MATH 433

Applied Algebra

Lecture 30:
Isomorphism 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 $f(k) = k \mod n$. Then $f : \mathbb{Z} \to \mathbb{Z}_n$ is a homomorphism of the group $(\mathbb{Z}, +)$ onto the group $(\mathbb{Z}_n, +)$.

- 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.

- Natural projection onto a quotient group.

Given a group G with a normal subgroup H, we define $f : G \to G/H$ by $f(g) = gH$ for all $g \in G$.

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.

$f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$. Also, $f(e_G) = f(e_G)e_H$.
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 $\ker(f)$.

Indeed, the trivial subgroup $\{e_H\}$ is always normal.

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 $g_1, g_2 \in G$. In other words, an isomorphism is a bijective homomorphism.

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 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 $f([a]_6) = ([a]_2, [a]_3)$. Alternatively, both groups are cyclic of order 6.

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

Examples of isomorphic groups

- $G \times H \cong H \times G$.

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

- If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$.

If $f_1 : G_1 \to H_1$ and $f_2 : G_2 \to H_2$ are isomorphisms, then a map $f : G_1 \times G_2 \to H_1 \times H_2$ given by $f(g_1, g_2) = \bigl(f_1(g_1), f_2(g_2)\bigr)$ for all $g_1 \in G_1$ and $g_2 \in G_2$ is also an isomorphism.

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

An isomorphism $\phi : G/\ker f \to f(G)$ 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.

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

$\mathbb{Z}_4$ is cyclic while $\mathbb{Z}_2 \times \mathbb{Z}_2$ 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 $(\mathbb{R} \setminus \{0\}, \times)$.

$(\mathbb{R} \setminus \{0\}, \times)$ 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 finitely generated Abelian groups

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

Theorem 2 Any nontrivial 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 $p_1, p_2, \ldots, p_r$ are prime numbers and $m_1, m_2, \ldots, m_r$ 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 $p_1^{m_1}, p_2^{m_2}, \ldots, p_r^{m_r}$ and $q_1^{n_1}, q_2^{n_2}, \ldots, q_s^{n_s}$ coincide up to rearranging their elements.

- Abelian groups of order 15.

The prime factorisation of 15 is $3 \cdot 5$. It follows from the classification that any Abelian group of order 15 is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_5$. In particular, all such groups are cyclic.

- Abelian groups of order 16.

Since $16 = 2^4$, there are five different ways to represent 16 as a product of prime powers (up to rearranging the factors): $16 = 2^4 = 2^3 \cdot 2 = 2^2 \cdot 2^2 = 2^2 \cdot 2 \cdot 2 = 2 \cdot 2 \cdot 2 \cdot 2$. It follows from the classification that Abelian groups of order 16 form five isomorphism classes represented by groups $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

- Abelian groups of order 36.

There are four ways to decompose 36 as a product of prime powers: $36 = 2^2 \cdot 3^2 = 2^2 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 3^2 = 2 \cdot 2 \cdot 3 \cdot 3$. By the classification, all Abelian groups of order 36 form four isomorphism classes represented by $\mathbb{Z}_4 \times \mathbb{Z}_9$ (the cyclic group), $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Simple groups

Definition. A nontrivial group G is called **simple** if it has no normal subgroups other than the trivial subgroup and G itself.

Examples.

- Cyclic group of a prime order.
- Alternating group $A(n)$ for $n \geq 5$.

Theorem (Jordan, Hölder) For any finite group G there exists a sequence of subgroups $H_0 = \{e\} \triangleleft H_1 \triangleleft \dots \triangleleft H_k = G$ such that H_{i-1} is a normal subgroup of H_i and the quotient group H_i/H_{i-1} is simple. Moreover, the sequence of quotient groups $H_1/H_0, H_2/H_1, \dots, H_k/H_{k-1}$ is determined by G uniquely up to isomorphism and rearranging the terms.

All finite simple groups are classified (up to isomorphism, there are 18 infinite families and 26 sporadic groups). The largest sporadic group (**monster group**) has order $\approx 8 \times 10^{53}$.