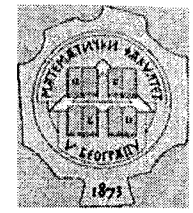

Mathematical Faculty

University of Belgrade

Dalal Ramadan Saad Matoug

Finitely Generated Abelian Groups

Master thesis

Supervisor:

Prof. Aleksandar Lipkovski, PhD.

Belgrade, 2012.

УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ
ИНВ. БР. 243
БИБЛИОТЕКА

Introduction

In this work about finitely generated abelian groups , before to get define of finitely generated abelian groups , we must explain some definitions about group , generating set of group and abelian group with some theorems . We will use an additive notation for all abelian groups , meaning that the group operation is denoted by $+$.

We first study in chapter one some theorems related to finitely generated abelian groups , the group G under additive operation $+$ is abelian group if for all a and b belong to G then $a + b = b + a$

In the other chapters we will study what does finitely generated mean as well as subgroup of finitely generated abelian groups . Finally , we will present for some important theorems ' Fundamental theorem of finitely generated abelian groups ' , the type of finitely generated abelian groups and applications with some examples .

Contents

CHAPTER

1

Group and Torsion Group

(1-1) Definition:-

A group is an nonempty set G together with a binary operation

$(a,b) \to a * b \; ; G \times G \to G$ satisfying the following :

1- Associativity $\forall a,b,c \in G \quad (a*b)*c = a*(b*c)$
2- Identity $\forall a \in G \, , \exists e \in G \quad a*e = e = e*a$
3- Inverse $\forall a \in G \, , \exists a' \in G \quad a*a' = e = a'*a$

then $(G,*)$ is a group

and $(G,*)$ is an abelian group (commutative group) if $\forall a,b \in G$

$$a*b = b*a$$

(1-2) Examples :-

1- $(\mathrm{R},+),(\mathrm{Z},+),(\{1,-1\},\cdot)$ are groups (all abelian groups)

2- Symetric groups $S_n \; , n \in N$ group of permutations

$N = \{1,2,\dots,n\}$ basis set and functions is bijection

$$f: N \longrightarrow N$$

$$g: N \to N$$

$(f \circ g)(n) = f\big(g(n)\big)$

$(S_n \, , \circ)$ is a group but non abelian group .

For example: $|S_3| = 3! = 3 \times 2 \times 1$

$$213.132 = 312$$

$$132.213 = 231$$

$$(213).(132) \neq (132).(213)$$

(1-3) Definition :-

If S is a subset of a group G , then $< S >$ the subgroup generated by S , is the smallest subgroup of G containing every element of S . If $G =< S >$ then we say S generates G , and the elements in S are called group generators . If S is the empty set , then $< S >$ is the trivial group $\{e\}$, and if there is only a single elements a in S, in this case , $<a>$ is the cyclic subgroup of power of a .

(1-4) Examples :-

1- $Z =< 1 >$ (generated by $\{1 \, , 1 -\}$) .
2- $nZ =< n >$, $2Z =< 2 >$.

3- $Z/_{nZ} \cong Z_n = \{0,1,\dots,n-1\}$ and generated by 1 .

(1-5) Definition:-

G is cyclic group if it can be generated by single element .

Classification of cyclic group

(1-6) Theorem :-

Every cyclic group $(G,+)$ is isomorphic either to the additive Z or to additive group Z_n for some positive integer n .

proof

Let g generate G and so $G =< g >$. Consider $\theta: Z \to G$ defined $\theta(m) = mg$ for all integer m . Then θ is Z-linear .

Now θ is surjective (onto) since every element of G is of the form $\theta(m)$ for some $m \in Z$, that is $im\,\theta = G$ meaning that G is the image of θ , the kernel of θ is

$$ker\theta = \{m \in Z\ ;\ \theta(m) = 0\} = \{m \in Z\ ; mg = 0\} = k$$

which is the order ideal of g .

There is a non negative integer n (n is smallest positive number in $ker\theta$) with

$\ker\theta =< n >$.

Suppose $n = 0$. Then is injective (one to one) because $\theta(m) = \theta(m')$, then

$\theta(m - m') = \theta(m) - \theta(m') = 0$ showing that $m - m'$ belong to $ker\theta =< 0 > = \{0\}$. So $m - m' = 0$ that's $m = m'$. Therefore is bijective and $\theta = Z \cong G$, that is , all infinite cyclic groups are isomorphic to additive group Z of integers .

Suppose $n > 0$. As above we suppose $\theta(m) = \theta(m')$. This mean $m - m' \in ker\theta = k =< n >$ and so $m - m'$ is an integer multiple of n , that is , $m \equiv m'(mode\ n)$.

The steps can be reversed to show that $m \equiv m'(mode\ n)$ implies $\theta(m) = \theta(m')$. So θ has the same effect on integers m and m' which are congruent $(mode\ n)$. In other word θ has in the same effect on all integers of each congruence class $\overline{m}$, and makes sense to introduce the mapping $\tilde{\theta}: Z_n \to G$ define by $\tilde{\theta}(\overline{m}) = \theta(m)$ for all $m \in Z$. As θ is additive and surjective , the same is true of $\tilde{\theta}$. As θ has different effect on different congrucne classes $(mode\ n)$, we see that $\tilde{\theta}$ is an injective . Therefore $\tilde{\theta}: Z_n \cong G$ which shows every cyclic group of finite order n is isomorphic to the additive group Z_n .

(1-7) Definition :-

Let $(G,+)$ be an abelian group and let $S = \{g_1, g_2, \dots, g_r\}$ be a finite, nonempty subset of G . If , for any integers $a_1, \dots, a_r$, the relation

$$a_1 g_1 + \cdots + a_r g_r = 0$$

Implies that $g_1 = g_2 = \cdots = g_r = 0$, then S is said to be independent . If S is independent and generates G , and if $1 \notin S$, then S is called a basis of G .

(1-8) Definition:-

Free abelian group is an abelian group with a basis . That is , every element of G can be written uniquely as a finite linear combination of elements of the basis , with integer coeffecients .

(1-9) Definition:-

A finite set $I = \{a_1, \dots, a_n\} \subset A$ abelian group is a set of independent element (or $a_1, \dots, a_n$ are independent) if for $k_1, \dots, k_n \in Z$

$k_1 a_1 + \cdots + k_n a_n = 0 \implies k_1 = \cdots = k_n = 0$

(1-10) Examples:-

1- $a_1 = (1,0)$, $a_2 = (0,1)$ are independent .

Because $k_1 a_1 + k_2 a_2 = (k_1, 0) + (0, k_2) = (0,0)$

$(k_1, k_2) = (0,0) \implies k_1 = k_2 = 0$

2- $a_1 = (1,0)$, $a_2 = (2,0)$ are dependent .

Because $k_1 a_1 + k_2 a_2 = (k_1, 0) + (2k_2, 0) = (0,0)$

$$\Rightarrow k_1 + 2k_2 = 0$$

(1-11) Torsion element :-

Let $(A , +)$ an abelian group . An element $a \in A$ is said to be a torsion element if it has Finite period n , that's mean $na = 0$.

(1-12) Torsion subgroup :-

Let G is an abelian group . Then the torsion subgroup of G is

$G_T = \{ g \in G , ng = 0 \quad for\ some\ n \in Z \}$.

(1-13) Lemma :-

Let G be an abelian group . The subset of G_T is subgroup of G .

Proof

Let G_T be the torsion subgroup of G

$0 \in G_T$, so G_T is nonempty

Let $a, b \epsilon G_T$, I must show $a - b \epsilon G_T$

Find positive integers m, n , such that $ma = 0$ and $nb = 0$ then

$$mn(a - b) = mna - mnb = 0 - 0 = 0$$

therefore $a - b \epsilon G_T$ and $G_T < G$.

(1-14) Torsion group :-

G an abelian group and G_T is torsion subgroup . Then G is torsion group if $G = G_T$ for all elements of G are finite order .

(1-15) Torsion free :-

G group is torsion free if the only element of finite order is the identity .

(1-16) Examples :-

1: Every finite group is torsion group .

Proof

Let $G = \{a_1, a_2, \dots, a_n\}$ finite and $(G, +)$ is finite group, then

$\forall g \in G$, $\{ng \mid n \in Z\} \subset G$ this subgroup must be finite

$\exists\, m \neq k$ such that $mg = kg$

$(m - k)g = 0$ g has finite order.

2: The group $(Z , +)$ is torsion free .

3: Q rational numbers are torsion free but not free abelian .

Remark

The finite abelian group is just the torsion subgroup of G.

(1-17) Definition:-

If A is an abelion group and p a prime number , we denote by $A(p)$ the subgroup of all elements $x \in A$ whose period is a power of p . Then

$A(p)$ is a torsion group and is $p - group$ if it is finite .

(1-18) Definition :-

A p a prime number , a $p - group$ is a periodic group in which each element has a power of p as its order : each element is of prime power order .

(1-19) Definition:

If $(G,*)$ and $(H,\cdot)$ are abelian groups, their direct sum is the group

$(G\oplus H,\star)$, $G\oplus H = G \times H$ as set

$\forall\, g_1, g_2 \in G \;\; , h_1, h_2 \in H \;\; (g_1, h_1) \star (g_2, h_2) = (g_1 * g_2 \, , h_1 \cdot h_2)$ and if G , H are finite then $|G| = m$, $|H| = n$

$|G\oplus H| = mn$

(1-20) Example :-

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

$C + D = C \oplus D$.

Solution:-

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

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

(1-21) Theorem :-

Let A be a torsion abelion group . Then A is the direct sum of its subgroups $A(p)$ for all primes p such that $A(p) \neq 0$.

Proof

There is a homomorphism $\oplus A(p) \longrightarrow A$

Which to each elements (x_p) in the direct sum associates elements $\sum x_p$ in A . We prove that this homomorphism is both surjective and injective .

Suppose x is in the kernel , so $\sum x_p = 0$. Let q be prime . Then

$$x_q = \sum_{p \neq q} (-x_p)$$

Let m be the least common multiple of periods of elements x_p , with $x_q \neq 0$ and $p \neq q$. Then

$mx_q = 0$. But also $q^r\, x_q = 0$ for some positive integer r .

If d is the greatest common divisor of m , q^r then $dx_q = 0$, but $d = 1$, so $x_q = 0$. Hence

The kernel is trivial and the homomorphism is injective .

For each positive integer m , denote by A_m the kernel of multiplication by m , the subgroup of $x \in A$ such that $mx = 0$ .We prove :

If $m = rs$ with r, s positive relative prime integers , then

$A_m = A_r + A_s$

In the fact there exist integers u , v such that $ur + vs = 1$. Then

$x = x(1) = x(ur + vs) = urx + vsx$, and $urx \epsilon A_s$ while $vsx \epsilon A_r$.
Repeating this process inductively, we conclude :-

$if\ m = \prod_{p/m} P^{e(p)}$ then $A_m = \sum_{p/m} A_{p^{e(p)}}$

Hence the map $\oplus A(p) \longrightarrow A$ is surjective .

(1-22) Example :-

Let $A = {}^{Q}/_{Z}$. Then ${}^{Q}/_{Z}$ is torsion abelian group , isomorphic to the direct sum of its subgroups $({}^{Q}/_{Z})\,(p)$. Each $({}^{Q}/_{Z})\,(p)$ consists of those elements which can be reperesented by rational number ${}^{a}/_{p^k}$ with $a \epsilon Z$ and k some positive integer .

(1-23) Remark :-

A finitely generated abelian group is free only if it is torsion free , that is , it contains no elements of finite order other than the identity ; Suppose G is free finitely generated , and $g_1, \dots, g_k$ is a basis . Let $g \in G$. Then , from definition of basis , $g = m_1 g_1 + \cdots + m_k g_k$. If $ng = 0$, then $nm_1 g_1 + \cdots + nm_k g_k = 0$ so $nm_1 = \cdots = nm_k = 0$ and if $n \neq 0 \implies m_1 = \cdots = m_k = 0 \implies g = o$.

(1-24) Theorem :-

Let A be finitely generated torsion $^-$ free abelian group. Then A is free .

Proof

Assume $A \neq 0$, let S be finite set of generators , and let $x_1, \dots\dots, x_n$ be a maximal subset of S having the property that whenever $v_1, \dots\dots, v_n$ are integers such that

$v_1 x_1 + \dots\dots + v_n x_n = 0$

then $v_j = 0\ for\ all\ j.\ (Note\ n \geqq 1\ since\ A \neq 0)$.

Let B be the subgroup generated by $x_1, \dots\dots, x_n$. Then B is free .

Given $y \epsilon A$ there exists integers $m_1, \dots\dots, m_n$,

m not all zero such that $my + m_1 x_1 + \cdots \dots + m_n x_n = 0$,

by assumption of maximality on $x_1, \dots\dots x_n$, $m \neq 0$, because in the other case ,

all $m_j = 0$. Hence my lies in B . This is true for every one of a finite set of generators y of A , whence there exists on integer $m \neq 0$ such that $mA \subset B$. The map

$$h: x \to mx$$

of A into itself is a homomorphism , having trivial kernel since A is torsion free .

(1-25) Example :-

Prove that:-

Every finitely generated torsion group is a finite .

Solution:-

By fundamental theorem of finitely generated abelian groups (which will be stated and proved later) , if G is finitely generated it is the direct sum of a finite number of cyclic groups . If G is a torsion group , then it is the direct sum of a finite number of cyclic groups . Hence G is finite .

(1-26) Definition:-

The free group F_S with a basis S is the universal group generated by the set . This can be formalized by the following universal property given any function f from S to a group G , there exists a unique homomorphism $\varphi: F_S \to G$

That's , homomorphism $F_S \to G$ is one to one correspondence with function $S \to G$.

(1-27) Theorem :-

Let A be finitely generated abelion group , and let A_T be the subgroup consisting of all elements of A having finite period . Then A_T is finite , and A/A_T is free .

proof

We recall that a finitely generated torsion abelian group is obviously finite .

Let A be finitely generated by n elements , and let F be the free abelian group on n generators . By universal property ,

there exists a surjective homomorphism $F \xrightarrow{\phi} A$ of F onto A . The subgroup $\phi^{-1}(A_T)$ of F is finitely generated , hence A_T itself is finitely generated , hence finite .

Next , we prove A/A_T has no torsion . Let $\bar{x}$ be an element of A/A_T such that $m\bar{x} = 0$ for some integer $m \neq 0$. Then for any representative of x of $\bar{x}$ in A , we

have $mx \in A_T$, whence $q\,mx = 0$ for some integer $q \neq 0$. Then $x \in A_T$, so $\bar{x} = 0$ and A / A_T is torsion free .

By theorem *(1-24)* A / A_T is free .

(1-28) Corollary of (1-24) :-

Let $G \neq \{0\}$ be finitely generated torsion free abelian group . Then G is free abelion group of rank r that is $G \cong Z$.

CHAPTER

2

Finitely Generated Abelian Groups

(2-1) Definition :-

An abelian group G is finitely generated if there are elements $x_1, \ldots, x_n \in G$ such that every element $x \in G$ can be written

$$x = a_1x_1 + \cdots + a_nx_n \ , \ a_i \in Z \ .$$

With integers, the set $\{x_1, \ldots, x_n\}$ is a generating of G or generate G .

(2-2) Definition :-

Let G be finitely generated abelian group . The abelian group rank of G is defined to be the size of greatest possible independent set of G .

(2-3) Examples :-

1- The integers $(Z \ , +)$ are finitely generated abelian group (generating set $\{1\}$) .

2- The integers modulo n , nZ are finitely generated abelian groups .

3- The group$(Q \ , +)$ of rational numbers isn't finitely generated: if $\alpha_1, \alpha_2, \ldots \alpha_n$ are rational numbers, pick a natural number w coprime to all the denominators of $\alpha_1, \ldots, \alpha_n$ then $1/w$ can't be generated by $\alpha_1, \alpha_2, \ldots \alpha_n$.

4- The group $(Q^* \ , \cdot \ )$ of non-zero rational numbers is also not finitely generated .

(2-4) Remarks :-

1- Every finite group is obviously finitely generated .

2- Finitely generated group is a group that has a finite generating set .

3- A group that isn't finitely generated is sometimes saied to be infinite generated .

(2-5) Definition :-

Let G be any group . If a , b $\in$ G then commutator of a and b is the element $aba^{-1}b^{-1}$, ofcourse , if a and b commute then $aba^{-1}b^{-1} = e$. Now define C to be the set $C = \{x_1, x_2, \ldots, x_n | n \geq 1\}$ each x_i is commutator subgroup .

Remark:-

A finitely generated non abelian group may have subgroups that are not finitely generated .

for example :- the commutator subgroup of the free group on 2 generators isn't finitely generated . We begin with lemma (a free group of countably infinite rank isn't finitely generated) . Now the proof ; let A be a countably infinite set and suppose $F(A)$ is finitely generated . Say by S . Now only a finite number of elements of A

appear as letters in the words in S . Thus some words in $F(A)$ isn't in $< S >$. Contradiction

Now , the solution for example : Let $F_2 = F(a, b)$ be the free group of rank 2 and Let $C = \{ [x , y] \mid x , y \in F_2 \}$ be the set of commutators in F_2 , $c = xy\, x^{-1}\, y^{-1}$.

$< c > = F_2' \subset F_2$ by the universal property of free groups and using the inclusion $C \longrightarrow F_2'$, there exists a unique group homomorphism $\phi : F(c) \longrightarrow F_2'$

whish surjective by construction . Now $w \in ker\ (\phi)$, $\phi\ (w) = 1$ is a word in $F_2' \leq F_2$, since this group is free on a and b . We must have $w = 1$. Thus ϕ is an injective and we have $F_2' \cong F(c)$ hence

F_2' is a free group of an infinite rank , by lemma (A=c infinite) .

F_2' is not finitely generated .

Remark:-

Not every abelian group of finite rank is finitely generated .

for example :- the rank 1 group Q is one counterexample and the $rank - 0$ group given by a direct sum of countably infinitely many copies of Z_2 is another one .

Subgroup of finitely generated abelian groups

(2-6)) Lemma :-

Let $G = < a_1 > \oplus \ldots \oplus < a_n >$ be the direct sum of infinite cyclic groups . If $b_1 = a_1 + r_2 a_2 + \ldots + r_n a_n$ where $r_2 , \ldots , r_n$ are integers . Then

$$G = < b_1> \oplus < a_2 > \oplus \ldots \oplus < a_n > .$$

Proof

As $< b_1, a_2, \ldots, a_n >= < a_1, \ldots, a_n >= G$, we must only show that if $s_1 , \ldots , s_n$ are any integers , then

$$s_1 b_1 + s_2 a_2 + \ldots + s_n a_n = 0 \qquad *$$

implies all s_i are 0

Substituting $b_1 = a_1 + r_2 a_2 + \cdots + r_n a_n$ into $(*)$ and collecting terms , we obtain

$$s_1 a_1 + (s_1 + s_1 r_2) a_2 + \cdots + (s_n + s_n r_n) a_n = 0$$

As $G = \{a_1\} \oplus \ldots \oplus \{a_n\}$,

$$s_1 = s_2 + s_1 r_2 = \ldots = s_n + s_1 r_n = 0$$

Thus $s_1 = s_2 = \ldots = s_n = 0$.

(2-7) Lemma:-

Let G be free abelian , 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

$H = < u_1c_1, \dots, u_nc_n >$.

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 arbitrary basis $c_1, \dots, c_n$ for G. Then $H = < u_1c_1, \dots, u_nc_n >$ 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

$h = qa_1 + q_2a_2 + \cdots + q_na_n$, $q_2, \dots, q_n$ integers (1)

Then q is termed the size of the basis $\{a_1, a_2, \dots, a_n\}$.

Assume $\{a_1, a_2, \dots, a_n\}$ is a basis of smallest size , 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 $q_2, \dots, q_n$. If q_i is not divisible by q , $q_i = r_iq + s_i$ where $0 < s_i < q$. Hence

$$h = q(a_1 + r_ia_i) + \cdots + s_ia_i + \cdots + q_na_n$$

But if we put $b_1 = a_i$, $b_2 = a_2, \dots$, $b_i = a_1 + r_ia_i, \dots, b_n = a_n$, we obtain a basis by ***lemma (2-6)*** . 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 $q_i = r_iq$. Then

$$h = q(a_1 + r_2a_2 + \cdots + r_na_n)$$

Let $c_1 = a_1 + r_2a_2 + \cdots + r_na_n$. Then , by lemma (2-6) , $\{c_1, a_2, \dots, a_n\}$ is a basis for G . Also

$$h = qc_1 \qquad (2)$$

If $k = t_1a_1 + \cdots + t_na_n \in H$, it follows that t_1 is divisible by q . For if $t_1 = uq + v$ with $0 \leq v < q$, then $l = k - uh \in H$ has v as its coefficient of a_1 . As $v < q$, by the minimality of q, $v = o$. Therefore

$$l = k - uh \in < a_1, \dots, a_n >$$

Hence $l \in < a_1, \dots, a_n > \cap H = L$, say . From this we conclude that if $k \in H$, then

$$k = uh + l \qquad (3)$$

Whrer $l \in L$.

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 $u_2c_2, \dots, u_nc_n$. Hence by (3) every element of H belongs to $< h, u_2c_2, \dots, u_nc_n >$. On the other hand , H contains $h, u_2c_2, \dots, u_nc_n$. Thus

$$H =< h, u_2c_2, \dots, u_nc_n >$$

Put $u_1 = q$. By (2)

$$H =< u_1c_1, u_2c_2, \dots, u_nc_n >$$

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

(2-8) Theorem:-

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

Proof

By ***Lemma (2-7)*** there exist a basis $c_1 , \dots, c_n$ of G and integers $u_1 , \dots, u_n$ such that $H = < u_1c_1, \dots u_nc_n >$. *If* $u_1, \dots, u_i$ are nonzero, and $u_{i+1} = u_{i+2} = \dots = u_n = 0$ then

$$< u_1c_1, \dots, u_nc_n >=< u_1c_1 > \oplus \dots \oplus < u_ic_i >$$

See example ***(1-19)*** , hence the result .

(2-9) Example :-

Let G be a p-group . Suposse $G =< a > \oplus B$. Prove that $G =< a + b > \oplus B$ where $b \in B$ is of order less than or equal to the order of a .

Proof

If $x \in < a + b > \oplus B$, then $x = r(a + b) = b_1$ where $b_1 \in B$ and r is an integer . Thus $ra = b_1 - rb$. Since $< a > \cap B = \{0\}$, $ra = 0$. Then r is divisible by the power of p which is the order of a . Consequently $rb = 0$. Hence $b_1 = 0$ and $x = 0$. Clearly $< a + b > \oplus B = G$.

(2-10) Corollary :-

Every subgroup of finitely generated abelian group is a finitely generated .

Proof

Let A is a finitely generated abelian group , it is isomorphic to some factor group of a finitely generated free abelian group G , say $A \cong {}^{G}/_{N}$.

The subgroups of ${}^{G}/_{N}$ are of the form ${}^{H}/_{N}$ where H is a subgroup of G

By theorem ***(2-8)***

H is a finitely generated and therefore , so is ${}^{H}/_{N}$, consequently

Every subgroup of A is a finitely generated .

(2 -11) Theorem :-

Suppose G is a finitely generated abelian group . Then there are finitely generated free abelian groups F_1 and F_2 and a homomorphism

$\psi: F_1 \to F_2$ such that $G \cong F_1/\psi(F_2)$.

Proof

Let $x_1 , \dots , x_m$ be generators for G . let $F_1 = Z^m$ and let

$\phi = F_1 \longrightarrow G$ be the map that sands *ith* generator (0,0, … ,1, … ,0) of Z^m to x_i . Then

ϕ is a surjective homomorphism , and ***by corollary (2-10)*** the kernel $ker\phi$ of ϕ is a finitely generated abelian group .

Let $F_2 = Z^n$ and fix surjective homomorphism $\psi: F_2 \longrightarrow ker(\phi)$

Then $F_1/\psi(F_2)$ is isomorphic to G

Suppose G is a nonzero finitely generated abelian group . There are free abelian groups F_1 and F_2 and homomorphism

$\psi = F_2 \longrightarrow F_1$ Such that $G \cong {}^{F_1}/_{\psi(F_2)}$.

CHAPTER

3

Fundamental Theorem of Finitely Generated Abelian Group

Fundamental Theorem of finitely generated abelian groups

(3 - 1) Theorem :-

Every finitely generated abelian group is isomorphic to direct sum of cyclic groups .

Proof

$G \cong {}^{F}/_{H}$ where F is a finitely generated free abelian group and ***by Lemma (2-7)*** F has basis $c_1 , \dots , c_n$ such that $H = < u_1 c_1, \dots , u_n c_n >$ for some nonnegative integers $u_1 , \dots , u_n$.

Suppose $F = A \oplus B$ and A_1, B_1 be subgroups with $A_1 \subseteq A$, $B_1 \subseteq B$ and $H = A_1 + B_1$

Let $G = {}^{A}/_{A_1} \oplus {}^{B}/_{B_1}$, Let $\theta = A \to {}^{A}/_{A_1}$,

$\phi = B \to {}^{B}/_{B_1}$.

There exist ψ homomorphism of F into G . Then

$ker\ \psi \supseteq ker\theta = A_1$

$ker\ \psi \supseteq ker\phi = B_1$. Thus

$ker\ \psi \supseteq A_1 + B_1$. Now let $x \epsilon\ ker\ \psi$. Then $x = a + b$, $a \epsilon A$, $b \epsilon B$.

$x\psi = (a + A_1) + (b + B_1)$ and

this is an identity element only if $a \in A_1$, $b \in B_1$

Hence $x \in A_1 + B_1$ and so $ker\psi = A_1 + B_1$

By homomorphism theorem ${}^{F}/_{H} \cong G$.

To complete prove we will need the following Lemma and Corollary .

(3 - 2) Lemma :-

Suppose $G = A \oplus B$, Let A_1 , B_1 be subgroups with $A_1 \subseteq A$, $B_1 \subseteq B$ and $N = A_1 + B_1$. Then ${}^{G}/_{N} = {}^{A}/_{A_1} \oplus {}^{B}/_{B_1}$.

Proof

Let $K = {}^{A}/_{A_1} \oplus {}^{B}/_{B_1}$, and let $\theta = A \to {}^{A}/_{A_1}$ and $\phi = B \to {}^{B}/_{B_1}$ be the natural homomorphisms . θ, ϕ extand to a homomorphism ψ of G into K . Then

$$ker\psi \supseteq ker\theta = A_1$$

and $ker\psi \supseteq ker\phi = B_1$, thus

$$ker\psi \supseteq A_1 + B_1 = N$$

Now we prove that $ker\psi \subset N$

Let $x \in ker\psi$, then $x = a + b$, $a \in A$, $b \in B$.

$x\psi = (a + A_1) + (b + B_1)$ and this identity element only if $a \in A_1$ and $b \in B_1$. Hence

$x \in A_1 + B_1 = N$ and so $ker\psi = A_1 + B_1 = N$

by the homomorphism theorem ${}^{G}/_{N} \cong K$

(3 - 3) Corollary :-

Let F be free abelian with basis $c_1, \dots, c_n$. Let $H =< u_1c_1, \dots, u_nc_n >$ where $u_1, \dots, u_n$ are nonnegative integers . Then F/H is the direct sum of cyclic groups of orders $u_1', \dots, u_n'$ where $u_i' = u_i$ if $u_i \neq 0$ and $u_i' = \infty$ if $u_i = 0$.

This end's the proof of the Theorem (3-1)

(3 - 4) Example :-

If $|< a >| = m$, $|< b >| = n$, $(m,n) = 1$, then

$G =< a > \oplus < b >$ is cyclic of order mn .

Solution :-

We show that $G =< a + b >$. If h is the order of $a + b$ then $h(a + b) = ha + hb$ implies $ha = hb = 0$ by the definition of a direct sum

consequently

h is divisible by the order of a and the order of b . Since $(m,n) = 1$, mn/h and we conclude $mn = h$, so that $G =< a + b >$.

(3 - 5) Corollary :-

If G is finitely generated , It is the direct sum of a finite number of infinite cyclic groups and cyclic groups of prime power order .

Proof

It is only necessary to show that a cyclic group of composite order is the direct sum of cyclic groups of prime power order .

This can be done using induction in *(3 - 4)* .

(3 - 6) Corollary :-

If G is a group without non zero elements of finite order and G is finitely generated , then G is free abelian .

Proof

G is the direct sum of a finite number of cyclic groups each of which must be infinite cyclic as G has no elements of finite order .

The type of a finitely generated abelian groups :-

We say that two decompositions are of the same kind if they have the same number of summands of each order . For example , two decompositions of a group into the direct sum of three cyclic groups of order 4 and two cyclic groups of infinite order are said to be of the same kind .

Every finitely generated group can be decomposed into the direct sum of a finite number of cyclic groups of prime power or else infinite order .

(3 - 7) Theorem :-

Any two decompositions of a group G into the direct sum of a finite number of cyclic group which are either of prime power $(\neq 1)$ or of infinite order , are of the same kind .

Proof

We shall separate the proof into four cases :

1- both decompositions involve only infinite cyclic groups .

2- both decompositions involve only cyclic groups of order a power of fixed prime p .

3- both decompositions involve no infinite cyclic groups .

4- the general case .

Case 1 . $G = I_1 \oplus \dots \oplus I_k = \widehat{I_1} \oplus \dots \oplus \widehat{I_l}$

Where I_j , $\widehat{I_l}$ for $j = 1, \dots, k$ and $i = 1, \dots, l$ respectively , are infinite cyclic groups .

Using the fact (If F is group freely generated by two finite sets X and Y , then $|x| = |y|$), we conclude that $K = L$.

Example:- Prove , by considering the direct sum of cyclic groups of order 2 , that if G is the direct sum of K infinite cyclic groups and also the direct sum of L infinite cyclic groups , then $K=L$.

Solution

Let $G =< x_1 > \oplus \ldots \oplus < x_k >$. Let $H =< 2x_1, \ldots, 2x_k >$. Then ***by corollary (3-3)*** , ${}^{G}/_{H}$ is direct sum of K cyclic groups of order 2 . Thus $|{}^{G}/_{H}| = 2^k$. Clearly $H \subset 2G$. Also if $g \in G$, $g = r_1x_1 + \cdots + r_kx_k$. Then $2g = r_1(2x_1) + \cdots + r_k(2x_k) \in H$ from which $2G \subseteq H$. Thus $H = 2G$.

Now by a similar argument we conclude that if G is direct sum of L infinite cyclic groups , $|{}^{G}/_{2G}| = 2^l$. Thus $L = K$.

Case 2 . Both decompositions involve only cyclic groups of order a power of a fixed prime .

We shall write for any integer n , $nG = \{ng | g \in G\}$. If G is a group , nG is a subgroup (***Example (3-9)***)

To prove ***case 2*** we will need the following lemma

(3 - 8) Lemma :-

Let $G = A \oplus B$. If n is any integer , then $nG = nA \oplus nB$.

Proof

As $nA \cap nB \subseteq A \cap B = \{0\}$, $< nA, nB >= nA \oplus nB$.

If $g \in nG$, there exists $h \in H$ such that $nh = g$.

Let $h = a + b$, $a \in A$ and $b \in B$. then $g = nh = na + nb$

Accordingly $nG \subseteq nA \oplus nB \subseteq nG$ and so $nG = nA \oplus nB$.

(3-9) Example :-

Prove that nG is a subgroup of G where n is a given integer .

Solution

If $h, k \in nG$, $h = nf$, $k = ng$ where $f, g \in G$. Hence $h - k = n(f - g) \in nG$, and so nG is a subgroup .

(3 -10) Corollary :-

Let $G = A_1 \oplus \ldots \oplus A_k$. Let n be an integer , then $nG = nA_1 \oplus \ldots \oplus nA_k$.

Proof

This corollary be generalization to ***lemma (3 - 8).***

Case 3. G is expressed in two ways as the direct sum of a finite number of cyclic groups of prime power order .

We have dealt with case where only one prime is involved . We proceed by induction on the number of primes involved . Let p be one of the primes involved . Let $A_1, \dots, A_m$ be all the direct summands of order a power of p in the one decomposition , $B_1, \dots, B_n$ the other direct summands involved, so that

$$G = A_1 \oplus \dots \oplus A_m \oplus B_1 \oplus \dots \oplus B_n$$

Putting $A = A_1 \oplus \dots A_m$ and $B = B_1 \oplus \dots \oplus B_n$, it follows that $G = A \oplus B$.

Let $X_1, \dots, X_k$ be all the direct summands of order a power of p in the second decomposition $Y_1, \dots, Y_l$ the remaining direct summand , so that

$$G = X_1 \oplus \dots \oplus X_k \oplus Y_1 \oplus \dots \oplus Y_l$$

Put $X = X_1 \oplus \dots \oplus X_k$, $Y = Y_1 \oplus \dots \oplus Y_l$. Then $G = X \oplus Y$. We claim that $A = X$ and $B = Y$

Let $g \in A$. Then $g = x + y$ where $x \in X$ and $y \in Y$. Now the order of any nonzero element of Y is coprime to p . As g is of order a power of p , $y = 0$. Hence $g \in X$ and so $X \subseteq A$ and we conclude that $A = X$. By the similar argument $B = Y$.

Thus $A_1 \oplus \dots \oplus A_m = X_1 \oplus \dots \oplus X_k$ and $B_1 \oplus \dots \oplus B_n = Y_1 \oplus \dots \oplus Y_l$. By the induction hypothesis $A_1 \oplus \dots \oplus A_m$ and $X_1 \oplus \dots \oplus X_k$ on the one hand , and $B_1 \oplus \dots \oplus B_n$ and $Y_1 \oplus \dots \oplus Y_l$ on the other , are of the same kind . Hence the two decompositions are of the same kind .

Example:- Let G be an abelian group , $G = X \oplus Y$. Let $x \in X$, $y \in Y$. Prove that *(1)* If x and y are finite orders , then the order of $x + y$ is least common multiple (Lcm) of the orders of x and y . *(2)* If x is of infinite order , $x + y$ is of infinite order .

Solution

(1) Let $L = Lcm$ of the orders of x and y . Then $L(x + y) = Lx + Ly = 0$. Now if m =order of $x + y$, then $m(x + y) = mx + my = 0$ implies $mx = 0$ and $my = 0$. This in turn implies that the order of x divides m and the order of y divides m .

(2) If x is of infinite order and $m(x + y) = 0$, then $mx + my = 0$. But by the uniqueness of such expressions in direct sums , $mx = my = 0$. Since x is of infinite order , $m = 0$.

Case 4.Let G be expressed as the direct sum of cyclic groups of prime power order or of infinite order in two ways , say

$$G = I_1 \oplus \dots \oplus I_m \oplus F_1 \oplus \dots F_n = \hat{I}_1 \oplus \dots \oplus \hat{I}_k \oplus \hat{F}_1 \oplus \dots \oplus \hat{F}_l$$

Where I_j , $\hat{I}_j$ are infinite cyclic groups and F_j , $\hat{F}_j$ are groups of prime power order .

Let $T(G)$ (the torsion subgroup) be the set of all elements of finite order . Then $T(G)$ is the direct sum of the direct summands of finite order in both cases . Thus

$$T(G) = F_1 \oplus \dots \oplus F_n = \hat{F}_1 \oplus \dots \oplus \hat{F}_l$$

Hence by ***case 3*** , $F_1 \oplus \dots \oplus F_m$ and $\hat{F}_1 \oplus \dots \oplus \hat{F}_l$ are of the same kind .

Also $G/T(G) \cong I_1 \oplus \dots \oplus I_m \cong \hat{I}_1 \oplus \dots \oplus \hat{I}_k$. $I_1 \oplus \dots \oplus I_m$ is the direct sum of k infinite cyclic groups . Then $k = m$ by case 1 . Therefore we have proved that $I_1 \oplus I_2 \oplus \dots \oplus I_m \oplus F_1 \oplus \dots \oplus F_n$ and $\hat{I}_1 \oplus \hat{I}_2 \oplus \dots \oplus \hat{I}_k \oplus \hat{F}_1 \oplus \dots \oplus \hat{F}_l$ are of the same kind .

Example:- Let $G = I_1 \oplus \dots \oplus I_m \oplus F_1 \oplus \dots \oplus F_n$ where each I_j is torsion free and each F_i finite . Let $T(G)$ be the set of all elements of finite order . Prove that

$$T(G) = F_1 \oplus \dots \oplus F_n .$$

Solution

Clearly $T(G) \supseteq F_1 \oplus \dots \oplus F_n$. If $g \in T(G)$, $g = i_1 + \dots + i_m + f_1 + \dots + f_n$ where $i_1, \dots, i_m$ are elements of $I_1, \dots, I_m$, and $f_1, \dots, f_n$ are elements of $F_1, \dots, F_n$ respectively . As g is of finite order r , say $rg = ri_1 + \dots + ri_m + rf_1 + \dots + rf_n = 0$ by definition of direct sum , $ri_1 = ri_2 = \dots = ri_m = rf_1 = \dots = rf_n = 0$ since $I_1, \dots, I_m$ are torsion free , we have $i_1 = i_2 = \dots = i_m = 0$. Thus $g \in F_1 \oplus \dots \oplus F_n$.

If finitely generated group G is the direct sum of cyclic groups of orders $p_1^{r_1}, \dots, p_k^{r_k}$ and s infinite cyclic groups , where $p_1, \dots, p_k$ are primes , $p_1 \leq p_2 \leq \dots \leq p_k$, $r_1, \dots r_k$ positive integers with $r_i \geq r_{i+1}$ if $p_i = p_{i+1}$, then the ordered $k+1-$ *tuple* $(p_1^{r_1}, \dots, p_k^{r_k}; s)$ is called ***the type of G*** . Usually it applied only to p-groups .

(3 - 11) Example:-

If the type of G is $(f_1, \dots, f_k; f)$ and that of G is $(g_1, \dots, g_p; g)$ where $f_1 = p_1^{r_1}$, $f_2 = p_2^{r_2}$, $\dots$, $f_k = p_k^{r_k}$, $g_1 = q_1^{s_1}$, $\dots$, $g_l = q_l^{s_l}$ and $p_k < q_1$, where the p_i are primes , find the type of $F \oplus G$.

Solution

We have $p_1 \leq \dots \leq p_k < q_1 \leq \dots \leq q_l$. Hence the type of $F \oplus G$ is $(f_1, \dots, f_k, g_1, \dots, g_l; f+g)$.

(3- 12) Theorem :-

If F and G are two finitely generated group , then they are isomorphic if and only if they have the same type .

Proof

Let $F = A_1 \oplus \dots \oplus A_k$. If $\phi = F \to G$ is an isomorphism , then $G = A_1\phi \oplus \dots \oplus A_k\phi$. As $A_i\phi \cong A_i$, it follows that F and G have the same type

conversely , if F and G have the same type they are clearly isomorphic .

(3 - 13) Examples :-

1: Let $G = A \oplus B$ where A and B are cyclic of order 2 . Find C and D such that $G = C \oplus D$ where C and D are cyclic of order 2 and $C \neq A$ and $C \neq B$.

Solution:-

Let $A = \{0, a\}$, $B = \{0, b\}$. Put $C = \{0, a + b\}$. Then C is cyclic of order 2 . Also put $D = B$. Then $C + D = \{0, a + b, b, a + b + b = a\}$ and so $C + D = G$ also $C \cap D = \{0\}$. Thus $G = C \oplus D$.

2: IF F, G and H are finitely generated abelian groups , show that

$$F \oplus G = F \oplus H \quad \text{implies} \quad G \cong H .$$

Solution:-

Express F, G and H as direct sums of cyclic groups of prime power and infinite orders . If the type of F is $(f_1, \dots f_k : f)$ and that of G is $(g_1, \dots g_n : g)$ while that of H is $(h_1, \dots, h_m : h)$, then the type of $F \oplus G$ is $(a_1, \dots, a_{k+n} : f + g)$ where $a_1, \dots, a_{k+n}$ is $f_1, \dots, f_k$, $g_1, \dots, g_n$ in some order , while the type of $F \oplus H$ is $(b_1, \dots, b_{k+m} : f + h)$ where $b_1, \dots, b_{k+m}$ is $f_1, \dots, f_k$, $h_1, \dots, h_m$ in some order .

For two abelian groups to be isomorphic by ***theorem (3-12)*** their types are the same . Accordingly the types of G and H are the same and $G \cong H$.

3: If $F = A_1 \oplus \dots \oplus A_k$ and $\phi : F \to G$ is an isomorphism , then $G = A_1\phi \oplus \dots \oplus A_k\phi$.

Solution:-

We must show that every element of G is uniquely of the form $A_1\phi + \cdots + A_k\phi$. where $a_1, \dots, a_k$ belong to $A_1, \dots, A_k$ respectively

Now if $g \in G$, there exists $f \in F$ such that $f\phi = g$. But $f = a_1 + \cdots + a_k$ and so $g = a_1\phi + \cdots + a_k\phi$. *If* $a_1\phi + \cdots + a_k\phi = a_1'\phi + \cdots + a_k'\phi$

then $(a_1 - a_1')\phi + \cdots + (a_k - a_k')\phi = 0$

Let $h = a_1 - a_1' + \cdots + a_k - a_k'$. h belongs to $ker\phi$. Since ϕ is an isomorphism , $h = 0$, by the uniqueness of expression of direct sums $a_1 - a_1' = a_2 - a_2' = \cdots = a_k - a_k' = 0$ so that $a_1 = a_1'$, $a_2 = a_2'$, ... , $a_k = a_k'$ therefore each elements of G is expressible in the form

$a_1\phi + \cdots + a_k\phi$ is one and only one way .

Application and examples

(3-14) Theorem :-

Let A be finitely generated abelian group then

$$A \cong Z^s \oplus {}^{Z}/_{a_1 Z} \oplus \ldots\ldots \oplus {}^{Z}/_{a_r Z} \qquad \ldots\ldots\ldots \mathbf{4}$$

Where s is a nonnegative integer and a_i are non zero non units in Z , such that $a_1 | a_2 | \ldots | a_r$ **5**

Further , the decomposition **4** of A subject to the condition **5** is unique

(Z° is interpreted as the trivial group (o))

If A is generated by $(x_1, \ldots, x_n)$ subject to $\sum_{j=1}^{n} a_{ij} x_j = 0$, $1 \leq i \leq m$ then

$$A \simeq \overbrace{Z \times \ldots \times Z}^{(n-r)copies} \times {}^{Z}/_{a_1 Z} \times \ldots \times {}^{Z}/_{a_r Z}$$

Where $a_1, \ldots, a_r$ are the invariant factor of the $m \times n$ matrix $A = (a_{ij})$

(3-15) Definition:-

Let $A , B \in F^{n \times m}$ be two matrices of the same size we say that

A is left equivalent to B iff there exists $Q \in GL_m(F)$ such that $A = QB$

A is right equivalent to B iff there exists $P \in GL_n(F)$ such that $A = BP^{-1}$

A is right left equivalent to B iff there exists $Q \in GL_m(F)$ and $P \in GL_n(F)$ such that $A = QBP^{-1}$

Where $A \cong B$ denote any of these three relations , we have

$C_2 - C_1$ means ; column 2 minus column 1 .

$(-1)R_3$ means ; multiply row 3 by (-1) .

$C_1 \leftrightarrow C_2$ means ; interchange of column 1 and 2 .

$R_3 - (3)R_2$ means ; from row 3 subtract row 2 multiplied by 3 .

(3-16) Examples :-

1) The abelian group generated by $x_1$and x_2 subject to $2x_1 = 0\,, 3x_2 = 0$ is an isomorphic to $Z/_{(6)}$ because the matrix of constraints is $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ which is equivalent to $\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$.

2) Find the abelian group generated by $\{x_1, x_2, x_3\}$subject to

$$5x_1 + 9x_2 + 5x_3 = 0$$

$$2x_1 + 4x_2 + 2x_3 = 0$$

$$x_1 + x_2 - 3x_3 = 0$$

Solution:-

$$A = \begin{pmatrix} 5 & 9 & 5 \\ 2 & 4 & 2 \\ 1 & 1 & 3- \end{pmatrix}$$

Perform $C_2 - C_1$, $R_1 - 2R_2$, $C_3 - C_1$, $R_3 - R_1$, $(-1)R_3$, and $C_1 - C_2$ in succession to obtain that A is equivalent to

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ Hence

The desired abelian group is isomorphic to

$$Z/_{1Z} \times Z/_{2Z} \times Z/_{4Z} = Z/_{(2)} \times Z/_{(4)}\,.$$

References

1- Baumslag B. , Schaum's outline of Theory and Problems of Group Theory , New York University , 1968.

2- Bhattacharya P. B. , Basic Abstract Algebra , University of Cambridge , 1999.

3- Dummit D. S. , Abstract Algebra , University of Vermont , Springer ,2004

4- Hungerford T. W. , Algebra, GTM , Springer.

5- Kurosh A. G. , The Theory of Groups , USA , 1960.

6- La Harpe , Topics in Geometric Group Theory , University of Chicago , 2000.

7- Lang S. , Algebra , GTM , Springer , 2002.

8- Machi A. , An introduction to ideas and methods of the Theory of Groups , London , 2012.

9- Nicholson W. K. , Introduction to Abstract Algebra ,fourth edition , 2012.

10- Norman C. , Finitely Generated Abelian Groups and Similarity of matrices over a field , University of London ,2012.

11- Silverman J. H. ; Tate J. , Rational Points on elliptic curves , UTM, New York , 1992.

12- Wikipedia , The free encyelopedia (en.wikipedia.org)