MATH 433

Applied Algebra

Lecture 31:
Isomorphism of groups.
Classification of finite Abelian groups.

Homomorphism of groups

Definition. Let G and H be groups. A function $f : G \to H$ is called a **homomorphism** of the groups if $f(g_1g_2) = f(g_1)f(g_2)$ for all $g_1, g_2 \in G$.

Properties of homomorphisms:

- The identity element e_G in G is mapped to the identity element e_H in H.
- $f(g^{-1}) = (f(g))^{-1}$ for all $g \in G$.
- If K is a subgroup of G, then $f(K)$ is a subgroup of H.
- If L is a subgroup of H, then $f^{-1}(L)$ is a subgroup of G.
- If L is a normal subgroup of H, then $f^{-1}(L)$ is a normal subgroup of G.
- $f^{-1}(e_H)$ is a normal subgroup of G called the **kernel** of f.

Isomorphism of groups

Definition. Let G and H be groups. A function $f : G \to H$ is called an **isomorphism** of the groups if it is bijective and $f(g_1 g_2) = f(g_1)f(g_2)$ for all $g_1, g_2 \in G$.

The group G is said to be **isomorphic** to H if there exists an isomorphism $f : G \to H$. Notation: $G \cong H$.

Theorem Isomorphism is an equivalence relation on the set of all groups.

Classification of groups consists of describing all equivalence classes of this relation and placing every known group into an appropriate class.

Theorem The following features of groups are preserved under isomorphisms: **(i)** the number of elements, **(ii)** the number of elements of a particular order, **(iii)** being Abelian, **(iv)** being cyclic, **(v)** having a subgroup of a particular order or particular index.

Examples of isomorphic groups

- $(\mathbb{R}, +)$ and $(\mathbb{R}_+, \times)$.

An isomorphism $f : \mathbb{R} \to \mathbb{R}_+$ is given by $f(x) = e^x$.

- Any two cyclic groups $\langle g \rangle$ and $\langle h \rangle$ of the same order.

An isomorphism $f : \langle g \rangle \to \langle h \rangle$ is given by $f(g^n) = h^n$ for all $n \in \mathbb{Z}$.

- $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$.

An isomorphism $f : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ is given by $f([a]_6) = ([a]_2, [a]_3)$.

- $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_3 \times \mathbb{Z}_2$.

An isomorphism $f : \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_3 \times \mathbb{Z}_2$ is given by $f([a]_2, [b]_3) = ([b]_3, [a]_2)$.

Examples of isomorphic groups

- $D(3)$ and $S(3)$.

The dihedral group $D(3)$ consists of symmetries of an equilateral triangle. Each symmetry permutes 3 vertices of the triangle, which gives rise to an isomorphism with $S(3)$.

- $GL(2, \mathbb{Z}_2)$ and $S(3)$.

Each matrix in $GL(2, \mathbb{Z}_2)$ defines an invertible linear operator on the vector space $\mathbb{Z}_2^2$. The vector space has only 3 nonzero vectors: $(1, 0)$, $(0, 1)$ and $(1, 1)$, which are permuted by the operator. This gives rise to an isomorphism with $S(3)$.

- Given a homomorphism $f : G \to H$, the quotient group $G/\ker f$ is isomorphic to $f(G)$.

An isomorphism is given by $\phi(gK) = f(g)$ for any $g \in G$, where $K = \ker f$, the kernel of f.

Examples of non-isomorphic groups

- $S(3)$ and $\mathbb{Z}_7$.

$S(3)$ has order 6 while $\mathbb{Z}_7$ has order 7.

- $S(3)$ and $\mathbb{Z}_6$.

$\mathbb{Z}_6$ is Abelian while $S(3)$ is not.

- $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$.

$\mathbb{Z}$ is cyclic while $\mathbb{Z} \times \mathbb{Z}$ is not.

- $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Q}$.

$\mathbb{Z} \times \mathbb{Z}$ is generated by two elements $(1, 0)$ and $(0, 1)$ while $\mathbb{Q}$ cannot be generated by a finite set.

Examples of non-isomorphic groups

- $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \times)$.

$(\mathbb{R} \setminus \{0\}, \times)$ has an element of order 2, namely, -1. In $(\mathbb{R}, +)$, every element different from 0 has infinite order.

- $\mathbb{Z} \times \mathbb{Z}_3$ and $\mathbb{Z} \times \mathbb{Z}$.

$\mathbb{Z} \times \mathbb{Z}_3$ has an element of finite order different from the identity element, e.g., $(0, [1]_3)$, while $\mathbb{Z} \times \mathbb{Z}$ does not.

- $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Orders of elements in $\mathbb{Z}_8$: 1, 2, 4 and 8; in $\mathbb{Z}_4 \times \mathbb{Z}_2$: 1, 2 and 4; in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: only 1 and 2.

- $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Both groups have elements of order 1, 2 and 4. However $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ has $2^3 - 1 = 7$ elements of order 2 while $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has $2^4 - 1 = 15$.

Classification of finite Abelian groups

Let G be an Abelian group. Given elements $g_1, g_2, \dots, g_k$, consider a map $f : \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_k \rangle \to G$ defined by $f(n_1 g_1, n_2 g_2, \dots, n_k g_k) = n_1 g_1 + n_2 g_2 + \cdots + n_k g_k$ for all $n_1, n_2, \dots, n_k \in \mathbb{Z}$. This map is a homomorphism. We say that $g_1, g_2, \dots, g_k$ is a **basis** for G if f is an isomorphism.

Theorem Any finitely generated Abelian group G admits a basis. As a consequence, G is isomorphic to a direct product of cyclic groups.

Theorem Let $n = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$ be the prime factorisation of an integer n. Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_1^{m_2}} \times \cdots \times \mathbb{Z}_{p_s^{m_s}}$.

Main Theorem Any finite Abelian group is isomorphic to a direct product of cyclic groups $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$. Moreover, we can assume that the orders $m_1, m_2, \dots, m_k$ of the cyclic groups are prime powers, in which case this direct product is unique (up to rearrangement of the factors).