

United Arab Emirates University

Scholarworks@UAEU

Theses

Electronic Theses and Dissertations

4-2024

FAITHFUL REPRESENTATION OF FREE GROUPS AND CONGRUENT SUBGROUPS OF $SL_3(\mathbb{Z})$

Julius Kurian

Follow this and additional works at: https://scholarworks.uaeu.ac.ae/all_theses



Part of the [Mathematics Commons](#)



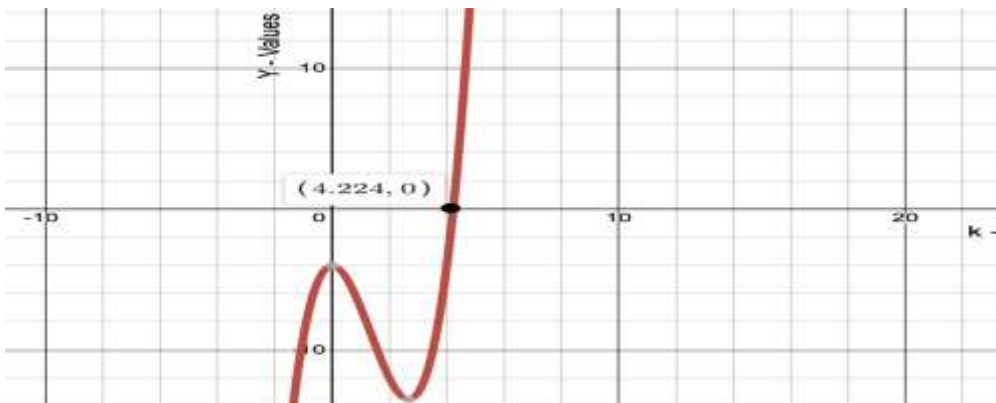
MASTER THESIS NO. 2024: 74

College of Science

Department of Mathematical Sciences

**FAITHFUL REPRESENTATION OF FREE GROUPS AND
CONGRUENT SUBGROUPS OF $SL_3(\mathbb{Z})$**

Julius Kurian



April 2024

United Arab Emirates University

College of Science

Department of Mathematical Sciences

FAITHFUL REPRESENTATION OF FREE GROUPS
AND CONGRUENT SUBGROUPS OF $SL_3(\mathbf{Z})$

Julius Kurian

This thesis is submitted in partial fulfillment of the requirements for
the degree of Master of Science in Mathematics

April 2024

United Arab Emirates University Master Thesis
2024:XX

Cover : Image of the graph of the reduced cubic equation for the minimum k value.

(Photo by : Julius Kurian)

©2024 Julius Kurian, Al Ain, UAE

All Rights Reserved

Print: University Print Service, UAEU 2024

Declaration of Original Work

I, Julius Kurian, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled "*Faithful Representation of Free Groups and Congruent Subgroups of $SL_3(\mathbb{Z})$* ", hereby, solemnly declare that this is the original research work done by me under the supervision of Professor Alexandr Zubkov, in the College of Science at UAEU. This work has not previously formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

Student's Signature: _____



Date: September 1, 2024

Approval of the Master Thesis

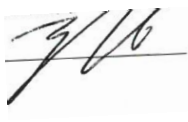
This Master Thesis is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Alexandr Zubkov

Title: Professor

Department of Mathematical Sciences

College of Science

Signature: 

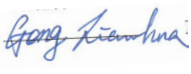
Date September 1, 2024

2) Member: Jianhua Gong

Title: Professor

Department of Mathematical Sciences

College of Science

Signature: 


Date September 1, 2024

3) Member (External Examiner): Pavel Kolesnikov

Title: Professor

Novosibirsk State University, Russia.

Department of Mathematics

Signature: 

Date September 1, 2024

This Master Thesis is accepted by:

Dean of the College of Science: Professor Maamar Benkraouda

Signature _____

Date _____

Dean of the College of Graduate Studies: Professor Ali Al-Marzouqi

Signature _____

Date _____

Abstract

This thesis is concerned with the matrix representation of a free non-abelian group by matrices of size ≥ 3 . We proceed from defining an equivalence class and then transitioning to free groups. We discuss in details the group $G_n(k)$ which is the group generated by the matrices filled with first, (second, etc.) column, except for the intersection with the diagonal, and we have ones on the diagonal and zeros at the other places. The filled places are occupied by the same parameter k . An alternative proof for the known fact that $G_n(3)$ is not *free* is provided. The main objective of this thesis is to find a lower bound for the parameter. An explicit value of the lower bound is found which is a refinement of a previous lower bound.

Keywords: Free group, Equivalence classes, Mennicke subgroup, Congruence subgroup, Principal congruence subgroup.

Title and Abstract (in Arabic)

تمثيلات مغلصة للزمر الحرة والزمير الجزئي المتطابقة من $SL_3\mathbb{Z}$

الملخص

تتيم هذه الأطروحة بالتمثيل المصفوفي لمجموعة حرة غير أبيلية بواسطة مصفوفات حجم المجموعة ≥ 3 . نبدأ من تحديد فئة التكافؤ ومن ثم الانتقال إلى المجموعات الحرة. نناقش المجموعة بالتفصيل $G_n(k)$ (الثاني، الخ) العمود، باستثناء التقاطع مع القطر، ولدينا أرقام على القطر وأصفار في الأماكن الأخرى. الأماكن المملوءة مشغولة بنفس المعلمة k . دليل بديل للحقيقة المعروفة أن $G_n(3)$ ليس تم توفير حر الهدف الرئيسي من هذه الأطروحة هو إيجاد حد أدنى للمعلمة k . تم العثور على قيمة صريحة للحد الأدنى وهي عبارة عن تحسين للحد الأدنى السابق.

مفاهيم البحث الرئيسية: المجموعة الحرة، فئة التكافؤ، مجموعة مينيكى الفرعية، التطابق مجموعة فرعية، مجموعة فرعية التطابق الرئيسي.

Acknowledgements

I have received exceptional support and assistance throughout the process of finishing my thesis. Without the support of my professor, family, and friends, I could not have achieved my objective. It gives me immense authentic pleasure to convey my gratitude to Professor Alexandr Zubkov, my advisor, for his unwavering support of my thesis, his motivation, vast knowledge, and patience. Throughout the entire process of researching and writing this thesis, I have had his support. I would like to express my thanks to the Mathematics Department Faculty, particularly Dr. Adama Diene, department head, and Dr. Farrukh Mukhamedov, master's coordinator, for their inspiration. A word of special thanks is reserved for Dr. Muhammad Syam, who encouraged me throughout the course. Of course, my biggest and most emphatic thanks is for my family, all of them, but particularly my sister, who followed up with me on the development of this manuscript, for their daily efforts and sacrifices they have made.

Dedication

To Julian and Shevonne

Table of Contents

Title	i
Declaration of Original Work	iii
Approval of the Master Thesis	iv
Abstract	vi
Title and Abstract (in Arabic)	vii
Acknowledgments	viii
Dedication	ix
Table of Contents	x
Chapter 1: Outline	1
1.1 Overview	1
1.1.1 Thesis Objective	2
Chapter 2: Groups	3
2.1 Introduction	3
2.1.1 Binary Operation	3
2.1.2 Equivalence Classes of Words	9
Chapter 3: Universality of Free Groups	16
3.1 Introduction	16
3.1.1 Universal Factor Group	17
3.1.2 Free Subgroups	20
Chapter 4: Representation	27
4.1 Introduction	27
4.1.1 The Group $G_n(2)$, $n \geq 3$	28
4.1.2 The Faithfulness of the Representation	38
Chapter 5: Conclusion	48
References	49

Chapter 1: Outline

1.1 Overview

In this thesis, we investigate various representation of free groups by matrices. The second chapter begins with an introductory definitions about groups, examples of groups and definition of subgroup. We define a binary operation and equivalence class of words. The set of all equivalence class under a binary operation forms a group is proved which lays the foundation for the definition of a free group.

In the third chapter, the universal definition of a free group is introduced. Free groups are a key concept in group theory, a field of abstract algebra. Jakob Nielsen introduced them in 1924, building on the earlier ideas of Walther von Dyck from the late 19th century. The emergence of free groups originated from examining geometric transformations and their algebraic properties. Walther von Dyck, a German mathematician, proposed generators and relations for groups in 1882, setting the groundwork for the future advancement of free groups. Jakob Nielsen, a Danish mathematician, further developed the theory of free groups in the 1920s. He introduced the notion of a free group on a set, which is the group generated by the elements of that set subject only to the requirement that no non-trivial product of these elements equals the identity element. Free groups are used in different mathematical fields like geometric group theory, topology, and algebraic geometry. They act as basic components for more

advanced groups and help in comprehending the organization of groups overall. In general, the progression of free groups has been motivated by the curiosity to comprehend the fundamental makeup of groups and their connections to other mathematical entities. Informally, a group is free on a set of generators if no relation holds among these generators except the trivial relations that hold among any set of elements in any group. Definitions about generators and relations are defined and the Ping Pong lemma is proved which is used to prove that the matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ generate a free group of rank 2. [8]

In the fourth chapter, linear representations are defined. The group $G_n(k)$ is treated in detailed and the results related to the group $G_n(k)$ is discussed, namely

- $G_3(2) \geq M\Gamma_3(32)$.
- Any group $G_n(2)$ is not free, provided $n \geq 3$.

The faithfulness of the representation $X_i \mapsto U_{i3}(2)$, $1 \leq i \leq 3$ is discussed and an explicit lower bound for the parameter k is found compared to the previous work [1].

1.1.1 Thesis Objective

This work investigates the matrix representation of a free group.

Chapter 2: Groups

2.1 Introduction

In this section, we discuss basic definition about groups and provide some examples about groups. The main objective of this chapter is to define the equivalence classes of words and the fact that equivalence classes define a free group. Examples used in this section are well-known and can be found in [5].

2.1.1 Binary Operation

A binary operation on a set S is a rule which combines the elements of an ordered pair from S to form an element of S . The most common binary operations are addition, subtraction, and multiplication of integers. Division of integers is not a binary operation on integers, because an integer divided by an integer may no longer be an integer.

Definition 2.1.1. Let U be an arbitrary set. A binary operation on U is a function that assigns every ordered pair of elements of U an element in U .

The binary operator takes inputs from U , say, $a, b \in U$ and produces a single output $ab \in U$.

Definition 2.1.2. Let S be a non-empty set together with a binary operation that assigns to each ordered pair (a, b) of elements of S an

element in S denoted by ab . We say S is a group under this binary operation if the following properties are satisfied :

1. *Associativity*: The operation is associative ; that is, $(ab)c = a(bc)$ for all a, b, c in S .
2. *Identity*: There exists an element e in S , such that $ae = ea = a$ for all $a \in S$.
3. *Inverses*: For every element $a \in S$, there exists an element $b \in S$ such that $ab = ba = e$.

In other words, a group is a set together with an associative operation such that there is an identity, all elements have an inverse, and different pair of elements can be combined without exiting the set known as the property of *closure*. If a group has the property that $ab = ba$ for every pair of elements a and b , the group is said to be *Abelian*. A group is *non-Abelian* if there exists some pair of elements a and b for which $ab \neq ba$.

Example 2.1.1. The set of integers \mathbb{Z} , \mathbb{Q} , \mathbb{R} form a group under addition. In each case the identity is 0 and the inverse of the element s is $-s$.

Example 2.1.2. A rectangular array of form $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is called a 2×2 matrix. The set of all 2×2 matrices with real entries is a group under

component-wise addition.

$$\begin{pmatrix} p_1 & q_1 \\ r_1 & s_1 \end{pmatrix} + \begin{pmatrix} p_2 & q_2 \\ r_2 & s_2 \end{pmatrix} = \begin{pmatrix} p_1 + p_2 & q_1 + q_2 \\ r_1 + r_2 & s_1 + s_2 \end{pmatrix}$$

The identity is

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

The inverse of

$$\begin{pmatrix} p & q \\ r & r \end{pmatrix} \text{ is } \begin{pmatrix} -p & -q \\ -r & -s \end{pmatrix}.$$

The *determinant* of a 2×2 matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is the number $ps - qr$. If

A is a 2×2 matrix, $\det(A)$ denotes the determinant of A .

The set

$$GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} e & f \\ g & h \end{pmatrix} \mid e, f, g, h, \in \mathbb{R}, eh - fg \neq 0 \right\}$$

of 2×2 matrices with real entries and non-zero determinant is a non-

Abelian group under the operation

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

The product of non-singular matrices is also a non-singular matrix. Since, for any pair of 2×2 matrices A and B , $\det(AB) = (\det A)(\det B)$.

Associativity follows from associativity of matrix operations.

The identity element is

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$

$$\text{The inverse of } \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \frac{1}{ps - qr} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}.$$

The above non-commutative group is called the *general linear group* of 2×2 matrices over \mathbb{R} .

Example 2.1.3. The set of 2×2 matrices with real number entries is not a group under the operation defined above.

The reason being, inverses do not exist when the determinant of a matrix is 0.

Example 2.1.4. Consider D_4 , the dihedral group. The notation $R = R_{90}$ for 90° around the center of square and H , a reflection across a horizontal axis, generate the group.

R and H are related in the following ways:

$$R^4 = H^2 = (RH)^2 = R_0 \text{ (the identity)}.$$

Other relations between R and H , such as $HR = R^3H$ and $RHR = H$, also exist, but they are derived from the above equations. For instance:

$$(RH)^2 = R_0$$

implies

$$HR = R^{-1}H^{-1},$$

and

$$R^4 = H^2 = R_0$$

implies

$$R^{-1} = R^3 \text{ and } H^{-1} = H,$$

hence

$$HR = R^3H.$$

Thus, D_4 is a group that is generated by a pair of elements a and b subject to the relations $a^4 = b^2 = (ab)^2 = e$ and such that all other relations between a and b can be derived from these. Any group generated by 2 elements a and b fulfilling the relations $a^4 = b^2 = (ab)^2 = e$ is isomorphic to D_4 .

Definition 2.1.3. If a subset H of a group S is itself a group under the operation of S , we say that H is a subgroup of S . It is denoted by $H \leq S$.

Definition 2.1.4. A subgroup H of a group G is called a *normal subgroup* of G if $aH = Ha$ for all $a \in G$. It is denoted by $H \triangleleft G$.

2.1.2 Equivalence Classes of Words

For any set $S = \{c_1, c_2, c_3, \dots\}$ of distinct symbols, we form a new set $S^{-1} = \{c_1^{-1}, c_2^{-1}, c_3^{-1}, \dots\}$ by replacing each element x in S by x^{-1} . Define the set $W(S)$ to be the collection of all formal finite strings of the form $x_1x_2\cdots x_k$, where each $x_i \in S \cup S^{-1}$. The elements of $W(S)$ are called words from S . We introduce the string with no elements to be in $W(S)$. This word is called as *empty word* and is denoted by e . Define multiplication as an operation on the words, such that

$$w_1 * w_2 = \text{concatenation of } w_1w_2$$

$$= \text{write } w_1 \text{ then write } w_2.$$

Consider $w_1 = aba$ and $w_2 = bbaa..$ Define $w_1 * w_2 = ababbaa$ and also, $w_2 * w_1 = bbaaaba$. The above operation $*$ is not commutative, but it is associative.

Consider $w_1 = aba$ and $w_2 = bbaa$ and $w_3 = aab$, then

$$(w_1 * w_2) * w_3 = (ababbaa) * aab$$

$$= ababbbaaab$$

and

$$w_1 * (w_2 * w_3) = aba * (bbaaab)$$

$$= ababbbaaab.$$

therefore , $(w_1 * w_2) * w_3 = w_1 * (w_2 * w_3)$, so $*$ is associative.

Identity: Let $e = \text{identity}$, be a special word which when concatenated with any word produces w ,
i.e.,

$$e * w = w = w * e, \forall w \in W(S).$$

Thus, it follows that $e =$ is just empty word.

Inverse: Given any element w , there exist w^{-1} such that $w * w^{-1} = e$.

In general, inverses do not exist.

Definition 2.1.5. Given 2 words w_1 and $w_2 \in W(S)$ we say that $w_1 \sim w_2$, if $w_1 = w_2$ or w_2 can be obtained from w_1 by a sequence of basic rewriting rule. These rules are as follows : If $w = Laa^{-1}R$, where $L = \text{left subword}$ and $R = \text{right subword}$ of w , then $w \rightarrow LR$. Similarly , if $w = La^{-1}aR$, then $w \rightarrow LR$ as well.

The reverse operation also holds, we can replace a word $w = LR$ by the new words :

$$w = LR \rightarrow Laa^{-1}R$$

$$w = LR \rightarrow La^{-1}aR$$

for arbitrary letter $a \in S$.

If $w_1 \sim w_2$, then w_1 can be transformed by the opposite sequence of rewriting rules to obtain w_2 .

Proposition 2.1.1. *We have that $' \sim '$ is an equivalence relation.*

Proof. Reflexive : $w \sim w$

Clearly, it is reflexive as we do not add or delete any subword aa^{-1} or $a^{-1}a$.

Symmetry : $w_1 \sim w_2$ then $w_2 \sim w_1$

If w_1 is transformed to w_2 by the basic rewriting rules, then the reverse rules can be applied to obtain w_1 from w_2 , that is

$$\text{therefore, } w_1 \sim w_2 \Rightarrow w_2 \sim w_1$$

Transitive: $w_1 \sim w_2$ and $w_2 \sim w_3 \Rightarrow w_1 \sim w_3$

By the rewriting rules, if w_1 can be transformed to w_2 and then w_2 is transformed to w_3 . Then combining all already preformed rules we can transform w_1 to w_3 .

Example 2.1.5. Let $ab^{-1}baa^{-1}a^{-1}abbb^{-1}a^{-1}a$ be a word, by the associativity property we have :

$$a(b^{-1}b)(aa^{-1})(a^{-1}a)bbb^{-1}a^{-1}a$$

$$\rightarrow a(aa^{-1})(a^{-1}a)bbb^{-1}a^{-1}a$$

$$\rightarrow a(a^{-1}a)bbb^{-1}a^{-1}a$$

$$\rightarrow ab(bb^{-1})a^{-1}a$$

$$\rightarrow ab(a^{-1}a)$$

$$\rightarrow ab$$

is the equivalent reduced word of smallest length.

Any equivalence relation partitions the set into a collection of disjoint equivalence classes. In the next section we show that the set of equivalence classes of words form a group.

2.1.2.1 Equivalence Classes Form a Group

Let S be a set of distinct symbols. For any word $w_1 \in W(S)$, let $[w]$ denote the set of all words in $W(S)$ equivalent to w . Then the set of all equivalence classes of elements of $W(S)$ is a group under the operation $*$.

Proposition 2.1.2. $W(S)/\sim$ has a well-defined binary operation given by $[w_1] \cdot [w_2] = [w_1 * w_2]$.

Proof. Let $x_1 \in [w_1]$ and $x_2 \in [w_2]$ i.e. $[w_1] = [x_1]$ and $[w_2] = [x_2]$.

We show : $[x_1 * x_2] = [w_1 * w_2]$.

Given : $x_1 \sim w_1$ and $x_2 \sim w_2$.

To show : $x_1 * x_2 \sim w_1 * w_2$.

Consider w_1 and apply the rewriting rules to transform w_1 to a new word z_1 and then keep applying the rules to obtain x_1 . Similarly, on w_2 applying the rewriting rules to transform w_2 to a new word z_1' and then keep applying the rules to obtain x_2 .

$$\Rightarrow w_1 * w_2 \rightarrow z_1 * w_2 \rightarrow z_2 * w_2 \rightarrow \cdots \rightarrow x_1 * w_2.$$

Similarly , from left concatenation,

$$x_1 * w_2 \rightarrow x_1 * z_1' \rightarrow x_1 * z_2' \rightarrow \cdots \rightarrow x_1 * x_2$$

$$\Rightarrow w_1 * w_2 \sim x_1 * x_2,$$

whence the binary operation is well-defined.

Theorem 2.1.3. $W(S)$ is a group under operation $*$.

Proof. For arbitrary $w_1, w_2, w_3 \in W(S)$ we have

$$\begin{aligned}
 ([w_1] \cdot [w_2]) \cdot [w_3] &= [w_1 * w_2] \cdot [w_3] \\
 &= [(w_1 * w_2) * w_3]. \\
 &= [w_1 * (w_2 * w_3)]. \\
 &= [w_1] \cdot ([w_2] \cdot [w_3]),
 \end{aligned}$$

hence the operation \cdot is associative.

The identity element of $W(S)/\sim$: Consider $e = [\phi]$ as the empty word to be the identity element.

$$[w] \cdot [\phi] = [w * \phi] = [w] \text{ and}$$

$$[\phi] \cdot [w] = [\phi * w] = [w].$$

- Inverse element of $W(S)/\sim$.

For any given element $[w]$ in G we need to find another element such that $[w][?] = [\phi]$, the empty word.

$$\text{Consider } [w] \cdot [w^{-1}] = [w * w^{-1}] = [ww^{-1}] = [\phi] = e.$$

$$\text{Similarly, } [w^{-1}] \cdot [w] = [w^{-1} * w] = [w^{-1}w] = [\phi] = e.$$

Combining all together we conclude that $(W(S)/\sim, \cdot)$ is a group.

In what follows $(W(S)/\sim, *)$ is called the free group on S and it is denoted by $F(S)$.

Chapter 3: Universality of Free Groups

3.1 Introduction

In this section, we define a free group as an universal object in the category of groups and formulate some standard results in the free group theory. The Ping pong lemma [9] is proved and its applications are given. Standard definitions about generators and relations can be found in this chapter, which are available in [5], [2].

Definition 3.1.1. Given a non-empty set S , and a map $\theta : S \rightarrow F$, a group F , the pair (F, θ) is said to be a free group on S , if for any function $\alpha : S \rightarrow G$ to any group G , there is a unique homomorphism $\tilde{\alpha} : F \rightarrow G$ such that $\alpha = \tilde{\alpha} \circ \theta$

Theorem 3.1.1. *The group $F(S)$ is a free group in the sense of the above definition.*

Proof. Let T be a group and $\alpha : S \rightarrow T$ be a function.

We extend this map to $\tilde{\alpha} : F(S) \rightarrow T$ by the rule

$$[w] \mapsto \alpha(x_1) \dots \alpha(x_k),$$

provided $w = x_1 \dots x_k$, $x_1, \dots, x_k \in S \cup S^{-1}$. Besides,

$\alpha(a^{-1}) = \alpha(a)^{-1}$ for any $a \in S$.

Clearly, $\tilde{\alpha}$ is well- defined, for inserting and deleting expression of the form aa^{-1} or $a^{-1}a$ in elements of $W(S)$ corresponds to inserting or deleting the identity in T .

To prove $\tilde{\alpha}$ is *operation - preserving* :

In fact, we have

$$\begin{aligned}\tilde{\alpha}([x_1x_2 \cdots x_n] \cdot [y_1y_2 \cdots y_m]) &= \tilde{\alpha}([x_1x_2 \cdots x_ny_1y_2 \cdots y_m])) \\ &= \alpha(x_1)\alpha(x_2) \cdots \alpha(x_n)\alpha(y_1)\alpha(y_2) \cdots \alpha(y_m) \\ &= \tilde{\alpha}([x_1x_2 \cdots x_n])\tilde{\alpha}([y_1y_2 \cdots y_m]).\end{aligned}$$

3.1.1 Universal Factor Group

Theorem 3.1.2. *An arbitrary group is a factor group of some free group.*

Proof. Let H be any group and let S be a subset that generates H .

Let Y be any set that is in one-to-one correspondence with S .

Let $F(Y)$ be a free group on set of generators Y .

If $\alpha : Y \rightarrow S$ is a bijection , then by the universal property of $F(Y)$

gives a surjective homomorphism from $F(Y)$ to H .

Theorem 3.1.3. *Let K be any group. Then K is a free group on the generating set X if and only if no reduced word in $X \cup X^{-1}$ of positive length is the identity.*

Proof. Consider the unique homomorphism $\theta : F(X) \rightarrow K$ that extends the inclusion map X into K . The conditions of theorem are equivalent to bijectivity of θ , since each class $[w]$ contains the unique reduced word of minimal length. Thus θ is an isomorphism and K is a free group.

Conversely, If K is free on X , then the unique homomorphism $\phi : K \rightarrow F(X)$ extending the inclusion of X into $F(X)$ (which exists because K is free on X) is the inverse of θ since X generates K . Thus, ϕ is an isomorphism which means it is a bijection and the condition holds.

Example 3.1.1. Let $S = \{a\}$ be a free group on one element denoted by $F(S)$. The set $F(S)$ is isomorphic to $(\mathbb{Z}, +)$.

Solution: Consider $S' = \{a, a^{-1}\}$ Any word in alphabet S' is a finite product of letters a and a^{-1} .

To prove : $F(S) \cong \mathbb{Z}$

One can define a surjective homomorphism $\phi : F(S) \rightarrow \mathbb{Z}$, induced by the function $S \rightarrow \mathbb{Z}, a \mapsto 1$. Let w be any word in S' . Let n and m denote the number of a in w and the number of a^{-1} in w , respectively. By the induction on the length one can show that any word w can be transformed to the equivalent word $w' = a^k$, where $a^k = \underbrace{a \cdots a}_k$ provided $k \geq 0$, otherwise $a^k = \underbrace{a^{-1} \cdots a^{-1}}_{|k|}$. Moreover, $\phi([w]) = \phi([w']) = k$.

Thus, it follows immediately that ϕ has trivial kernel, hence it is an isomorphism.

3.1.2 Free Subgroups

Let G be a group and let $F(X) \rightarrow G$ be a surjective homomorphism as in Theorem 3.3.

The elements of the kernel R of the epimorphism $F(X) \rightarrow G$, are called the relators of the group G , in terms of the alphabet X . If a subset R_1 of these relators is such that the smallest normal subgroup containing R_1 is R itself, then we call R_1 a set of defining relators in the alphabet X . Since, $G \simeq F(X)/R$, the alphabet X and the set R_1 of words completely determines G up to isomorphism. [10]

Definition 3.1.2. The pair $\langle X|R_1 \rangle$, is called *a presentation of the group G in terms of generators and relations*, or, more precisely, a presentation of G and expressed as $G \simeq \langle X|R_1 \rangle$. Groups that can be defined by a finite set of generators and relations are referred to as finitely presented groups. [9]

Definition 3.1.3. Let G_1 and G_2 be groups and $\langle X_1|R_1 \rangle$ and $\langle X_2|R_2 \rangle$ be their presentations in terms of generators and relations. Then the group $\langle X_1 \sqcup X_2 | R_1 \sqcup R_2 \rangle$ is said to be a *free product* of the groups G_1 and G_2 . It is denoted by $G_1 * G_2$.

Observe that the natural functions $X_1 \rightarrow G_1 * G_2$ and $X_2 \rightarrow G_1 * G_2$ are uniquely extended to the homomorphisms $j_1 : F(X_1) \rightarrow G_1 * G_2$ and $j_2 : F(X_2) \rightarrow G_1 * G_2$. Since $j_1(R_1) = e = j_2(R_2)$, they induce the

unique homomorphisms $i_1 : G_1 \rightarrow G_1 * G_2$ and $i_2 : G_2 \rightarrow G_1 * G_2$.

Theorem 3.1.4. *The free product is universal in the following sense :*

*Any couple of homomorphisms $f_1 : G_1 \rightarrow H$ and $f_2 : G_2 \rightarrow H$ can be uniquely extended to the homomorphism $f : G_1 * G_2 \rightarrow H$ such that $fi_1 = f_1$ and $fi_2 = f_2$.*

Proof. Note that the homomorphisms f_1 and f_2 are in one-to-one correspondence with the homomorphisms $h_1 : F(X_1) \rightarrow H$ and $h_2 : F(X_2) \rightarrow H$, such that $h_1(R_1) = e = h_2(R_2)$. By the universal property of a free group, there is the unique homomorphism $h : F(X_1 \sqcup X_2) \rightarrow H$ such that $h|_{X_1} = h_1|_{X_1}$ and $h|_{X_2} = h_2|_{X_2}$. Thus $h(R_1 \sqcup R_2) = h_1(R_1) \cup h_2(R_2) = e$ and therefore, h induces the unique homomorphism $f : G_1 * G_2 \rightarrow H$. Moreover, it is clear that $fi_1 = f_1$ and $fi_2 = f_2$.

The group $G_1 * G_2$ can be explicitly constructed in the way similar to the above for $F(S)$.

Consider the elements of G_1 and G_2 as the *formal letters* (g) and (h) , $g \in G_1, h \in G_2$. As above, we can define the set of all words $W((G_1) \sqcup (G_2))$ in the alphabet $(G_1) \sqcup (G_2) = \{(g), (h) \mid g \in G_1, h \in G_2\}$ with the associative operation $*$ (concatenation).

Rewriting rules are :

$$L(g)(g')R \rightarrow L(gg')R,$$

$$L(h)(h')R \rightarrow L(hh')R,$$

$$L(e)R \rightarrow LR$$

and their reverses as well, where L and R are left and right subwords of the word $w = (x_1) \cdots (x_k)$, $(x_1), \dots, (x_k) \in (G_1) \sqcup (G_2)$.

Theorem 3.1.5. *A subgroup of a free group is free again.*

The proof of the above theorem can be found in [8].

3.1.2.1 Construction

If G_1 and G_2 are groups, a word in G_1 and G_2 is a product of the form

$$g_1 g_2 \cdots g_n$$

where each g_i is either an element of G_1 or an element of G_2 . Such a word may be reduced using the operations:

- remove the identity element from either in G_1 or G_2 .
- replace a pair of the form g_1g_2 by its product in G_1 , or a pair h_1h_2 by its product in G_2 .

3.1.2.2 Ping Pong Lemma

Lemma 3.1.6. *Suppose G is a group acting on a set S . Suppose there are two non-empty subsets S_1, S_2 of S with S_2 not included in S_1 and subgroups G_1 and G_2 of G such that G_1 has at least 3 elements and satisfy $g(S_2) \subset S_1, h(S_1) \subset S_2, \forall g \in G_1 \setminus 1, h \in G_2 \setminus 1$. Then, the subgroup G_0 of G generated by G_1 and G_2 is isomorphic to the free product of G_1 and G_2 .*

Proof. Assume $G_1 \cap G_2 \neq \{1\}$. For, if $1 \neq g_1 = g_2 \in G_1 \cap G_2$, then look at some $s_2 \in S_2 \setminus S_1$. Then, for $x_1 \in G_1, x_1 \neq 1, g_1^{-1}$,

$$s_2 = x_1 g_1 g_2^{-1} x_1^{-1}(s_2) \in S_1$$

since x_1^{-1} carries s_2 into an element of S_1 which is, in turn, taken by g_2^{-1} into an element of S_2 which is finally taken by $x_1 g_1$ to an element of S_1 . Thus, $s_2 \in S_1$, a contradiction. Therefore, $G_1 \cap G_2 = \{1\}$.

Consider any reduced word of the form $w = g_1 h_1 g_2 h_2 \cdots g_r$

where $g_i \in G_1 \setminus 1$ and $h_i \in G_2 \setminus 1$. Note that $w(S_2) \subseteq S_1$. If $w = 1$, then for each $s_2 \in S_2$, we have $s_2 = w(s_2) \in S_1$. thus $S_2 \subseteq S_1$, a contradiction. So $w \neq 1$.

Now, if $w = h_1 g_1 \cdots h_r$ is a reduced word, we get $x_1 \in G_1$ such that $x_1 \neq 1$. Then the reduced word $x_1 h_1 g_1 \cdots h_r x_1^{-1} \neq 1$ by the above argument. So, $w \neq 1$.

If $w = g_1 h_1 \cdots g_r h_r$ is a reduced word, then get $x_1 \in G_1, x_1 \neq 1, g_1^{-1}$. So, $x_1 w x_1^{-1} \neq 1$ follows from the previous argument. Hence, $w \neq 1$.

Similarly, if $w = h_1 g_1 \cdots h_r g_r$ is a reduced word, then $g_r w g_r^{-1}$ is a nontrivial word by the last statement. Hence $w \neq 1$.

Example 3.1.2. The two matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ generate a subgroup of $\text{SL}(2, \mathbb{Z})$ which is isomorphic to free group of rank 2. [6]

Proof. Let $G_1 = \left\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \mid n \in \mathbb{Z} \right\}$
and $G_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \mid n \in \mathbb{Z} \right\}$ be the infinite cyclic groups

of $\text{SL}(2, \mathbb{Z})$ generated respectively by the matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \text{ respectively.}$$

The group $\text{SL}(2, \mathbb{Z})$ acts linearly on \mathbb{R}^2 in the usual way. Let

$$S_1 = \left\{ \begin{pmatrix} p \\ q \end{pmatrix} \in \mathbb{R}^2 \mid |p| > |q| \right\}$$

and

$$S_2 = \left\{ \begin{pmatrix} p \\ q \end{pmatrix} \in \mathbb{R}^2 \mid |p| < |q| \right\}.$$

It is easy to check that the subgroups G_1, G_2 and the sets

S_1, S_2 satisfy the conditions of ping-pong lemma, hence they generate

a subgroups of $\text{SL}(2, \mathbb{Z})$ that is isomorphic to $\mathbb{Z} * \mathbb{Z}$.

Observe that the two matrices $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$

generate a free subgroup of rank 2 in $\text{SL}(2, \mathbb{Z})$ for any $m \geq 2$, for the

same reasons, but not for $m = 1$. In fact, we have

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

is of finite order.

Note $\mathrm{SL}(2, \mathbb{Z})$ is generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Chapter 4: Representation

4.1 Introduction

In this chapter, we state the results related to the group $G_n(k)$, which is generated by the matrices

$$U_{in}(k) = E_n + \sum_{1 \leq j \neq i \leq n} k e_{ji}, 1 \leq i \leq n,$$

where E_n is the identity $n \times n$ matrix, and e_{ij} is the matrix whose all entries are zero except the entry in i -th row and j -th column, is equal to 1, $1 \leq i, j \leq n$. Besides, k is an real number. Results obtained in this chapter are derived from [1], [3].

These matrices determine a linear representation of the free group $F(X)$ of rank n , as

$$X_i \mapsto U_{in}(k), 1 \leq i \leq n, F(X) \rightarrow \text{SL}(n).$$

Note that if $n = 2$ and $k \geq 2$, then this is well known Sanov's faithful representation of the free group of rank 2 (see Example 3.10 above). These representations are investigated in [1]. More precisely, it was proved that they are faithful for any $n \geq 3$ and $k \geq 5$. Using the same method as in [1], we improve the lower bound for k . Also, we give another proof of the fact that $G_n(2)$ is not free, whenever $n \geq 3$.

Definitions of representation and examples related to representation are stated can be also found [7, 10].

Given a vector space V , let $GL(V)$ denote the group of invertible linear transformations from V to itself. This group is naturally isomorphic to the group of all invertible $n \times n$ matrices $GL(n)$, where $n = \dim V$. The subgroup of $GL(n)$ consisting of all matrices with determinant 1 is said to be *special linear group*. It is denoted by $SL(n)$.

Definition 4.1.1. A representation of a group G is group homomorphism $\phi : G \rightarrow GL(V)$ where V is a vector space.

If the homomorphism is injective, then the representation is said to be **faithful**. The image of a faithful representation is isomorphic to the original group.

Example 4.1.1. The function

$$X_1 \mapsto U_{12}(2), X_2 \mapsto U_{22}(2)$$

determines the linear representation of the free group of rank two, $F(X) \rightarrow SL(2)$.

4.1.1 The Group $G_n(2)$, $n \geq 3$

Lemma 4.1.1. Assume that $2 \leq r \leq n$. In this case, the correspondence $U_{ir}(k) \leftrightarrow U_{in}(k)$, $1 \leq i \leq r$, can be extended to an embedding of $G_r(k)$ in $G_n(k)$.

Proof. In the ring of matrices $M_n(\mathbb{R})$, we generate a subring K by the elements $(s_{1n}, s_{2n}, \dots, s_{rn})$. where

$$s_{1n} = \sum_{1 \leq i, \neq j \leq r} e_{j1}, s_{2n} = \sum_{1 \leq i, \neq j \leq r} e_{j2}, \dots, s_{rn} = \sum_{1 \leq i, \neq j \leq r} e_{jr}$$

It is clear that K is the homomorphic image of the absolutely free associative ring $\mathbb{Z}(x_1, x_2, \dots, x_r)$ with respect to the homomorphism $x_i \mapsto s_{in}$.

Denote by I the kernel of the corresponding homomorphism. Elementary calculations show that $x_i^2, x_i x_j x_i - x_i$, and $x_i x_j x_l - x_i x_l \in I, \forall i \neq j, i \neq l, j \neq l$. Moreover, the ideal I is generated by these elements.

Indeed, modulo these relations, each element of the ring $\mathbb{Z}(x_1, x_2, \dots, x_r)$ can be transformed to an expression of the form

$$u \cdot 1 + \sum_{1 \leq i, \neq j \leq r} v_{ij} x_i x_j, u, v_{ij} \in \mathbb{R}.$$

If this element belongs to the ideal I , then, writing this

expression in $M_n(\mathbb{R})$, we obtain the relation

$$0 = uE_n + \sum_{1 \leq i \neq j \leq r} v_{ij} s_{in} s_{jn}.$$

After a simple recalculation we obtain,

$$0 = uE_n + \sum_{1 \leq i \neq j \leq r} v_{ij} (\sum_{k \neq i, 1 \leq k \leq n} e_{kj})$$

Changing the addition once more, we arrive at the expression

$$uE_n + \sum_{1 \leq k \leq n, 1 \leq j \leq r} (e_{kj}) (\sum_{i \neq k, j, 1 \leq i \leq r} v_{ij}) = 0$$

The case $r = n = 2$ can be treated directly, so that $u = v_{12} = v_{21} = 0$. Assume that $n \geq 3$ and $r = 2$. In this case, the coefficient of e_{31} is v_{21} and that of e_{32} is v_{12} .

It remains to treat the case in which $n \geq 3$ and $r \geq 3$. Let $1 \leq j, k_1, k_2 \leq r$, where $j \neq k_1, j \neq k_2$, and $k_1 \neq k_2$. We obtain

$$\sum_{i \neq j, k_1, 1 \leq i \leq r} v_{ij} = \sum_{i \neq j, k_2, 1 \leq i \leq r} v_{ij} = 0.$$

In particular, $v_{k_1 j} = v_{k_2 j}$. Since, j, k_1, k_2 is arbitrary, it

follows that all v_{ij} are pairwise equal, and hence they are zero. This implies, $u = 0$. The dimension n of the matrices play no role in the argument. Hence, $K \cong Z(x_1, x_2, \dots, x_r)/I \cong Z[s_{1r}, s_{2r}, \dots, s_{rr}]$. Specifically, the correspondence $s_{in} \leftrightarrow s_{ir}$, $1 \leq i \leq r$, can be extended to an isomorphism of $Z[s_{1r}, s_{2r}, \dots, s_{rr}]$ onto $Z[s_{1n}, s_{2n}, \dots, s_{rn}]$. Clearly, under this isomorphism, each U_{ir} is mapped into U_{in} .

Lemma 4.1.2. *An arbitrary permutation of the generators $U_{in}(k)$ can be extended to an automorphism of the group $G_n(k)$.*

Proof. As usual, it suffices to prove the lemma for the transpositions. Let $U_{in}(k) \mapsto U_{jn}(k)$, $U_{jn}(k) \mapsto U_{in}(k)$, and $U_{ln}(k) \mapsto U_{ln}(k)$ for $l \neq i, j$. The ring $Z[s_{1n}, \dots, s_{nn}]$ is isomorphic to the quotient ring $Z(x_1, \dots, x_r)/I$. The substitution $x_i \mapsto x_j$, $x_j \mapsto x_i$, $x_l \mapsto x_l$, $l \neq i, j$ rearranges the generators of the ideal I only. Clearly, this substitution induces an automorphism $Z(x_1, x_2, \dots, x_r)/I$, i.e., a ring automorphism of $Z[s_{1n}, \dots, s_{nn}]$. This automorphism induces the desired automorphism of the group $G_n(k)$.

$$\text{Let } A_1 = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Consider the products

$$B_1 = A_1 U_{33}(2) A_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \quad C_1 = A_1 U_{23}(2) A_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}.$$

By Sanov's result, the group $G_2(2)$ consists of all matrices of the form

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z})$$

for which $\alpha \equiv \delta \equiv 1(mod 4)$ and $\beta \equiv \gamma \equiv 0(mod 2)$. Therefore, this means that the group $\langle B_1, C_1 \rangle$ consists of all matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \gamma & \delta \end{pmatrix} \text{ where, } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G_2(2).$$

Also, the following holds

$$D^k = \begin{pmatrix} 1-4k & -4k & -4k \\ 2k & 1+2k & 2k \\ 2k & 2k & 1+2k \end{pmatrix}$$

where

$$D = A_1 U_{13}(2) A_1^{-1} = \begin{pmatrix} -3 & -4 & -4 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1-4 & -4 & -4 \\ 2 & 1+2 & 2 \\ 2 & 2 & 1+2 \end{pmatrix}$$

For any matrix define

$$u(B_1, C_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \gamma & \delta \end{pmatrix}$$

and for any $k \in \mathbf{Z}$ we have,

$$D^{-k} u(B_1, C_1) X^k = \begin{pmatrix} 1+x & 4kf+x & 4kt+x \\ p+(4k^2-p)r-4k^2z & \alpha+2kg-x/2 & \beta+2kh-x/2 \\ p+(4k^2-p)z-4k^2r & \gamma-2kh-x/2 & \delta+2ky-x/2 \end{pmatrix} \quad (4.1)$$

where

$$f = \alpha + \gamma - 1, \quad t = \beta + \delta - 1, \quad r = \alpha + \beta, \quad y = \gamma - \delta,$$

$$g = t - z + 1, \quad h = f - z + 1, \quad x = 8k^2(s-2), \quad p = -2k(1-4k), \quad z = \alpha + \beta + \gamma + \delta.$$

Let $\text{M}\Gamma_n(k)$ denote the subgroup of $\text{SL}(n)$ consisting of all matrices (a_{ij}) such that

$$a_{ii} \equiv 1 \pmod{k^2}, \quad a_{ij} \equiv 0 \pmod{k}, \quad 1 \leq i \neq j \leq n.$$

We call it *Mennicke congruent subgroup* (cf. [4]). The following theorem is the corrected version of the theorem $G_3(2) \geq \Gamma_3(32)$ as proved in [1].

Theorem 4.1.3. $G_3(2) \geq \text{M}\Gamma_3(32)$.

Proof. Let $\alpha = 1 + 4m$, $\delta = 1 - 4m$, $\beta = 4m$, $\gamma = -4m$ and find a matrix of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 16km & @ & @ \\ -16km & @ & @ \end{pmatrix},$$

where the corner

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & @ & @ \\ 0 & @ & @ \end{pmatrix}$$

is an element in the group $\langle B_1, C_1 \rangle$. Using the cancellation property with an appropriate element of this group, we have, the matrix

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 16 & 1 & 0 \\ -16 & 0 & 1 \end{pmatrix}.$$

The subgroup generated by $U_{32}(2)$ and $U_{33}(2)$ consists of all

matrices of the form

$$\begin{pmatrix} 1 & \alpha + \gamma - 1 & \beta + \delta - 1 \\ 0 & \alpha & \beta \\ 0 & \gamma & \delta \end{pmatrix}, \quad \text{where } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G_2(2),$$

therefore, we have

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 - 16 & -16 \\ -16 & 16 & 1 + 16 \end{pmatrix} \in G_3(2)$$

and

$$R = D^{-1}ND = P = \begin{pmatrix} 1 & 0 & 0 \\ 16 & 1 - 16 & -16 \\ -16 & 16 & 1 + 16 \end{pmatrix} \in G_3(2)$$

and,

$$RN^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 16 & 1 & 0 \\ -16 & 0 & 1 \end{pmatrix} \in G_3(2).$$

Multiply by $U_{13}(2)^8$, we have the transvection

$$t_{21}(32) = \begin{pmatrix} 1 & 0 & 0 \\ 32 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in G_3(2).$$

Also,

$$NP^{-1}U_{13}^8 = t_{31}(32) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 32 & 0 & 1 \end{pmatrix} \in G_3(2).$$

Let $\sigma \in S_n$ be an arbitrary permutation on n symbols. The mapping $U_{in}(k) \mapsto U_{\sigma(i),n}(k)$ is an automorphism of the group $G_n(k)$. Also, by induction on the length of the element $u \in G_n(k)$, we can prove that $u^\sigma b^t = (u(b^\sigma)^t)^\sigma$, where $b \in \mathbf{R}^n$ and $(b^\sigma)_i = b_{\sigma^{-1}(i)}$, $1 \leq i \leq n$. Consider the permutation

$$\kappa : U_{13}(2) \mapsto U_{23}(2), U_{23}(2) \mapsto U_{13}(2).$$

Let the standard basis of the space \mathbf{R}^3 , be as, $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0, 0, 1)$. Using this fact we

derive,

$$t_{21}(32)^{\kappa} e_1^t = (t_{21}(32) e_2^t)^{\kappa} = (e_2^{\kappa})^t = e_1^t.$$

Also,

$$t_{21}(32)^{\kappa} e_2^t = (32, 1, 0)^t, \quad t_{21}(32)^{\kappa} e_3^t = e_3^t$$

Therefore, $t_{21}(32)^{\kappa} = t_{12}(32) \in G_3(2)$. Similarly, the other transvections $t_{ij}(32)$, $1 \leq i \neq j \leq 3$ can be generated. By the main result of this [4], our statement immediately follows.

Theorem 4.1.4. *Any group $G_n(2)$ is not free, provided $n \geq 3$.*

Proof. Since $G_3(2)$ is embedded to $G_n(2)$, all we need is to prove that $G_3(2)$ is not free. Assume the opposite. By Theorem 4.5 the group $G_3(2)$ contains matrices $t_{12}(32)$ and $t_{13}(32)$. It is easy to see that these two matrices are commuting. Moreover, they generate a subgroup of $G_3(2)$ that is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. The latter is obviously not free, a contradiction.

Remark 4.1.1. In [1] many nontrivial relations between the generators of $G_3(2)$ are found. But in the strict sense of the word, this does not mean the lack of freeness of this group. Of course, the

representation $X_i \mapsto U_{i3}(2)$, $1 \leq i \leq 3$, is not faithful, but it is still possible that there is another set of generators which freely generate $G_3(2)$. This gap in the original proof is amended here.

4.1.2 The Faithfulness of the Representation

Theorem 4.1.5. *For all $n \geq 3$ and $k \geq \frac{8 \times 2^{\frac{2}{3}}}{3 \sqrt[3]{3\sqrt{273+59}}} + \frac{\sqrt[3]{2(3\sqrt{273+59})}}{3} + \frac{4}{3}$, the group $G_n(k)$ is free, and $U_{in}(k)$, $1 \leq i \leq n$ are its free generators.*

Proof. Without loss of generality, we may assume that $k \geq 0$.

Let $v = v_s = U_{r_s n}(k)^{l_s} \cdots U_{r_1 n}(k)^{l_1}$ be an arbitrary reduced word in the alphabet formed by the generators $U_{in}(k)$. In other words, $r_i \neq r_{i+1}$, $1 \leq i \leq s-1$ and $l_1, l_2, \dots, l_s \in \mathbf{Z} \setminus 0$. As usual, denote by $e_1 \dots e_n$ the standard basis of \mathbb{R}^n .

Our objective is to show that $ve_{r_1}^t = b^t$ and that all coordinates of the vectors b are nonzero. Moreover, all these coordinates, possibly except for b_{r_s} , are of the same sign. In particular, $ve_{r_1}^t \neq e_{r_1}^t$, and hence $v \neq E_n$.

We say that a vector b satisfies the condition (l) with parameters $a, d > 0$ if all coordinates of b are nonzero, all b_i with

$i \neq l$ are of the same sign and satisfy the relation

$$0 < a \leq \left| \frac{b_i}{b_l} \right|$$

and, for any $i, j \neq j$, we have either

$$1 \leq \left| \frac{b_i}{b_l} \right| \leq d$$

or

$$\frac{1}{d} \leq \left| \frac{b_j}{b_i} \right| \leq 1.$$

Let us show by induction on the length of v that $ve_{r_1}^t$ satisfies condition (r_s) with parameters a and d that depend on k only. As we progress, some inequalities for a and d arise which we justify by the induction step.

Base of Induction :

Take a and d such that $\frac{1}{k} < a < k$ and $1 \leq d < k$. In this case, the vector

$$U_{r_1 n}(k)^{l_1} e_{r_1}^t = (kl_1, \dots, 1, \dots, \underbrace{r_1}, 1, \dots, kl_1)^t$$

obviously satisfies condition (r_1) with parameters a and d .

Inductive step : Simplifying the notation , we set $i = r_s$ and $j = r_{s+1}, i \neq j$. Assume that the vector $v_s e_{r_1}^t = b^t$ satisfies the condition (i) with parameters a and d .

Let $U_{jn}(k)^l b^t = (b')^t = (b'_1, \dots, b'_n)^t$, where $b_j = b'_j$ and $b'_m = b_m + kl b_j$ for all $m \neq j$. By assumption, $b_j = b'_j \neq 0$. Hence,

$$\left| \frac{b'_m}{b'_j} \right| = \left| \frac{b_m}{b_j} + lk \right| \geq k - \left| \frac{b_m}{b_j} \right| \geq a$$

for any $m \neq j$.

If $m = i$, then $\left| \frac{b_i}{b_j} \right| \leq \frac{1}{a}$, and for the inductive step we must have $k - \frac{1}{a} \geq a$. If $m \neq i$, then $\left| \frac{b_m}{b_j} \right| \leq d$, and hence $k - d \geq a$. The first inequality is equivalently to the inequalities

$$\frac{k - \sqrt{k^2 - 4}}{2} \leq a \leq \frac{k + \sqrt{k^2 - 4}}{2}$$

Since,

$$k - d \leq k - 1 < \frac{k + \sqrt{k^2 - 4}}{2}$$

we finally obtain two inequalities,

$$\frac{k - \sqrt{k^2 - 4}}{2} \leq a \leq k - d \quad \text{and} \quad 1 \leq d < k$$

. Let $m \neq s, m \neq j$, and $s \neq j$. Denote by x the absolute value

$$\left| \frac{b'_m}{b'_s} \right| = \left| \frac{kl + \frac{b_m}{b_j}}{kl + \frac{b_s}{b_j}} \right|$$

Our subsequent argument depends on the sign of l .

1. Let $l > 0$. If $m, s \neq i$, then, by assumption, the coefficients b_j, b_m, b_s are of the same sign, i.e. $\frac{b_m}{b_j} > 0$ and $\frac{b_s}{b_j} > 0$. Depending on which number is larger, $\frac{b_m}{b_j}$ or $\frac{b_s}{b_j}$, we have either $1 \leq x \leq \frac{k+d}{k+\frac{1}{d}}$ or $\frac{k+\frac{1}{d}}{k+d} \leq x \leq 1$. Thus, we must have

$$\frac{k+d}{k+\frac{1}{d}} \leq d \quad \text{and} \quad \frac{1}{d} \leq \frac{k+\frac{1}{d}}{k+d}$$

However, these inequalities are equivalent and follow from the condition $d \geq 1$.

We assume now that $m = i$. By the induction assumption we have $\frac{b_i}{b_j} \leq \frac{1}{a}$ and $\frac{b_s}{b_j} > 0$. If $\frac{b_i}{b_j} \geq \frac{b_s}{b_j} > 0$, then

$$1 \leq x \leq \frac{k+\frac{1}{a}}{k+\frac{1}{d}} \leq d, \quad \text{i.e.} \quad ka+1 \leq a(kd+1)$$

. Otherwise,

$$1 \geq x \geq \frac{k-\frac{1}{a}}{k+d} \geq \frac{1}{d}$$

The case $s = i$ can be treated similarly.

2. Let $l < 0$. In this case we must estimate the expression

$$y = \left| \frac{kl - \frac{b_m}{b_j}}{kl - \frac{b_s}{b_j}} \right|$$

As above, we first assume that $m, s \neq i$. Repeating the argument

of part 1, we obtain a pair of inequalities of the form

$$1 \leq y \leq \frac{k - \frac{1}{d}}{k - d} \leq d \quad \text{and} \quad \frac{1}{d} \leq \frac{k - d}{k - \frac{1}{d}} \leq y \leq 1$$

This pair can be reduced to a single inequality, $kd - 1 \leq d^2(k - d)$. If $m = i$ (or $s = i$), then in case of $\frac{b_i}{b_j} \geq \frac{b_s}{b_j} > 0$ we obtain the inequality

$$1 \geq y \geq \frac{k - \frac{1}{a}}{k - \frac{1}{d}} \geq \frac{1}{d}.$$

Otherwise, we have $1 \leq y \leq \frac{k + \frac{1}{a}}{k - d} \leq d$. Simplifying we obtain

$$a(kd - 1) \leq d^2(ka - 1) \quad \text{and} \quad ka + 1 \leq ad(k - d).$$

Thus, for the inductive step to be realizable, the parameters a and d must satisfy the system of inequalities

$$\frac{k - \sqrt{k^2 - 4}}{2} \leq a \leq k - d, \quad 1 \leq d < k, \quad (4.2)$$

$$ka + 1 \leq a(kd - 1), \quad (4.3)$$

$$a(k + d) \leq d(ka - 1), \quad (4.4)$$

$$kd - 1 \leq d^2(k - d), \quad (4.5)$$

$$a(kd - 1) \leq d^2(ka - 1), \quad (4.6)$$

$$ka + 1 \leq ad(k - d). \quad (4.7)$$

We observe that some of the inequalities mentioned above are unnecessary. Inequality (7) is better than inequality (3) and (5) as d is positive. Inequality (4) is much stronger than (6). The above inequalities can be reduced to just 3 inequalities, namely, (2), (4), (7).

Let $\phi(k)$ be the set of solutions of the reduced system of inequalities.

4.1.2.1 Inequality Solution

Consider,

$$ka + 1 \leq adk - ad^2.$$

Rearranging the above inequality we have :

$$a(dk - d^2 - k) \geq 0$$

$-d^2 + dk - k > 0$, because $a > 0$ and the inequality is greater than 1

$$-d^2 + dk - k > 0$$

The above inequality in d has a real solution only if the discriminant is greater than 0. Solving the above quadratic inequality using the quadratic formula in d , leads to

$$\frac{-k \pm \sqrt{k^2 - 4k}}{-2}$$

which has a real solution only if

$$k \geq 0 \text{ or } k \geq 4$$

By the inequality 4.7, one can also derive that

$$ka + 1 \leq ad(k - d)$$

$$k + \frac{1}{a} \leq dk - k^2$$

$$\frac{1}{a} \leq dk - d^2 - k$$

$$\frac{1}{a} \leq -d^2 + dk - k$$

Also, we know $0 < \frac{1}{k} < \frac{1}{a} < k$

$$\frac{1}{k} < -d^2 + dk - k$$

cross-multiplying k , it simplifies to

$$dk^2 - kd^2 - k^2 > 1$$

rearranging the above inequality and dividing by the negative sign yields

$$d^2k - k^2d + k^2 + 1 < 0$$

Again, solving the above quadratic inequality in d , we have

$$\frac{k^2 - \sqrt{k^4 - 4(k^2 + 1)k}}{4k}$$

which simplifies as

$$\frac{k^2 - \sqrt{k^4 - 4k^3 - 4k}}{4k}$$

We observe that it has a real solution only if the discriminant ≥ 0 .

$$k^4 - 4k^3 - 4k \geq 0$$

i.e.

$$k^4 \geq 4(k^2 + 1)k$$

$$k^3 \geq 4(k^2 + 1), \text{ since } k > 0$$

$$k^3 - 4k^2 - 4 \geq 0$$

The inequality represents a cubic equation of the form $ax^3 + bx^2 + cx + d = 0$. The above inequality can be solved by substituting $k = x - \frac{4}{3}$. This transforms it as

$$\left(x - \frac{4}{3}\right)^3 - 4\left(x - \frac{4}{3}\right)^2 - 4 \geq 0$$

on expanding which simplifies as,

$$x^3 - \frac{16}{3}x - \frac{236}{27} \geq 0$$

Now, let $x = y + \frac{\lambda}{y}$, then the above inequality gets transformed

as

$$\left(y + \frac{\lambda}{y}\right)^3 - \frac{16}{3}\left(y + \frac{\lambda}{y}\right) - \frac{236}{27} \geq 0$$

$$\text{let } \lambda = \frac{16}{9}; z = y^3$$

$$\Rightarrow z^2 - \frac{236}{27}z + \frac{4096}{729} \geq 0$$

Solving the inequality in z , we have

$$z \geq \frac{2}{27}(59 + 3\sqrt{273})$$

We consider only the positive root of z . Substitute $z = y^3$

$$\Rightarrow y^3 = \frac{2}{27}(59 + 3\sqrt{273})$$

$$\Rightarrow y = \frac{\sqrt[3]{2}}{3}(\sqrt[3]{59 + 3\sqrt{273}})$$

$$\text{but } x = y + \frac{16}{9y}$$

$$\Rightarrow x = \frac{8 \times 2^{\frac{2}{3}}}{3\sqrt[3]{3\sqrt{273} + 59}} + \frac{\sqrt[3]{2(3\sqrt{273} + 59)}}{3}$$

Finally, substitute $k = x + \frac{4}{3}$

$$\Rightarrow k = \frac{8 \times 2^{\frac{2}{3}}}{3\sqrt[3]{3\sqrt{273} + 59}} + \frac{\sqrt[3]{2(3\sqrt{273} + 59)}}{3} + \frac{4}{3}$$

The above inequality has a minimum value solution for this root k . Theorem is completely proved.

Chapter 5: Conclusion

In [1] it was observed that the above system of inequalities has a solution for all $k \geq 5$. But the system has never been solved therein. Here this system is solved and the lower bound for k is improved. In fact, the above mention root of quibic equation has an approximation (up to first three digits) 4.224.

References

- [1] A.N. Zubkov, *On a matrix representation of a free group*, Mathematical Notes, 1998, 64, pages 745-752, Springer.
- [2] Yu I, Merzlyakov, *Linear groups*, Journal of Soviet Mathematics, 1980, 14(1).
- [3] D. A. Suprunenko, *The Groups of Matrices*, Nauka, Moscow, 1972.
- [4] Mennicke, J., *A remark on the congruence subgroup problem*, Math. Scand. 86 (2000), no. 2, 206–222.
- [5] Gallian, J. A, *Contemporary Abstract Algebra*, Houghton Mifflin College Div, Boston, MA, 1998.
- [6] Lyndon.R, Ullman. J, *Pairs of 2×2 matrices that generate free products*, Michigan Mathematics Journal, 2002 , 15(2).
- [7] Van Der Waerden, B., Artin, E., Noether, E., *Algebra: Based in Part on Lectures by E. Artin and E. Noether*, Springer Science and Business Media, 2003.
- [8] Lyndon, R.C, Schupp, P.E. *Combinatorial Group Theory*, V 89, Springer-Verlag, 1977.
- [9] Magnus,W.,Karrass,A.,Solitar,D. *Combinatorial Group Theory:Presentations of Groups in Terms of Generators and Relations*, Dover Publications, 2004.

- [10] Kargapolov, M. I., Merzliakov, I. I., Gurns, R. *Fundamentals of the Theory of Groups. In Graduate texts in mathematics*, Srpinge-Verlag, 1979.

**UAEU**جامعة الإمارات العربية المتحدة
United Arab Emirates Universitywww.uaeu.ac.ae

UAEU MASTER THESIS NO. 2024:74

This work investigates the matrix representation of a free group. The group $G_n(k)$ is discussed. An alternative proof for the known fact that $G_n(3)$ is not *free* is provided. The main objective of the thesis is to find a lower bound for the parameter k .

Julius Kurian received his Master of Science in Mathematical Science from the Department of Mathematical Sciences, College of Science, United Arab Emirates University and his Bachelor of Science in Mathematics from the University of Mumbai, India.

UAEUعمادة المكتبات
Libraries Deanshipجامعة الإمارات العربية المتحدة
United Arab Emirates University