University of Belgrade

Faculty of Mathematics

FREE ABELIAN GROUPS

Master thesis

By

Khola Algale

Supervisor:

Prof.dr.Aleksandar Lipkovski

Belgrade 2012

To my Parents

To my Husband

Acknowledgment

Foremost, I would like to express my sincere gratitude to my supervisor, Prof.dr. Aleksandar Lipkovski for the continuous support of my Master study, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better supervisor and mentor for my Master study.

Besides my supervisor, I would like to thank the rest of my thesis committee for their work.

My sincere thanks also goes to my teachers in Libya for everything, and helping me to get to this place.

Last but not the least; I would like to thank my family and all people who helped me to finish this work.

Khola Algale

Content

Introduction 3
The Groups: Definitions, Examples, Basic Properties 4
The Group: 4
Subgroups: 6
Normal subgroups: 7
Cyclic groups: 7
Permutation group: 9
Quotient group: 10
Abelian group: 12
Direct Product and Direct Sum of Abelian Groups 14
Direct product of groups 14
Direct sum of abelian groups: 17
The difference between direct product and direct sum for infinite sum of groups 19
The Torsion and the Basis of an Abelian Groups 22
The torsion of an abelian group 22
The basis of an abelian group 25
Free Abelian Groups 29
The homomorphic property of free abelian groups 30
The subgroup of free abelian group 33
References 38

Introduction

The study of groups arose early in the nineteenth century in connection with the solution of equations. Originally a group was a set of permutations with the property that the combination of any two permutations again belongs to the set. Subsequently this definition was generalized to the concept of an abstract group, which was defined to be a set, not necessarily of permutations, together with a method of combining its elements that is subject to a few simple laws.

The theory of abstract groups plays an important part in present day mathematics and science. Groups arise in a bewildering number of apparently unconnected subjects. Thus they appear in crystallography and quantum mechanics, in geometry and topology, in analysis and algebra, in physics, chemistry and even in biology.

In the early days of group theory attention was confined almost entirely to finite groups. But recently, and above all in the last two decades, the infinite group has come into its own. The results obtained on infinite abelian groups have been particularly penetrating.

So in this research we will talk about free abelian groups and the important theorems in this topic.

We divided this research into four chapters as follows:

Chapter 1 presents the group theory in general, definitions, examples and some theorems.

Chapter 2 shows that the concept of direct product and direct sum of abelian groups and we made clear that in the abelian group it is usual to use additive notation: $x + y$. The reason for this is that while multiplication of various mathematical objects (matrices, functions etc.) is non-commutative, addition invariably commutes. So by using additive notation the commutativity seems perfectly natural.

Chapter 3 is concerned with the torsion and the basis of abelian groups and we explained the definitions and the theorems and some examples.

Chapter 4 is on free abelian groups. Two important things of free abelian groups are treated: the homomorphic property of free abelian groups and the subgroup of free abelian groups.

Chapter 1

The Groups: Definitions, Examples, Basic Properties

The Group:

In mathematics, a group is an algebraic structure consisting of a set together with an operation that combines any two of its elements to form a third element. To qualify as a group, the set and the operation must satisfy a few conditions called group axioms, namely closure, associative, identity and inversibility.

Definition 1.01:

A group $(G,*)$ is a nonempty set G together with a binary operation $*$ on G such that the following conditions hold:

1. Closure:
   For all $a, b \in G, a * b \in G$.
2. Associativity:
   For all $a, b, c \in G, (a * b) * c = a * (b * c)$.
3. Identity element:
   There exists an identity element $e \in G$ such that for all $a \in G, a * e = e * a = a$.
4. Inverse element:
   For each $a \in G$ there exists an inverse element $a^{-1} \in G$ such that
   $a * a^{-1} = a^{-1} * a = e$.

Terminology:

We shall call the group additive if the operation is a kind of addition. In this case, it is standard to denote the operation by $(+)(a + b)$, the identity by 0 and the inverse of a in G by $(-a)$. We shall call the group multiplicative if the operation is a kind of multiplication. In this case we often write (ab) or $(a \cdot b)$ to denote the operation, and we denote the identity by e or 1, and the inverse of a in G by (a^{-1}).

Basic Properties of groups:

1. (Uniqueness of the identity): The identity element of G is unique.
2. (Properties of the inverse):
   i. Every element $a \in G$ has a unique inverse.
   ii. For every $a \in G$, we have $(a^{-1})^{-1} = a$ (two inverses get back to the original)
   iii. For all $a, b \in G$, the inverse of the product is given by $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.
3. (The cancellation law): let G be a group, and let $a, b, c \in G$

i. If $ab = ac$, then $b = c$

ii. If $ac = bc$, then $a = b$

Examples of groups:

1. The sets of integers, rational numbers, real numbers and complex numbers are groups, where the group operation is the operation of addition.
2. The sets of non-zero rational numbers $(Q \setminus \{0\})$, non-zero real numbers $(R \setminus \{0\})$ and non-zero complex numbers $(C \setminus \{0\})$ are also groups, where the group operation is the operation of multiplication.
3. For each positive integer n the set Z_n of integers modulo n is a group, where the group operation is addition modulo $n(Z_2, +)$.
4. For each positive integer n the set Z_n^* of integers modulo n is a group, where the group operation is multiplication modulo n.
5. For each positive integer n the set of all non-singular $n \times n$ matrices is a group, where the group operation is matrix multiplication.
6. The set $\{1, -1\}$ is a group with the operation multiplication.
7. The set $\{1, -1, i, -i\}$ is a group with the operation multiplication.

First example: the integers $(\boldsymbol{Z}, +)$.

One of the most familiar groups is the set of integers Z which consists of the numbers:

$$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$$

The following properties of integer addition serve as a model for the abstract group axioms given in the definition below:

1. For any two integers a and b, the sum $(a + b)$ is also an integer. Thus, adding two integers never yields some other type of number, such as a fraction. This property is known as closure under addition.
2. For all integers a, b and c, $(a + b) + c = a + (b + c)$. Expressed in words, adding a to b first and then adding the result to c gives the same final result as adding a to the sum of $b$and c, a property known as associativity.
3. If a is any integer, then $0 + a = a + 0 = a$. Zero is called the identity element of addition because adding it to any integer returns the same integer.
4. For every integer a, there is an integer b such that $a + b = b + a = 0$. The integer b is called the inverse element of the integer a and is denoted$(-a)$.

The integers together with the operation $+$, form a group and the integers with the operation of multiplication instead of addition $(Z, \cdot)$ do not form a group.

The closure, associativity and identity axioms are satisfied, but inverse does not exist. For example $a = 2$ is an integer, but the only solution to the equation $a \cdot b = 1$ in this case is $b = \frac{1}{2}$, which is a rational number, but not an integer. Hence not every element of Z has a (multiplicative) inverse.

Subgroups:

Definition 1.02:

A group G is said to be a finite group if the set G has a finite number of elements. In this case, the number of elements is called the order of G, denoted by $|G|$.

Examples:

1. The order of Z_n is n.
2. The order of S_n is $n!$.

Definition 1.03:

Let G be a group and let H be the subset of G. Then H is called a subgroup of G If H is itself a group, under the operation induced by G.

If H is a subgroup of G, we shall write $H < G$.

Properties:

1. The set $\{e\}$ whose only element is the identity is a subgroup of any group. It is called a trivial subgroup.
2. A subgroup H of G is said to be proper if $H \neq G$.
3. Every group is a subgroup of itself.
4. The null set { } is never a subgroup (since the definition of group states that the set must be non-empty).

Theorem 1.01:

If H is a nonempty subset of the group G then H is a subgroup of G if and only if $a, b \in H$ implies that $ab^{-1} \in H$.

Proof:

First we need to show if H is a subgroup of G then $ab^{-1} \in H$.

Since $a, b \in H$ then $ab^{-1} \in H$, because H is a group by itself. Now, suppose that if for any $a, b \in H \subseteq G$ we have $ab^{-1} \in H$. We want to show that H is a subgroup. Which we will accomplish by proving it holds the group axioms.

- Since $aa^{-1} \in H$ by hypothesis, we conclude that the identity element is in H: $e \in H$. (Existence of identity).
- Now that we know $e \in H$ for all a, b in H we have that $eb^{-1} = b^{-1} \in H$ so the inverses of elements in H are also in H. (Existence of inverses).
- Let $a, b \in H$. Then we know that $b^{-1} \in H$ by last step. Appling hypothesis shows that $a(b^{-1})^{-1} = ab \in H$.

So H is closed under the operation.

Examples:

1. Q^* and R^* are subgroups of C^*, the multiplicative group of complex numbers.
2. Subgroups of Z.
3. $SL_n(R)$, the set of all $n \times n$ matrices over R with determinant 1, is a subgroup of $GL_n(R)$

Normal subgroups:

Definition 1.04:

A subgroup, N of a group G, is called a normal subgroup of G if $gng^{-1} \in N$ for every $g \in G$, we write $N \triangleleft G$.

$N \triangleleft G \Leftrightarrow \forall n \in N, \forall g \in G, gng^{-1} \in N$.

For any subgroup, the following conditions are equivalent to normality.

- For all g in N, $gNg^{-1} \subseteq N$
- For all g in N, $gNg^{-1} = N$
- The sets of left and right cosets of N in G coincide.
- For all g in G, $gN = Ng$

Properties:

1. The subgroup $\{e\}$ consisting of just the identity element of G and G itself are always normal subgroups of G. And if these are the only normal subgroups, then G is said to be simple.
2. All subgroups N of an abelian group G are normal, because $gN = Ng$.

Cyclic groups:

Definition 1.05:

In group theory, a cyclic group is a group that can be generated by a single element, i.e., a group G is called cyclic if there exists an element g in G such that

$G = \{g^n \ / \ n \ is \ an \ integer\}$ (where the operation is multiplication),
$G = \{ng \ / \ n \ is \ an \ integer\}$ (where the operation is addition).

We refer to g as a generator of G.

Properties:

1. If G is a cyclic group then every subgroup of G is cyclic.
2. Every cyclic group is abelian.
   Because if x, y are in G, then $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$.
3. Every finite cyclic group is isomorphic to the group of integers modulo n under addition.
4. Every infinite cyclic group is isomorphic to Z (the set of all integers) under addition.

Theorem 1.02:

Every subgroup of a cyclic group is cyclic.

Proof:

Let G be a cyclic group, so that $G = \langle g \rangle$, and let $H < G$. Then H is a set of powers of g. Choose n to be the smallest positive exponent of elements in H:

$n = min\{i \in N \ / \ i > 0 \ and \ g^i \in H\}$.

Then I claim that every element of H is a power of $a = g^n$, giving the result.

Indeed, if $h \in H$ is not the identity, then either h or h^{-1} is of the form g^m with $m > 0$, so that $m = n$. Dividing m by n gives

$m = qn + r$

With $r < n$ or $r = 0$ whence

$g^m = (g^n)^q g^r$, giving

$g^r = g^m (g^{-n})^q$

A product of elements of H, showing that $g^r \in H$. By the choice of m, we must have $r = 0$, giving

$h(or \ h^{-1}) = g^m = (g^n)^q$

Proving the result.

Examples:

1. The integers under addition is acyclic group. The numbers $\{1, -1\}$ is a generator.

2. The group $G = \{1, -1, i, -i\} \subseteq C^*$ (the group operation is multiplication of complex numbers) is cyclic with generator i. In fact $\langle i \rangle = \{i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i\} = G$. Note that $-i$ also a generator for G since $\langle -i \rangle = \{(-i)^0 = 1, (-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i\} = G$.
3. The group $G = {Z_7}^*$ is a cyclic group with generator 3. $\langle 3 \rangle = \{1 = 3^0, 3 = 3^1, 2 = 3^2, 6 = 3^3, 4 = 3^4, 5 = 3^5\} = G$.
4. The group $G = {Z_8}^*$ is not cyclic. Indeed since ${Z_8}^* = \{1,3,5,7\}$ and $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1,3\}$, $\langle 5 \rangle = \{1,5\}$, $\langle 7 \rangle = \{1,7\}$, it follows that ${Z_8}^* \neq \langle a \rangle$ for any $a \in {Z_8}^*$.
5. The group $(Z_n, +)$ is cyclic group.

Permutation group:

Definition 1.06:

A permutation of a set of objects is an arrangement of those objects into a particular order.

In algebra and particularly in group theory, a permutation of a set S is defined as a bijection from S to itself (i.e., a map $S \to S$ for which every element of S occurs exactly once as image value).

And the group operation is the composition of permutations in G.

Note that the group of all permutation of a set is the symmetric group. The term permutation group is usually restricted to mean a subgroup of the symmetric group.

The number of permutations of n distinct objects is: $n \times (n-1) \times (n-2) \times \ldots \times 2 \times 1$, which number is called "n factorial", and written "$n!$".

For example, there are six permutations of the set {1,2,3}, namely (1 2 3), (1 3 2), (2 1 3), (2 3 1), (3 1 2), (3 2 1).

Notations:

There are three main notations for permutations of a finite set S.

1. In Cauchy's two-line notation:
   One lists the elements of S in the first row, and for each one its image under the permutation below it in the second row. For instance, a particular permutation of the set {1,2,3,4,5} can be written as:
   $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$
   This means that σ satisfies $\sigma(1) = 2, \sigma(2) = 5, \sigma(3) = 4, \sigma(4) = 3, \sigma(5) = 1$.
2. In one-line notation:

One gives only the second row of this array, so the one line notation of the permutation above is (2 5 4 3 1)

3. Cycle notation:
   The third method of notation focuses on the effect of successively applying of the permutation. It expresses the permutation as a product of cycle corresponding to the orbits (with at least two elements) of the permutation.
   There are in general many different cycle notations for the same permutation f. For example:
   $\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix} = (1\ 2\ 5)(3\ 4) = (3\ 4)(1\ 2\ 5) = (3\ 4)(5\ 1\ 2)$

Product and inverse:

The product of two permutations is defined as their composition as functions, in other words $\sigma \cdot \pi$ is the function that maps any element x of the set to $\sigma(\pi(x))$. Note that the rightmost permutation is applied to the argument first, because of the way function application is written.

For example:

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

The identity permutation, which maps every element of the set to itself, is the neutral element for this product.

In two-line notation the identity is:

$$\begin{pmatrix}1&2&3&\dots&n\\1&2&3&\dots&n\end{pmatrix}$$

Since bijections have inverses, so do permutations, and the inverse σ^{-1} of σ is again a permutation. Explicitly, whenever $\sigma(x) = y$ one also has $\sigma^{-1}(y) = x$. In two-line notation the inverse can be obtained by interchanging the two lines. For instance;

$$\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix}^{-1} = \begin{pmatrix}2&5&4&3&1\\1&2&3&4&5\end{pmatrix}$$

Quotient group:

In mathematics, specifically group theory, a quotient group (or factor group) is a group obtained by identifying together elements of a larger group using an equivalence relation.

In a quotient group, the equivalence class of the identity element is always a normal subgroup of the original group, and the other equivalence classes are the cosets of this normal subgroup.

The resulting quotient is writtenG / N, where G is the original group and N is the normal subgroup. (This is pronounced "G modulo N").

Definition 1.07:

Let N be a normal subgroup of a group G. We define the set G / N to be the set of all left cosets of N in G, i.e. $G / N = \{gN: g \ in \ G\}$ together with binary operation given by:

$$gN \cdot hN = ghN.$$

The group operation on G / N is the product of subsets of G. In other words, for each gN and hN, the product of gN and hN is $(gN)(hN)$. This operation is closed, because $(gN)(hN)$ really is a left coset. $(gN)(hN) = g(Nh)N = g(hN)N = (gh)(NN) = (gh)N$.

The normality of N is used in this equation. Because of the normality of N, the left cosets and right cosets of N in G are equal, and so G / N could be defined as a set of right cosets of N in G.

For Example: Consider the group with addition modulo 6.

$G = \{0,1,2,3,4,5\}$, let $N = \{0,3\}$

The quotient group is:

$$G / N = \{gN: g \in G\} = \{g\{0,3\}: g\epsilon\{0,1,2,3,4,5\}\}.$$

$$= \{0\{0,3\}, 1\{0,3\}, 2\{0,3\}, 3\{0,3\}, 4\{0,3\}, 5\{0,3\}\}.$$

$$= \{\{(0+0) mod\ 6, (0+3)\ mod\ 6\}, \{(1+0)mod\ 6, (1+3)\ mod\ 6\}, \{(2+0)mod\ 6, (2+3)\ mod\ 6\}, \{(3+0)mod\ 6, (3+3)\ mod\ 6\}, \{(4+0)mod\ 6, (4+3)\ mod\ 6\}, \{(5+0)mod\ 6, (5+3)\ mod\ 6\}\}$$

$$= \{\{0,3\}, \{1,4\}, \{2,5\}, \{3,0\}, \{4,1\}, \{5,2\},\} = \{\{0,3\}, \{1,4\}, \{2,5\}\}$$

Properties:

1. The quotient group G / G is isomorphic to the trivial group (the group with one element), and $G / \{e\}$ is isomorphic to G.
2. The order of G / N, by definition, the number of elements, is equal to $|G: N|$, the index of N in G. If G is finite, the index is also equal to the order of G divided by the order of N. Note that G / N may be finite, although both G and N are infinite (e.g. $Z / 2Z$).
3. Every quotient group of acyclic group is cyclic.
4. Every quotient group of abelian group is also abelian.

Examples:

1. Consider the group of integers Z (under addition) and the subgroup $2Z$ consisting of all even integers. This is a normal subgroup, because Z is abelian. There are only two cosets: the set of even integers and the set of odd integers; therefore, the quotient group $Z\ /\ 2Z$ is the cyclic group with two elements. This quotient group is isomorphic with the set $\{0,1\}$ with addition modulo 2; informally, it is sometimes said that $Z\ /\ 2Z$ equals the set $\{0,1\}$ with addition modulo 2.
2. A slight generalization of the last example. Once again consider the group of integers Z under addition. Let n be any positive integer. We will consider the subgroup nZ of Z consisiting all multiples of n. Once again nZ is normal in Z because Z is abelian. The cosets are the collection $\{nZ,\ 1+nZ,\ \ldots\ ,(n-2)+nZ,\ (n-1)+nZ\}$.
3. Consider the group of real numbers R under addition, and the subgroup Z of integers. The cosets of Z in R are all sets of the form $a+Z$, with $0 \leq a < 1$ a real number. Adding such cosets is done by adding the corresponding real numbers, and subtracting 1 if the result is greater than or equal to 1.

Abelian group:

In abstract algebra, an abelian group, also called a commutative group , is a group in which the result of applying the group operation to two group elements does not depend on their order (the axiom of commutativity).

Definition 1.08:

An abelian group is a set A together with an operation "$\cdot$" that combines any two elements a and b to form another element denoted $a \cdot b$. The symbol "$\cdot$" is a general placeholder for concretely given operation. To qualify as an abelian group, the set and operation $(A,\cdot)$ must satisfy five requirements known as the abelian group axioms: closure, associativity, identity element, inverse element, and finally commutativity: For all a, b in A, $a \cdot b = b \cdot a$.

More compactly, an abelian group is a commutative group. A group in which the group operation is not commutative is called a "non-abelian group" or "non-commutative group".

Notation:

There are two main notational conventions for abelian groups – additive and multiplicative.

Convention	Operation	Identity	Powers	Inverse
Addition	$x+y$	0	nx	$-x$
Multiplication	xy	e *or* 1	x^n	x^{-1}

Remark

Every cyclic group is an abelian group although not every abelian group is a cyclic group. For example the rational number under addition is not cyclic but is abelian.

Examples:

1. There are very familiar examples of groups under addition namely the integers Z, the rational numbers Q, the real numbers R and the complex numbers C.
2. $(Q^*,\cdot), (R^*,\cdot), (c^*,\cdot)$ where the star means "without 0".
3. The set Z_n of integers modulo n is abelian group under addition.
4. The set $Z_n{}^*$ of integers modulo n is abelian group under multiplication.

There are more examples in the next chapter.

Chapter 2

Direct Product and Direct Sum of Abelian Groups

Direct product of groups

In the mathematical field of group theory, the direct product is an operation that takes two groups G and H and constructs a new group. Usually denoted $G \times H$. This operation is the group-theoretic analogue of the Cartesian product of sets. And is one of several important notions of direct product in mathematics.

In the context of abelian groups, the direct product is sometimes referred to as the direct sum, and is denoted $G \oplus H$. Direct sums play an important role in the classification of abelian groups: according to fundamental theorem of finite abelian groups, every finite abelian group can be expressed as the direct sum of cyclic groups.

Definition 2.01:

Given groups G and H, the direct product $G \times H$ is defined as follows:

1. The elements of $G \times H$ are ordered pairs (g, h) where $g \in G$ and $h \in H$. That is, the set of elements of $G \times H$ is the Cartesian product of the sets G and H.
2. The binary operation on $G \times H$ is defined componentwise:
   $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$

The resulting algebraic object satisfies the axioms for a group specifically:

1. Associativity:
   The binary operation on $G \times H$ is indeed associative.
2. Identity element:
   The direct product has an identity element, namely $(1_G, 1_H)$, where 1_G is the identity element of G and 1_H is the identity element of H.
3. Inverse element:
   The inverse of an element (g, h) of $G \times H$ is the pair (g^{-1}, h^{-1}). Where g^{-1} is the inverse of g in G, and h^{-1} is the inverse of h in H.

Examples:

1 - Examples of product of abelian groups:

i. Let R be the group of real numbers under addition. Then the direct product $R \times R$ is the abelian group of all two-component vectors (x, y) under the operation of vector addition:

$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$

ii. $(Z_4, +)$

$Z_4 = \{0,1,2,3\}$ modulo 4.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

iii. Let G and H be cyclic groups with two elements each:

G

*	1	a
1	1	a
a	a	1

H

*	1	b
1	1	b
b	b	1

Then the direct product $G \times H$ is isomorphism to the Klein four-group.

*	(1,1)	(a,1)	(1,b)	(a,b)
(1,1)	(1,1)	(a,1)	(1,b)	(a,b)
(a,1)	(a,1)	(1,1)	(a,b)	(1,b)
(1,b)	(1,b)	(a,b)	(1,1)	(a,1)
(a,b)	(a,b)	(1,b)	(a,1)	(1,1)

We note $G \times H$ is abelian group.

iv. Klein four-group

In mathematics, the Klein four-group is the group $Z_2 \times Z_2$, the direct of two copies of the cyclic group of order 2.

The Klein four-group is the smallest none-cyclic group. It is abelian and isomorphic to the direct sum $Z_2 \oplus Z_2$, and not isomorphic to Z_4.

*	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

An elementary construction of the Klein four-group is the multiplication group {1,3,5,7} with the action being multiplication modulo 8. Here a is 3, b is 5, and ab is $3 \times 5 = 15 \equiv 7 \pmod 8$.

2- Examples of products of non-abelian groups:

i. Permutation group.

$S_n = \{1,2,3, \dots\}$, $\quad |S_n| = 1 \cdot 2 \cdot 3 \dots n = n!$

$S_3 = \{1,2,3\}$, $\quad |S_3| = 1 \cdot 2 \cdot 3 = 6$. It has 6 elements

$$\emptyset_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \emptyset_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \emptyset_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\emptyset_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \emptyset_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \emptyset_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$S_3 = G \cdot H$

$G = \{1\,2\,3, 2\,1\,3\} = \{\emptyset_0, \emptyset_4\}$.

$H = \{1\,2\,3, 2\,3\,1, 3\,1\,2\} = \{\emptyset_0, \emptyset_1, \emptyset_5\}$.

$G \times H \overset{\text{def}}{=} \{\alpha_0(\emptyset_0, \emptyset_0), \alpha_1(\emptyset_0, \emptyset_1), \alpha_2(\emptyset_0, \emptyset_5), \alpha_3(\emptyset_4, \emptyset_0), \alpha_4(\emptyset_4, \emptyset_1), \alpha_5(\emptyset_4, \emptyset_5)\}$.

$G \times H$

$\cdot$	α_0	α_1	α_2	α_3	α_4	α_5
α_0	α_0	α_1	α_2	α_3	α_4	α_5
α_1	α_1	α_2	α_0	α_4	α_5	α_3
α_2	α_2	α_0	α_1	α_5	α_3	α_4
α_3	α_3	α_4	α_5	α_0	α_1	α_2
α_4	α_4	α_5	α_3	α_1	α_2	α_0
α_5	α_5	α_3	α_4	α_2	α_0	α_1

We note $G \times H$ is abelian.

Because:

$$\alpha_2 \cdot \alpha_3 = (\emptyset_0, \emptyset_5) \cdot (\emptyset_4, \emptyset_0) \overset{\text{def}}{=} (\emptyset_0 \cdot \emptyset_4, \emptyset_5 \cdot \emptyset_0) = (\emptyset_4, \emptyset_5) = \alpha_5$$

$$\alpha_3 \cdot \alpha_2 = (\emptyset_4, \emptyset_0) \cdot (\emptyset_0, \emptyset_5) \overset{\text{def}}{=} (\emptyset_4 \cdot \emptyset_0, \emptyset_0 \cdot \emptyset_5) = (\emptyset_4, \emptyset_5) = \alpha_5$$

$$G \cdot H = \{\emptyset_0, \emptyset_4\} \cdot \{\emptyset_0, \emptyset_1, \emptyset_5\} = \{(\emptyset_0, \emptyset_0), (\emptyset_0, \emptyset_1), (\emptyset_0, \emptyset_5), (\emptyset_4, \emptyset_0), (\emptyset_4, \emptyset_1), (\emptyset_4, \emptyset_5)\} = \{\emptyset_0, \emptyset_1, \emptyset_5, \emptyset_4, \emptyset_2, \emptyset_3\}$$

$G \cdot H$

$\cdot$	$\emptyset_0$	$\emptyset_1$	$\emptyset_2$	$\emptyset_3$	$\emptyset_4$	$\emptyset_5$
$\emptyset_0$	$\emptyset_0$	$\emptyset_1$	$\emptyset_2$	$\emptyset_3$	$\emptyset_4$	$\emptyset_5$
$\emptyset_1$	$\emptyset_1$	$\emptyset_5$	$\emptyset_4$	$\emptyset_2$	$\emptyset_3$	$\emptyset_0$
$\emptyset_2$	$\emptyset_2$	$\emptyset_3$	$\emptyset_0$	$\emptyset_1$	$\emptyset_5$	$\emptyset_4$
$\emptyset_3$	$\emptyset_3$	$\emptyset_4$	$\emptyset_5$	$\emptyset_0$	$\emptyset_1$	$\emptyset_2$
$\emptyset_4$	$\emptyset_4$	$\emptyset_2$	$\emptyset_1$	$\emptyset_5$	$\emptyset_0$	$\emptyset_3$
$\emptyset_5$	$\emptyset_5$	$\emptyset_0$	$\emptyset_3$	$\emptyset_4$	$\emptyset_2$	$\emptyset_1$

We note $G \cdot H$ is non-abelian

So $S_3 = G \cdot H \neq G \times H$

ii. $GL(n, R)$ invertible $n \times n$ matrix:
$(det\ A \neq 0), n = 2.$

$$A = \begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix}, \qquad |A| = -1 - 6 = -7$$

$$B = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}, \qquad |B| = 6 - 5 = 1$$

$$A \cdot B = \begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} 2+10 & 1+6 \\ 6-5 & 3-3 \end{bmatrix} = \begin{bmatrix} 12 & 7 \\ 1 & 0 \end{bmatrix}$$

$$B \cdot A = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix} = \begin{bmatrix} 2+3 & 4-1 \\ 5+9 & 10-3 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 14 & 7 \end{bmatrix}$$

$A \cdot B \neq B \cdot A$

So, $(GL(2, R), \cdot)$ is non-abelian group.

Direct sum of abelian groups:

The direct sum of abelian groups is a prototypical example of a direct sum.

Given two abelian groups $(A, *)$ and $(B, \cdot)$ their direct sum $A \oplus B$ is the same as their direct product, i.e. its underlying set is the Cartesian product $A \times B$ with the group operation $\circ$ given componentwise:

$$(a_1, b_1) \circ (a_2, b_2) = (a_1 * a_2, b_1 \cdot b_2)$$

This definition generalizes to direct sums of finitely many abelian groups.

For an infinite family of abelian groups $A_i\ for\ i \in I$, the direct sum $\oplus_{i \in I} A$ is a proper subgroup of the direct product. It consists of the elements $(a_i) \in \prod_{i \in I} A_i$ such that a_i is the identity element of A_i for all but finitely many i.

In this case, the direct sum is indeed the coproduct in the category of abelian groups.

Definition 2.02:

An abelian group G is said to be the direct sum of its subgroups $G_1, \dots\dots\dots\dots, G_n$ if each $g \in G$ can be expressed uniquely in the form

$$g = g_1 + \dots\dots\dots + g_n$$

Where $g_i \in G_i, i = 1, \dots\dots\dots, n$. In this case, we write $G = G_1 \oplus \dots\dots\dots \oplus G_n$ or

$$G = \sum_{i=1}^{n} G_i.$$

If $G = G_1 \oplus \dots\dots\dots \oplus G_n$, then $G_i \cap G_j = \{0\}$ for $i \neq j$.

The following theorem provides a simple criterion for determining when a group is the direct sum of its subgroups.

Theorem 2.01:

Let $G_1, G_2, \dots\dots\dots, G_n$ be subgroups of a group G and suppose each element of G can be expressed as the sum of elements from the subgroups $G_1, G_2, \dots\dots\dots, G_n$.
Suppose also that an equation

$$0 = g_1 + \cdots\cdots + g_n$$

With $g_i \in G_n$ for $i = 1, \dots\dots, n$, holds only if $g_1 = g_2 = \cdots\cdots = g_n = 0$.
Then G is the direct sum of the subgroups $G_1, G_2, \dots\dots\dots, G_n$.

Proof:

If $g \in G$, then

$$g = g_1 + \cdots\cdots + g_n$$

With $g_i \in G_i, i = 1, 2, \dots\dots, n$. We need only show that this expression is unique. Suppose

$$g = g_1^* + \cdots\cdots + g_n^*$$

Is another such expression. Then

$$0 = (g_1 - g_1^*) + \cdots\cdots + (g_n - g_n^*)$$

By our hypothesis, $(g_1 - g_1^*) = (g_2 - g_2^*) = \cdots\cdots (g_n - g_n^*) = 0$.
Hence $g_i = g_i^*$ for $i = 1,2, \dots\dots\dots, n$ and the two expressions for g are identical.

We generalize our definition of direct sum to apply to the direct sum of an infinite number of subgroups.

Definition 2.03:

An abelian group G is said to be the direct sum of its subgroups $G_i, i \in I$, if for each

$g \in G, g \neq 0$. There is a unique expression for g of the form

$$g = g_1 + \cdots\cdots + g_k$$

Where $g_j \in G_J, J = 1, \ldots\ldots, k$ with $\acute{1}, \acute{2}, \ldots\ldots, \acute{k}$ distinct elements of I and no g_i is Zero.

We note that if $G = \sum_{i \in I} G_i$ and $i, j \in I, i \neq j$ then $G_i \cap G_j = \{0\}$.

Example:

Let $G = H \oplus K$ and $H = L \oplus M$. Prove that $G = L \oplus M \oplus K$.

Solution:

Every element g of G can be expressed in the form $g = h + k$ where $h \in H$ and $k \in K$. But $h = l + m$ where $l \in L$ and $m \in M$. Hence $g = l + m + k$. Now if $g = l_1 + m_1 + k_1$ with $l_1 \in L, m_1 \in M$ and $k_1 \in K$, put $l_1 + m_1 = h_1 \in H$. Then $g = h + k = h_1 + k_1$ and consequently $h = h_1$ and $k = k_1$. As $h = l + m = l_1 + m_1$, $l = l_1$ and $m = m_1$. Hence the result.

The difference between direct product and direct sum for infinite sum of groups

Direct product and direct sum are really the same thing. Direct product is used for multiplicative groups, and direct sum is used for additive (abelian) groups. Both of them assign a group structure on the Cartesian product of two groups, the difference is only whether the groups are written multiplicatively or additively.

Actually, to be specific, direct sums and direct products are not the same thing when an infinite number of groups are involved, as a direct sum of free abelian groups is always free abelian, while this is not true with direct products. In the infinite case, direct sums are sequences with only finitely many non-identity (zeroes) elements, while direct products have no such restriction.

Example: $Z^{\oplus \mathbb{N}} \subsetneq Z^{\mathbb{N}}$

Integers $Z = \{0, \pm 1, \pm 2, \pm 3, \ldots\ldots\}$.

Integers sequence: $a_1, a_2, a_3, \ldots\ldots, a_n, \ldots\ldots$ $(n \in \mathbb{N} = \{1, 2, 3, \ldots\ldots\}, a_n \in Z)$.

$Z^{\mathbb{N}} = \{f: \mathbb{N} \to Z\} = \{(a_1, a_2, a_3, \ldots)/a_n \in Z, n \in \mathbb{N}\}$.

$f: \mathbb{N} \longrightarrow Z$ function

$1 \longmapsto a_1$

$2 \longmapsto a_2$

$3 \longmapsto a_3$

$a = (a_1, a_2, a_3, \dots\dots)$

$b = (b_1, b_2, b_3, \dots\dots)$

$a + b = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \dots)$

$(Z^{\mathbb{N}}, +)$ Abelian group.

$\prod_{i\in\mathbb{N}} A_i$ *Choice functions*

$f \in \prod_{i\in\mathbb{N}} A_i$

$1 \longmapsto a_1 \in A_1$

$2 \longmapsto a_2 \in A_2$

$3 \longmapsto a_3 \in A_3$

$\mathbb{N} \longrightarrow \bigcup_{i\in\mathbb{N}} A_i\,, \qquad f(i) \in A_i$

Infinite direct product

$Z^{\mathbb{N}} = \prod_{i\in\mathbb{N}} Z_i\,, Z_i = Z$

$A_1 \times A_2 \times \cdots\cdots$

$Z \times Z \times Z \times \cdots\cdots$

Subset of finite support sequences

$(a_1, a_2, \dots\dots, a_n, 0, 0, \dots\dots) \in Z^{\mathbb{N}}$

$(1, 2, 3, 0, 0, 0, \dots\dots)$

$e_1 = (1,0,0, \dots)$

$e_2 = (0,1,0, \dots)$

$Z \oplus Z \oplus \dots\dots\dots\dots = \lambda_1 e + \lambda_2 e_2 + \dots\dots\dots\dots\dots\dots + \lambda_m e_m$ (any m but finite)

$= (\lambda_1, \lambda_2, \dots, \lambda_m, 0,0, \dots\dots\dots\dots)$

$A =$ Set of all sequences with only finitely many non-zeroes element.

So $A \subset Z^{\mathbb{N}}, A \neq Z^{\mathbb{N}}$

A is subgroup, $a, b \in A \Rightarrow a + b \in A$

$A = Z^{\oplus \mathbb{N}}$

This is a direct sum.

$Z^{\oplus \mathbb{N}} \subsetneq Z^{\mathbb{N}}$

$(1, 2, 3, 0, 0, \ldots\ldots) = (1, 0, 0, 0, \ldots\ldots) + (0, 2, 0, 0, \ldots\ldots) + (0, 0, 3, 0, \ldots\ldots)$

$$= 1 \cdot e_1 + 2 \cdot e_2 + 3 \cdot e_3$$

$e_n = (0, 0, 0, \ldots\ldots, 1, 0, \ldots\ldots)$ basic sequence.

$e_1, e_2, e_3, \ldots\ldots$ form a basis in $Z^{\oplus \mathbb{N}}$.

Chapter 3

The Torsion and the Basis of an Abelian Groups

The torsion of an abelian group

In abstract algebra, the term torsion refers to a number of concepts related to elements of finite order in groups.

Definition 3.01:

Let G be a group. An element g of G is called a torsion element if g has finite order.

The torsion of a group G is the set $T(G) = \{g \in G: g^n = e, n \in \mathbb{N}\}$ in the multiplication or $T(G) = \{g \in G: g \cdot n = 0, n \in \mathbb{N}\}$ in the addition.

An abelian group G is called a torsion (or periodic) group if every element of G has finite order, and is called torsion-free if every element of G except the identity has infinite order, i.e. $T(G) = \{e\}$.

An abelian group that is neither periodic nor torsion-free is called mixed group. $(\mathbb{Z}_2 \oplus \mathbb{Z})$ In this group, there are elements of order 2 and elements of infinite order.

The torsion subgroup $T(G)$ of an abelian group G is the subgroup of G constisting of all elements that have finite order.

Theorem 3.01:

The torsion subgroup $T(G)$ of an abelian group G is a subgroup of G.

Proof:

Since $0 \in T(G)$, $T(G)$ is not empty. If $a, b \in T(G)$, i.e. $m \cdot a = 0$ and $n \cdot b = 0$ for some positive integers m, n then $mn(a - b) = 0$ and so $a - b \in T(G)$, $T(G)$ is a subgroup.

Properties:

1. Every free abelian group is torsion-free, but the converse is not true, as is shown by the additive group of the rational number "Q". See the example page (32).

Theorem 3.02:

If A is free abelian group $\Rightarrow$ A is torsion free.

Proof:

Otherwise, A is not torsion free $\Rightarrow \exists a \in A, \exists n \in \mathbb{N}, na = 0, a \neq 0, n \neq 0$.

Contradiction, because $na = 0$.

Is non-trivial linear combination of 1 element (a).

$n_1a_1 + n_2a_2 + \cdots\cdots + n_ra_r = 0 \Longrightarrow n_1 = n_2 = \cdots\cdots n_r = 0.$

But we have $na = 0, a \neq 0, n \neq 0.$

So every free abelian group is torsion free.

2. Every finite abelian group is torsion group. Not every torsion group is finite.
   For example $(Q \cap [0,1))$
   $([0,1],\dot{+})$ is abelian group

   $\alpha = 0, \alpha_1\alpha_2 \cdots\cdots$

   $\beta = 0, \beta_1\beta_2 \cdots\cdots$

   $\alpha \dot{+} \beta = \begin{cases} \alpha + \beta & if \quad \alpha + \beta < 1 \\ \alpha + \beta - 1 & if \quad \alpha + \beta \geq 1 \end{cases}$

   $A = Q \cap [0,1)$ is a subgroup.

   A is infinite torsion group.

   $\frac{p}{q} \in A \subseteq [0,1), \qquad 0 \leq p < q$

   $q \cdot \frac{p}{q} = \frac{p}{q} \dot{+} \cdots\cdots \dot{+} \frac{p}{q} = 0 \ (\equiv p \ mod \ \mathbb{Z}).$

Theorem 3.03:

Every finite group is periodic $(Gfinite \ \rightarrow T(G) = G).$

Proof:

G is finite group.

$\forall x \in G, x \neq 0$

$\{x, 2x, 3x, \ldots, nx, \ldots\} \subseteq G$

$\{nx | n \in \mathbb{N}\} \subseteq G$

$\exists n, m \in \mathbb{N}, mx = nx, n < m$

$mx - nx = 0$

$(m-n)x = 0,\ m-n > 0$

x has a finite order (x is a torsion element).

Theorem 3.04:

If G is an abelian group and $T(G)$ is its torsion subgroup then the factor group $G/T(G)$is torsion-free.

Proof:

To show $G/T(G)$ is torsion-free, suppose $g + T(G)$ is a coset of finite order in $G/T(G)$. Then for some $n \in \mathbb{Z}^+, n\big(g + T(G)\big) = ng + T(G) = T(G)$. Thus $ng \in T(G)$ and so for some $m \in \mathbb{Z}^+, m(ng) = 0$. Hence g is of finite order, $g \in T(G)$ and so $g + T(G) = T(G)$ is the zero coset of $G/T(G)$.

Examples:

1. $(\mathbb{Z}_n, +)$ is torsion group

   $\mathbb{Z}_n = \{0,1,2, \dots, n-1\}$

   $\forall x \in \mathbb{Z}_n, n \cdot x = 0\ mod\ n, n \neq 0.$

   x has finite order

2. $(\mathbb{Q}, +)$ is torsion-free

   $\frac{p}{q} \in \mathbb{Q},\ \frac{p}{q} \neq 0$

   $n \cdot \frac{p}{q} = 0 \rightarrow \frac{np}{q} = 0 \rightarrow np = 0 \rightarrow n = 0,\ p \neq 0.$

   $\frac{p}{q}$ doesn't have finite order.

3. $(\mathbb{Z}, +)$ is torsion –free

   $1 \in \mathbb{Z},\ n \cdot 1 = n \neq 0$

   1 doesn't have finite order

4. $\mathbb{R}^*$ the group of non-zero real numbers under multiplication is a mixed group, its torsion subgroup is $\{\pm 1\}$.

   $x \in \mathbb{R}^*$

   x is torsion if $x^n = e$

   $\exists n: x^n = 1 \rightarrow\ x = 1\ or\ x = -1.$

   $\mathbb{R}^*$ is a mixed group and its torsion subgroup is $\{\pm 1\}$.

5. The torsion subgroup of $\mathbb{R}/\mathbb{Z}$ is $\mathbb{Q}/\mathbb{Z}$ $(T(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z})$

   $\exists n, n \in \mathbb{N}: n(\alpha + \mathbb{Z}) = 0$

   $n\alpha + \mathbb{Z} = 0$

   $n\alpha \in \mathbb{Z}$

   $\alpha \in \mathbb{Q}$

   Because: $n\alpha = p \in \mathbb{Z}$

   $$\alpha = \frac{p}{n} \in \mathbb{Q}.$$

The basis of an abelian group

Definition 3.02:

A basis X of an abelian group G over integers is a linearly independent subset of G that generates G.In more detail, suppose that $X = \{x_1, x_2, x_3, \dots, x_r\}$ is a finite subset of an abelian group G over integers. Then X is a basis if it satisfies the following conditions:

- The linear independence property
  For all $n_i \in \mathbb{Z}$ and $x_i \in X$, if $n_1x_1 + n_2x_2 + \cdots\cdots + n_rx_r = 0$, then necessarily $n_1 = n_2 = \cdots\cdots = n_r = 0$.
- The generating property
  Every non-zero element g in G can be expressed in the form $g = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ for $n_i \in \mathbb{Z}$ and distinct $x_i \in X$.

Definition 3.03:

An abelian group is free if it has a basis.

Examples:

1. $\mathbb{Z}^2$

   The set $S = \{e_1, e_2\}$ where $e_1 = (1,0)$, $e_2 = (0,1)$ is a generating set of $\mathbb{Z}^2$

   $(n_1, n_2) = n_1e_1 + n_2e_2$ it is also linearly independent.

   $n_1e_1 + n_2e_2 = 0$

   $\rightarrow n_1(1,0) + n_2(0,1) = (0,0)$

   $\rightarrow (n_1, 0) + (0, n_2) = (0,0)$

   $\rightarrow n_1 = 0 \ and \ n_2 = 0$

Therefore S is a basis for $\mathbb{Z}^2$. It is called the standard basis for $\mathbb{Z}^2$. These vectors also have a special name, (1, 0) is i and (0, 1) is j.

2. $\mathbb{Z}^3$
   Similarly, the standard basis for $\mathbb{Z}^3$ is the set $\{e_1, e_2, e_3\}$ where $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ and $e_3 = (0,0,1)$.
   These vectors also have a special name, they are i, j and k respectively.

3. The collection $\{i, i+j, 2j\}$ is not a basis for $\mathbb{R}^2$.

   $i = (1,0), j = (0,1), i+j = (1,1), 2j = (0,2)$

   $n_1 i + n_2 j = (n_1, n_2)$

   It is not generating $\mathbb{R}^2$ because $n_1, n_2 \in \mathbb{Z}$ so it doesn't generate all of $\mathbb{R}^2$.

   It is not linearly independent, no collection of 3 or more vectors from $\mathbb{R}^2$ can be independent.

4. The collection $\{i+j, j+k\}$ is not a basis for $\mathbb{R}^3$.

   $i + j = (1,1,0)$

   $j + k = (0,1,1)$

   $n_1(1,1,0) + n_2(0,1,1) = 0$

   $(n_1, n_1, 0) + (0, n_2, n_2) = (0,0,0)$

   $(n_1, n_1 + n_2, n_2) = (0,0,0)$

   $n_1 = 0, n_2 = 0$

   Although it is linearly independent, it doesn't generate all of $\mathbb{R}^3$.

Remark:

If G is an abelian group, and $X = \{x_1, x_2, \dots \dots, x_r\}$ is a basis of G, then we know that every element g of G can be expressed as a linear combination in X in unique way.

In other word, there exists unique coefficients $n_1, n_2, \dots, n_r$ such that

$$g = n_1 x_1 + n_2 x_2 + \cdots + n_r x_r$$

Theorem 3.05:

Let G denote an abelian group and $X(x_1, x_2, \dots, x_r)$ a basis of G. Every element in G can be written in a unique way as a linear combination in X.

Proof:

Since X is a basis, we know that it generates G. If $g \in G$, then there exists cofficients $n_1, n_2, \dots, n_r$ such that $g = n_1x_1 + n_2x_2 + n_rx_r$, suppose there is another way to write g. That is, there exists coefficients $c_1, c_2, \dots, c_r$ such that $g = c_1x_1 + c_2x_2 + \cdots + c_rx_r$. Then

$$n_1x_1 + n_2x_2 + n_rx_r = c_1x_1 + c_2x_2 + \cdots + c_rx_r$$

In other words, $(n_1 - c_1)x_1 + (n_2 - c_2)x_2 + \cdots\cdots + (n_r - c_r)x_r = 0$. Since X is a basis, it must be linearly independent. The unique solution to $(n_1 - c_1)x_1 + (n_2 - c_2)x_2 + \cdots\cdots + (n_r - c_r)x_r = 0$ must be the trivial solution.

It follows that $n_i - c_i = 0$ for $i = 1, 2, \dots, n$ in other words $n_i = c_i$ for $i = 1, 2, \dots\dots, n$. Therefore, the two representations of g are the same.

Definition 3.04:

Every free abelian group F has many different bases, but all basses have the same cardinality (number of elements) and this number is called the rank of F, denoted $rk(F)$.

Properties:

1. Free abelian groups of rank 0 are exactly the periodic abelian groups.
2. The zero group is regarded as a free abelian group of rank 0.
3. Every subgroup H of a free abelian group F of rank r is a free abelian group of rank $\leq r$. (See the theorem 4.03).

   Ex:

   Let $F = \mathbb{Z}$ and $H = 2\mathbb{Z}$. Then $H \leq F$ as a proper subgroup with $rk(F) = rk(H) = 1$.

Examples:

1. $\mathbb{Z}$

   The group of integers is a free abelian group of rank 1 finitely generated by 1 or -1.

2. $\mathbb{Z}^2$

   The set of all ordered pairs (x, y) where x and y are in $\mathbb{Z}$. We have already seen that the standard basis for $\mathbb{Z}^2$ was $\{(1, 0), (0, 1)\}$.this basis has 2 elements, therefore $rk(\mathbb{Z}^2) = 2$.

3. $\mathbb{Z}^3$

   The set of all ordered triples (x, y, z) where x, y and z in $\mathbb{Z}$. Similarly, the standard basis for $\mathbb{Z}^3$ is $\{(1, 0,0), (0, 1,0), (0,0,1)\}$. This basis has 3 elements, therefore $rk(\mathbb{Z}^3) = 3$.

4. $\mathbb{Z}^n$

   The set of all ordered n-tuples $(x_1, x_2, \dots, x_n)$ where $x_1, x_2, \dots\dots, x_n$ are in $\mathbb{Z}$. Similarly, the standard basis for $\mathbb{Z}^n$ is $\{(1, 0,0, \dots,0), (0, 1,0, \dots,0), \dots, (0,0,0, \dots,0,1)\}$.

This basis has n elements, therefore $rk(\mathbb{Z}^n) = n$.

So, the free abelian group of rank n for a natural number n is isomorphic to the group $\mathbb{Z}^n$, which is a direct product of n copies of the group of integers.

Theorem 3.06:

Groups Z^2 and Z^3 are non-isomorphic. More generally, if n and m are different positive integers, then Z^n and Z^m are non-isomorphic.

Proof:

Let $A, \grave{A}$ are free abelian groups.

$A = \langle B \rangle,\ B = \{b_1, b_2, \dots\dots, b_n\},\ n = cardB(n = rankA).$

$\grave{A} = \langle \grave{B} \rangle,\ \grave{B} = \{b_1, b_2, \dots\dots, b_m\},\ m = cardB\big(m = \grave{rank}\grave{A}\big).$

If $n = m \longrightarrow A \cong \grave{A}$

$rankA = rank\grave{A} \Leftrightarrow A \cong \grave{A}$

$Z^2 = \langle a, b \rangle, \qquad a = (1,0), b = (0,1), \qquad rankZ^2 = 2.$

$Z^3 = \langle a, b, c \rangle, \qquad a = (1,0,0), b = (0,1,0), c = (0,0,1), \qquad rankZ^3 = 3.$

$Z^2 \cong Z^3 \longrightarrow rankZ^2 = rankZ^3, i.e. 2 = 3$

And this is not true, so $Z^2 and\ Z^3$ are non-isomorphic.

Chapter 4

Free Abelian Groups

In abstract algebra, 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 way as a finite linear combination of elements of the basis, with integer coefficients.

And as well as we pointed out earlier that every abelian group is free if it has a basis and every free abelian group is torsion-free, but the converse is not true. And this is evident through the following example:

Example: $(\mathbb{Q}, +)$

The rational numbers with addition is not free abelian group because it does not have a basis although it is torsion-free.

Let $\alpha, \beta \in \mathbb{Q}$

$\alpha = \frac{p}{q}, \beta = \frac{p'}{q'}$

$$p'q\alpha + (-pq')\beta = p'q\frac{p}{q} + (-pq')\frac{p'}{q'}$$

$$= p'p - pp'$$

$$= 0$$

α, β are not independent.

So any two elements in $\mathbb{Q}$ are dependent over $\mathbb{Z}$.

Also $\{\alpha_1, \dots, \alpha_k\}$is not generating (generating set is not finite).

$\alpha_i = \frac{p_i}{q_i}, p_i, q_i \in \mathbb{Z}, \alpha_i \in \mathbb{Q}$

$\alpha = n_1\frac{p_1}{q_1} + \cdots + n_k\frac{p_k}{q_k}$ (there is no such denominator).

Let $< \frac{1}{2}, \frac{1}{3} >= \{n_1\frac{1}{2} + m\frac{1}{3}\}$

therefore $\frac{1}{5}, \frac{1}{7} \notin \{n_1\frac{1}{2} + n_2\frac{1}{3}\}$

So $\mathbb{Q}$ is not free abelian group.

The homomorphic property of free abelian groups

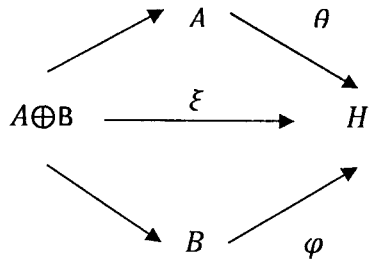
If F is a free abelian group with basis X, then we have the following universal property: For every arbitrary function F from X to some abelian group A, there exists a unique group homomorphism from F to A which extends F. This universal property can also be used to define free abelian group.

Let $G = A \oplus B$ and let H be a group which contains isomorphic copies $\bar{A}$ and $\bar{B}$ of A and B respectively. Suppose that $H = \bar{A} + \bar{B}$ (but not necessarily that $H = \bar{A} \oplus \bar{B}$). What connection, if any, is there between G and H?.

It turns out that H is homomorphic image of G. This follows from next theorem. This theorem when applies to particular cases leads also to important result which is the concept of a free abelian group.

Theorem 4.01:

Let $G = A \oplus B$ and let H be any group. Let $\theta, \emptyset$ be homomorphisms of A into H and B into H respectively. Then there exists a homomorphism $\xi: G \to H$ such that $\xi_A = \theta, \xi_B = \emptyset$.



Proof:

If g ∈ G, then $g = a + b$ uniquely where $a \in A, b \in B$. Define $g\xi = a\Theta + b\emptyset$. ξ is uniquely defined and so is a mapping of G to H.

Note that if $g_i = a_i + b_i$ where $a_i \in A$ and $b_i \in B$ $(i = 1,2)$, then

$$(g_1 + g_2)\xi = ((a_1 + b_1) + (a_2 + b_2))\xi = ((a_1 + a_2) + (b_1 + b_2))\xi$$

$$= (a_1 + a_2)\Theta + (b_1 + b_2)\,\emptyset = a_1\Theta + a_2\Theta + b_1\emptyset + b_2\emptyset$$

$$= a_1\Theta + b_1\emptyset + a_2\Theta + b_2\emptyset = (a_1 + b_1)\xi + (a_2 + b_2)\xi$$

$$= g_1\xi + g_2\xi$$

Hence ξ is the required homomorphism as $\xi_A = \Theta, \xi_B = \emptyset$.

In exactly the same way we can prove that if $G = \sum_{i\in I} G_i$ and if for each $i \in I, \Theta_i: G_i \to H$ is a homomorphism of G_i to H, then there exists a homomorphism $\Theta: G \to H$ such that $\Theta_{G_i} = \Theta_i$. We shall often say that Θ extends the mappings Θ_i or that Θ is an extension of the mapping Θ_i.

Corollary:

The direct sum $G = \sum_{i\in I} G_i$ satisfies the following condition: for every mapping $\Theta: X \to H, H$ any abelian group, there exists a homomorphism $\Theta^*: G \to H$ sush that $\Theta_x^* = \Theta$.

A group G which contains a subset X such that

$(i) G = gp(X)$.

(ii) For every mapping $\Theta: X \to H, H$ any abelian group, there exists a homomorphism $\Theta^*: G \to H$ sush that $\Theta_x^* = \Theta$,

is called a free abelian group. G is said to be freely generated by X and X is called a basis for G.

We have shown that the direct sum of infinite cyclic groups is a free abelian group.

Conversely we have the following.

Theorem 4.02:

If G is a free abelian group freely generated by a set $X = \{x_i | i \in I\}$, then G is the direct sum of its subgroups $G_i = gp(x_i)$ and each G_i is infinite cyclic for all $i \in I$.

Proof:

This theorem is proved by showing that G is isomorphic to a direct sum of infinite cyclic groups. To this end let H be the direct sum of its subgroups H_i,

$$H = \sum_{i\in I} H_i$$

where $H_i = gp(h_i)$ is an infinite cyclic group generated by h_i (we know a direct sum exists).

Let $\Theta: X \to H$ be the mapping defined by $x_i\Theta = h_i$. Then Θ can be extended to a homomorphism Θ^* of G into H, by the definition of a free abelian group.

On the other hand H is the direct sum of the infinite cyclic groups H_i. Thus by the last corollary, the mapping $\emptyset: \{h_i | i \in I\} \to X$ defined by $h_i\emptyset = x_i$ can be extended to a homomorphism $\emptyset^*$ of H into G. Actually $\emptyset^*$ and Θ^* are inverse isomorphisms. To see this, suppose $g \in G$. Then $g = n_1x_{1'} + \cdots + n_rx_{r'}$ where $1', \ldots, r' \in I$ and $n_1, \ldots \ldots, n_r \in Z$. Accordingly,

$$(g\Theta^*)\emptyset^* = [n_1(x_{1'}\Theta^*) + \cdots + n_r(x_{r'}\Theta^*)]\emptyset^* = (n_1h_{1'} + \cdots + n_rh_{r'})\emptyset^*$$

$$= n_1(h_{1'}\emptyset) + \cdots + n_r(h_{r'}\emptyset) = n_1x_{1'} + \cdots + n_rx_{r'}$$

$$= g$$

and so $\Theta^*\emptyset^*$ is the identity mapping on G. Similarly $\Theta^*\emptyset^*$ is the identity mapping on H.

This implies that Θ^* is a one-to-one mapping of G onto H. For if $g, g' \in G$, then $g\Theta^* = g'\Theta^*$ implies that $(g\Theta^*)\emptyset^* = (g'\Theta^*)\emptyset^*$. Since $(g\Theta^*)\emptyset^* = g$ and $(g'\Theta^*)\emptyset^* = g'$, we have $g = g'$.

Further more if $h \in H$, then $h = (h\emptyset^*)\Theta^*$. Thus Θ^* is one-to-one and onto.

Note that each G_i is infinite cyclic, since Θ^* is an isomorphism and $G_i\Theta^* = H_i$. Finally we show that G is the direct sum of its subgroups G_i. If $1', \ldots, r'$ are distinct elements of I and $g_1, \ldots, g_r$ are nonzero elements of $G_{1'}, \ldots, G_{r'}$ respectively, then if

$$g_1 + \cdots + g_r = 0$$

it follows that $g_1\Theta^* + \cdots + g_r\Theta^* = 0$. But then, as $g_i\Theta^* \in H_i$ and $g_i\Theta^* \neq 0$, we have a contradiction as $H = \sum_{i\in I} H_i$. Finally $gp(G_i | i \in I) = G$, and so $G = \sum_{i\in I} G_i$.

Corollary:

Every abelian group is the homomorphic image of some free abelian group.

Proof:

If G is an arbitrary group whose elements are $g_i, i \in I$ and $gp(x_i), i \in I$ is infinite cyclic, then as we have seen, $F = \sum_{i\in I} gp(x_i)$ is free abelian and the mapping $\Theta: x_i \to g_i$ extends to a homomorphism of F onto G.

So a free abelian group is a direct sum of infinite cyclic groups. If these cyclic groups are generated by elements $x_i (i \in I)$, then the free abelian group F will be

$$F = \oplus_{i\in I} < x_i >$$

Thus, F consists of all finite linear combinations

$$g = n_1x_1 + n_2x_2 + \cdots + n_rx_r$$

with different $x_1, \ldots, x_r$ where n_i are integers $\neq 0$.

Example:

Let G be the group that is the direct sum $\mathbb{Z} \oplus \mathbb{Z}$ of two copies of the infinite cyclic group $\mathbb{Z}$. Symbolically, $G = \{(a, b) | a, b \in \mathbb{Z}\} = \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$.

One basis for this group is $\{(1,0), (0,1)\}$. If we say $e_1 = (1,0)$ and $e_2 = (0,1)$, then we can write the element $(4, 3)$ as

$(4,3) = 4e_1 + 3e_2$. Where "multiplication" is defined in following way: $4e_1 = e_1 + e_1 + e_1 + e_1$.

Remark:

Note that a free abelian group is not a free group except in two cases: a free abelian group having an empty basis (rank0, giving the trivial group) or having just 1 element in the basis (rank1, giving the infinite cyclic group).

Other abelian groups are not free groups because in free groups ab must be different from ba if a and b are different elements of the basis, while in free abelian groups they must be identical.

The subgroup of free abelian group

If F is free abelian group, every subgroup H of F is free abelian group.

Theorem 4.03:

Let G be free abelian group of rank n. Then any subgroup H of G is free abelian group of rank less than or equal to n.

We will prove this theorem by using a lemma about subgroups of free abelian groups.

Lemma:

Let G be free abelian group, the direct sum of n cyclic groups. Let H be a subgroup of G. Then there exists a basis $c_1, \dots, c_n$ of G and integers $u_1, \dots, u_n$ such that $H = gp(u_1c_1, u_2c_2, \dots, u_nc_n)$.

Proof:

We use a, b, c to denote basis elements of G, h, k, l to denote elements of H, q, r, s, t, u, v to denote integers. We prove the result by induction on n. For $n = 1$, G is cyclic.

Assume the result is true for free abelian groups of rank less than n where $n > 1$. Let G be free abelian of rank n. We assume also that $H \neq \{0\}$. For if $H = \{0\}$, we may take an arbitraty basis $c_1, \dots, c_n$ for G. Then $H = gp(u_1c_1, \dots, u_nc_n)$ where $u_1 = \cdots = u_n = 0$.

To every basis we associate an integer, called its size (with respect to H). Let $\{a_1, \dots, a_n\}$ be a basis for G and let q be the smallest nonnegative integer such that there exists $h \in H$ with

$$h = qa_1 + q_2a_2 + \cdots + q_na_n, \quad q_2, \dots, q_n \text{ integers} \qquad (1)$$

Then q is termed the size of the basis $\{a_1, \dots, a_n\}$.

Assume $\{a_1, \dots, a_n\}$ is a basis of smallest size, i.e. if $\{b_1, \dots, b_n\}$. is a basis of G, then the size of $\{b_1, \dots, b_n\}$ is not less than q.

Let h be as in equation (1).

We show that q divides $q_2, \dots, q_n$. From the division algorithm, if q_i is not divisible by $q, q_i = r_i q + s_i$ where $0 < s_i < q$. Hence

$$h = q(a_1 + r_i a_i) + \cdots + s_i a_i + \cdots + q_n a_n$$

But if we put $b_1 = a_i, b_2 = a_2, \dots, b_i = a_1 + r_i a_i, \dots, b_n = a_n$, we obtain a basis. Furthermore this basis is of smaller size than the size of $\{a_1, \dots, a_n\}$, contrary to our assumption. Thus $s_i = 0$ and q divides q_i for $i = 2, \dots, n$. Let $q_i = r_i q$, then

$$h = q(a_1 + r_2 a_2 + \cdots + r_n a_n)$$

Let $c_1 = a_1 + r_2 a_2 + \cdots + r_n a_n$. Then $\{c_1, a_2, \dots, a_n\}$ is a basis for G. Also

$$h = q c_1 \tag{2}$$

If $k = t_1 a_1 + \cdots + t_n a_n \in H$, it follows that t_1 is divisible by q. For if $t_1 = uq + v$ with $0 \leq v < q$, then $\mathrm{I} = k - uh \in H$ has v as its coefficient of a_1. As $v < q$, by the minimality of $q, v = 0$. Therefore

$$\mathrm{I} = k - uh \in gp(a_2, \dots, a_n)$$

Hence $\mathrm{I} \in gp(a_2, \dots, a_n) \cap H = L$, say. From this we conclude that if $k \in H$, then

$$k = uh + \mathrm{I} \tag{3}$$

where $\mathrm{I} \in L$.

By the inductive hypothesis there exist a basis $c_2, \dots, c_n$ and integers $u_2, \dots, u_n$ such that L is generated by $u_2 c_2, \dots, u_n c_n$. Hence by (3) every element of H belongs to $gp(h, u_2 c_2, \dots, u_n c_n)$. On other hand, H contains $h, u_2 c_2, \dots, u_n c_n$. Thus

$$H = gp(h, u_2 c_2, \dots, u_n c_n)$$

Put $u_1 = q$. By (2)

$$H = gp(u_1 c_1, u_2 c_2, \dots, u_n c_n)$$

Also, $c_1, \dots, c_n$ a basis for G. Hence the result follows.

Proof:

By lemma above, there exists a basis $c_1, \dots, c_n$ of G and integers $u_1, \dots, u_n$ such that $H = gp(u_1 c_1, u_2 c_2, \dots, u_n c_n)$. If $u_1, \dots, u_i$ are nonzero, and $u_{i+1} = u_{i+2} = \cdots = u_n = 0$, then $gp(u_1 c_1, u_2 c_2, \dots, u_n c_n) = gp(u_1 c_1) \oplus \dots \oplus gp(u_i c_i)$.

Example:

Let $G = A \oplus B$ and let C, D be subgroups of A, B respectively, show that $C + D = C \oplus D$.

(This can obviously be generalized to the direct sum of any number of groups)

Solution:

As $\{0\} = A \cap B \supseteq C \cap D$, we have $C \cap D = \{0\}$.

Thus $C + D = C \oplus D$.

Theorem 4.04:

There are countably many countable non-isomorphic free abelian groups. They are exactly: $Z, Z^2, Z^3, \ldots\ldots\ldots, Z_\infty$.

Proof:

Every countable free abelian group A is isomorphic to some of these groups:

1. A is countable.
2. A is free.

$A = \langle S \rangle$, S is a set of free generated, $S \subseteq A, S$ must be at least countable.

- If $|S| = n, n \in N$, the rank $A = n$, so $A \cong Z^n$.
- $|S| = \aleph_0$, i.e. $S = \{s_1, s_2, \ldots\ldots\}$, rank $A = \aleph_0$.

$x \in A, x = \alpha_1 s_1 + \cdots\cdots + \alpha_n s_n$, for $s_i \in S, \alpha_i \in Z$.

So there are as many elements in A as there are finite linear combination.

Theorem 4.05:

Every two uncountable free abelian groups of the same cardinality are isomorphic.

Proof:

Suppose: Z^A, Z^B are free abelian groups.

$Z^A = \langle A \rangle, \qquad Z^B = \langle B \rangle$

If $|Z^A| = |Z^B|$, then $Z^A \cong Z^B$.

We will prove if Z^A and Z^B are uncountable free abelian groups of the same cardinality, then $|A| = |B|$.

If Z^A is uncountable free abelian group then $|Z^A| = |A|$.

$Z^A = \langle A \rangle, \qquad A = \{a_i \ / \ i \in I\}$

$x \in Z^A, \qquad x = \alpha_1 a_1 + \cdots\cdots \alpha_n a_n, \qquad \alpha_1, \ldots\ldots, \alpha_n \in Z, \qquad a_1, \ldots\ldots, a_n \in A$

So there are elements in Z^A as there are finite sequence $(\alpha_1, \ldots\ldots, \alpha_n, a_1, \ldots\ldots, a_n)$, $\alpha_1, \ldots\ldots, \alpha_n \in Z, \ a_1, \ldots\ldots, a_n \in A$

$A = \{a_1, a_2, \ldots\ldots\}, \qquad |A| = k$

$Z_\infty = Z \cup Z^2 \cup Z^3 \cup \cdots\cdots$

$A_\infty = A \cup A^2 \cup A^3 \cup \cdots\cdots$

$Z^A = Z \times A \cup Z^2 \times A^2 \cup Z^3 \times A^3 \cup \cdots\cdots$

$|Z^A| = |Z \times A| + |Z^2 \times A^2| + |Z^3 \times A^3| + \cdots\cdots$

$= |Z| \cdot |A| + |Z|^2 \cdot |A|^2 + |Z|^3 \cdot |A|^3 + \cdots\cdots$

$= \aleph_0 \cdot k + {\aleph_0}^2 k^2 + {\aleph_0}^3 \cdot k^3 + \cdots\cdots$

$= \aleph_0 \cdot k + \aleph_0 \cdot k + \aleph_0 \cdot k \cdots\cdots$

$= \aleph_0 (k + k + \cdots\cdots\cdots)$

$= \aleph_0 \cdot k$

$= k$

$|Z^A| = |A| = k$

So $|A| = |Z^A| = |Z^B| = |B|$, i.e. $|A| = |B|$

i.e. $rank Z^A = rank Z^B$ hence $Z^A \cong Z^B$.

Theorem 4.06:

If some abelian identity $u = v$ holds on the group Z, then $u = v$ is true in every abelian group.

Proof:

$u = v$ is true in Z.

$u(x_1, x_2, \ldots\ldots, x_n) = v(x_1, x_2, \ldots\ldots, x_n)$

$a_1, a_2, \ldots\ldots, a_n \in A$

$u(a_1, a_2, \ldots\ldots, a_n) \equiv v(a_1, a_2, \ldots\ldots, a_n)$

If A, B such that $A \vDash u = v$ and $B \vDash u = v$ then $A \times B \vDash u = v$

And if $A \vDash u = v$ then $A^2 \vDash u = v, A^3 \vDash u = v, \ldots\ldots$

Suppose $u = v$ holds in Z

$Z \vDash u = v, \quad Z$

$Z^2 \vDash u = v, \quad Z + Z$

$Z^3 \vDash u = v, \quad Z + Z + Z$

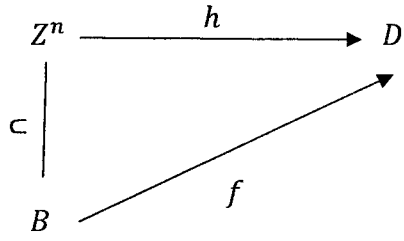
$\vdots \quad \vdots \quad \vdots \quad \vdots \qquad \vdots$

We proved $u = v$ holds in all free abelian group of finite many.

Now let D be an abelian group, $d_1, d_2, \dots\dots, d_n \in D$, then $u^D(d_1, \dots\dots, d_n) \equiv v^D(d_1, \dots\dots, d_n)$.

Let us choose $Z^n = Z + Z + \cdots\cdots + Z, rank Z^n = n$.

$B = \{b_1, b_2, \dots\dots, b_n\}$.



$f = \begin{pmatrix} b_1, \dots\dots, b_n \\ d_1, \dots\dots, d_n \end{pmatrix}$

There is $h: Z^n \longrightarrow D$

$h(b_i) = d_i$

$$u^D(d_1, \dots\dots, d_n) = u^D(hb_1, \dots\dots, hb_n)$$
$$= h\left(u^{Z_n}(b_1, \dots\dots, b_n)\right)$$
$$= h\left(v^{Z_n}(b_1, \dots\dots, b_n)\right)$$
$$= v^D(hb_1, \dots\dots, hb_n)$$
$$= v^D(d_1, \dots\dots, d_n).$$

References

[1] Tony Gaglione, An introduction to group theory, Mathematics, Department, U.S, 1992.[2] László Fuchs, Infinite Abelian Groups, New York and London, Academic Press, volume I, 1970.

[3] Benjamin Baumslag, Ph.D. Bruce Chandler, Ph.D., Schaum's Outline Of Theory And Problems Of Group Theory, Department of Mathematics, New York University, 1968.

[4] http://dogschool.tripod.com/

[5] http://en.wikipedia.org/wiki/Quotient_group

[6] http://en.wikipedia.org/wiki/Abelian_group

[7] http://en.wikipedia.org/wiki/Direct_product_of_groups

[8] http://en.wikipedia.org/wiki/Direct_sum

[9] http://answers.yahoo.com/question/index?qid=20080819115233AAfMI98

[10] http://web.science.mq.edu.au/~chris/groups/chap12.pdf

[11] http://en.wikipedia.org/wiki/Basis_(linear_algebra)

[12] http://en.wikipedia.org/wiki/Free_abelian_group