UNIT 5 : DIRECT PRODUCTS OF GROUPS AND FINITE ABELIAN GROUPS

UNIT STRUCTURE

5.1 Learning Objectives

5.2 Introduction

5.3 External Direct Product (Definitions and Examples)

5.4 Properties of External Direct Product

5.5 Internal Direct Product (Definitions and Examples)

5.6 Properties of Internal Direct Product

5.7 Structure of Finite Abelian Groups

5.8 Let Us Sum Up

5.9 Answer to Chek You Progress

5.10 Further Readings

5.11 Model Questions

5.1 LEARNING OBJECTIVES

After going through this unit, you will able to know -

- the concept of External direct product of groups
- properties of External direct product of groups
- the concept of Internal direct product of groups
- properties of Internal direct product of groups
- structure of finite abelian groups.

5.2 INTRODUCTION

The idea of this unit is to discuss how we can combine groups to from other groups. The reason for doing this is also to see the reverse, that a complicated group could possibly be broken down into a combination of simpler groups.

A finite abelian group is a nonempty finite set with a binary operation which satisfies, in addition to the group axioms, the commulative law. Given an arbitrary group, there is no reason to expect, if a and b are elements of

the group, that the symbols ab and ba should represent the same element. Consider, for example, the group of 2 × 2 nonsingular matrices with entries from the integers modulo p with the operation of matrix multiplication. Since matrix multiplication is non commutative, we would not, in general, expect the product AB of two arbitrary matrices A and B to equal the product BA. As we shall see, however, when the group at hand is endowed with the property of commutativity, many of the notions of group theory are simplified. This simplification admits a through investigation of finite abelian groups and makes the complete classification of finite abelian groups possible.

In this unit we will examine examples of finite abelian groups and several fundamental results. Additionally, we will consider a few theorems from the broader theory which are made more definitive in the finite abelian case.

5.3 EXTERNAL DIRECT PRODUCT (DEFINITIONS AND EXAMPLES)

Definition 5.3.1 : Let $G_1, G_2,.....,G_n$ be a finite collection of groups. The external direct product of $G_1, G_2,.....,G_n$ written as $G_1 \oplus G_2 \oplus .....\oplus G_n$ is the set of all n-tuples for which the *i*th component is an element of G_i and the operation is component wise. In symbols,

$$G_1 \oplus G_2 \oplus .....\oplus G_n = \{(a_1, a_2,.....,a_n) | a_i \in G_i\}$$

where $(a_1, a_2,....,a_n)\ (b_1, b_2,.....,b_n) = (a_1b_1, a_2b_2, ...,a_nb_n)$. It is understood that each product a_ib_i is performed with the operation of G_i. None that in the case that each G_i is finite, we have by properties of sets that $|G_1 \oplus G_2 \oplus .....\oplus G_n| = |G_1||G_2|.....|G_n|$

Example 1: Let $G_1, G_2,.....,G_n$ be n groups and $G = G_1 \oplus G_2 \oplus .....\oplus G_n$ be their external direct product. Then we can show that G is a group under the operation define as

$$ab = (a_1, a_2....,a_n)\ (b_1, b_2....,b_n) = (a_1b_1, a_2b_2,.....,a_nb_n)$$

for all $a = (a_1, a_2....,a_n),\ (b_1, b_2....,b_n) \in G$

Let $a = (a_1, a_2....,a_n),\ b = (b_1, b_2....,b_n),\ c = (c_1, c_2....,c_n) \in G$

Closure Property : By definition

$ab = (a_1, a_2....,a_n)\ (b_1, b_2....,b_n) = (a_1b_1, a_2b_2,.....,a_nb_n)$

for all $a = (a_1, a_2....,a_n),\ b = (b_1, b_2....,b_n) \in G$. Since $a_ib_i \in G_i,\ 1 \le i \le n$, we get $ab \in G$.

This prove that G is closed.

Assosciativity :

$$(ab)c = \left[(a_1, a_2....,a_n)\ (b_1, b_2....,b_n)\right](c_1, c_2....,c_n)$$
$$= (a_1b_1, a_2b_2,.....,a_nb_n)\ (c_1, c_2....,c_n)$$
$$= \left((a_1b_1)c_1, (a_2b_2)c_2,.....(a_nb_n)c_n\right)$$
$$= (a_1(b_1c_1), a_2(b_2c_2), ...,a_n(b_nc_n)$$

since $(a_ib_i)c_i = a_i\,(b_ic_i)$ for all i.

$$= (a_1, a_2....,a_n)\left[(b_1c_1, b_2c_2,.....,b_nc_n)\right]$$
$$= a\ (bc)$$

Existence of identity : For each i = 1, 2, ..., n, let e_i be the identity of G_i,and e = $(e_1, e_2, ...,e_n) \in G$

$$ae = (a_1, a_2,... ...,a_n)\ (e_1, e_2, ...,e_n)$$
$$= (a_1e_1, a_2e_2,..... .....,a_ne_n)$$
$$= (a_1, a_2,... ...,a_n)$$
$$= a$$

Similarly, we can show ea = a.

Existence of Inverse : For given any $a = (a_1, a_2,.... .....,a_n) \in G$ there exists

$a^{-1} = (a_1^{-1}, a_2^{-1}, ..., a_n^{-1}) \in G$ such that

$$aa^{-1} = (a_1, a_2,.... .....,a_n)\ (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$$
$$= (a_1a_1^{-1}, a_2\,a_2^{-1}, ..., a_n\,a_n^{-1})$$
$$= (e_1, e_2, ...,e_n)$$
$$= e$$

Similarly, we can show $a^{-1}a = e$. Thus $a^{-1} = (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$ is the inverse of $a = (a_1, a_2,.... .....,a_n)$ in G.

Hence $G = G_1 \oplus G_2 \oplus ....\oplus G_n$ is a group.

Example 2: Consider $Z_2 \oplus Z_2$. This is the group with set :

{ (0, 0), (1, 0), (0, 1), (1, 1)}

and a sample operation would be (1, 0) + (1, 1) = (0, 1).

Example 3: Consider $U(10) \oplus U(5)$. This is the group with set :

{(1, 1), (1, 2), (1, 3), (1, 4), (3, 1), (3, 2), (3, 3), (3, 4), (7, 1), (7, 2), (7, 3), (7, 4), (9, 1), (9, 2), (9, 3), (9, 4)} and a sample operation would be (3, 3) (7, 4) = (1, 2)

Example 4: The set U(8) of all positive integers less then 8 and relative prime to 8 i.e. U (8) = {1, 3, 5, } is a group under multiplication modulo 8. The set U (10) of all positive integers less then 10 and relative prime to 10 i.e. U (10) = {1, 3, 7, 9}is a group under multiplication modulo 10. Then

$U(8) \oplus U(10)$ = {(1, 1), (1, 3), (1, 70), (1, 9), (3, 1), (3, 3), (3, 7), (3,9), (5,1), (5, 3), (5, 7), (5, 9), (7, 1), (7, 3), (7, 7), (7, 9)} is the external direct product of groups U(8) and U(10).

Clearly $U(8) \oplus U(10)$ is a group under the operation defined as

(a, b) (c, d) = (r, s)

where $r \in U(8)$ is the remainder when ac is divided 8 and $s \in U(10)$ is the remainder when bd is divided 10.

Example 5: Consider $Z_2 \oplus Z_3$ = {(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)}

Clearly, this is an Abelian group of order 6. Consider the subgroup of $Z_2 \oplus Z_3$ generated by (1, 1). Since the operation is each component is addition, we have (1, 1) = (1, 1), 2(1, 1) = (0, 2), 3(1, 1) = (1, 0), 4 (1, 1) = 0, (, 1), 5 (1, 1) = (1, 2), and 6 (1, 1) = (0, 0). Hence $Z_2 \oplus Z_3$ is cyclic. It follows that $Z_2 \oplus Z_3$ is isomorphic to Z_6.

Example 6: A group of order 4 is isomorphic to Z_4 or $Z_2 \oplus Z_3$. To verify this, Let G = {e, a, b, ab}. If G is not cyclic, then it follows from Lagrange's Theorem that |a| = |b| = |ab| = 2. Then the mapping
$e \to$ (0, 0), $a \to$ (1, 0), $b \to$(0, 1) and $ab \to$ (1, 1) is an isomorphism from G onto $Z_2 \oplus Z_3$

We see from Example 5 and 6 that in some cases $Z_m \oplus Z_n$ is isomorphic Z_{mn} and in some cases it is not.

5.4 PROPERTIES OF EXTERNAL DIRECT PRODUCTS

Theorem 5.4.1 The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2,.....g_n)|=\text{lcm}(|g_1|,|g_2|.....,|g_n|)$$

Proof : Denote the identity of G_i by e_i. Let s = $=\text{lcm}(|g_1|,|g_2|.....,|g_n|)$ and

$t=|(g_1, g_2,.....g_n)$. Becasue the fact that s is a multiple of each $|g_i|$ implies that

$$(g_1,g_2,.....,g_n)^s=(g_1^s, g_2^s,.....,g_n^s)=(e_1, e_2,.....,e_n)$$

we know that $t \le s.$ On the other hand, from $(g_1', g_2',.....,g_n')=(g_1,g_2,.....,g_n)'$

$=(e_1, e_2,.....,e_n)$ we see that t is a common multiple of $|g_1|,|g_2|,.....,|g_n|$. Thus $s \le t$.

Example 7: For each divisor r of m and s of n, the group $Z_m \oplus Z_n$ has a subgroup isomorphic to $Z_r \oplus Z_s$. To find a subgroup of , say, $Z_{30} \oplus Z_{12}$ isomorphic to $Z_6 \oplus Z_4$, we observe that $\langle 5\rangle$ is a subgroup of Z_{30} of order 6 and $\langle 3\rangle$ is a subgroup of Z_{12} of order 4, so $\langle 5\rangle \oplus \langle 3\rangle$ is the desired subgroup.

Theorem 5.4.2 Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if |G| and |H| are relatively prime.

Proof : Let |G| = m and |H| = n, so that $|G \oplus H|$ =mn. To prove the first half of the theorem, we assume $G \oplus H$ is cyclic and show that m and n are relatively prime. Suppose that gcd (m, n) = d and (g, h) is a generator of $G \oplus H$. Since $(g,h)^{\frac{mn}{d}}=\left((g^m)^{\frac{n}{d}}, (h^n)^{\frac{m}{d}}\right)=(e,e)$, we have $mn=|(g,h)| \le \frac{mn}{d}$..

Thus, d = 1.

To prove the order half of the theorem, let $G=\langle g\rangle$ and $H=\langle h\rangle$ and suppose gcd (m, n) = 1.

Then, $(g,h)|=\text{lcm}(m,n)=mn=|G \oplus H|$, so that (g, h) is a generator of $G \oplus H$.

Corollary 5.4.3 An external direct product $G_1 \oplus G_2 \oplus .....\oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if | G_i | and | G_j | are relatively prime when $i \neq j$

Corollary 5.4.4: Let $m = n_1 n_2 ....n_k$. Then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus .....\oplus Z_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

Example 8: We can break down groups using prime factorizations, for example we know that :

$$Z100 \approx Z4 \oplus Z25$$

Note : We can't break these apart without co-primality, for example Z_4 not isomorphic to $Z_2 \oplus Z_2$.

Example 9: The Group of Units Modulo n as an External Direct Product. The U-groups, provide a convenient way to illustrate the preceding ideas. We first introduce some notation. If k is a divisor of n, Let $U_k(n) = \{x \in U(n): x \equiv 1(\mathrm{mod}\, k)\}$

For example, $U_7(105)$ = {1, 8, 22, 29, 43, 64, 71, 92}. It can be readily shown that $U_k(n)$ is indeed a subgroup of U(n).

Theorem 5.4.5: Suppose s and t are relatively prime. Then U(st) is isomorphic to the external direct product of U(s) and U(t), Moreover, U_s(st) is isomorphic to U(t) and U_t(st) is isomorphic to U(s).

Proof : There is an isomorphisms for U(st) to $U(s) \oplus U(t)$ is $x \to (x(\mathrm{mod}\, s), x(\mathrm{mod}\, t))$.

Similarly there is an isomorphism from U_s(st) to U(t) is $x \to x\ (\mathrm{mod}\, t)$ and an isomorphism from U_t(st) to U(s) is $x \to x\ (\mathrm{mod}\, s)$

Corollary 5.4.6: Let $m = n_1 n_2 .....n_k$, where gcd (n_i, n_j) = 1 for $i \neq j$. Then

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus .....\oplus U(n_k)$$

Theorem 5.4.7: Every group of order p^2, where p is a prime is isomorphic to Zp^2 or $Z_p \oplus Z_p$.

Proof : Let G be a group of order p^2, where p is a prime. If G has an element of order p^2, then G is isomorphic to Zp^2. So we may assume that every non identity element of G has order p. First we show that for any element a, the subgroup < a > is normal in G. If this is not the case, then

there is an element b in G such that bab^{-1} is not in < a >. Then < a > and $<bab^{-1}>$ are distinct subgroups of order p. Since < a > $\cap$ $< bab^{-1}>$ = {e}. From this it follows that the distinct left cosets of $< bab^{-1} >$ are $< bab^{-1} >$, a $< bab^{-1} >$, $a^2 < bab^{-1} >$ ..., $a^{p-1} < bab^{-1} >$. Since b^{-1} must lie in one of these cosets, we may write b^{-1} in the form $b^{-1} = a^i b a^j b^{-1}$ for some i and j. Cancelling the b^{-1} terms, we obtain e = $a^i b a^j$ and therefore $b = a^{\tau j} \in < a >$.This contradiction verifies our assertion that every subgroup of the form < a > is normal in G. To complete the proof let x be any non identity element in G and y be any element of G not in < x >. Then by comparing order we seen that $G =< x > \times < y > \cong < Z_p \oplus Z_p$.

Theorem 5.4.8 : Let $G_1, G_2, ...G_n$ be groups and let G = G_1 × G_2 × ..... × G_n be their direct product.

a) For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $i \neq j$ and arbitrary elements of G_i in position i is a subgroup of G isomorphic to G_i. In notation,

$$G_i \cong \{(1,1,....,1,g_i,1,....,1)| g_i \in G_i\}$$

Then G_i is a normal subgroup G and $G/G_i \approx G_1 \times G_2 \times .... \times G_{i-1} \times G_{i+1} \times ..... \times G_n$

b) If $x \in G_i$ and $y \in G_j$ for $i \neq j$, then xy = yx.

Proof :

a) Since the operation in G is defined componentwise, it follows easily from the subgroup criterion that {(1, 1, ...1, g_i, 1, ..., 1)| $g_i \in G_i$} is a subgroup of G. Furthermore, the map $g_i \mapsto (1,1, ...,1,g_i,1,.....,1)$ is seen to be an isomorphism of G_i, with this subgroup. Identify G_i, with this isomorphic copy in G.

To prove the remaining parts of (a) consider the map $\varphi : G \to G_1 \times G_2 \times .....\times G_{i-1} \times G_{i+1} \times ....\times G_n$ defined by,

$$(g_1, g_2, ...g_n) = (g_1, g_2, ...g_{i-1}, g_{i+1}, ..., g_n)$$

The map φ is a homomorphism since

$$((g_1, g_2, ...g_n)\ (h_1, h_2, ...h_n))$$
$$= (g_1h_1, g_2h_2.....,g_nh_n)$$
$$= (g_1h_1, g_2h_2.....,g_{i-1}\,h_{i-1}, g_{i+1}\,h_{i+1},.....,g_nh_n)$$

$= (g_1, g_2.....,g_{i-1}, g_{i+1},.....,g_n)\ (h_1,h_2.....,h_{i-1},h_{i+1},.....,h_n)$

$= \varphi(g_1, g_2, ...g_n)\ \varphi(h_1, h_2, ...h_n)$

Since the entries in position j are arbitrary element of G_j for all j, φ is surjective. Furthermore,

$$\text{Ker}\varphi = \{(g_1, g_2, ...g_n) | g_i = 1 \text{ for all } i \neq j\} = G_i$$

This proves that G_i is a normal subgroup of G (in particular, it again proves this copy of G, is a subgroup) and the First Isomorphism Theorem gives the final assertion of part (a).

b) If x = (1, ...1, g_i, 1, ..., 1) and y = (1, ..., 1, g_i, 1, ..., 1) where the indicated entries appear in positions i, j respectively then xy = (1, ..., 1, g_i, 1,...., 1, g_i,1, ..., 1) = yz where i < j.

Hence Proved.



CHECK YOUR PROGRESS

Q.1. What is the order (8, 56) in $Z_{12} \oplus Z_{60}$

Q.2. Determine the number of elemets of order 5 in $Z_{25} \oplus Z_5$.

Q.3. Determine the number of cyclic subgroups of order 10 in $Z_{100} \oplus Z_{25}$.

5.5 INTERNAL DIRECT PRODUCT (DEFINITIONS AND EXAMPLES)

Definition 5.5.1 : We say that G is the internal direct product of H and K and write G = H × K if H and K are normal subgroups of G and G = HK and $H \cap K = \{e\}$.

Example 10 Consider the group and the following subgroups H = {0, 2, 4}, K = {0, 3}. Note thate {h * k : h ∈ H, k ∈ K } = {0, 1, 2, 3, 4, 5} = G, so the first condition is met. Also the identity for Z_6 is e = 0 and $H \cap K = \{0\}$ so the second condition is met. Lastly, Z_6 is an abelian group so the third condition is met. Which implies (Z_6 +) is internal direct product of subgroups H = {0, 2, 4} and K = (0, 3}.

Definition 5.5.2 Let $H_1, H_2,.....,H_n$ be a finite collection of normal subgroups of G. We say that G is the internal direct product of

$H_1, H_2,.....,H_n$ and write $G = H_1 \times H_2 \times ..... \times H_n$, if

1. $G = H_1H_2.....H_n = \{h_1h_2.....h_n : h \in H_i\}$
2. $(H_1H_2.....H_i) \cap H_{i+1} = \{e\}$ for i =1, 2, ..., n–1.

5.6 PROPERTIES OF INTERNAL DIRECT PRODUCT

Theorem 5.6.1 If a group G is the internal direct product of a finite number of subgroups $H_1H_2.....H_n$ then G is isomorphic to the external direct product of $H_1H_2.....H_n$. In notation.

$$H_1 \times H_2 \times ..... \times H_n \cong H_1 \oplus H_2 \oplus ..... \oplus H_n$$

Proof : We first show that the normality of the H's together with the second condition of the definition guarantees that h's from different H_i's commute. For if $h_i \in H_i$ and $h_j \in H_j$ with $i \neq j$, then

$(h_ih_jh_i^{-1})\, h_j^{-1} \in H_jh_j^{-1} = H_j$ and $h_i\,(h_jh_i^{-1}h_j^{-1})\, h_j^{-1} \in j_iH_i = H_i$

Thus $h_ih_jh_i^{-1}\, h_j^{-1} \in H_i \bigcap H_j = \{e\}$ and therefore $h_ih_j = h_jh_i$. We next claim that each member of G can be expressed uniquely in the form $h_1h_2....h_n$ where $h_i \in H_i$. That there is at least one such representation is the content of condition I of the the definition. To prove uniqueness, suppose that $g = h_1h_2....h_n$ and $g = h_1'h_2'....h_n'$ where h_i and h_i' belongd to H for i =1, 2, ...n.

Then using the fact that the h's from different H_i's commute, we can solve the equation

$$h_1h_2....h_n = h_1'h_2'....h_n'$$

For $h_n'h_n^{-1}$ to obtain

$$h_n'h_n^{-1} = (h_1')^{-1}h_1(h_2')^{-1}h_2....(h_{n-1}')^{-1}\, h_{n-1}$$

But then $h_n'h_n^{-1} \in H_1, H_2,....., H_{n-1} \bigcap H_n = \{e\}$

So that $n_n'h_n^{-1} = e$ and therefore $h_n' = h_n$. At this point we can cancel h_n and h_n' from opposite sides of the equal sign in equation (1) and repeat the preceding argument to obtain $h_{n-1}' = h_{n-1}$. Continue in this fashion , we eventually have $h_i' = h_i$ for i = 1, 2, ..., n. We now define a map $\theta : G \to H_1 \oplus H_2 \oplus ..... \oplus H_n$ by $\theta(h_1h_2....h_n) = (h_1h_2....h_n)$

Then we can easily prove that θ is an isomorphism.



CHECK YOUR PROGRESS

Q.4. Let G = $\langle a \rangle$ be a cyclic group of order 6. Let H = {e, a^2,a^4} and K = {e, a^3). Show that G is a internal direct product of H and K.

Q.5. Show that a group of order is either cyclic or is an internal direct product of two cyclic groups of order 2 each.

Q.6. Let N be normal subgroup of G. If G = H × K where H and K are subgroups of G, then prove that either N is abelian orN intersects H or K non trivially.

Q.7. Show that S_3 can not be written as internal direct product of two non trivial subgroups.

Q.8. If H and K are normal subgroups of G, show that $G/_{H \cap K}$ is isomorphic to a subgroup of $\equiv G/_H \times G/_K$.

5.7 STRUCTURE OF FINITE ABELIAN GROUPS

Definition 5.7.1 A finite abelian group is a nonempty finite set with a binary operation which satisfies, in addition to the group axioms, the commutative law.

Theorem 5.7.2 All cyclic groups are abelian.

Proof : Let G = <g> be a cyclic group of order n. Let r, s, be integers less than n. We want to prove that $g^r g^s = g^s g^r$.

If we expand the left-hand side and apply the associative law, we have

$$g^r g^s = \underbrace{g.g.....g}_{\text{r factors}}.\underbrace{g.g.....g}_{\text{s factors}}$$

$$= \underbrace{g.g.....g}_{\text{s factors}}.\underbrace{g.g.....g}_{\text{r factors}}$$

Theorem 5.7.3 An abelian group G is simple if and only if it is finite and of prime order.

Proof : Suppose G is a simple abelian group. By definition, its only normal subgroups are {e} and G. Since all subgroups of an abelian group

are normal, these are its only subgroups. If g is a non-identity element of G, then <g> = G, so that G is cyclic. Since |G| and 1 must be the only divisors of |G|, hence, |G|, is a prime number.

On the other hand, if G is a finite group of prime order, then it has only trivial subgroups and must be simple.

Example 11 Let S be any finite set and let P(S) represent the set of all subsets of S. P(S) is called the power set of S. For A, $B \in P(S)$, define an operation * by A *B = (A$\bigcap$ B)\(A$\bigcap$ B).

With this operation P(S) is a finite abelian group. The identity element of P(S) is θ and each element of P(S) acts as its own inverse since every non-identity element has order 2. If |S| = n, then |P(S)|= $\sum_{r=0}^{n}\binom{n}{r}=2^n$.

Let S = {a, b, c} then P(S) contains 2^3 = 8 elements and exhibits the following Cayley table.

*	θ	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
ϕ	ϕ	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
{a}	{a}	ϕ	{a, b}	{a, c}	{b}	{c}	{a, b, c}	{b, c}
{b}	{b}	{a, b}	ϕ	{b, c}	{a}	{a, b, c}	{c}	{a, c}
{c}	{c}	{a, c}	{b, c}	ϕ	{a, b, c}	{a}	{b}	{a, b}
{a, b}	{a, b}	{b}	{a}	{a, b, c}	ϕ	{b, c}	{a, c}	{c}
{a, c}	{a, c}	{c}	{a, b, c}	{a}	{b, c}	ϕ	{a, b}	{b}
{b, c}	{b, c}	{a, b, c}	{c}	{b}	{a, c}	{a, b}	ϕ	{a}
{a, b, c}	{a, b, c}	{b, c}	{a, c}	{a, b}	{c}	{b}	{a}	ϕ

So for n > 1, P(S) is a noncyclic abelian group.

Example 12: Let $\{0, 1\}^n$ represent all n-tuples of 0's and 1's. Define an operation of component-wise addition on these n-tuples by = $a_i + b_i$ (mod2) where i represent the ith component. Then $\{0, 1\}^n$ is a finite abelian group of order 2^n. The identity element of $\{0, 1\}^n$ is (0, 0, ..., 0), i.e. the n-tuple consisting of n 0's

Since 0 + 0 = 0 and 1 + 1 = 0 modulo 2, every element is its own inverse. Hence, every non-identity element has order 2. In fact, it should be obvious that $\{0, 1\}^n \approx P(S)$, where |S| = n.

Theorem 5.7.4: (Cauchy's theorem for finite abelian groups) Let G be a finite abelian group and p a prime number such that p divides |G|. Then there exists $a \in G,\ a \neq e$, such that $a^p = e$

Proof : We will use induction on |G|. First, note that the result holds obiously in the case G = {e}. Next, let us assume that the theorem holds for all abelian groups of order smaller than |G|.

If G is a simple group, then by Theorem 5.7.3, it must be a cyclic group of prime order. As a consequence, |G| = p and G contains p – 1 elements $a \neq e$, such that $a^p a^{|G|} = e$.

Suppose instead that G is not simple and has a proper subgroup H. Because H is an abelian group and |H| < |G|, then if p divides |H|, by the induction hypothesis there exists $h \in H,\ h \neq e$ such that $h^p = e$. Since $h \in G$ as well, we have found an element of G which satisfics our requirements. Therefore, we may assume that p does not divide |H|. $H \lhd G$ since G is an abelian group; hence we can form G/H, likewise an abelian group. Since p does not divide |H|, then p must divide $|G/H|$, because $|G/H| = \frac{|G|}{|H|} < |G|$. Since G/H is an abelian group of order less than |G| and since p divides $|G/H|$, the induction hypothesis guarantees the existence of $k \in G/H, k \neq e_{G/H}$ such that $k^p = e_{G/H}$. Now the elements of G/H have the form k = Hb, where $b \in G$, so that $k^p = (Hb)^p = Hb^p$. Since $e_{G/H} = He$, then $k^p = e_{G/H}$, but $k^p \neq e_{G/H}$, implies that $Hb^p = H$, $Hb \neq H$; therefore, $b^p \in H,\ b \neq H$. Therefore $\left(b^p\right)^{|H|} = e$; i.e. $\left(b^{|H|}\right)^{|p} = e$. i.e. $\left(b^{|H|}\right)^{|p} = e$. Let $c = b^{|H|}$, so that $c^p = \left(b^{|H|}\right)^p = e$. We need only establish that $c \neq e$. Suppose, to the contrary, that c = e. Then $\left(b^{|H|}\right)^{|p} = e$ and $(Hb)^{|H|} = H$. But $(Hb)^p = H$ and p does not divide |H|, so Hb = H and $b \in H$, contrary to our previous observation. It follows, then, that

$c \neq e,\ c^p = e$ and our induction is complete.

Corollary 5.7.5: (Sylow's theorem) Let G be a finite abelian group and p a prime number such that p^m divides |G|, but p^{m+1} does not for some positive integer m. Then G has a unique subgroup S of order p^m.

Proof : Sylow's theorem guarantees the existence of S, so we want to show here that S is unique. Suppose that T is another subgroup of G of order p^m, $S \neq T$.

Since S and T are abelian, ST = TS. Now $|ST| = \frac{|S||T|}{|S \cap T|} = \frac{p^m p^m}{|S \cap T|}$.

Since $S \neq T$. $|S \cap T| < p^m$, so $|ST| = p^n$ for some n >m. Because G is an abelian group, ST is a subgroup of G and |ST| divides |G|. This, of couse, implies that p^n divides |G|, hence, we have a contradiction. We must conclude that S = T and that S is the unique Sylow p-subgroup of G.

Recall that Langrange's theorem assets that if G is any finite group, then |G| is divisible by the order of any subgroup of G. In general, the converse of Lagrange's theorem is false, the fact that a given positive integer n divides |G| does not guarantee the existence of a subgroup of G with order n. Once again, however, including commutativity in our assumptions provides a nice result, namely the following partial converse to Langrange's theorem in the finite abelian case.

Theorem 5.7.6: Let G be a finite abelian group. If n divides |G|, then g contains a subgroup of order n.

Proof : If |G| = 1, then the theorem holds trivailly.

Case 1. If |G| is a power of a single prime p, we may write $|G| = p^m$, where m is a positive integer. A divisor of |G|, then, has the general from $|G| = p^{m_i}$ where $1 \leq m_i \leq m$. By Sylow's theorem, G has at least one subgroup corresponding to each such n.

Case 2. If |G| involves powers of more than one distinct prime factor, we may write $|G| = p^{m1} p^{m2} \ldots p^{pk}$ where the p_i's are distinct primes and the $m_i s$ are positive integers. We need to consider four subcases.

(a) $n = p_i,\ 1 \leq i \leq k$. By Cauchy's theorem, if p_i dividing |G|, then G contain an element of order p_i therefore by Sylow's theorem, G must contain a subgroup of order p_i.

(b) $n = p_i^{m_j}, 1 \le i \le k$. If $p_i^{m_j}$ is the maximal power of p_i dividing |G|, then G contains subgroups of order $p_i^{m_j}$ namely the Sylow p_i-subgroups.

(c) $n = p_i^{m_j}, 1 \le i \le k$ and $m_j < m_i$. The same argument applies here as in Case 1. If $p_i^{m_j}$ is the highest power of p_i divides |G|, then G has subgroups of orders $p_i^{m_j}, 1 \le i \le k$.

(d) $n = p_i^{mj} p_r^{ms}$, where $p_i \ne pr$, $1 \le i, r \le k$, $m_j \le m_i$ and $m_s \le m_r$, $1 \le j, s, \le k$. Since G is an abelian group, the product of two of its subgroups is again a subgroup of G. By (c), G has subgroups of order p_i^{mj} and p_r^{ms}; hence, G has a subgroup of order $p_i^{mj} p_r^{ms}$. This result generalizes for all suitable n which contain the products of powers of two or more distinct primes.

Definition 5.7.7: Let G be a group and p a prime number. If the order of every element of G is a power of p, then G is called a p-group. Of course, |G| is likewise a power of p.

Definition 5.7.8: Let G be a finite abelian group and let p be a prime number. Define $G_p = \{g \in G : |g| = p^n$ for some integer $n \ge 0$. We call G_p the p-component of G.

Theorem 5.7.9: (Primary decomposition theorem) Every finite abelian group G is a direct sum of p-groups.

Proof : Assume |G| > 1, since the theorem holds trivially in case |G| = 1. Let P = {p:p divides |G|, p a prime}. Now for $p \in P$, the p-component of G is nonempty since $0 \in G_p$ for all primes $p \in P$. Furthermore, because G is an abelian group, G_p must be a subgroup of G. We want to show that $G = \oplus_{p \in P} G_p$. To do so we must be able to express every $g \in G$ uniquely in the form $\sum_{p \in P} g_p$, where $g_p \in G_p$. Since |G|, we can express |g| as |g| = $\prod_{p \in P} n_p$ where each n_p is a power of p. Next, let $m_p = \frac{|g|}{n_p}$ for each $p \in P$. Since the greatest common divisor of the m_p's is 1, the Euclidean algorithm insures the existence of integers a_p such that $1 = \sum_{p \in P} a_p m_p$. Multiplying both sides by g we get $g = \sum_{p \in P} a_p m_p g$. Now since $n_p(a_p m_p g) = a_p |g| g = 0$, we conclude that $a_p m_p g \in G_p$. Let $g_p = a_p m_p g$ and we have $g = \sum_{p \in P} g_p$ with $g_p \in G_p$.

Suppose that g can also be expressed as $g = \sum_{p \in P} h_p$, with $h_p \in G_p$. Then 0 = g – g = $\sum_{p \in P} g_p - \sum_{p \in P} h_p = \sum_{p \in P} (g_p - h_p)$. Now

$|g_p - h_p|$ must be a power of p; hence $\left|\sum_{p\in P}(g_p - h_p)\right|$ is the least common multiple of the orders to all the $g_p - h_p$. But $\left|\sum_{p\in P}(g_p - h_p)\right| = |0| = 1$, implies that $|g_p - h_p| = 1$ for each $p \in P$. Therefore, $g_p - h_p = 0$; thus, $g_p = h_p$ for all $p \in P$. Hence, the expression of each $g \in G$ as the sum of one element from each p-component of G is unique.

In other words, Theorem 5.7.9 says that the p-groups which do the trick are precisely the p-components. So, alternatively, we can express Theorem as follows : A finite abelian group G is the direct sum of its p-components for the various primes p which divide |G|.

Definition 5.7.10 A mapping f is said to be idempotent if f o f = f.

Theorem 5.7.11 If f is any idempotent endomorphism of a group G with *Im*(f) $\lhd$ G, then $G = \ker f \oplus \mathrm{lm}(f)$.

Proof : Suppose $f : G \to G$ is an idempotent endomorphism such that *Im*(f) $\lhd$ G. We want to show that each $g \in G$ can be represented uniquely as a sum z + y, with z$\in$ kerf and y$\in$ *Im*(f). Now g = (g-f(g)+f(g), where f(g) is obviously in *Im*(f). Since f(g-f(g)) = f(g+f(-g)) = f(g)+f(f(-g) and f of = f, therefore f (g+f(-g) = f(g) + f(-g)) = 0 implies that g - f(g) kerf. To see that this sum is unique, suppose g = z + y with z$\in$ kerf and y$\in$ *Im*(f), so that f(z) = 0 and for some $a \in G, f(a) = y$. Then f(g) = f(z + y) = f(z) + f(y) = 0+f(y)= f(f(a)) = f(a) = y and thus, z = g- f(g).

Theorem 5.7.12: Let G be a finite p-group with $g \in G$ of maximal order. Then $\langle g\rangle$ is a direct summand of G.

Proof : If G = $\langle g\rangle$, we are done; therefore, assume $G \neq \langle g\rangle$. Let $a \in G$. Then $a \notin \langle g\rangle$. Since G is a p-group, then for some positive integer n, $p^n a \notin \langle g\rangle$. Therefore, there exists $b \in G$, $b \notin \langle g\rangle$ such that $pb \in \langle g\rangle$ (fore instance, $b = p^{n-1}a$. Since g is of maximal order, $|g| > |pb|$ and for some integer m, pb = pmg. So 0 = pb – pmg = p(b – mg) and $b - mg \notin \langle g\rangle$, since $b \notin \langle g\rangle$.

However, since |b – mg| = p, it is clear that $\langle b - mg\rangle \bigcap \langle g\rangle = \{0\}$. Thus, there exists a nonzero subgroup, call it S, of G such that $S \bigcap \langle g\rangle = \{0\}$.

Next, consider the quotient group G/S. Note that in G/S. $|S + g| = |g|$ hence, S + g must be an element of maximal order in G/S.

By induction on |G|, since $\left|G/S\right| < |G|$, we conclude that $\langle S + g\rangle$ is a direct summand of G/S. Then the following composition of mappings

$$G \xrightarrow{\theta} G/S \xrightarrow{\varphi} \langle S+g\rangle \xrightarrow{\mu} \langle g\rangle \xrightarrow{\vartheta} G$$

where θ is the natural homomorphism, φ is a projection of G/S onto its direct summand, μ maps m(S + g) to mg and ϑ is an inclusion mapping, is an idempotent endomorphism of G with image $\langle g\rangle$. Hence, by Theorem 5.7.10 $\langle g\rangle$ is a direct summand of G.

Theorem 5.7.13: Every finite abelian p-group G is a direct sum of cyclic groups.

Proof : Let $g \in G$ be of maximal order. By Theorem 5.7.11, there is a subgroup S of G such that G = S + $\langle g\rangle$. Since |S| < |G|, then by induction on |G|, we have that S is a direct sum of cyclic groups; hence, S + $\langle g\rangle$ = G is a direct sum of cyclic groups.

Example 13: For an integer > 1, let U_n represent the collection of all positive integers less than n and relatively prim to n. Under the operation of multiplication modulo n, U_n is a group. U_n called the group of units of Z_n, is simply the reduced residue system modulo n of number theory fame $|U_n| = \phi(n)$, where ϕ is the Euler ϕ-function. If, n = p where p is a prime number, then U_p is a cyclic group; in face, U_p is just Z_p. However, for some values of n, U_n is a noncyclic finite abelian group.

In the preceding theorems we have progressed from finite abelian groups to p-groups to cyclic groups, reducing the complexity of the structure at each step. We are now prepared to state and prove the Fundamental Theorem, which not only assets that we can decompose every finite abelian group, but also that this decomposition is, in a sense, unique.

Theorem 5.7.14: (Fundamental Theorem of Finite Abelian Groups) Every finite abelian group is a direct sum of cyclic groups. Moreover, if G is a finite p-group and if

$$\begin{aligned} G &= G_1 \oplus G_2 \oplus \ldots\ldots \oplus G_m \\ &= H_1 \oplus H_2 \oplus \ldots\ldots \oplus H_n \end{aligned}$$

are direct sum decompositions of G into nonzero cyclic p-groups, then m = n and $G_i \approx H_i$ for all i, after suitable rearrangement of subscripts.

Proof : The first statement, often by itself referred to as the

Fundamental Theorem of Finite Abelian Groups, follows immediately by combining Theorem 5.7.9 and 5.7.12.

We prove the second assertion by induction on m. If m = 1, then G = G_1 is itself a cyclic p-group; therefore, there exists $g \in G$ such that |g| = |G|.

Expressing g in terms of the second decomposition, we have $g = h_1 + h_2 + ... + h_n$.

where $h_i \in H_i$ for all i = 1, 2, ...n. Let |g| = p^t, i.e., t is the least positive integer such that $p^t g = 0$.

Then $0 = p^t g = p^t(h_1 + h_2 + ... + h_n) = p^t h_1 + p^t h_2 + ...p^t h_n$; thus, for all $i, | h_i | \leq p^t$.

Suppose, next, that $| h_i | < p^t$ for all i, say $| h_i | < p^r$, r <t. Then $p^r g = p^r h_1 + p^r h_2 + ... + p^r h_n = 0$, a contradiction since t is the least integer such that $p^t g = 0$. Therefore, we must conclude that for some $i, p^t = | g | = | h_i |$ thus, $| G | = | H_i |$ and $G = H_i$. As a consequence, n = 1 and we have $G_1 \approx H_1$.

Assume now that m > 1. Renumber the G_i so that $| G_1 | \geq | G_i |$ for all $i \geq 2$. Next choose $g_1 \in G$ such that $G = \langle g_1 \rangle$ and wirte $g_1 = h_1 + h_2 + ... + h_n$. Now, as shown above, $| g_1 |$ is the maximum of the $| h_i |$, say $| g_1 | = | h_j |$ for some j. Since $| g_1 | = | G_1 |$ and $| h_j | \leq | H_j |$, we have that $| G_1 | \leq | H_j |$. In a similar fashion, suppose $\langle h_{i'} \rangle = H_j$. Then $h_{j'} = g_{1'} + g_{2'} + ... + g_{m'}$ with $| h_{j'} | \leq | g_{k'} |$, where $| g_{k'} |$ is the maximum of the $| g_{i'} |$. Since $| h_{j'} | = | H_j |$ and $g_{k'} | \leq | G_k |$, we have $| H_j | \leq | G_k |$. Thus, combining these results we see that $| G_1 | = | H_j |$.

Without loss of generality, let j = 1. Now $G_1 \bigcap (H_2 \oplus H_3 \oplus ... ... \oplus H_n) = \{0\}$, since if $tg_1 = t(h_1 + h_2 + ... + h_n) =$, $x_1 + x_2 + ... + x_n$ where $x_i \in H_i$, then $th_1 = 0$ and, in turn, $tg_1 = 0$. Now, since $| G_1 \oplus (H_2 \oplus H_3 \oplus ..... \oplus H_n) | = | H_1 \oplus (H_2 \oplus H_3 \oplus ..... \oplus H_n |$, we have that $G = G_1 \oplus (H_2 \oplus H_3 \oplus ..... \oplus H_n)$. Therefore,

$$G/G_1 \approx G_2 \oplus G_3 \oplus ..... \oplus G_m \approx H_2 \oplus H3 \oplus ... .H_n$$

Let $a : H_2 \oplus H_3 \oplus ... .H_n \to G_2 \oplus G_3 \oplus ... .G_m$ and by the induction hypothesis, $G_i \approx a(H_i)$ for all $i \geq 2$ after suitable resubscripting.

Clearly, $H_i \approx a(H_i)$ for all $i \geq 2$; therefore, $G_i \approx H_i$ for all i. So any two decompositions of a finite p-group G have the same number of summands of a given order.

Example 14: Consider $G = Z_2 \oplus Z_2$ and its cyclic subgroups :

$H_1 = \{(0, 0) (0, 1)\}$

$H_2 = \{(0, 0) (1, 0)\}$

$H_3 = \{(0, 0) (1, 1)\}$

G can be written in the following ways as a direct sum of these cyclic subgroups :

$$G = H_1 \oplus H_2 = H_1 \oplus H_3 = H_2 \oplus H_3$$

while, as the example suggest, there may be several ways to express a given finite abelian group as the direct sum of cyclic groups, the Fundamental Theorem demonstrates that a correspondence exists in these direct sum decompositions between summands of the same order which make the decomposition unique.

Example 15: In Example 11, for|S| = 3, we see that P(S) can be realized as a direct product of cyclic groups by $\langle\{a\}\rangle \times \langle\{b\}\rangle\langle\{c\}\rangle$; hence for $|S| = 3, P(S) \approx Z_2 \oplus Z_2 \oplus Z_2$. In general, then for |S| = 3 P(S) is isomorphic to the direct summand for n copies of Z_2.

Thus, the Fundamental Theorem fully discloses the structure of finite abelian groups. Morever, every finite cyclic group of order n is isomorphic to Z_n and applying this to the case when $n = p^k$, we see that it allows us to almost effortlessly exhibit one group from each isomorphism class to finite abelian groups. In face, to determine the number of distinct isomorphism classes of abelian groups of a given order n, we need only determine all possible ways of factoring n as a power of primes.

Example 16: There are six distinct prime power factorizations of = 108 = $2^2 . 3^3$; thus six isomorphism classes of abelian groups of order 108 exist. Following is a list of one representative from each class :

$$Z_{2^2} \oplus Z_{3^3},\ Z_{2^2} \oplus Z_{3^2} \oplus Z_3,\ Z_{2^2} \oplus Z_3 \oplus Z_3 \oplus Z_3$$

$$Z_2 \oplus Z_2 \oplus Z_{3^3},\ Z_2 \oplus Z_2 \oplus Z_{3^2} \oplus Z_3,\ Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3 \oplus Z_3$$

Example 17: There are six isomorphism classes of abelian groups of order n = 594473 = 11^2. 17^3. To derive a set of class representatives, simply replace the primes 2 and 3 in Example 16 with 11 and 17 respectively.

Generalizing examples 16 and 17, it is clear that there are six isomorphism classes of abelian groups of order n = $p^2.q^3$ for any distinct primes p and q.

If G is a finite p-group, then $G = G_1 \oplus G_2 \oplus ... ... \oplus G_m$, where each G_i is cyclic. For convenience, let us assume throughout this discussion that the G_i are written in descending order of cardinality. Since each of the G_i's is a cyclic group, so each is completely determined by $|G_i|$. Therefore, $\{|G_1|, |G_2|, ..., |G_m|\}$ serves as an invariant of G. The second assertion of the Fundamental Theorem insures that these invariants do not depend on any particular decomposition of G into a direct sum of cyclic groups; i.e if $G \approx H$, then G and H have the same invariants. As a consequence, if we know the invariants $\{i_1, i_2, ..., i_m\}$ of a p-group G, where the i_j are powers of p, say $i_j = p^{k_j}$, we can construct G simply by forming the direct sum $Z_{i_1} \oplus Z_{i_2} \oplus ..... \oplus Z_{i_m}$, where Z_{i_j}, represents the cyclic group of order i_j.

Definition 5.7.25: Let n be an integer. The sequence of positive integers $n_1, n_2, ..., n_r$ where $n_1 \geq n_2 \geq ..... \geq n_r$ is called a partition of n provided that $n = \sum_{i=1}^{r} n_i$. We shall denote the number of partitions of a given integer n by P(n).

Example 18: P (1) - 1 since 1 = 1 is the only partition of 1. P(2) = 2 since 2 = 1+1 = 2. P(4) = 5 since 4 = 1+1+1+1 = 2+1+1=2+2+3+1=4.

Theorem 5.7.16: Let p be a prime number and n a positive integer. The number of nonisomorphic abelian groups of order p^n is equal to P(n).

Proof : Let G be an abelian group of order p^n with invariants $\{i_1, i_2, ..., i_m\}$ such that $i_j = p^{n_j}$ and $n = \sum_{j=1}^{m} n_j$. Then G is the direct sum of cyclic groups $G = G_1 \oplus G_2 \oplus ..... \oplus G_m$, where $|G_j| = p^{n_j}$; i.e. $G_j \approx Z_{p^{n_j}}$. However, there are P(n) distinct partitions of n and, thus P(n) is the number of nonisomorphic abelian groups of order p^n.

Example 19: The number of nonisomorphic abelian groups of order 7^5 is P(5) = 7 since 5 = 1+1+1+1+1=2+1+1+1=3+1+1=4+1=2+2+1=3+2. We can represent the isomorphic classes of abelian groups of order 7^5 as

follows :

$Z_7 \oplus Z_7 \oplus Z_7 \oplus Z_7 \oplus Z_7$, $Z_{7^2} \oplus Z_7 \oplus Z_7 \oplus Z_7$, $Z_{7^3} \oplus Z_7 \oplus Z_7$, $Z_{7^4} \oplus Z_7$, $Z_{7^2} \oplus Z_{7^2} \oplus Z_7$, $Z_{7^3} \oplus Z_{7^2}$, Z_{7^5}

Note that the result in Theorem 5.7.15 is entirely independent of the choice of p. So, for a given n, there are precisely the same number of nonisomorphic abelian groups of orders 2^n, 3^n,..., p^n,...., if p is a prime number.

Using the primary decomposition theorem, we can generalize Theorem 5.7.15 to all finite abelian groups and thus have a means to count the number of nonisomorphic abelian groups of any given order.

Corollary 5.7.17: Let n be a positive integer such that $n = p_1^{n_1}.p_2^{n_2}.....p_m^{n_m}$, whre the $p_i's$ are distinct prime numbers. The number of nonisomorphic abelian groups of order n is equal to $\prod_{i=1}^{m} P(n_i)$.

Proof : Let G_{p_i} be a p_i-component of a group G with $|G_{p_i}| = p_i$. By Theorem 5.7.15, there are $P(n_i)$ such nonisomorphic p_i-components possible. Since $G = G_{p_1} \oplus G_{p_2} \oplus ..... \oplus G_{p_m}$ and $|G| = \prod_{i=1}^{m} |G_{p_i}|$, then there are $\prod_{i=1}^{m} P(n_i)$ nonisomorphic abelian groups of order n.

Example 20: There are 105 nonisomorphic abelian groups of order n = 24149664 = $11^3.7.3^4$, 2^5 since P(3). P(1). P(4). P(5) = 3.1.5.7 = 105.

So far we have examined an invariant for cyclic groups and p-groups only. Our final step is to broaden these results to find the invariant which applies to all finite abelian groups. In this regard, we will expand the result of the second assertion of the Fundamental Theorem to encompass all finite abelian groups.

Since the direct sum of two cyclic groups is cyclic group if and only if their orders are relatively prime. So, in general, if A_1, A_2, ...A_n are cyclic groups such that $(|A_i|,|A_j|) = 1$ whenever $i \neq j$ and $\langle a_i \rangle = A_i$, then $A_1 \oplus A_2 \oplus .....\oplus A_n$ is itself a cyclic group generated by the element $\sum_{j=1}^{n} a_i$.

Theorem 5.7.18: Let G be a finite abelian group. If

$$G = G_1 \oplus G_2 \oplus ... . \oplus G_m$$
$$= H_1 \oplus H_2 \oplus ... . \oplus H_n$$

are direct sum decompositions of G into nonzero cyclic groups with $|G_i|$ divisibe by $|G_{i+1}|$ and $|H_i|$ divisible by $|H_{i+1}|$ for all suitable i, then m = n and $G_i \approx H_i$ for all i.

Proof : Let K be a p-component of G. Then K is the direct sum of the p-components of each G_i i.e. = $\oplus_{i=1}^{m}(G_i)_p$. Since G_i is cyclic, its subgroup $(G_i)_p$ is likewise cyclic. In similar fashion, K= $\oplus_{i=1}^{n}(H_i)_p$. By our assumptions, we have $|(G_i)_p| \geq |(G_{i+1})_p|$ and $|(H_i)_p| \geq |(H_{i+1})_p|$; therefore, we have that $|(G_i)_p| = |(H_i)_p|$, whence $(G_i)_p \approx (H_i)_p$ for all i. SInce this result holds for all p dividing | G | and $G_i = \oplus_{p\in P}(G_i)_p$, $H_i = \oplus_{p\in P}(H_i)_p$ we have that

$G_i \approx H_i$ for all i.



CHECK YOUR PROGRESS

Q.9: Express Z_{12} as a direct sum of its two subgroups.

Q.10: Show that $U_{15} \approx Z_4 \oplus Z_2$



5.8 LET US SUM UP

- Let $G_1, G_2, ..., G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, ..., G_n$ written as $G_1 \oplus G_2 \oplus ..... \oplus G_n$ is the set of all n-tuples for which the *i*th component is an element of G_i and the operation is componenwise. In symbols,

$$G_1 \oplus G_2 \oplus ..... \oplus G_n = \{(g_1, g_2, ..., g_n) | g_i \in G_i\}$$

where $(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n)$. It is understood that each product a_ib_i is performed with the operation of G_i. Note that in the case that each G_i is finite, we have by properties of sets that

$$|G_1 \oplus G_2 \oplus ..... \oplus G_n| = |G_1||G_2| ..... |G_n|$$

- The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2, ..., g_n)| = \text{lcm}(|g_1|, |g_2|, ... |g_n|)$$

● Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if |G| and |H| are relatively prime.

● Suppose s and t are relatively prime. Then U(st) is isomorphic to the external direct product of U(s) and U(t). Moreover, $U_s(st)$ is isomorphic to U(t) and $U_t(st)$ is isomorphic to U(s).

● Let H_1, H_2, ..., H_n be a finite collection of normal subgroups of G. We say that G is the internal direct product of $H_1, H_2, ..., H_n$ and write $G = H_1 \times H_2 \times ..... \times H_n$, if

1. $G = H_1 H_2 ..... H_n = \{h_1 h_2 ..... h_n : h_1 \in H_i\}$
2. $(H_1 H_2 ..... H_i) \cap H_{i+1} = \{e\}$ for i = 1, 2, ..., n–1.

● If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, ..., H_n$, then G is isomorphic to the external direct product of $H_1, H_2, ..., H_n$. In notation

$H_1 \times H_2 \times ..... \times H_n \cong H_1 \oplus H_2 \oplus .... \oplus H_n$.

● Every group of order p^2, where p is a prime is isomorphic to Z_{p^2} or $Z_p \oplus Z_p$

● Let $G_1, G_2, ..., G_n$ be groups and let $G = G_1 \times G_2 \times ..... \times G_n$ be their direct product.

a. For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and arbitrary elements of G_i in posititin i is a subgroup of G isomorphic to G_i. In notation,

$$G_i \cong \{(1, 1, ..., 1, g_i, 1, ..., 1)\} g_i \in G_i\}$$

Then G_i is a normal subgroup G and

$$G/G_i \approx G_1 \times G_2 \times .... \times G_{i-1} \times G_{i+1} \times .... \times G_n$$

b. If $x \in G_i$ and $y \in G_j$ for $i \neq j$, then $xy \neq yx$.

● A finite abelian group is a nonempty finite set with a binary operation which satisfies, in addition to the group axioms, the commutative law.

● An abelian group G is simple if and only if it is finite and of prime order.

● **(Cauchy's theorem for finite abelian groups)** Let G be a finite abelian group and p a prime number such that p dividies |G|. Then there exists $a \in G$, $a \neq e$, such that $a^p = e$.

● Let G be a finite abelian group. If n divides |G|, then G contains a subgroup of order n.

● **(Primary decomposition theorem)** Every finite abelian group G is a direct sum of p-groups.

● If f is any idempotent endomorphism of a group G with $\mathrm{lm}(f) \lhd G$, then G = kerf $\oplus$ lm(f).

● Let G be a finite p-group with $g \in G$ of maximal order. Then $\langle g \rangle$ is a direct summand of G.

● Every finite abelian p-group G is a direct sum of cyclic groups.

● **(Fundamental Theorem of Finite Abelian Groups)** Every finite abelian group is a direct sum of cyclic groups. Moreover, if G is a finite p-group and if

$$G = G_1 \oplus G_2 \oplus \ldots \ldots \oplus G_m$$
$$= H_1 \oplus H_2 \oplus \ldots \ldots \oplus H_n$$

are direct sum decompositions of G into nonzero cyclic p-groups, then m = n and $G_i \approx H_i$ for all i, after suitable rearrangement of subscripts.

● Let p be a prime number and n a positive integer. The number of nonisomorphic abelian groups of order p^n is equal to P(n).

● Let G be a finite abelian group. If

$$G = G_1 \oplus G_2 \oplus \ldots \ldots \oplus G_m$$
$$= H_1 \oplus H_2 \oplus \ldots \ldots \oplus H_n$$

are direct sum decompositions of G into nonzero cyclic groups with $|G_i|$ divisible by $|G_{i+1}|$ and $|H_i|$ divisible by $|H_{i+1}|$ for all suitable i, then m = n and $G_i \approx H_i$ for all i.



5.9 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q.No.1 Since gcd (8, 12) = 4, the order of 8 is $\frac{12}{4} = 3$ in Z_{12}.

The order of 56 in Z_{60} is 15. Since lcm (3, 15)=15, therefore order of (8, 56) is 15 in $Z_{12} \oplus Z_{60}$.

Ans to Q. No. 2

We determine the number of elements of order 5 in $Z_{25} \oplus Z_5$. By Theorem 5.04.01, we may count the number of elements (a, b) in $Z_{25} \oplus Z_5$ with the property that 5 = |(a, b)| = lcm (|a|, |b|). Clearly this requires that either |a| = 5 and |b| = 1 or 5, or |b| = 5 and |a| = 1 or 5. We consider two mutally exclusive cases.

Case 1. |a| = 5 and |b| = 1 or 5. Here there are four choices for a (namely, 5, 10, 15 and 20) and five choices for b. This gives 20 elements of order 5.

Case 2. |a| = 1 and |b| = 5. This time there is one choice for a and four choices for b, so we obtain four more elements of order 5.

Thus $Z_{25} \oplus Z_5$ has 24 elements of order 5.

Ans to Q.No. 3

We determine the number of cyclic subgroups of order 10 in $Z_{100} \oplus Z_{25}$. We begin by counting the number of elements (a, b) of order 10.

Case1. |a| = 10 and |b| = 1 or 5. Since Z_{100} has a unique cyclic subgroup of order 10 and any cyclic group of order 10 has four generators, there are four choices for a. Similarly, there are five choices for b. This gives 20 possibilities for (a, b)

Case 2. |a| = 2 and |b| = 5. Since any finite cyclic group of even order has a unique subgroup of order 2, there is only choice for a. Obviously, there are four choices for b. So, this case yields four more possibilities for (a, b).

Thus $Z_{100} \oplus Z_{25}$ has 24 elements of order 10.

Ans to Q.No. 4

We have G = $\langle a \rangle$ is a cyclic group of order 6 and H = {e, a^2, a^4}, K = {e, a^3}. Then clearly H and K are normal subgroups of G. Also

$$H \cap K = \{e\}$$

and

$$HK = \{e, ea^3, a^3e, a^2a^3, a^4e, a^4a^3\}$$
$$= \{e, a, a^2, a^3, a^4, a^5\}$$

Hence G is internal direct product of H and K.

Ans to Q.No.5

Let G be a non cyclic group of order 4. Then $G \cong K_4 \cong Z_2 \times Z_2$ where $K_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ and Z_2 is a cyclic group of order 2. In view of above problem G is internal direct of two cyclic groups of order 2 each.

Ans to Q. No. 6

Suppose $N \cap H = \{e\}$ and $N \cap K = \{e\}$. Since G = H × K and N is normal in G, therefore nh = hn for all $n \in N, h \in H$ and nk = kn for all $n \in N, k \in K$.

$n_1, n_2 \in N$.

Then $n_2 \in N \Rightarrow n_2 \in G \Rightarrow n_2 = h_2k_2, h_2 \in H, k_3 \in K$.

$$n_1, n_2 = n_1(h_2k_2) = (n_1h_2)k_2 = (h_2n_1)k_2 = h_2(n_1k_2) = (h_2n_1)k_2 = (n_1h_2)k_2$$

$$= n_1(h_2k_2)$$

$$= n_1n_2$$

Hence N is abelian.

Ans to Q. No. 7

Suppose S_3 is an internal direct product of its subgroups H and K where $H \neq \{1\}$ and $K \neq \{1\}$. Then S_3 = HK and $H \cap K = \{1\}$ and H and K are normal in S_3.

Now $|S_3| = 6 = |H||K|$

$\Rightarrow$ either |H| = 2 or |K| = 2 as |H| and |K| > 1.

In S_3, subgroups of order 2 are {1, (12)}, {1, (13)} and {1, (23)} and none of these is normal subgroup of S_3. Hence S_3 can't be written as internal direct product of non trivial subgroups.

Ans to Q. No. 8

Define $\theta : G \to G/H \times G/K$ such that $\theta(x) = (Hx, Kx)$ for all $x \in G$.

Let x = y $\Rightarrow$ Hx = Hy and Kx = Ky

$\Rightarrow$ (Hx, Kx) = (Hy, Ky)

$\Rightarrow \theta(x) = \theta(y)$

Hence is θ well defined.

Let $x, y \in G$. Then $\theta(xy)$ = (Hxy, Kxy)

= (HxHy, KxKy)

= (Hx, Kx) (Hy, Ky)

= θ (x) (y)

Hence θ is a homomorphism. It is obvious that θ is onto. Therefore by fundamental theorem of homomorphism, $G/\ker\theta \cong G/H \times G/K$

Now $\ker\theta$ = identity of $G/H \times G/K$

$$= \{x \in G \mid (Hx, Kx) = (H, K)\}$$

$$= \{x \in G \mid (Hx = H, Kx = K)\}$$

$$= \{x \in G \mid (x \in H, x \in K)\}$$

$$= \{x \in G \mid (x \in H \cap K)\}$$

$$= H \cap K$$

Ans to Q.No. 9

We have Z_{12} = {0,1, ...,11} and |0| = 1, |1| = |5| = |7| = |11| = 12, |2| = |10| = 6, |3| = |9| = 4 = 2^2, |4| = |8| = 3, |6| = 2.

Let $G_1 = \{0,3,6,9\}$ and $G_2 = \{0,4,8\}$

So, by the primary decomposition theorem $Z_{12} = G_1 \oplus G_2$.

Ans to Q. No. 10

We have $U_{15} = \{1,2,4,7,8,11,13,14\}$ is a noncyclic 2-group. Now, 2, 7, 8 and 13 are all elements of maximal order in U_{15}. So, for example, $\langle 2 \rangle$ is a direct factor of U_{15}. In fact, since $\langle 2 \rangle$ = {1, 2, 4, 8} and $\langle 11 \rangle$ = {1, 11}, we can express U_{15} as the direct product of cyclic groups by $U_{15} = \langle 2 \rangle \times \langle 11 \rangle \approx Z_4 \oplus Z_2$



5.10 FURTHER READING

1) Gallian, J. A. Contemporary Abstract Algebra. 9th edition. Cengage Learning, 2015.
2) Bhattacharya, P. B. Jain, S. K. and Nagpaul, S. R. Basic Abstruct Algebra. 2nd edition, Cambridge University Press, 2003.
3) Khanna, V. K. and Bhammbri, S. K. A Course in Abstract Algebra. Vikas Publishing house, 1999.

4) Luther, S. and Passi, I. B. S. Algebra. Vol. I-Groups, Vol. II-Rings, Narosa Publishing House (Vol. I – 1996, Vol. II – 1990).

5) Hungerford, T. W., Algebra. (1974). Springer-Verlag. New York.

6) J. B. Fraleigh, A First Course in Abstract Algebra (4th edition), Narosa Publishing House, New Delhi, 2002.



5.11 MODEL QUESTIONS

Q.1. Let G be a group with identity e_G and let H be a group with identity e_H. Prove that G is isomorphic to $G \oplus \{e_H\}$ and that H is isomorphic to $\{e_G\} \oplus H$.

Q.2. Show that $H \oplus K$ is Abelian if and only if H and K are Abelian.

Q.3. For any two groups G_1 and G_2, prove that $G_1 \oplus G_2$ is isomorphic to $G_2 \oplus G_1$.

Q.4. Prove that the group of complex numbers under addition is isomorphic to $R \oplus R$, where R is group of real numbers under addition.

Q.5. How many elements of order 9 does $Z_3 \oplus Z_9$ have?

Q.6. If H and K are subgroups of a group G such that G = H × K, show that $G/H \cong K$ and $G/K \cong H$.

Q.7. Let G be a group. Let $H = \{(g, g) \mid g \in G\}$, Show that $H \lhd G \times G$ and H is a normal in G × G if and only if G is abelian.

Q.8. Show that the multiplicative group of non zero real numbers in an internal direct product of two non-trivial subgroups.

Q.9. Prove that the group Q of all rational numbers under addition can't be written as direct sum of two non trivial subgroups.

Q.10. Find all the non-isomorphic abelian groups of order

(i) 20 (ii) 360 (iii) 15 (iv) 35

*** ***** ***