Structure Theorem for Finitely Generated Abelian Groups and its Applications

Joyal Roy P

Department of Mathematics (Shift -II)
St. Joseph College(Autonomuos)
Thiruchirapalli-620 002 Tamil Nadu India.

October 20, 2017

Outline

Definition 1.1.

A binary operation $*$ on a nonempty set S is a function from $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$ or simply ab.

Definition 1.1.

A binary operation $*$ on a nonempty set S is a function from $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$ or simply ab.

Definition 1.2.

A non-empty set G with a binary operation $*$ defined on it is a group if it satisfies the following

1. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
2. There is a element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$. (The element e is called the identity element in G.)
3. For every $a \in G$, there is a^{-1} in G such that $a * a^{-1} = a^{-1} * a = e$. ($a^{-1}$ is called the inverse of element a in G.)

Definition 1.1.

A binary operation $*$ on a nonempty set S is a function from $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$ or simply ab.

Definition 1.2.

A non-empty set G with a binary operation $*$ defined on it is a group if it satisfies the following

1. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
2. There is a element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$. (The element e is called the identity element in G.)
3. For every $a \in G$, there is a^{-1} in G such that $a * a^{-1} = a^{-1} * a = e$. ($a^{-1}$ is called the inverse of element a in G.)

A group G is said to be abelian if $a * b$ for all $a, b \in G$.

Definition 1.3.

A non-empty subset H of a group $(G, *)$ is said to be a subgroup of G if

1. For all $a, b \in H$, $a * b \in H$
2. $e \in H$, where e is identity element of G.
3. If $a \in H$, then $a^{-1} \in H$.

Definition 1.3.

A non-empty subset H of a group $(G, *)$ is said to be a subgroup of G if

1. For all $a, b \in H$, $a * b \in H$
2. $e \in H$, where e is identity element of G.
3. If $a \in H$, then $a^{-1} \in H$.

Theorem 1.4 (Lagrange's Theorem).

If G is a finite group and H is a subgroup of G, then order of H divides the order of group G.

Definition 1.3.

A non-empty subset H of a group $(G, *)$ is said to be a subgroup of G if

1. For all $a, b \in H$, $a * b \in H$
2. $e \in H$, where e is identity element of G.
3. If $a \in H$, then $a^{-1} \in H$.

Theorem 1.4 (Lagrange's Theorem).

If G is a finite group and H is a subgroup of G, then order of H divides the order of group G.

Corollary 1.5.

If G is a finite group and $a \in G$, then order of a divides order of G.

Questions

If a set S has n elements, then

1. How many binary operations can be defined on S?

Questions

If a set S has n elements, then

1. How many binary operations can be defined on S?
2. How many of these binary operations gives a group structure on S?

Questions

Given positive integer n

1. How many non-isomorphic groups are there of order n? Among these groups how many of them are abelian?
   or
   Find number of abelian and non-abelian groups of order n up to isomorphism.
   or
   Characterize the groups of order n.

Questions

Given positive integer n

1. How many non-isomorphic groups are there of order n? Among these groups how many of them are abelian?

   or

   Find number of abelian and non-abelian groups of order n up to isomorphism.

   or

   Characterize the groups of order n.

2. What is converse of Lagrange's theorem? Is it true?

Theorem 2.1.

Let G be any group and $a \in G$, then the subset $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

Theorem 2.1.

Let G be any group and $a \in G$, then the subset $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

Definition 2.2.

Let G be any group and $a \in G$. Then $\langle a \rangle$ is called cyclic subgroup of G generated by a.

Theorem 2.1.

Let G be any group and $a \in G$, then the subset $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

Definition 2.2.

Let G be any group and $a \in G$. Then $\langle a \rangle$ is called cyclic subgroup of G generated by a.

Definition 2.3.

Let G be a group. If there exists an element $a \in G$ such that $\langle a \rangle = G$, then G is called cyclic group and a is called a generator of G.

Elementary Properties of Cyclic Groups

1. Every cyclic group is abelian.

Elementary Properties of Cyclic Groups

1. Every cyclic group is abelian.
2. Every group of prime order is cyclic and hence it is abelian.

Elementary Properties of Cyclic Groups

1. Every cyclic group is abelian.
2. Every group of prime order is cyclic and hence it is abelian.
3. Subgroup of a cyclic group is cyclic.

Elementary Properties of Cyclic Groups

1. Every cyclic group is abelian.
2. Every group of prime order is cyclic and hence it is abelian.
3. Subgroup of a cyclic group is cyclic.
4. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a cyclic group with respect to addition modulo n.

Elementary Properties of Cyclic Groups

1. Every cyclic group is abelian.
2. Every group of prime order is cyclic and hence it is abelian.
3. Subgroup of a cyclic group is cyclic.
4. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a cyclic group with respect to addition modulo n.
5. Let G be any cyclic group. If order of G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$, and if order og G is n (finite), then G is isomorphic to $(\mathbb{Z}_n, +_n)$.

Elementary Properties of Cyclic Groups

1. Every cyclic group is abelian.
2. Every group of prime order is cyclic and hence it is abelian.
3. Subgroup of a cyclic group is cyclic.
4. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a cyclic group with respect to addition modulo n.
5. Let G be any cyclic group. If order of G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$, and if order og G is n (finite), then G is isomorphic to $(\mathbb{Z}_n, +_n)$.
6. Let G be a cyclic group. If order of G is infinite, then G has exactly two generators and if order og G is n (finite), then G has exactly $\varphi(n)$ generators.

Elementary Properties of Cyclic Groups

1. Every cyclic group is abelian.
2. Every group of prime order is cyclic and hence it is abelian.
3. Subgroup of a cyclic group is cyclic.
4. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a cyclic group with respect to addition modulo n.
5. Let G be any cyclic group. If order of G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$, and if order og G is n (finite), then G is isomorphic to $(\mathbb{Z}_n, +_n)$.
6. Let G be a cyclic group. If order of G is infinite, then G has exactly two generators and if order og G is n (finite), then G has exactly $\varphi(n)$ generators.
7. If G is a finite cyclic group of order n, then for every divisor d of n G has a unique subgroup of order d.

Remark

If G is a group and $a_1 \in G$ for $i \in I$, then the subgroup H of G generated by $\{a_i : i \in I\}$ has elements precisely those elements of G that are finite products of integral powers of the a_i, where powers of a fixed a_i may occur several times in the product.

Remark

If G is a group and $a_1 \in G$ for $i \in I$, then the subgroup H of G generated by $\{a_i : i \in I\}$ has elements precisely those elements of G that are finite products of integral powers of the a_i, where powers of a fixed a_i may occur several times in the product.

Definition 2.4.

Let G be a group and let $a_i \in G$ for all $i \in I$. The smallest subgroup of G containing $\{a_i : i \in I\}$ is the subgroup generated by $\{a_i : i \in I\}$. If this subgroup is all of G, then $\{a_i : i \in I\}$ generates G and the a_i are generators of G. If there is a finite set $\{a_i : i \in I\}$, that generates G, then G is finitely generated.

Definition 3.1.

Let $G_1, G_2, \ldots, G_n$ be groups. For $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots b_n)$ be any two elements in $\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$, we define $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots b_n)$ to be the element $(a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Then $\prod_{i=1}^{n} G_i$. is a group, the direct product of the groups G_i, under this binary operation.

Example

Consider the groups $\mathbb{Z}_2$ and $\mathbb{Z}_3$. Then
$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1)(0,2), (1,0), (1,1), (1,2)\}$
Here $(1,1)(0,2) = (1,0)$.

Elementry Properties of direct product

Theorem 3.2.

The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{m\times n}$ if and only if m and n are relatively prime, that is, the $gcd(m, n) = 1$.

Elementry Properties of direct product

Theorem 3.2.

The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{m\times n}$ if and only if m and n are relatively prime, that is, the $gcd(m, n) = 1$.

Corollary

The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \ldots m_n}$ if and only if the numbers m_i for $i = 1, 2, \ldots, n$ are such that the g.c.d of any two of them is 1.

Theorem 4.1 (Fundamental Theorem for Finitely Generated Abelian groups or Structure Theorem for Finitely Generated Abelian groups).

Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_k)^{r_k}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number of factors $\mathbb{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.

Remark

Every finite abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_k)^{r_k}}$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers such that $(p_1)^{r_1}(p_2)^{r_2}\ldots(p_k)^{r_k} = o(G)$.

Applications of Structure Theorem

Problem

Find all abelian groups, up to isomorphism, of order 360.
(The phrase up to isomorphism signifies that any abelian group of order 360 should be structurally identical (isomorphic) to one of the groups of order 360 exhibited.)

Applications of Structure Theorem

Problem

Find all abelian groups, up to isomorphism, of order 360.
(The phrase up to isomorphism signifies that any abelian group of order 360 should be structurally identical (isomorphic) to one of the groups of order 360 exhibited.)

Corollary

The number of finite abelian groups of order p^α up to isomorphism, where p is prime, is equal to $\mathfrak{p}(\alpha)$, that is the number of partitions of α.

Applications of Structure Theorem

Corollary

The number of finite abelian groups of order $n = (p_1)^{\alpha_1}(p_2)^{\alpha_2}\dots(p_k)^{\alpha_k}$ up to isomorphism, where $p_1, p_2, \dots p_k$ are distinct primes, is equal to $\mathfrak{p}(\alpha_1)\mathfrak{p}(\alpha_2)\dots\mathfrak{p}(\alpha_k)$.

Applications of Structure Theorem

Corollary

The number of finite abelian groups of order $n = (p_1)^{\alpha_1}(p_2)^{\alpha_2}\dots(p_k)^{\alpha_k}$ up to isomorphism, where $p_1, p_2, \dots p_k$ are distinct primes, is equal to $\mathfrak{p}(\alpha_1)\mathfrak{p}(\alpha_2)\dots\mathfrak{p}(\alpha_k)$.

Theorem 5.1 (Converse of Lagrange's Theorem).

If m divides the order of finite abelian group G, then G has a subgroup of order m.

Applications of Structure Theorem

Definition 5.2.

A group G is decomposable if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is indecomposable.

Applications of Structure Theorem

Definition 5.2.

A group G is decomposable if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is indecomposable.

Theorem 5.3.

The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

Applications of Structure Theorem

Definition 5.2.

A group G is decomposable if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is indecomposable.

Theorem 5.3.

The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

Theorem 5.4.

If m is a square free integer, that is, m is not divisible by the square of any prime, then every abelian group of order m is cyclic.


Thank you