STUDY ON FREE ABELIAN GROUPS AND FREE GROUPS

A Dissertation submitted in partial fulfillment of

the requirement for the award of

DEGREE OF MASTER OF SCIENCE

IN MATHEMATICS

By

MARY SANDREENA P.A

REGISTER NO: SM16MAT010

(2016 – 2018)

DEPARTMENT OF MATHEMATICS

ST.TERESA'S COLLEGE, (AUTONOMOUS)

ERNAKULAM, KOCHI - 682011

APRIL 2018

DEPARTMENT OF MATHEMATICS

ST.TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

CERTIFICATE

This is to certify that the dissertation entitled "A STUDY ON FREE ABELIAN GROUPS AND FREE GROUPS" is a bonafide record of the work done by MARY SANDREENA P.A under my guidance as partial fulfillment of the award of the degree of Master of Science in Mathematics at St.Teresa's College (Autonomous), Ernakulam affiliated to Mahatma Gandhi University, Kottayam. No part of this work has been submitted for any other degree elsewhere.

Smt NISHA OOMMEN (Supervisor)

Assistant Professor

Department Of Mathematics

St.Teresa's College,(Autonomous)

Ernakulam

Smt Teresa Felitia (HOD)

Associate Professor

Department of Mathematics

St. Teresa's College (Autonomous)

Ernakulam

External Examiners:

1. ....

2. ....

DECLARATION

I hereby declare that the work presented in this project is based on the original work done by me under the guidance of Smt NISHA OOMMEN, Assistant Professor, Department of Mathematics, St Teresa's College (Autonomous) Ernakulam and has not been included in any other project submitted previously for the award of any degree.

ERNAKULAM | MARY SANDREENA P.A

APRIL 2018 | **REGISTER NO: SM16MAT010**

ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and I am extremely privileged to have got this all along the completion of my project

I owe my deep gratitude to my project guide, Smt NISHA OOMMEN, Assistant Professor, Department of Mathematics, St Teresa's College (Autonomous) Ernakulam for the keen interest she has taken in guiding and helping me to complete this work.

I am equally grateful to all the teaching staff of the Department of Mathematics for their support and suggestions. I express my special thanks to our HOD **Smt** Teresa Felitia who helped me in various aspects to complete my project successfully.

Last but not least , I express my grateful thanks to Almighty God without whose grace nothing would have been possible.

ERNAKULAM

APRIL 2018

MARY SANDREENA P.A

REGISTER NO: SM16MAT010

CONTENTS

INTRODUCTION

In abstract algebra, a free abelian group is an abelian group with a basis. Being an abelian group means that it is a set with an addition operation that is associative, commutative, and invertible. A basis is a subset such that every element of the group can be found by adding or subtracting basis elements, and such that every element's expression as a linear combination of basis elements is unique.
The elements of a free abelian group with basis B may be described in several equivalent ways. These include formal sums over B, expressions of the form $\sum a_i b_i$ where each coefficient a_i is a nonzero integer, each factor b_i is a distinct basis element, and the sum has finitely many terms. Alternatively, the elements of a free abelian group may be thought of as signed multisets containing finitely many elements of B, with the multiplicity of an element in the multiset equal to its coefficient in the formal sum. Also the free abelian group with basis B may be described by a presentation with the elements of B as its generators and with the commutators of pairs of members as its relators.

The free group F over a given set S consists of all expressions (words, or terms) that can be built from members of S, considering two expressions different unless their equality follows from the group axioms. The members of S are called generators of F. An arbitrary group G is called free if it is isomorphic to F for some subset S of G, that is, if there is a subset S of G such that every element of G can be written in one and only one way as a product of finitely many elements of S and their inverses.

Chapter 1

PRELIMARIES

Definition 1.1 ***GROUPS:***

A group is an ordered pair (G,) where G is a nonempty set and * is a binary operation on G such that the following properties hold:*
(1) for all a,b,c $\in$ G ;a$*$(b$*$c)=(a$*$b)$*$c. (associative law.)
(2) there exist e$\in$G such that,for any a$\in$G, a$*$e = a = e$*$a. (existence of identity).
(3) for each a$\in$G,there exist b$\in$G such that a$*$b = e = b$*$a. (existence of inverse)

Examples
(Z,+): the integers with addition.
(R,+): the real numbers with addition.
(R,$\times$): the non-zero real numbers with multiplication.*

Definition 1.2 ***ABELIAN GROUPS:***

A group is called commutative or abelian if a$*$b=b$*$a for all a,b $\in$ G.

Examples
(Z,+): the integers with addition.
(R,+): the real numbers with addition.
(R,$\times$): the non-zero real numbers with addition.*

Definition 1.3 ***QUOTIENT GROUPS:***

Let G be a group and H be a subgroup of G, then the group $G|H$ of all cosets of H in G under the binary operation $aH*bH = abH$ is called the quotient group of G by H.

Examples
$Z_6 \mid <3>$
$Z \mid 5Z$

Definition 1.4 ***NORMAL SUBGROUPS:***

Let G be a group.A subgroup H of G is said to be a normal subgroup of G if $aH = Ha$ for all $a \in G$.
Every subgroup of a commutative group is a normal subgroup.
A subgroup H of G is normal iff $gng^{-1} \in N$, $\forall g \in G$ and $n \in N$.

Definition 1.5 ***HOMOMORPHISM:***

Let $(G,*)$ and $(G_1,*_1)$ be two groups and f is called a homomorphism of G into G_1 if for all $a,b \in G$,
$f(a*b) = f(a) * f(b)$

Example
$h:R \longrightarrow R^+$ is an example of homomorphism from the group $(R,+)$ to the group $(R^+,\bullet)$

Definition 1.6 ***MONOMORPHISM and EPIMORPHISM :***

Let G and G_1 be two groups and $f : G \longrightarrow G_1$ be a homorphism of groups. Then,
(a) f is called a monomorphism if f is an injective function.
(b) f is called an epimorphism if f is a surjective function.

Definition 1.7 ***ENDOMORPHISM:***

An endomorphism is a homomorphism whose domain equals codomain.

Definition 1.8 ***ISOMORPHISM:***

A homomorphism f from a group G to a group G_1 is called an isomorphism if the function $f: G \longrightarrow G_1$ is a bijective function.A group G is said to be isomorphic to a group G_1 if there exist an isomorphism from G onto G_1 and we denote it by $G \cong G_1$.

Definition 1.9 ***First Isomorphism Theorem:***

Let $f: G \longrightarrow G_1$ be a homomorphism of groups. Then the quotient group $G \mid ker(f)$ is isomorphic to the subgroup Imf of G_1 ,where the kernel of f and Imf is the image of f.

Definition 1.10 ***TORSION GROUPS:***

The torsion subgroup A_T of an abelian group A is the subgroup of A consisting of all elements of finite order. An abelian group A is called a torsion(or periodic) group if evry element of A has a finite ordeer and is called torsion-free if every element of A exept the identity is of inifinite order.

Definition 1.11 ***COMMUTATOR SUBGROUPS:***

Let G be a group and a,b $\in$ G. The element $aba^{-1}b^{-1}$ is called a commutator of the group G. Let U= $aba^{-1}b^{-1}$; a,b $\in$ G. If G^1 is the subgroup of G generated by U,then G^1 is called the commutator subgroup of G.

Definition 1.12 ***Lagrange's Theorem:***

Lagranges theorem states that for any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.

Definition 1.13 ***Sylow-p-subgroup:***

Let G be any group with cardinality $p^m n$ where p is any prime and m,n are any two positive integers such that p does not divide n. Let H be any subgroup of G such that o(H)=p^m, then H is called a sylow p subgroup of G.

Definition 1.14 ***First Sylow Theorm:***

Let G be a finite group and $\mid G \mid = p^m n$ where m and n are any two positive integers such that p does not divide n, then,
1. G contains a subgroup of order p^i ; 1$\leq i \leq n$
2. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1}, where 1$\leq i < n$

Definition 1.15 ***WEAK DIRECT PRODUCT:***

A weak direct product of a family of groups $\{G_i\}$ $i \in I$ is the subgroup of $\prod G_i$ given by $\prod G_i := \{(a_i)i \in I | a_i \neq e_i \in G_i\}$ for finitely many i only
If all groups Gi are abelian then $\prod G_i$ is denoted by $\oplus G_i$ and it is called the direct sum of $\{G_i\}$

Chapter 2

FREE ABELIAN GROUPS

DEFINITION.

A Free abelian group is an abelian group that has a basis in the sense that every element of the group can be written in one and only one as a finite linear combination of elements of the basis with integer coefficients.
Hence the free abelian groups over a basis B are also known as formal sums.

In other words,

A Z-basis for an abelian group A is a subset X of A with the following properties.

$* < X >= G$ i.e., every element a $\in$ A may be written as a=$\Sigma_{x\in X} n_x.x$ where $n_x \neq 0$ in Z and for finitely many x $\in$ X
$*$ X is Z-independent, i.e., for any collection of integers, $\{n_x\}$ such that only finitely many are non-zero, i.e., we've
$\Sigma_{x\in X} n_x.x = 0 \implies n_x = 0, \forall x \in X.$

And an abelian group G having an Z-basis is called a free abelian group.

Examples

1. The integers under the addition operation form a free abelian group with the basis$\{1\}$. Every integer n is a linear combination of basis elements

with integer coefficients, namely n=n*1 with the coefficient n.Also each integer can be formed by using addition or substraction to combine some number of copies of the number 1 and hence each integer has a unique representation as an integer multiple of the number 1.

2. Integer lattice also forms a free abelian group.
The two-dimensional integer lattice consisting of the points in the plane with integer cartesian coordinates form a free abelian group under vector addition with the basis {(1,0) , (0,1)}

If we say e_1=(1,0) and e_2=(0,1),
then the element (9,7) can be written as
$(9, 7) = 9e_1 + 7e_2$.

where multipilication is defined so that
$7e_2 = e_2 + e_2 + e_2 + e_2 + e_2 + e_2 + e_2$

In this basis there is no other way to write (9,7)

But with different basis {(2,0) , (1,1)},
it can be written as
(9,7) = (2,0) + 7*(1,1).

More generally every lattice forms a finitely generated free abelian group. The d-dimensional integer lattice has a natural basis consisting of the positive integer unit vectors,but it has many other bases as well.
If M is a d×d integer matrix with determinant ±1, then the rows of M form a basis and conversely every basis has this form.

3. The trivial group {0} is also considered to be free abelian,with basis the empty set. It may be interpreted as a direct product of zero copies of Z.

PROPERTIES

* RANK of a free abelian group is defined to be the cardinality of the basis of the free abelian group.

Every 2 basis of the free abelian group have the same cardinality.

Also Free abelian groups of same rank are isomorphic

A free abelian group is finitely generated if and only if its rank is a finite number n, in whhich case the group is isomorphic to Z_n

$*$ Direct product of two free abelian group is itself free abelian with basis the disjoint union of basis of two groups.

More generally,the direct product of any finite number of free abelian group is free abelian with basis the disjoint union of the basis of two groups. But it need not be necessarilly true for infinite number of free abelian groups.

Theorem 2.1 *Let X be the subset of non-zero abelian group G. then the following conditions are equivalent*

1. *Each non-zero element a in G can be expressed uniquely in the form* $a = n_1x_1 + n_2x_2 + ... + n_rx_r$. *for* $n_i \neq 0$ *in Z and distinct* x_i *in X*
2. *X generates G and* $n_1x_1 + n_2x_2 + ... + n_rx_r = 0$ *for* n_i *in Z and distinct* $x_i \in X$ *iff* $n_1 = n_2 = ... n_r = 0$

Proof:
$1 \Longrightarrow 2$
Assume that any non-zero element a in G can be expressed uniquely as

$$a = n_1x_1 + n_2x_2 + ... + n_rx_r.$$

for $n_i \neq 0$ *in Z and distinct* x_i *in X*

We have G is a non-zero abelian group, i.e., $G \neq 0$.
Also $0 \notin X$
For;
If $x_i = 0$ *and* $x_j \neq 0$ *where* $x_i, x_j \in X \subseteq G$.
then, $x_j = x_i + x_j$, *which would contradict the uniqueness of the expression for* x_j

$\therefore 0 \notin X$
And also from (1) it is clear that X generates G.
Again if $n_1 = n_2 = \ldots\ldots\ n_r = 0$*,then*
$n_1x_1 + n_2x_2 + \ldots\ldots + n_rx_r = 0$

Now suppose that $n_1x_1 + n_2x_2 + \ldots\ldots + n_rx_r = 0$
we have to shhow that $n_1 = n_2 = \ldots\ldots\ n_r = 0$

If possible suppose $n_i \neq 0$ *for some i (say* n_1*)*
we have $n_1 = n_2 = \ldots\ldots\ n_r = 0$
$\implies x_1 = n_1x_1 + n_2x_2 + \ldots\ldots + n_rx_r$
$\implies x_1 = (1+n_1)_1 + n_1x_1 + n_2x_2 + \ldots\ldots + n_rx_r$
which is a contradiction for uniqueness of expression of x_1*.*
$\therefore$ *If* $n_1 + n_2 + \ldots\ldots + n_r = 0$*, then* $n_1 = n_2 = \ldots\ldots\ n_r = 0$

$2 \implies 1$
Since X generates G, we've $a = n_1x_1 + n_2x_2 + \ldots\ldots + n_rx_r$*.*
we've to show that this expression is unique

we've if $n_1 + n_2 + \ldots\ldots + n_r = 0$*, then* $n_1 = n_2 = \ldots\ldots\ n_r = 0$
If possible support that:
$a = n_1x_1 + n_2x_2 + \ldots\ldots + n_rx_r$
$a = m_1x_1 + m_2x_2 + \ldots\ldots + m_rx_r$

Subtracting we get,
$0 = (n_1 - m_1)x_1 + (n_2 - m_2)x_2 + \ldots\ldots + (n_r - m_r)x_r$*.*

Then by our assumption we get
$n_1 - m_1 = n_2 - m_2 = \ldots\ldots\ldots = n_r - m_r = 0$
$\implies n_i = m_i\ \forall i = 1, 2, \ldots\ldots, r.$
i.e., expression of any element a in G is unique.
Hence proved.

RESULT

An abelian group having a generating set X satisfying the conditions stated in above theorem is a free abelian group and X is a basis for the group.

UNIVERSAL PROPERTY OF FREE ABELIAN GROUPS

If F is a free abelian group with basis B , then we've the following universal property;
for every arbitrary function f from B to some abelian group A , there exist a group homomorphism from F to A which extends f.
i.e., the abelian group of base B is unique upto an isomorphism.

PROPOSITION 1

A subset X of an abelian group G is a basis of G if and only if every mapping of X into an abelian group A can be extended uniquely to a homomorphism of G$\longrightarrow$A.

Proof:

Let X consist of the elements x_i ; i $\in$ I.
Suppose that X is a basis of G.
Let x_i : $\longmapsto a_i$ be the mapping of X into any abelian group A.

The mapping
$x = \sum_i \alpha_i x_i \mapsto \sum_i \alpha_i a_i$
is a well defined homomorphism of G into A and maps x_i into a_i.
However it is the only homomorphism of G which maps x_i to a_i for each i $\in$ I .

Conversely,
Suppose that G and X have the stated property.
Let A be a free abelian group with basis a_i , i $\in$ I.
There is a homomorphism ϕ : G $\longrightarrow$ A such that $\phi(x_i) = a_i$; i $\in$ I.

As a free abelian with basis a_i, there is a homomorphism ψ : A $\longrightarrow$ G such that $\psi(a_i)$ = x_i ; i $\in$ I.
Then $\psi \circ \phi$ is an endomorphism of G which maps x_i into a_i .
Since the identity endomorphhism I_G of G has the same property , by the uniqueness part of the stated condition ,
it follows that $\psi \circ \phi = I_G$.
The endomorphism $\phi \circ \psi$ of A maps each of the generators a_i , i $\in$ I of A to itself and is therefore the identity endomorphism I_A of A.

Thus ϕ is an isomorphism of G with a mapping x_i to a_i.
Thus ψ is an isomorphism of G with A mapping x_i to a_i.
Since the elements a_i ; i $\in$ I forms a Z-basis of A, the elements x_i ; i $\in$ I form Z-basis of G.

COROLLARY

Free abelian groups of same rank are isomorphic.

Proof:

If G and G$'$ are two free abelian groups with basis x_i and $x_i{}'$ where i $\in$ I, then the homomorphism ϕ of G into G$'$ which maps x_i and $x_i{}'$; i $\in$ I , is an isomorphism of G with G$'$, with inverse the homomorphism ψ of G$'$ into G which maps x_i to $x_i{}'$; i $\in$ I .

COROLARY

Every abelian group A is homomorphic image of a free abelian group . More precisely if A is generated by a system of cardinality p , it is a homomorphic image of a free abelian group of rank p.

Proof:

Suppose that the elements a_i,i $\in$ I generates A .
Let G be free abelian of rank p = card(I) and let x_i , i $\in$ I be a basis of G.
There exist a homomorphism ϕ :G $\longrightarrow$ A such that $\phi(x_i)$ = a_i ; i $\in$ I .

Since the elements a_i , $i \in I$, generate A,
ϕ is surjective
And hence proved

PROPOSITION

If G is any free abelian group,then any two bases of G have the same cardinality

Proof:

Let B and B′ be any 2 bases of G.
We've to show that $| B |= | B' |$

Also we have the isomorphism
$\oplus_{x\in B}$ Z $\cong$ G $\cong$ $\oplus_{x\in B'}$ Z.

Case 1:

When B and B′ are finite sets.
Let $| B |=$ m and $| B' | =$ n

Take 2G = $\{2g|g \in G\}$ which is a subgroup of G.

Also we have G $\cong$ $\oplus_{x\in B}$ Z.

$\Longrightarrow G/2G \cong \oplus_{x\in B} Z/2Z$.

Similarly since we have G $\cong$ $\oplus_{x\in B'}$ Z.

$\Longrightarrow G/2G \cong \oplus_{x\in B'} Z/2Z$.

i.e., now we have,

2^m=$| \oplus_{x\in B} Z/2Z| \cong G/2G \cong | \oplus_{x\in B'} Z/2Z| = 2^n$

$\Longrightarrow$ m=n.

Case 2 :

Consider the case if B is finite and B$'$ is infinite
As in previous case this would give

$\oplus_{x\in B}Z/2Z \cong G/2G \cong \oplus_{x\in B'}Z/2Z$

This is however a contradction,
since $\oplus_{x\in B}Z/2Z$ is a finite group and $\oplus_{x\in B'}Z/2Z$ is an infinite group.
$\therefore$ Such a case doesn't exist.

Case 3:

Both B and b$'$ are infinite sets

If B is infinite then $|B| = |\oplus_{x\in B} Z|$

$\therefore$ It follows that

$|B| = |\oplus_{x\in B} Z| = |G| = |\oplus_{x\in B'} Z| = |B'|$

$\implies |B| = |B'|$

LEMMA

If f: $G \to H$ is an epimorphism of abelian groups and H is free abelian group , then
G $\cong H\oplus$ ker(f).

Proof:

We have
" If f: $G \to H$ and g: $H \to G$ are any two homomorphism such that fg= I$_{d_H}$,then,
G $\cong H\oplus$ ker(f).

It follows that we only need to construct the homomorphism g.

We have H is a free abelian group, so let B be the basis of H.
Also f: $G \to H$ is an epimorphism
i.e., f is onto
$\implies \forall x \in B, \exists a_x \in G$ such that $f(a_x) = x$

Now let G be any abelian group.
Then by universal property ,
there exist a unique homomorphism g: $H \to G$ such that g(x)=$a_x \forall x \in B$
$\implies$ fg(x) = x $\forall x \in B$
$\implies$ fg = I_{d_H}.

THEOREM 2.2

Let G be a free abelian group of rank n and let H be a subgroup of G. Then H is free abelian and rank (H)$\leq$ rank (G)

Proof:

Since G is a free abelian group of rank n,
G$\cong Z \times Z \times ......Z\times$ (n summands)
$\implies$ G$\cong Z_n$ Suppose G = Z_n

We want to show that if H $\subseteq Z_n$ then , H is free abelian and rank(H) $\leq$ n.

We prove this using the method of induction on n.

When n=1;
then H=kZ for k$>$ 0
H =$\{0\}$ or H $\cong$ Z
$\implies$ H is free abelian and rank(H)$\leq$ rank(G)

Next suppose for some n, every subgroup of Z_n is free abelian and of rank $\leq$ n.

Now let H $\subseteq$ Z $_{n+1}$

Define f: $Z_{n+1} \rightarrow Z$ by f$(m_1, m_2, ..., m_{n+1})$ = m$_{n+1}$

then , ker(f)=$\{(m_1, m_2, ..., 0)|m_i \in Z\} \cong Z_n$

Now consider the epimorphism, f$/H : H \rightarrow Im(f/H)$, since$Im(f/H) \subseteq Z$
Thus $Im(f/H)$ is a free abelian group.

$\therefore$ By previous lemma we get,

H $\cong Im(f/H) \oplus ker(f/H)$

Also we have ker(f/H) = ker(f) $\cap$ H
$\Longrightarrow$ ker(f/H) is a subgroup of ker(f)
And since ker(f) is a free abelian group of rank n, by the inductive assumption we get that ker(f/H) is a free abelian group of rank $\leq$ n.

$\therefore$ H $\cong Im(f/H) \oplus ker(f/H)$
where Im(f/H) is a free abelian group of rank $\leq$ 1 and ker(f/H)is afree abelian group of rank$\leq$ n.

$\Longrightarrow$ H is a free abelian group of rank $\leq$ n+1

Chapter 3

FINITELY GENERATED ABELIAN GROUPS

In abstract algebra , an abelian group (G,+) is called finitely generated if there exists finitely many elements $x_1, x_2, ..., x_s$ in G such that every x in G can be written in the form
x=$n_1x_1 + n_2x_2 + ... + n_sx_s$
with integers n1, ..., ns.
In this case, we say that the set $\{x_1, ..., x_s\}$ is a generating set of G or that $x_1, ..., x_s$ generate G.
Every finite abelian group is finitely generated

EXAMPLES

1. The integers (Z,+) are a finitely generated abelian group.
2. The integers modulo n,(Z/nZ, +) are a finite (hence finitely generated) abelian group.
3. Any direct sum of finitely many finitely generated abelian groups is again a finitely generated abelian group.
4. Every lattice forms a finitely generated free abelian group.

   Here Z is an example of an infinite group which is finitely generated with the generating set $\{1, -1\}$

But every infinite group is not finitely generated
eg: the set of rational numbers under addition.

If G is free abelian of finite rank then G is ofcourse finitely generated.

THEOREM

If G is an abelian group generated by n elements.
Then G≅ F/H where F is a free abelian group of rank n and H is some subgroup of F.

Proof:

Let G be an abelian group generated by n elements
i.e., G=$< a_1, a_2, ..., a_n >$.

Let F be free abelian group and $\{x_1, ..., x_n\}$ be a basis of F.
Then we have a unique isomorphism f : $F \to G$ defined by $f(x_i) = a_i$.
Let H=ker(f).
and here Im(f)=G.

$\therefore$ By first isomorphism theorem ,
we have, G≅ F/H

PROPOSITION

Let G be a finitely generated abelian group with generating set $< a_1, a_2, ..., a_n >$. Let $\Phi : Z \times Z \times .... \times Z \to G$ (where there are n factors of Z) be defined by $\phi(h_1, ..., h_n) = h_1a_1 + h_2a_2 + ... + h_na_n$.
Then ϕ is a homorphism onto G.

Proof:

Consider $(h_1, ..., h_n)$, $(k_1, ..., k_n) \in Z \times Z \times .... \times Z$,

$\phi((h_1, ..., h_n) + (k_1, ..., k_n)) = \phi(h_1 + k_1, ..., h_n + k_n)$

$=(h_1+k_1)a_1+...+(h_n+k_n)a_n$

$=(h_1a_1+...+h_na_n)+(k_1a_1+...+k_na_n)$

$=\phi(h_1,...,h_n)+\phi(k_1,...,k_n)$

$\Longrightarrow \phi$ is an homorphism .

Since $a_1, a_2, ..., a_n$ generates G, ϕ is a homomorphism onto G.

PROPOSITION

If X=$\{x_1, x_2, ..., x_r\}$ is a basis for a free abelian group G and t $\in$ Z ,then for i$\neq$ j, the set Y=$\{x_1, x_2, ..x_{j-1}, x_j+tx_i, x_j, x_{j+1}, .., x_r\}$ is also a basis for G.

Proof:

To show that Y is a basis , we need to show that the set will span G and the elements are linearly independent
Given$\{x_1, x_2, ..., x_r\}$ spans G.

we can write $x_j=(-t)x_i+1(x_j+tx_{i)}$

$\Rightarrow x_j$ can be recovered from Y, which thus als generates G.

Suppose
$n_1x_1+n_2x_2+...+n_{j-1}x_{j-1}+n_j(x_j+tx_i)+n_{j+1}x_{j+1}+...+n_rx_r=0$

$n_1x_1+n_2x_2+...+(n_i+n_jt)x_i+...n_jx_j+...+n_rx_r=0$

And since X is a basis
$n_1=n_2=....=n_i+n_jt=...=n_j=...=n_r=0$

From $n_i+n_jt=...=n_j=0$, it follows that
$n_i=0$;

i.e., we get, $n_1 = n_2 =.... =n_i= ...=n_j=...= n_r = 0$

Also we got Y generates G.
$\therefore$ By theorem 2.1 Y is a basis of G.

PROPOSITION 4

Let G be a non-zero free abelian group of finite rank n and let K be a non-zero subgroup of G. Then K is free abelian of rank s $\leq$ n. Furthermore there exists a basis $\{x_1, x_2, ..., x_n\}$ for G and positive integers $d_1, ..., d_s$ such that
•$d_i|d_{i+1}$ for i = 1, . . . , s-1
•$\{d_1x_1, d_2x_2, ..., d_sx_s\}$ is a basis of K.

Proof:

Let G be a non-zero free abelian group of finite rank n
Let K be a non-zero subgroup of G.
Then we have K is also free abelian of rank$\leq$ n.
Now we have to show that K has a basis of the described form.

Suppose Y=$\{y_1, y_2, ..., y_n\}$ is a basis for G.
All non-zero elements in K can be expressed in the form
$k_1y_1 + k_2y_2 + ... + k_ny_n$ for some $|k_i|$ is non-zero.

Among all bases Y for G, select one Y_1 that yields the minimal such non-zero value $|k_i|$ as all non-zero elements of K are written in teerms of the basis elements in Y_1.

By renumbering the elements of Y_1 if necessary we can assume there is
$w_1 \in K$ such that $w_1 = d_1y_1 + k_2y_2 + ... + k_ny_n$
where $d_1 > 0$ and d_1 is the minimal attainable coefficient as just described.

Using the division algorithm, we write
$k_j = d_1q_j + r_j$ where $0 \leq r_j \leq d_1$ for j = 2,3,....,n

$w_1 = d_1y_1 + (d_1q_2 + r_2)y_2 + ... + (d_1q_n + r_n)y_n$

$\Longrightarrow$ w$_1$ $= d_1(y_1 + q_2y_2 + ... + q_ny_n) + r_2y_2 + ... + r_ny_n$

let x$_1$ $= y_1 + q_2y_2 + ... + q_ny_n$

$\Longrightarrow$ w$_1$ $=d_1x_1 + r_2y_2 + ... + r_ny_n$

Then by Proposition 3, $\{x_1, y_2, ..., y_n\}$ is also a basis for G.
Also from eq(1) and our choice of Y$_1$ for minimal coefficient d$_1$, we see that $r_2 = ...r_n = 0$
Thus $d_1x_1 \in K$

We now consider bases for G of the form $\{x_1, y_2, ..., y_n\}$,
Each element of K can be expressed in the form $h_1x_1 + k_2y_2 + ... + k_ny_n$.
Since $d_1x_1 \in K$, we can subtract a suitable multiple of d_1x_1 and then using the minimality of d_1 , we see actually have $k_2y_2 + ... + k_ny_n$ in K.
Among all such bases $\{x_1, y_2, ..., y_n\}$ we choose one Y$_2$ that leads to some k$_i$ $\nleq 0$ of minimal magnitude.

By renumbering the elements of Y$_2$
we can assume that there is w$_2$ $\in K$ such that w$_2$ $= d_2y_2 + +..... + k_ny_n$
where $d_2 > 0$ and is minimal as just described

Exactly as in the preceeding paragraph , we can modify our basis from
Y$_2$ $= \{x_1, y_2, ..., y_n\}$ to a basis Y$_3$ $= \{x_1, x_2, y_3, ..., y_n\}$ for G where
$d_1x_1, d_2x_2 \in K$
writing $d_2 = d_1q + r$; $0 \leq r \leq d_1$
we see that $\{x_1 + qx_2, x_2, y_3, ..., y_n\}$ is a basis for G and
$d_1x_1 + d_2x_2 = d_1x_1 + (d_1q + r)x_2 = d_1(x_1 + qx_2) + rx_2 \in K$

But by our minimal choice of d_1 , r=0.
$\Longrightarrow$ d$_1$ divides d$_2$

Proceeding in this manner , we will get $\{x_1, x_2, ...x_s, y_{s+1}, .., y_n\}$ as a basis for G where the only element of K of the form $k_{s+1}y_{s+1} + ... + k_ny_n$ is zero
i.e., all k$_i$ are zero
We then let $x_{s+1} = y_{s+1} = ... = x_n = y_n$ and a basis for G of the described form in the proposition.

PROPOSITION

Every finitely generated abelian group is isomorphic to a group of the form $Z_{m1} \times Z_{m2} \times ..... \times Z_{mr} \times Z \times Z...... \times Z$, where m_i divides m_{i+1} for i=1,2,....r-1.

Proof:

We know that $Z/nZ \cong Z_n$
$\therefore Z/1Z \cong Z/Z \cong Z_1 \cong 0$
Let G be a finitely generated abelian group generated by n elements.

Let F be a free abelian group of rank n.
Then we know that F$\cong Z \times Z \times Z...... \times Z$ (n factors)

Consider the homomorphism $\phi :$ F $\longrightarrow$ G and let K be the kernel of this homomorphism.
Also K is a subgroup of F.
Then by proposition 4, there is basis for F of the form $\{x_1, x_2, ..., x_n\}$ where $\{d_1x_1, d_2x_2, ..., d_sx_s\}$ is a basis of K and $d_i|d_{i+1}$ for i = 1, . . . , s-1

Now by proposition 1, we have G$\cong$ F/K.

But , F/K $\cong (Z \times Z \times Z...... \times Z)/(d_1Z \times d_2Z \times ..... \times d_sZ...... \times 0.... \times 0)$

$\cong (Z_{d_1} \times Z_{d_2} \times ..... \times Z_{d_s} \times Z...... \times Z)$

It is possible that d_i=1 , in which case $Z_{d_i} = 0$ and can be dropped from this product
similarly d_2 may be 1 and so on.

NOTE: This numbers m_i here are known as torsion coefficient of G.

FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUPS

Every finitely generated abelian group A is a direct sum of a free abelian of finite rank and cyclic subgroups

Chapter 4

FREE GROUPS

A set of group elements that satisfy no relations except those implied by the axioms is called free and a group that has a free set of generators is called free group.

In otherwords , a group is called a free group if no relation exist between its group generators other than the relationship between an element and its inverse required as one of the defining properties of a group.

for eg : Additive group of integers is free with a single generator namely 1 and its inverse.

To describe free group ,
we start with an arbitrary set S $=\{a, b, c, ...\}$, where the elements in S are called the symbols and a word is defined to be the finite string of symbols in which repetition is allowed.
for eg : a, aa, ba, aaba are words.

Two words can be composed by juxtaposition , that is placing them side by side:
aa , ba $\mapsto$ aaba

This is an associative law of composition on the set W of words.

We include the empty word in W as an identity element and we use the symbol 1 to denote it.

Then the set W becomes what is called the free semigroup on the set S. But it cannot be called as group because it lacks inverses and adding inverses complicates things a little.

Let S′ be the set consisting of symbols a and a^{-1} for every a in S
i.e., S′ = $\{a, a^{-1}, b, b^{-1}, c, c^{-1}, ...\}$
and let W′ be the semigroup of words made by using the symbols in S′.

If an element of S lies immediately next to its inverse , the word may be simplified by ommitting the pair , that is, if a word looks like
.......xx^{-1}...... or ....$x^{-1}x$...... for some x in S
we may agree to cancel the two symbols x and x^{-1} to reduce the length of the word.
A word is called reduced if no such cancellations can be made.

Starting with any word w in W′ , we can perform a finite sequence of cancelations and must eventually get a reduced word w_0 , possible the empty word 1, and such a word w_0 is called as the reduced form of W.

There may be more than 1 way to proceed with cancellations.
For instance,
starting with w= $abb^{-1}c^{-1}cb$, we can proceed in 2 ways:

$abb^{-1}c^{-1}cb$	$abb^{-1}c^{-1}cb$
$ac^{-1}cb$	$abb^{-1}b$
ab	ab

The same reduced word is obtained at the end though the symbols come from different places in the word

Definition : A group G is called a free group if there exists a generating set X of G such that every non-empty reduced group word in X denes a non-trivial element of G.

PROPOSITION

There is only one reduced form of a given word w.

Proof:

We prove this using method of induction(on lenth of w).
If w is reduced , then nothing is to be done.
Suppose that w is not reduced
i.e., there exist some pair of symbols that can be cancelled .
let w=.....xx^{-1}.....

Now if we show that we can obtain every reduced form of w by cancelling the pair xx^{-1} first , the proposition will follow by induction , because the word w is shorter.
Let w_0 be the reduced form of w.
It is obtained by some sequence of cancellations .
The first case is that our pair xx^{-1} is cancelled at some step in this sequence.
If so, we may suppose that xx^{-1} is cancelled first.
So this case is settled.

On the otherhand , since w_0 is reduced , the pair xx^{-1} cannot remain in w_0.
Atleast one of the two symbols must be cancelled at some time.
If the pair itself is not cancelled , the first cancellation involiving the pair must look like
....$x^{-1}xx^{-1}$.... or ....$xx^{-1}x$....
Note that the word obtained by this cancellation is the same as the one obtained by cancellin the pair xx^{-1}. So ath this stage we may cancel the original pair instead .
Then we are back in the first case , so the proposition is proved.

NOTE:

We call two words w and w′ in W′ equivalent and we write w$\sim$ w′ if they have the same reduced form.

PROPOSITION :

Product of equivalent words are equivalent
i.e., if w$\sim$ w$'$ and v$\sim$ v$'$ then wv$\sim$ w$'$ v$'$.

Proof:

Suppose that we have cancelled as much as possible in w to reduce w to w_0 and similarly made cancellations in v to reduce it to v_0
Then wv is reduced to w_0v_0.
Now we continue cancelling in w_0v_0 untill the word is reduced.
If w$\sim$ w$\sim$ w$'$ and v$\sim$ v$'$ and v$\sim$ v$'$,the same process when applied to w$'$v$'$ passes through w_0v_0 too, so it leads to the same reduced word.

PROPOSITION :

The set F of equivalence classes of words in W$'$ is a group , with the law of composition induced from multiplication (juxtaposition) in W$'$.

Proof:

Clearly multiplication of words holds the law of associativity.
And also the empty word acts as identity in F with respect to the multiplication.
Again we have to check if elements in F are invertible
let w=xy...z
$\Longrightarrow$ $w^{-1} = z^{-1}...y^{-1}x^{-1}$
then w.w^{-1}=xy...z$z^{-1}...y^{-1}x^{-1}$
then it can be reduced and we get w.w^{-1}=1.
$\Longrightarrow$ $^{-1}$ is the inverse of w.
$\therefore$ F satisfies all the axioms of a group.

NOTE:

The group F of equivalence classes of words in S$'$ is called the free group on the set S.Since S is a generating set of F and every non-empty reduced word in W$'$ defines a non-trivial element in F. Hence S is a free basis of F so that$F$ is free on X.

UNIVERSAL PROPERTY OF FREE GROUPS.

Let F be the free group on the set S $=\{a,b,c,..\}$ and G be a group. Any map of sets f :S $\longrightarrow$ G extends in a unique way to a group homomorphism $\phi : F \longrightarrow$ G

If we denote the image f(x) of an element x of S by x , then ϕ sends a word in S$'$ $=\{a,a^{-1},b,b^{-1},...\}$ to the corresponding product of the elements $\{a,a^{-1},b,b^{-1},...\}$ in G.

RELATIONS:

A relation R among elements $x_1,x_2,....x_n$ of a group G is a word r in the free group on the set $\{x_1,x_2,....x_n\}$ that evaluates to 1 in G.
We will denote such arelation either a r or for emphasis as r=1.

for example:
The dihedral group D$_n$ of symmetries of a regular n-sided polygon is generated by the rotation x through a angle $\frac{2\pi}{n}$ and areflection y, and these generators satisfy the relation

$x^n = 1 \qquad y^2 = 1 \qquad yx = x^{-1}y$

i.e., $x^n = 1 \qquad y^2 = 1 \qquad xyxy = 1$

One can use these relations to write the elements of D$_n$ in the form x^iy^j with $0 \leq i < n$ and $0 \leq j < 2$ and then one can compute the multiplication table for the group.
So the relations determine the group and they are therefore called the defining relations.
When the relations are more complicated , it can be difficult to determine the elements of the group and the multiplication table explicitly.

Chapter 5

GROUP PRESENTATIONS

Let S be the set of generators so that every element of the group can be written as a product of some of these generators and a set R of relations among those generators.
A presentation of a group is a set of elements that generate the group together with relators ,products of generators that give the identity element.
We then say G has presentation $< S|R >$.
Informally, G has the above presentation if it is the "freest group" generated by S subject only to the relations R.
Formally, the group G is said to have the above presentation if it is isomorphic to the quotient of a free group on S by the normal subgroup generated by the relations R.

The presentation $< S|R >$ is finitely generated if the set S is finite and is said to be finitely realted if R is finite. If both sets S and R are finite then it is said to be a finite presentation.

EXAMPLES:

Consider the group presentation with
S=$\{a\}$ and R=$\{a^6\}$
i.e., the presentation $+< a : \{a^6\} = 1 >$.
This group generated by one element a with the given relation is isomorphic to the group Z_6.

Now consider the group defined by two generators a and b with the relation

$a^2 = 1$,b^3=1 and ab=ba
i.e., the group with the presentation $< a, b : a^2, b^3, aba^{-1}b^{-1} >$
Thus every element in this group can be written as a product of non-negative powers of a and b.The realtion $aba^{-1}b^{-1} = 1$, i.e., ab=ba allows us to write all first all factors involving a and then all factors involving b ,i.e., every element of group is equal to some $a^m b^n$.
But $a^2 = 1$,b^3=1 show that there are six distinct elements 1,a,b,b^2,ab,ab^2.
Therefore the presentation gives us a group of order 6 that is abelian and by Fundamental theorem it must be cyclic and isomorphic to Z_6.

GROUPS OF ORDER 8.

Let G be a non-abelian group of order 8.
Since G is non-abelian , it has no elements of order 8.
So each element but the identity is of order 2 or 4.

If every element were of order 2,
then for a,b$\in$ G we would have $(ab)^2 = 1$
$\Longrightarrow$ ab.ab = 1

Consider ba = 1.ba.1 = a^2.ba.b^2 = $a(ab)^2b$ = ab
$\Longrightarrow$ ab = ba, which gives a contradiction to the assumption that G is not abelian.

$\Longrightarrow$ G must have an element of order 4.
Let $< a >$ be a subgroup of order 4.
$\Longrightarrow$ $< a >$ is a normal subgroup of G
Choose an element b $\notin < a >$
then the cosets $< a >$ and b$< a >$ exhaust all of G.
$\Longrightarrow$ a and b are generators of G and $a^4 = 1$

Now since $< a >$ is normal in G
G/$< a > \cong Z_2$
and we have $b^2 \in < a >$
If b^2=a or $b^2 = a^3$, then b would be of order 8
hence $b^2 = 1$ or $b^2 = a^2$

Finally , since $< a >$ is normal , we have bab^{-1} $\in < a >$ and since b$< a > b^{-1}$ is a subgroup conjugate to $< a >$ and hence isomorphic to $< a >$,
we see that bab^{-1} must be an element of order 4
Thus bab^{-1} = a or bab^{-1} = a^3

If bab^{-1} = a
$\implies$ ba= ab, which would make G abelian

Now if bab^{-1} = a^3 $\implies$ ba = a^{3}b
Thus we have 2 possibilities for G, namely
$G_1 : (a, b : a^4 = 1, b^2 = 1, ba = a^3b)$
$G_2 : (a, b : a^4 = 1, b^2 = a^2, ba = a^3b)$

$\implies$ a$^{-1} = a^3$ and b$^{-1} = b$ in G_1
$\implies$ a$^{-1} = a^3$ and b$^{-1} = b^3$ in G_2
These facts along with the relation ba= a^{3}b enables us to express every element in G_1 in the form $a^m b^n$
Since a^4 =1 and either $b^2 = 1$ or $b^2 = a^2$, the possible elements in group are:
1,a,a^2, a^3,b,ab,a^2b, a^3b

$\implies G_1$ and G_2 have order 8
Since ba=$a^3b \neq$ ab
We see both G_1 and G_2 are non-abelian.
Now the two groups are not isomorphic follows that, G_1 has two elements of order 4 namely a and a^3. On the otherhand ,in G_2 all elements but 1 and a^2 are of order 4

Now consider the computation
(a^{2}b)(a^{3}b) = a^2(ba)a^{2}b = a^5(ba)ab = a^8(ba)b = a^{11}b^2
For G_1, we have a^{11}b^2 = a^{11} =a^3
For G_2, we have a^{11}b^2 = a^{13}= a

By computing each elements to form the multiplication table we get, the group G_1 is the octic group and is isomorphic to the group D_4 whereas group G_2 is the quaternion group and is isomorphic to the multiplicative group $\{1, -1, i, -i, j, -j, k, -k\}$ of quaternions.

CONCLUSION

Just as the concept of basis is important in the study of real vector spaces in linear algebra,it is equally useful to consider Abelian groups which possess a basis.
An abelian group that possess a basis is called as free abelian group.
And here we focussed on free abelian group with finite basis and discussed various properties about it.
Then we move onto finitely generated abelian groups and study some theorems on free abelian groups and finitely generated abelian groups .
And the contents mentioned in this chapter deals with the proof of "fundamental theorem of finitely generated abelian groups".
The next chapter came up with a different concept called as "free group", a group which satisfy no relation except those implied by the group axioms followed by certain propositions.
In the last chapter we discussed about group presentations.The idea of a group presentation is to form a group by giving a set of generators for the group and certain equations or relations that we want the generators to satisfy.Also we have determined all groups of order 8 up to isomorphism using group presentation.

In short , this project deals with the study on free abelian groups and free groups and various properties regarding them. Also we tried to give a layout for the proof of fundamental theorem. It also discussed about the group presentation through which we identify the non-abelian groups of order 8 upto isomorphism.

REFERENCES

[1]Thomas W Hungerford,Algebra,Springer International Edition.

[2]John B Fraleigh, A First Course in Abstract Algebra,7th Edition.

[3] Michael Artin,Algebra,2nd Edition.

[4]P.M Cohn,Further Algebra and Applications,Springer International edition.

[5]Anthony W Knapp, BASIC ALGEBRA,Cornerstones.

[6]George M. Bergman, An invitation to General Algebra and Universal Constructions.