac{p_0 p_1}{a_0}. \tag{4.9}$$

For the same reason, since $d(u)$ is a polynomial with integral coefficient, $u d(u) = \frac{a_0}{p_2}$ for some $p_2|(a_n, a_{n-1}, \cdots a_1)$, hence $\frac{a_0}{p_2} = \frac{p_0 p_1}{a_0} \Rightarrow a_0^2 = p_0 p_1 p_2 \Rightarrow a_0^2 | p_0 p_1 p_2$. However, $(a_n, a_{n-1}, \cdots, a_1, a_0) = 1 \Rightarrow ((a_n, a_{n-1}, \cdots, a_1), a_0) = 1 \Rightarrow (p_1, a_0) = 1$ and $(p_2, a_0) = 1$, which means $a_0^2 | p_0$. From Lemma 4.6, $p_0 = -1$, then because $a_0 \in \mathbb{Z}^+$, $a_0 = 1$.

□

Now we can use Theorem 4.7 to give a new proof of Charnow [8]'s result.

Corollary 4.8 *Let u be rational. Then G_u has an element of finite order (other than the identity) if and only if u is the reciprocal of an integer.*

Proof. Suppose $u = -\frac{1}{a_1}$, where a_1 is an integer. Let

$$C = A^{-3}B^{a_1^2} = \begin{pmatrix} 1 & -3u \\ 0 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 0 \\ a_1^2 u & 1 \end{pmatrix} = \begin{pmatrix} -2 & -3u \\ \frac{1}{u} & 1 \end{pmatrix}$$

We have $C^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and hence $C \in G_u$ has order 3.

Conversely, assume G_u has some element (other than the identity) of finite order. Then, because u is rational, the irreducible polynomial of u is of the form $f(x) = a_1 x + a_0$, where $a_1 \neq 0$. Therefore, $a_0 = 1$ and $a_1 u + a_0 = 0 \Rightarrow u = -\frac{a_0}{a_1} = -\frac{1}{a_1}$ is the reciprocal of an integer.

□

Bibliography

[1] S. Bachmuth, H. Mochizuki *Triples of 2×2 matrices which generate free groups* , Proceedings of the American Math. Soc., **59** (1976), No.1 25–28.

[2] J. Bamberg, *No-free points for groups generated by a pair of 2×2 matrices*, J.London Math. Soc.(2), **62** (2000), 795-801.

[3] R. Beals, *Algorithms for matrix groups and the Tits alternative*, J. of Computer and System Sci., **58** (1999), 260–279.

[4] A. F. Beardon, *Pell's equation and two generator free Möbius groups*, Bull. London Math. Soc., **25** (1993), no. 6, 527–532.

[5] J. L. Brenner, R. A. MacLeod and D. D. Olesky, *Nonfree groups generated by two 2×2 matices*, Canadian J. of Math., **27** (1975), 237–245.

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

[7] B. Chang, S. A. Jennings and R. Ree, *On certain pairs of matrices which generate free groups*, Canadian J. of Math., **10** (1958), 279–283.

[8] A. Charnow, *A note on torsion free groups generated by pairs of matrices*, Canadian Mathematical Bulletin, **17** (1975), 747–748.

[9] M. Cohen, W. Metzler, and A. Zimmermann, *What does a basis of $F(a, b)$ look like?*, Math. Ann., **257** (1981), no. 4, 435–445.

[10] R. J. Evans, *Nonfree groups generated by two parabolic matrices.*, J. Res. Nat. Bur. Standards, **84** (1979), no. 2, 179–180.

[11] S. P. Farbman, *Non-free two-generator subgroups of $SL_2(\mathbb{Q})$*, Publicacions Matmátiques, **39** (1995), 379–391.

[12] J. Z. Gonçalves, M. Shirvani, *Free Groups in Central Simple Algebras without Tit's Theorem*, Preprint.

[13] J. Z. Gonçalves, A. Mandel, M. Shirvani, *Free products of units in algebras I. Quaternion algebras*, J. of Algebra, **214** (1999), 301–316.

[14] M. Hall, The Theory of Groups, Macmillan, New York, 1959

[15] J. A. Ignatov, *Free groups generated by two parabolic-fractional linear transformations.*, Modern algebra, **4** (1976), 87–90.

[16] J. A. Ignatov, *Free and nonfree subgroups of* $\mathrm{PSL}_2(C)$ *that are generated by two parabolic elements.* , Mat. Sb.(N.S.), **106(148)** (1978), no. 3, 372–379, 495.

[17] Y. A. Ignatov, *Rational nonfree points of the complex plane*, Algorithmic problems in the theory of groups and semigroups, **127** (1986), 72–80.

[18] Y. A. Ignatov, *Rational nonfree points of the complex plane. II.*, Algorithmic problems in the theory of groups and semigroups , **20** (1990), 53–59.

[19] Y. A. Ignatov, T. N. Gruzdeva, I. A. Sviridova, *Free groups of linear-fractional transformations*, Izv. Tul. Gos. Univ. Ser. Mat. Mekh. Inform., **5** (1999), no. 1, Matematika, 116–120.

[20] Y. A. Ignatov, A. V. Evtikhova, *Free groups of linear-fractional transformations*, ChebyshevskiĭSb., **3** (2002), no. 1(3), 78–81.

[21] Y. A. Ignatov, N. A. Kuzina, *Boundary points of a free domain*, ChebyshevskiĭSb., **4** (2003), no. 1(5), 82–84.

[22] J. A. Ignatov, *Groups of linear fractional transformations generated by three elements.*, Mat. Zametki, **27** (1980), no. 4, 507–513, 668.

[23] J. A. Ignatov, *Roots of unity as nonfree points of the complex plane*, Mat. Zametki, **27** (1980), no. 5, 825–827, 831.

[24] A. W. Knapp, *Doubly generated Fuchsian groups*, Michigan Math. J., **15** (1968), 289–304.

[25] S. Lang, Algebra, Springer, New York, 2002.

[26] R. C. Lyndon, D. E. Schupp, Combinatorial Group Theory, Springer, New York, 1977.

[27] R. C. Lyndon and J. L. Ullman, *Groups generated by two parabolic linear fractional transformations*, Canadian J. of Math., **21** (1969), 1388–1403.

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

[29] M. Y. Lyubich, V. V. Suvorov, *Free subgroups of* $SL_2(C)$ *with two parabolic generators*, J. Soviet Math., **41** (1988), no. 2, 976–979.

[30] A. M. Macbeath, *Packings, free products and residually finite groups*, Proc. Cambridge Philos. Soc., **59** (1963), 555-558.

[31] W. Magnus, A. Karrass, D. Solitar, Combinatorial group theory : presentations of groups in terms of generators and relations, Dover, New York, 1976.

[32] P. J. McCarthy, Algebraic Extensions of Fields, Chelsea, New York, 1976.

[33] M. Nagata, T. Nakayama, T. Tuzuku, *On an existence lemma in valuation theory*, Nagoya Math. J., **6** (1953). 59–61.

[34] M. Newman, *A conjecture on a matrix group with two generators*, J.Res. Nat. Bur. Stand., **B78** (1974), No.2 795-801.

[35] R. Ree, *On certain pairs of matrices which do not generate a free group*, Canadian Mathematical Bulletin, **4** (1961), 49–52.

[36] L. N. Sanov, *A property of a representation of a free group*, Dokl. Akad. Nauk SSSR, **57** (1947), 657–659.

[37] M. Shirvani, J. Z. Gonçalves, *Free products arising from elements of finite order in simple rings*, Proceedings of the American Math. Soc., **133** (2005), No.7 1917–1923.

[38] J. Tits, *Free subgroup in linear groups*, J. of Algebra, **20** (1972), 250–270.

[39] W. Watkins and J. Zeitlin, *The minimal polynomial of* $\cos(2\pi/n)$, Am. Math. Mon., **100** (1993), No.5, 471–474.

[40] B. A. F. Wehrfritz, Infinite Linear Groups, Springer-Verlag, New York, 1973.

[41] H. Whitney, *Elementary structure of real algebraic varieties*, Ann. of Math., **66** (1957), 545–556.