MATH 415

Modern Algebra I

Lecture 11:
Classification of groups.
Transformation groups.

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 $f(g_1g_2) = f(g_1)f(g_2)$ 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.

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

Some ideas behind the classification (Theorem 1)

Let G be an abelian group (with additive notation) and $g_1, g_2, \ldots, g_k \in G$. Consider a map $f : \mathbb{Z}^k \to G$ given by $f(n_1, n_2, \ldots, n_k) = n_1 g_1 + n_2 g_2 + \cdots + n_k g_k$ for all $n_1, n_2, \ldots, n_k \in \mathbb{Z}$.

Lemma 1 f is a homomorphism of groups.

In the case $\langle g_1, g_2, \ldots, g_k \rangle = G$, the map f is surjective.

Lemma 2 Any abelian group generated by k elements is isomorphic to a factor group of the group $\mathbb{Z}^k$.

(Crucial) Lemma 3 Given a subgroup H of the group $\mathbb{Z}^k$, there exists an isomorphism $f : \mathbb{Z}^k \to \mathbb{Z}^k$ (i.e., an automorphism of $\mathbb{Z}^k$) such that $f(H) = H_1 \times H_2 \times \cdots \times H_k$, where $H_1, H_2, \ldots, H_k$ are subgroups of $\mathbb{Z}$.

Lemma 4 Suppose $H_i \triangleleft G_i$ for $1 \le i \le k$. Then $(G_1 \times \cdots \times G_k)/(H_1 \times \cdots \times H_k) \cong (G_1/H_1) \times \cdots \times (G_k/H_k)$.

Some ideas behind the classification (Theorem 2)

Lemma 1 The direct product $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is a cyclic group if and only if the numbers $n_1, n_2, \ldots, n_k$ are pairwise coprime.

Lemma 2 Any nontrivial finite cyclic 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.

Proof. Suppose G is a cyclic group of finite order $n > 1$. Let $n = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$ be the prime factorization of the number n. Then the prime powers $p_1^{m_1}, p_2^{m_2}, \ldots, p_r^{m_r}$ are pairwise coprime numbers. It follows that $\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_r^{m_r}}$ is a cyclic group. The order of this direct product is n. Hence it is isomorphic to G as another cyclic group of order n.

In view of Lemma 2, Theorem 2 easily follows from Theorem 1.

Some ideas behind the classification (Theorem 3)

For any group G, let $F(G)$ denote the set of all elements of finite order in G.

Lemma 1 $F(G_1 \times G_2 \times \ldots \times G_k) = F(G_1) \times F(G_2) \times \ldots \times F(G_k)$.

Lemma 2 If a group G is abelian then $F(G)$ is a subgroup of G.

Lemma 3 If $G = \mathbb{Z}^n \times H$, where H is a finite abelian group, then $F(G) = \{\mathbf{0}\} \times H$. As a consequence, $F(G) \cong H$ and $G/F(G) \cong \mathbb{Z}^n$.

Lemma 4 If $\phi : G_1 \to G_2$ is an isomorphism of groups, then $\phi(F(G_1)) = F(G_2)$.

Lemma 5 If $\phi : G_1 \to G_2$ is an isomorphism of groups and H is a normal subgroup of G_1, then $\phi(H)$ is a normal subgroup of G_2, $\phi(H) \cong H$ and $G_2/\phi(H) \cong G_1/H$.

Lemma 6 $\mathbb{Z}^n \cong \mathbb{Z}^m$ only if $n = m$.

Some ideas behind the classification (Theorem 4)

Given a group G and an integer $n > 0$, let $O_n(G)$ denote the number of elements of order n in G and $\widetilde{O}_n(G)$ denote the number of elements $g \in G$ such that $g^n = e_G$.

Lemma 1 $\widetilde{O}_n(G) = \sum_{d|n} O_d(G)$.

Lemma 2 If $G \cong H$ then $O_n(G) = O_n(H)$ and $\widetilde{O}_n(G) = \widetilde{O}_n(H)$ for all $n > 0$.

Lemma 3 $\widetilde{O}_n(G_1 \times G_2 \times \ldots \times G_k) = \widetilde{O}_n(G_1)\widetilde{O}_n(G_2)\ldots\widetilde{O}_n(G_k)$.

Lemma 4 $\widetilde{O}_n(\mathbb{Z}_m) =$ gcd(n, m). In particular, $\widetilde{O}_{p^a}(\mathbb{Z}_{p^b}) = p^{\min(a,b)}$.

Lemma 5 Let $G = \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_r^{m_r}}$, where $p_1, p_2, \ldots, p_r$ are prime numbers and $m_1, m_2, \ldots, m_r$ are positive integers. Then the numbers $\widetilde{O}_n(G)$ determine the list $p_1^{m_1}, p_2^{m_2}, \ldots, p_r^{m_r}$ uniquely up to rearranging its terms.

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 $H_0 = \{e\} \lhd H_1 \lhd \ldots \lhd H_k = G$ such that H_{i-1} is a normal subgroup of H_i and the factor group H_i/H_{i-1} is simple for $1 \leq i \leq k$. Moreover, the sequence of factor groups $H_1/H_0, H_2/H_1, \ldots, H_k/H_{k-1}$ 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 $\approx 8 \times 10^{53}$.

In view of the Jordan-Hölder Theorem, classification of finite groups is reduced to the following problem.

Problem. Given a finite group H and a finite simple group K, classify all groups G such that $N \cong H$ and $G/N \cong K$ for some normal subgroup $N \triangleleft G$.

One solution is $G = H \times K$. Indeed, consider a projection map $p : H \times K \to K$ defined by $p(h, k) = k$. This map is a homomorphism of the group $H \times K$ onto K. We have that $\mathrm{Ker}(p) = H \times \{e_K\}$. Clearly, $\mathrm{Ker}(p) \cong H$. By the Fundamental Theorem on Homomorphisms, $G/\mathrm{Ker}(p) \cong K$. However the direct product need not be the only solution.

Example. $H = \mathbb{Z}_3$, $K = \mathbb{Z}_2$, $G = S_3$.

The symmetric group S_3 has a subgroup, the alternating group $A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$, which is isomorphic to $\mathbb{Z}_3$. The index $(S_3 : A_3)$ equals 2. It follows that A_3 is a normal subgroup and $S_3/A_3 \cong \mathbb{Z}_2$.

Transformation groups

Definition. A **transformation group** is a group where elements are bijective transformations of a fixed set X and the operation is composition.

Examples.

- Symmetric group S_X: all bijective functions $f : X \to X$.
- Translations of the real line: $T_c(x) = x + c$, $x \in \mathbb{R}$.
- $\mathrm{Homeo}(\mathbb{R})$: the group of all invertible functions $f : \mathbb{R} \to \mathbb{R}$ such that both f and f^{-1} are continuous (such functions are called **homeomorphisms**).
- $\mathrm{Homeo}^+(\mathbb{R})$: the group of all increasing functions in $\mathrm{Homeo}(\mathbb{R})$ (those that preserve orientation of the real line).
- $\mathrm{Diff}(\mathbb{R})$: the group of all invertible functions $f : \mathbb{R} \to \mathbb{R}$ such that both f and f^{-1} are continuously differentiable (such functions are called **diffeomorphisms**).

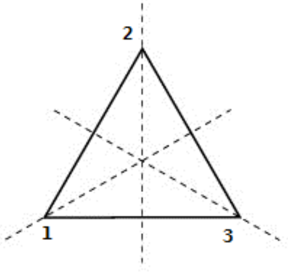
Groups of symmetries

Definition. A transformation $f : \mathbb{R}^n \to \mathbb{R}^n$ is called a **motion** (or a **rigid motion**) if it preserves distances between points.

Theorem All motions of $\mathbb{R}^n$ form a transformation group. Any motion $f : \mathbb{R}^n \to \mathbb{R}^n$ can be represented as $f(\mathbf{x}) = A\mathbf{x} + \mathbf{x}_0$, where $\mathbf{x}_0 \in \mathbb{R}^n$ and A is an orthogonal matrix ($A^T A = AA^T = I$).

Given a geometric figure $F \subset \mathbb{R}^n$, a **symmetry** of F is a motion of $\mathbb{R}^n$ that preserves F. All symmetries of F form a transformation group.

Example. • The **dihedral group** D_n is the group of symmetries of a regular n-gon. It consists of $2n$ elements: n reflections, $n-1$ rotations by angles $2\pi k/n$, $k = 1, 2, \ldots, n-1$, and the identity function.



Equlateral triangle

Any symmetry of a polygon maps vertices to vertices. Therefore it induces a permutation on the set of vertices. Moreover, the symmetry is uniquely recovered from the permutation.

In the case of the equilateral triangle, any permutation of vertices comes from a symmetry.