**INTRODUCTION**

In mathematics, 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, also called an integral basis, is a subset such that every element of the group can be uniquely expressed as an integer combination of finitely many basis elements.

In 1882 paper, Walter von dyck pointed out that these groups have the simplest possible presentation. The algebraic study of free groups was initiated by Jakob Nielsen in 1924, who gave them their name and established many of their basic properties.

Chapter I deals with Basic definition.

Chapter II deals with Free abelian groups.

Chapter III deals with Finitely generated abelian groups.

Chapter IV deals with Free product of groups.

Chapter V deals with Free groups

**CHAPTER I**

**BASIC DEFINITION**

**DEFINITION: 1.1**

A nonempty set of elements G is said to form a **group** if in G there is defined a binary operation, called the product and denoted by ‘∙’, such that

1. For alla, b G implies that a∙bG (closure law).
2. For all a, b, c G implies that a·(b∙c) = (a·b)∙c (associative law).
3. There exists an element e G such that a·e = e∙a = a for all a G (the existence of an identity element in G).
4. For every a G there exists an element G such that

a∙ = ·a = e (the existence of inverses in G).

**DEFINITION: 1.2**

A group G is said to be **abelian** (or **commutative**) if for every a, b G, a·b = b∙a.

**DEFINITION: 1.3**

Let G be a group. Then the number of elements in a group G is called the **order of the group G**.

Order of a group G is denoted by O(G).

**DEFINITION: 1.4**

A nonempty subset H of a group G is said to be a **subgroup** of G if, under the product in G, H itself forms a group.

**DEFINITION: 1.5**

A subgroup N of G is said to be a **normal subgroup** of G if for every gG and n N, N.

**DEFINITION: 1.6**

An isomorphism of a group G to itself is called an **automorphism** of G. The set of all automorphism of G is denoted by Aut G.

**DEFINITION: 1.7**

Let G be a group and ,,…., **normal subgroups** of G such that

1. G = ….
2. Given gG then g =…, in a unique way.

We then say that G is the **internal direct product** of ,,…. ,.

**DEFINITION: 1.8**

A mapping ϕ from a group G into a group Ḡ is said to be a **homomorphism** if for all a, b G, ϕ(ab) = ϕ (a)ϕ (b).

**DEFINITION: 1.9**

A homomorphism ϕ from G into Ḡ is said to be an **isomorphism** if ϕ is one-to-one and onto.

**DEFINITION: 1.10**

Two groups G, G\* are said to be **isomorphic** if

there is an **isomorphism** of G onto G\*. In this case we write **G ≈ G\*.**

1. G ≈ G.
2. G ≈ G\* implies G\* ≈ G.
3. G ≈ G\*, G\* ≈ G\*\* implies G ≈ G\*\*.

**DEFINITION: 1.11**

A nonempty set R is said to be an **associative ring** if in R there are defined two operations, denoted by ‘**+’** and ‘**·’** respectively, such that for all a, b, c in R:

1. a + b is in R.
2. a + b = b + a.
3. (a + b) + c = a + (b + c).
4. There is an element 0 in R such that a + 0 = a (for every a in R).
5. There exists an element -a in R such that a + (-a) = 0.
6. a · b is in R.
7. a· (b ·c) = (a· b)· c.
8. a· (b + c) = a· b + a· c and (b + c) ·a = b ·a + c ·a (the two distributive laws).

**DEFINITION: 1.12**

There is an element 1 in R such that a ·1 = 1 · a = a for every a in R; if there is such we shall describe R as a **ring with unit element.**

**DEFINITION: 1.13**

If the multiplication of R is such that a · b = b · a for

every a, b in R, then we call R a **commutative ring.**

**DEFINITION: 1.14**

If R is a commutative ring, then a non-zero element a R is called **zero-divisor** if there is non-zero element b R, such that ab = 0.

**DEFINITION: 1.15**

A commutative ring is an **integral domain** if it has no zero-divisors.

**DEFINITION: 1.16**

A ring is said to be a **division ring** if its nonzero elements form a group under multiplication.

**DEFINITION: 1.17**

A **field** is a commutative division ring, if every non-zero of R has a multiplication inverse in R.

**DEFINITION: 1.18**

A mapping ϕ from the ring R into the ring R' is said to be a **homomorphism** if

1. ϕ(a + b) = ϕ(a) + ϕ(b),
2. ϕ(ab) = ϕ(a)ϕ(b),

for all a, b R.

**DEFINITION: 1.19**

If a, b G, then b is said to be a **conjugate** of a in G if there exists an element c such that b = c-1ac.

This relation a ~ b is said to be conjugacy.

**DEFINITION: 1.20**

An integral domain R is said to be a **Euclidean ring**

if for every a 0 in R there is defined a non-negative d(a) such that

1. For all a, bR, both nonzero, d(a) d(ab).
2. For any a, b R, both nonzero, there exist t, r R such that a = tb + r where either r = 0 or d(r) < d(b).

**DEFINITION: 1.21**

In the Euclidean ring R, a and b in R are said to be **relatively prime,** if their greatest common divisor is a unit of R.

**DEFINITION: 1.22**

A polynomial p(x) in F[x] is said to be **irreducible** over F if wheneverp(x) = a(x)b(x) with a(x), b(x) F[x], then one of a(x) or b(x) has degree 0 (i.e., is a constant).

**DEFINITION: 1.23**

The polynomial f(x) = + x + · · · + , where the , ,..., are integers is said to be **primitive** if the greatest common divisor of, , ..., is 1.

**DEFINITION: 1.24**

A nonempty set V is said to be a **vector space** over a field F if V is an abelian group under an operation which we denote by ‘+’, and if for every F, v V there is defined an element, written v, in V subject to

1. (v + w) =v + w;
2. ( +)v = v + v;
3. (v) = ()v;
4. 1 v = v;

for all , F, v, wV (where the 1 represents the unit element of F under multiplication).

**DEFINITION: 1.25**

If V is a vector space over F and if ,…, V then any element of the form + + + · · · + where the F, is a **linear combination** over F of,…… ,.

**DEFINITION: 1.26**

If S is a nonempty subset of the vector space V, then L(S), the **linear span** of S, is the set of all linear combinations of finite sets of elements of S.

**DEFINITION: 1.27**

The vector space V is said to be **finite-dimensional** (over F) if there is a **finite subset** S in V such thatV = L(S).

**DEFINITION: 1.28**

If V is a vector space and if ,….,are in V, we say that they are **linearly dependent** over F if there exist elements ,…., in F, not all of them 0, such that + + · · · + = 0.

If the vectors ,…. , are not linearly dependent over F, they are said to be **linearly independent** over F.

**DEFINITION: 1.29**

A subset S of a vector space V is called a **basis** of V if S consists of linearly independent elements (that is, any finite number of elements in S is linearly independent) and V = L(S).

**DEFINITION: 1.30**

The vector space V over F is said to be an **inner**

**product space** if there is defined for any two vectors u, v V an element (u, v) in F such that

1. (u, v) = (;
2. (u, u) 0 and (u, u) = 0 if and only if u = 0;
3. (u + v, w) = (u, w) + (v, w);

for any u, v, w V and , F.

**DEFINITION: 1.31**

Let : G Ḡ be a homomorphism.

If ϕ is one-to-one, then it is called monomorphism. If ϕ is onto, then it is called an epimorphism.

**DEFINITION: 1.32**

Let H be a subgroup of a group G. Let a G.

Then the set aH = {ah | h H} is called the **left coset** of H defined by a in G. Similarly Ha = {ha | h H}is called **right** **coset** of H defined by a.

**DEFINITION: 1.33**

A polynomial p(x) in F[x], the polynomial ring in x over F, we shall associate with p(x) a group, called the

**Galois group** of p(x).

**DEFINITION: 1.34**

Suppose G is finite group and O(G) = n pm , where p is a prime number and p is not a divisor of n.

Then the subgroup H of G is said to be a **sylow subgroup** of G iff O(H) = pm .

**DEFINITION: 1.35**

The linear transformations S, TA(V) are said to be **similar** if there exists an invertible element C A (V) such that T = .

**CHAPTER II**

**FREE ABELIAN GROUPS**

**DEFINITION: 2.1**

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 coefficient

**EXAMPLE:**

The group Z Z is free abelian and {(1,0), (0,1)} is a basis. Similarly, a basis for the free abelian group Z Z Z is {(1,0,0), (0,1,0), (0,0,1)} and so on. Thus finite direct products of the group Z with itself are free abelian groups.

**DEFINITION: 2.2**

If G is a free abelian group then the **rank** of G is the cardinality of a basis of G.

**PROPERTIES:**

(i) Every two basis of the free abelian group have the same cardinality. Also Free abelian groups of same rank are isomorphic.

(ii) A free abelian group is finitely generated if and only if its rank is a finite number n.

(iii) 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 necessarily true for infinite number of free abelian groups.

**THEOREM: 2.3**

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 =+ + ....... + for 0 in Z and distinct in X

2. X generates G and + + ....... + = 0 for in Z and distinct ∈ X iff ==.......= 0

**PROOF:**

1 2

Assume that any non-zero element a in G can be expressed uniquely as

a =+ + ....... +.

for 0 in Z and distinct in X.

Given G is a non-zero abelian group, i.e., G 0.

We have X 0

It follows from 1 that 0 X.

For if = 0 and 0 where , ∈ X ⊆ G then, = + , which would contradict the uniqueness of the expression for .

From condition (1) it is clear that X generates G.

+ + ....... + = 0 if = =....... = 0

Suppose that + + ....... + = 0 with some

0 by dropping terms with zero coefficients and renumbering, we can assume all 0.

Then

= + + + ....... +

= (1+) + + ....... +

which gives two ways of writing 0 contradicting the uniqueness

assumption in condition 1.

If + + ....... + = 0, then = =....... = 0

2 1

Let a G. Since X generates G.

We see a can be written in the form

a = + + ....... +.

We have to show that this expression is unique.

We have if + + ....... + = 0, then

= =....... = 0.

Suppose a has another such expression in terms of elements of X. By using some zero coefficients in the two expressions, we can assume they involve the same elements in X and are of the form,

a = + + ....... +

a = + + ....... +

Subtracting we get,

0 = ( − ) + ( − ) +.....+ ( − ) .

Then by our assumption we get

− = − =........= − = 0

− = 0

= for i = 1, 2,..., r.

Thus the coefficients are unique.

Expression of any element a in G is unique.

**PROPOSITION: 2.4**

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 → A.

**PROOF:**

Let X consist of the elements for i ∈ I.

Suppose that X is a basis of G.

Let : be the mapping of X into any abelian group A.

The mapping x = is a well defined homomorphism of G into A and maps into .

However it is the only homomorphism of G which maps to for each i ∈ I.

Conversely,

Suppose that G and X have the stated property.

Let A be a free abelian group with basis , i ∈ I.

There is a homomorphism : G A such that () = ; i ∈ I.

As a free abelian with basis , there is a homomorphism ψ : A G such that ψ() = ; i ∈ I.

Then ψ ◦ is an endomorphism of G which maps into .

Since the identity endomorphism of G has the same property, by the uniqueness part of the stated condition.

It follows that ψ ◦ = .

The endomorphism ◦ ψ of A maps each of the generators , i ∈ I of A to itself and is therefore the identity endomorphism of A.

Thus is an isomorphism of G with a mapping to .

Thus ψ is an isomorphism of G with a mapping to .

Since the elements ; i ∈ I forms a Z-basis of A, the elements ; i ∈ I form Z-basis of G.

Hence the proof.

**PROPOSITION: 2.5**

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

**PROOF:**

Let B and be any 2 bases of G.

We have to show that | B |= | |

Also we have the isomorphism.

Z G Z.

**Case 1:**

When B and are finite sets.

Let | B |= m and | | = n

Take 2G = {2a|a ∈ G} which is a subgroup of G.

Also we have G Z.

We obtainG/2G Z/2Z.

Similarly since we have G Z.

G/2G Z /2Z.

This gives,

=| Z /2Z| = G/2G = | Z /2Z| =

m=n

**Case 2:**

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

Z /2Z G/2G Z /2Z

This is however a contradiction.

Since Z /2Z is a finite group and Z /2Z is an infinite group.

Such a case doesn’t exist.

**Case 3:**

Both B and are infinite sets.

If B is infinite then |B| = | Z | .

It follows that

|B| = | Z | = |G| = | Z | = ||

|B| = | |

Hence the two bases of G have the same cardinality.

**THEOREM: 2.6**

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) ≤ rank (G) .

**PROOF:**

Since G is a free abelian group of rank n.

Assume that G =

We want to show that if H ⊆ then, H is free abelian and rank(H) ≤ n.

We prove this using the method of induction on n.

If n=1; then H=kZ for k 0.

So H ={0} or H Z

H is free abelian and rank(H)≤ rank(G)

Next for some n, every subgroup of is free abelian and of rank ≤ n.

Now let H ⊆ .

Take the homomorphism

f: → Z

f(, , ..., ) =

We have,

Ker(f) = {( , , ..., 0)| ∈ Z} .

Since Im(f/H) ⊆ Z, thus Im(f/H) is a free abelian group.

We get,

H Im(f/H) ⊕ ker(f/H)

We also have

ker(f/H) = ker(f) ∩ H

It follows that 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 ≤ n.

H Im(f/H) ⊕ ker(f/H)

Where Im(f/H) is a free abelian group of rank ≤ 1 and

ker(f/H) is a free abelian group of rank ≤ n.

H is a free abelian group of rank ≤ n+1.

**CHAPTER III**

**FINITELY GENERATED ABELIAN GROUPS**

**DEFINITION: 3.1**

An abelian group (G,+) is called **finitely generated** if there exists finitely many elements , , ...., in G such that every x in G can be written in the form x = + , + ....... + with integers , ...,.

In this, we say that the set {, ..., } is a generating set of G or that , ..., generate G. Every finite abelian group is finitely generated.

**THEOREM: 3.2**

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 = , ,....,.

Let F be free abelian group and {,..., } be a basis of F.

We have a homomorphism

f : F → G defined by f() = .

Take H = ker(f).

Since f is an epimorphism by first isomorphism theorem.

First isomorphism theorem,

Let f : G → H be a homomorphism with kernel K. Then K is a normal subgroup of G and G/K Im(f).

we have,

F/Ker(f) Im(f)

GF/H.

Hence the proof.

**THEOREM: 3.3**

Let G be a finitely generated abelian group with

generating set { , ,...., }. Let : Z × Z × .... × Z → G (where there are n factors of Z) be defined by

(, ..., ) = + + ....... + .

Then is a homomorphism onto G.

**PROOF:**

From the meaning of for ∈ Z and ∈ G.

[(, ..., ) + (, ..., )] = (+, ..., +)

= (+) + ... + (+)

= ++…++

= ( + ... + ) + ( +...+)

= (, ..., ) + (, ..., )

is an homomorphism.

Since , ,...., generates G.

Hence is a homomorphism onto G.

**THEOREM: 3.4**

If X = {, ..., } is a basis for a free abelian group G and t ∈ Z, then for i j, the set

Y = {, , ... , + t , , ,..., } is also a basis for G.

**PROOF:**

To show that Y is a basis of G.

We need to show that the set will span G and the elements are linearly independent.

Given {, ..., } spans G.

Since = (−t) + 1(+ t)

We see thatcan be recovered from Y, which also this generates G.

Suppose,

+ + ... + + ( + t) + + ... + =0

Then

+ + ... + (+ t) + ... + ... + = 0

And since X is a basis

= =.... = + t = ...= =...= = 0

From = 0 and + t = 0.

It follows that = 0.

i.e., = =.... = ...= =...= = 0

we get Y generates G.

By theorem Y is a basis of G.

Hence Y is also a basis of G.

**THEOREM: 3.5**

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 ≤ n. Furthermore there exists a basis {, ..., } for G and positive integers , ...., where divides for

i = 1,…, S-1 such that {, , ..., } 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 ≤ n.

Now we have to show that K has a basis of the described form.

Suppose Y = {, ,..., } is a basis for G.

All non-zero elements in K can be expressed in the form

+ + ... +

for some || is non-zero.

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

By renumbering the elements of if necessary we can assume there is ∈ K such that

= + + ... +

where > 0 and is the minimal attainable coefficient as just described.

Using the division algorithm, we write = + where 0 ≤ < for j = 2,3,...,n.

Then,

= + ( + ) + ..... + ( +

= ( + + ... + ) + + ..... +

Let = + + ... +

= + + … +

Then by using theorem, {, , ..., } is also a basis for G.

Also from equation and our choice of for minimal coefficient , we see that = ..... = 0 .

Thus ∈ K

We now consider bases for G of the form {, , ..., }.

Each element of K can be expressed in the form + + ... +.

Since ∈ K, we can subtract a suitable multiple of and then using the minimality of to see that is multiple of .

We see actually have + ... + in K.

Among all such bases {, , ..., } we choose one that leads to some 0 of minimal magnitude.

By renumbering the elements of we can assume that there is ∈ K such that

= +...+

where <0 and is minimal as just described.

Exactly as in the preceding paragraph, we can modify our

basis from = {, , ..., } to a basis = {, , , ..., } for G where, ∈ K

Writing = q + r for 0 ≤ r <

We see that { + q,, , ..., } is a basis for G and

+ = + (q + r)

= ( + q) + r ∈ K

But by our minimal choice of we see r = 0.

So divides

We now consider all bases of the form {, , , ..., }for G and examine elements of K of the form + ... +

The process continues until we obtain a basis

{, , ... , , .., } where the only element K of the form + ... + is zero.

i.e., all are zero.

Then let = = .... = = and a basis for G of the described form in the proposition.

**THEOREM: 3.6**

Every finitely generated abelian group is isomorphic to a group of the form

× × ..... × × Z × Z...... × Z,

where divides for i = 1,2,....r-1.

**PROOF:**

It will be convenient to use as notations

Z/1Z Z/Z {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 = Z × Z × Z...... × Z for n factors.

Consider the homomorphism : F → G and let K be the kernel of this homomorphism. Also K is a subgroup of F.

Then there is basis for F of the form {, ,..., } where {, ,…, } is a basis of K and divides

for i = 1,…, S-1

By using theorem 3.1,

“ 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 ”.

We have G is isomorphic to F/K.

But,

F/K (Z × Z × Z.....× Z)/( Z × Z × ..... × Z...... × {0}.... × {0})

( × × ..... × × Z..... × Z)

It is possible that = 1 , in which case Z = {0} and can be dropped from this product .

similarly may be 1 and so on.

We let be the first >1, be the next , and so on.

**CHAPTER IV**

**FREE PRODUCTS OF GROUPS**

**DEFINITION: 4.1**

Let G be a group. If {}α∈J is a family of subgroups of G, we say that these groups generate G if every element x of G can be written as a finite product of elements of the groups .

This means that there is a finite sequence (,..., ) of elements of the groups such that x = ... . Such a sequence is called a **word** in the groups . It is said to **represent** the element x of G.

**DEFINITION: 4.2**

Let G be a group, let {}α∈J be a family of subgroups of G that generates G. Suppose that ∩ consists of the identity element alone whenever α β.

We say that G is the **free product** of the groups if for each x ∈ G, there is only one reduced word in the groups that represents x. In this, we write

G =

or in the finite case, G = ∗···∗ .

**LEMMA: 4.3**

Let G be a group. Let {} be a family of subgroups of G.

If G is the free product of the groups , then G satisfies the following condition.

Given any group H and any family of homomorphisms : → H, there exists a homomorphism h : G → H whose restriction to equals , for each α. Furthermore, h is unique.

**PROOF:**

Given x ∈ G with x 1, let (,..., ) be the reduced word that represents x.

If h exists, it must satisfy the equation

h(x) = h() … h() = () …h() (∗)

where is the index such that∈ .

Hence h is unique.

To show h exists, we define it by equation (∗) if x 1, and we set h(1) = 1.

Because the representation of x by a reduced word is unique, h is well defined.

We must show it is a homomorphism.

We first prove a preliminary result.

Given a word w = (,..., ) of positive length in the elements of the groups .

Let us define (w) to be the element of H given by the equation

(w) = () … ()

where is any index such that ∈ .

Now is unique unless = 1.

Hence is well-defined.

If w is the empty word, let (w) equal the identity element of H.

We show that if w' is a word obtained from w by applying one of our reduction operations, (w') = (w).

Suppose first that w' is obtained by deleting = 1 from the word w.

Then the equation (w') = (w) follows from the fact that () = 1.

Second, suppose that = and that

w' = (,..., ,…, ).

The fact that

() () = ()

where α = = , implies that(w) = (w').

It follows at once that if w is any word in the groups that represents x, then h(x) = (w).

For by definition of h, this equation holds for any reduced word w, and the process of reduction does not change the value of .

Now we show that h is a homomorphism.

Suppose that w = (,..., ) and w' = (,..., ) are words representing x and y respectively.

Let (w, w') denote the word (,..., , ,..., ), which represents xy.

It follows that

(w, w') = (w) (w').

h(xy) = h(x)h(y).

**DEFINITION: 4.4**

Let {}α∈J be an indexed family of groups. Suppose that G is a group, and that : → G is a family of monomorphisms, such that G is the free product of the groups ().

Then we say that G is the **external free product** of the groups , relative to the monomorphisms .

**THEOREM: 4.5**

Let a family { }α∈J of groups, there exists a group G and a family of monomorphisms : → G such that G is the free product of the groups ().

**PROOF:**

We assume that the groups are disjoint as sets. Then as before, we define a word in the elements of the groups to be an n-tuple w = (,..., ) of elements of .

It is called a reduced word if for all i, where is the index such that ∈ , and if for each i, is not the identity element of

We define the empty set to be the unique reduced word of length zero.

Note that we are not given a group G that contains all the as subgroups, so we cannot speak of a word representing an element of G.

Let W denote the set of all reduced words in the elements of the groups .

Let P(W) denote the set of all bijective functions

π : W → W.

Then P(W) is itself a group, with composition of functions as the group operation.

We shall obtain our desired group G as a subgroup of P(W).

**Step 1:**

For each index α and each x ∈ , we define a set map : W → W. It will satisfy the following conditions:

(1) If x = , the identity element of , then is the identity map of W.

(2) If x, y ∈ and z = x y, then = ◦ .

We proceed as follows. Let x ∈ . For notational purposes, let w = (,..., ) denote the general nonempty element of W, and let denote the index such that ∈ .

If x , define as follows.

1. (∅) = (x),
2. (w) = (x,,..., ) if α,
3. (w) = (x,..., ) if = α and x-1
4. (w) = (,..., ) if = α and = x−1

If x = , define to be the identity map of W.

Note that the value of is in each case a reduced word, that is, an element of W.

In cases (i) and (ii), the action of increases the length of the word.

In case (iii) it leaves the length unchanged, and in case (iv) it reduces the length of the word.

When case (iv) applies to a word w of length one, it maps w to the empty word.

**Step 2:**

We show that if x, y ∈ and z = x y, then = ◦ .

The result is trivial if either x or y equals , since in that case or is the identity map.

So let us assume henceforth that x and y .

We compute the values of and of ◦ on the reduced word w.

There are four cases to consider.

(i) Suppose w is the empty word.

We have πy (∅) = (y). If z =, then y = x-1 and (∅) = ∅ by (iv), while πz (∅) equals the same thing because πz is the identity map. If z , then

(∅) = (x y) = (z) = (∅).

In the remaining cases, we assume w = (,..., ), with ∈ .

(ii) Suppose α α1.

Then (w) = (y, ,..., ). If z = , then y = x−1 and (w) = (,..., ) by (iv), while (w) equals the same because is the identity map.

If z 1α, then

(w) = (xy,,..., )

= (z, ,..., )

= (w)

(iii) Suppose α = and y .

Then (w) = (y, ,...,). If xy = , then

(w) = (,..., ), while (w) equals the same thing because

z = xy.

If xy , then

(w) = (xy, ,..., )

= (z, ,..., )

= (w).

(iv) Finally, suppose α = and y = .

Then (w) = (,..., ), which is empty if n = 1.

We compute

(w) = (x, ,..., )

= (x(y), ,..., )

= (z, ,..., )

= (w).

**Step 3:**

The map is an element of p(W), and the map

: → P(W) defined by (x) = is a monomorphism.

To show that is bijective, we note that if y = x−1, then conditions (1) and (2) imply that ◦ and ◦ equal the identity map of W.

Hence belongs to P(W).

The fact that is a homomorphism is a consequence of condition (2).

To show that is a monomorphism.

We note that if x , then (∅) = (x).

So that is not the identity map of W.

**Step 4:**

Let G be the subgroup of P(W) generated by the groups ' = ().

We show that G is the free product of the groups '.

First, we show that '∩ ' consists of the identity alone if α β.

Let x ∈ and y ∈ . We suppose that neither nor is the identity map of W and show that .

But this is easy, for (∅) = (x) and (∅) = (y), and these are different words.

Second, we show that no nonempty reduced word

w'= (,..., )

in the groups ' represents the identity element of G.

Let be the index such that ∈ , then and

for each i.

We compute

( (···( (∅)))) = (,..., ),

So the element of G represented by w' is not the identity element of P(W).

**LEMMA: 4.6**

Let {}α∈J be a family of groups. Let G be a group. Let : → G be a family of homomorphisms. If the extension condition holds, then each is a monomorphism and G is the free product of the groups ().

**PROOF:**

We first show that each is a monomorphism.

Given an index β, let us set H = .

Let : → H be the identity if α = β, and the trivial homomorphism if α β.

Let h : G → H be the homomorphism given by the extension condition.

Then h ◦ = , so that is injective.

There exists a group G' and a family ' : → G' of monomorphisms such that G' is the free product of the groups ' ().

Both G and G' have the extension property.

The preceding theorem then implies that there is an isomorphism : G → G' such that ◦ = '.

It follows at once that G is the free product of the groups ().

**COROLLARY: 4.7**

Let G = ∗ , where is the free product of the subgroups {}α∈J and is the free product of the subgroups

{}β∈K . If the index sets J and K are disjoint, then G is the free product of the subgroups { }γ ∈J∪K .

**PROOF:**

If : H and: are families of

homomorphisms, they extend to homomorphisms :  and

:  by the preceding lemma.

Then and extend to a homomorphism.

h : G .

Hence G is the free product of the subgroups { }γ ∈J∪K .

**DEFINITION: 4.8**

If S is a subset of G, one can consider the intersection N of all normal subgroups of G that contain S.

It is easy to see that N is itself a normal subgroup of G. It is called the **least normal subgroup** of G that contains S.

**THEOREM: 4.9**

Let G = ∗ . Let be a normal subgroup of , for i = 1, 2. If N is the least normal subgroup of G that contains and , then G/N (/) ∗ (/).

**PROOF:**

The composite of the inclusion and projection

homomorphisms

→ ∗ → ( ∗)/N

carries to the identity element, so that it induces a homomorphism

: / → ( ∗ )/N.

Similarly, the composite of the inclusion and projection homomorphisms induces a homomorphism

: / → ( ∗ )/N.

We show that the extension condition holds with respect to and .

It follows that and are monomorphisms and that ( ∗ )/N is the external free product of / and / relative to these monomorphisms.

So let : / → H and : / → H be arbitrary homomorphisms.

The extension condition for ∗ implies that there is a homomorphism of ∗ into H that equals the composite

→ / → H

of the projection map and on , for i = 1, 2.

This homomorphism carries the elements of and to the identity element, so its kernel contains N.

Therefore it induces a homomorphism h : ( ∗ )/N → H that satisfies the conditions = h ◦ and = h ◦ .

**LEMMA: 4.10**

Let S be a subset of the group G. If N is the least normal subgroup of G containing S, then N is generated by all conjugates of elements of S.

**PROOF:**

Let N' be the subgroup of G generated by all conjugates of elements of S.

We know that N' ⊂ N.

To verify the reverse inclusion, we need merely show that N' is normal in G.

Given x ∈ N' and c ∈ G.

We show that cxc−1 ∈ N'.

We can write x in the form x =... , where each is conjugate to an element of S.

Then cc−1 is also conjugate to .

Because,

cxc−1 = (cc−1)(cc−1)…(cc−1)

cxc−1 is a product of conjugates of elements of S, so that cxc−1 ∈ N' as desired.

**CHAPTER V**

**FREE GROUPS**

**DEFINITION: 5.1**

Let G be a group. Let {} be a family of elements of G, for α ∈ J. We say the elements {} **generate** G if every element of G can be written as a product of powers of the elements .

If the family {} is finite, we say G is **finitely generated**.

**DEFINITION: 5.2**

Let {} be a family of elements of a group G. Suppose each generates an infinite cyclic subgroup of G.

If G is the free product of the groups {}, then G is said to be a **free group**, and the family {} is called a **system of** **free generators** for G.

**DEFINITION: 5.3**

Let {}α∈J be an arbitrary indexed family. Let denote the set of all symbols of the form for n ∈ Z. We make into a group by defining

. =

Then is the identity element of , and is the inverse of . We denote simply by .

The external free product of the groups {} is called the **free group on the elements** .

**DEFINITION: 5.4**

Let G be a group. If x, y ∈ G, we denote by [x, y] the

element

[x, y] = xyx−1 y−1

of G. It is called the **commutator** of x and y.

The subgroup of G generated by the set of all commutators in G is called the **commutator subgroup** of G and denoted [G, G].

**LEMMA: 5.5**

Let G be a group, the subgroup [G, G] is a normal subgroup of G and the quotient group G/[G, G] is abelian. If h : G → H is any homomorphism from G to an abelian group H, then the kernel of h contains [G, G], so h induces a homomorphism k : G/[G, G] →H.

**PROOF:**

**Step:1**

First we show that any conjugate of a commutator is in

[G, G].

We compute as follows.

g[x, y] g−1 = g(xyx−1 y−1)g−1

= (gxyx−1)(1)(y−1g−1)

= (gxyx−1)(g−1 y−1 yg)(y−1g−1)

= ((gx)y(gx) −1 y−1)(ygy−1g−1)

= [gx, y]·[y, g]

which is in [G, G], as desired.

**Step:2**

We show that [G, G] is a normal subgroup of G.

Let z be an arbitrary element of [G, G].

We show that any conjugate gzg−1 of z is also in [G, G].

The element z is a product of commutators and their inverses. Because ,

[x, y] −1 = (xyx−1 y−1) −1

= [y, x],

z actually equals a product of commutators.

Let z …, where each is a commutator.

Then ,

gzg−1 = (gg−1)(gg−1)···(gg−1)

which is a product of elements of [G, G] by Step 1 and hence belongs to [G, G].

**Step:3**

We show that G/[G, G] is abelian.

Let G' = [G, G].

We wish to show that

(aG' )(bG' ) = (bG')(aG'),

that is, abG' = baG' .

This is equivalent to the equation a−1b−1abG' = G'

and this equation follows from the fact that a−1b−1ab = [a−1, b−1], which is an element of G' .

**Step:4**

To complete the proof, we note that because H is abelian,

h carries each commutator to the identity element of H.

Hence the kernel of h contains [G, G].

So that h induces the desired homomorphism k .

Hence the proof.

**THEOREM: 5.6**

If G is a free group with free generators , then

G/[G, G] is a free abelian group with basis [], where [] denotes the coset of in G/[G, G].

**PROOF:**

We apply Lemma

Let G be an abelian group. Let {be a family of elements of G that generates G. Then G is a free abelian group with basis {if and only if for any abelian group H and any family {} of elements of H, there is a homomorphism h of G into H such that h() = for each .

Given any family {} of elements of the abelian group H.

There exists a homomorphism h : G → H such that h() = for each α.

Because H is abelian, the kernel of h contains [G, G].

Therefore h induces a homomorphism k : G/[G, G] → H that carries [] to .

**CONCLUSION**

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. Here we focussed on free abelian group with finite basis and discussed properties about it. Then we move onto finitely generated abelian groups and study some theorems on free abelian groups and finitely generated abelian groups. The next chapter came up with a concept called as free product of groups. In the last chapter we discussed about free group.

**APPLICATIONS**

Group concept can be applied to explore the symmetry of various games, which can lead to optimal strategies and decision making. Symmetries in network graphs can be studied using group theory methods, leading to better understanding and decision making regarding network structures.

This concept has application in physics, chemistry and computer science and even puzzles like Rubik’s cube can be represented using group theory. Additionally, facilitates problem solving and supplies essential tools for other branches of mathematics.

**BIBLIOGRAPHY**

1. **Thomas W. Hungerford**, Algebra,Springer International Edition.

2. **John B.Fraleigh**, A First Course in Abstract Algebra, seventh Edition.

3. **Michael Artin**, Algebra,second Edition.

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

5. **James Munkres**, Toplogy, second edition.

6. **S.K. Jain**, Basic abstract algebra, second edition.

7. **Serge Lang**, Algebra,Third edition

8. **Anthony W.Knapp**, Basic algebra,Cornerstones.

9. **Hermann** and **cie**,algebra commutative.

10. **Allen Hatcher**, Algebraic topology, 2000.

11. **Charles C.Pinter,** A Book of Abstract algebra,second edition.

12. **David S. Dummit** and Richard **M. Foote** Abstract algebra, third edition.