MATH 415

Modern Algebra I

Lecture 10: Homomorphisms of groups. Classification of groups.

Homomorphism of groups

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

Examples of homomorphisms:

- Residue modulo n of an integer.

For any $k \in \mathbb{Z}$ let $f(k)$ be the remainder of k under division by n. Then $f : \mathbb{Z} \to \mathbb{Z}_n$ is a homomorphism of the group $(\mathbb{Z}, +)$ onto the group $(\mathbb{Z}_n, +_n)$.

- Fractional part of a real number.

For any $x \in \mathbb{R}$ let $f(x) = \{x\} = x - \lfloor x \rfloor$ (fractional part of x). Then $f : \mathbb{R} \to [0, 1)$ is a homomorphism of the group $(\mathbb{R}, +)$ onto the group $([0, 1), +_1)$.

- Sign of a permutation.

The function $\operatorname{sgn} : S_n \to \{-1, 1\}$ is a homomorphism of the symmetric group S_n onto the multiplicative group $\{-1, 1\}$.

- Determinant of an invertible matrix.

The function $\det : GL(n, \mathbb{R}) \to \mathbb{R} \setminus \{0\}$ is a homomorphism of the general linear group $GL(n, \mathbb{R})$ onto the multiplicative group $\mathbb{R} \setminus \{0\}$.

- Linear transformation.

Any vector space is an abelian group with respect to vector addition. If $f : V_1 \to V_2$ is a linear transformation between vector spaces, then f is also a homomorphism of groups.

- Trivial homomorphism.

Given groups G and H, we define $f : G \to H$ by $f(g) = e_H$ for all $g \in G$, where e_H is the identity element of H.

Properties of homomorphisms

Let $f : G \to H$ be a homomorphism of groups.

- The identity element e_G in G is mapped to the identity element e_H in H.

$f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$. By cancellation in H, we get $f(e_G) = e_H$.

- $f(g^{-1}) = (f(g))^{-1}$ for all $g \in G$.

$f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$. Similarly, $f(g^{-1})f(g) = e_H$. Thus $f(g^{-1}) = (f(g))^{-1}$.

- $f(g^n) = (f(g))^n$ for all $g \in G$ and $n \in \mathbb{Z}$.

- The order of $f(g)$ divides the order of g.

Indeed, $g^n = e_G \implies (f(g))^n = e_H$ for any $n \in \mathbb{N}$.

Properties of homomorphisms

Let $f : G \to H$ be a homomorphism of groups.

- 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 and denoted $\mathrm{Ker}(f)$.

Isomorphism of groups

Definition. Let G and H be groups. A function $f : G \to H$ is called an **isomorphism** of 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 $(\mathbb{R}^+, \cdot)$.

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

Both groups are cyclic groups of order 6.

- $G \times H$ and $H \times G$ (where G and H are groups).

An isomorphism $f : G \times H \to H \times G$ is given by $f(g, h) = (h, g)$ for all $g \in G$ and $h \in H$.

Fundamental Theorem on Homomorphisms

Theorem Given a homomorphism $f : G \to H$, the factor group $G/\operatorname{Ker}(f)$ is isomorphic to $f(G)$.

Idea of the proof. An isomorphism is given by $\phi(gK) = f(g)$ for any $g \in G$, where $K = \operatorname{Ker}(f)$, the kernel of f.

Examples:

- $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $(\mathbb{Z}_n, +_n)$.
- $\mathbb{R}/\mathbb{Z}$ is isomorphic to $([0,1), +_1)$.
- S_n/A_n is isomorphic to $\mathbb{Z}_2$.
- $GL(n,\mathbb{R})/SL(n,\mathbb{R})$ is isomorphic to $(\mathbb{R} \setminus \{0\}, \cdot)$.

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.

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

$(\mathbb{R} \setminus \{0\}, \cdot)$ 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., $(0, 1)$, 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 abelian groups

Theorem 1 Any finitely generated abelian group is isomorphic to a direct product of cyclic groups.

Theorem 2 Any finite abelian group is isomorphic to a direct product of the form $\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_r^{m_r}}$, where $p_1, p_2, \dots, p_r$ are prime numbers and $m_1, m_2, \dots, m_r$ are positive integers.

Theorem 3 Suppose that $\mathbb{Z}^m \times G \cong \mathbb{Z}^n \times H$, where m, n are positive integers and G, H are finite groups. Then $m = n$ and $G \cong H$.

Theorem 4 Suppose that

$$\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_r^{m_r}} \cong \mathbb{Z}_{q_1^{n_1}} \times \mathbb{Z}_{q_2^{n_2}} \times \cdots \times \mathbb{Z}_{q_s^{n_s}},$$

where p_i, q_j are prime numbers and m_i, n_j are positive integers. Then the lists $p_1^{m_1}, p_2^{m_2}, \dots, p_r^{m_r}$ and $q_1^{n_1}, q_2^{n_2}, \dots, q_s^{n_s}$ coincide up to rearranging their elements.