MATH 415

Modern Algebra I

Lecture 11:
Classification of groups (continued).
Groups of symmetries.
Group actions on a set.

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.

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 $p_1, p_2, \ldots, p_r$ 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.

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 $H_0 = \{e\} \triangleleft H_1 \triangleleft \ldots \triangleleft H_k = G$ 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 several infinite series and 26 sporadic groups).

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 $N \lhd G$.

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 $S_3/A_3 \cong \mathbb{Z}_2$.

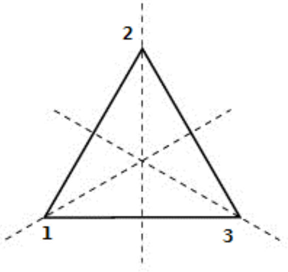
Groups of symmetries

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.

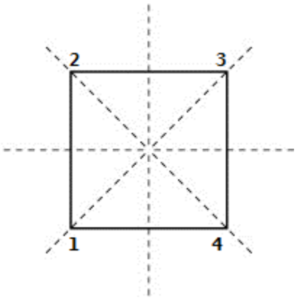
Example. • The **dihedral group** D_n is the group of symmetries of a regular n-gon. It consists of $2n$ elements: n reflections, $n-1$ rotations by angles $2\pi k/n$, $k = 1, 2, \dots, n-1$, and the identity function.



Equlateral triangle

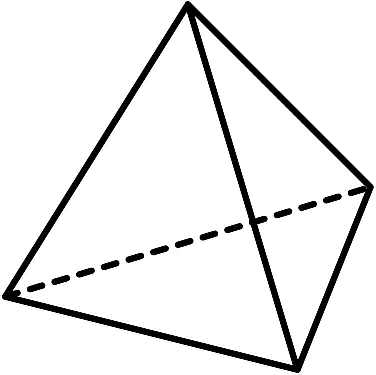
Any symmetry of a polygon maps vertices to vertices. Therefore it induces a permutation on the set of vertices. Moreover, the symmetry is uniquely recovered from the permutation.

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



Square

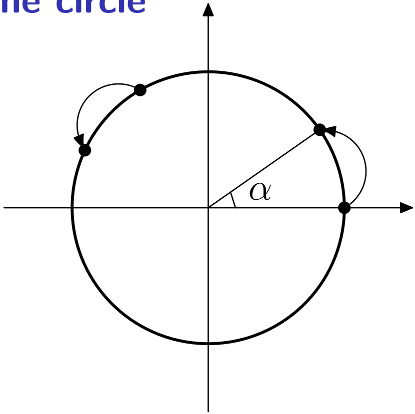
In the case of the square, not every permutation of vertices comes from a symmetry of the square. The reason is that a symmetry must map adjacent vertices to adjacent vertices.



Regular tetrahedron

Any symmetry of a polyhedron maps vertices to vertices. In the case of the regular tetrahedron, any permutation of vertices comes from a symmetry.

Rotations of the circle



Let $R_\alpha : S^1 \to S^1$ be the rotation of the circle S^1 by angle $\alpha \in \mathbb{R}$. All rotations R_α, $\alpha \in \mathbb{R}$ form a transformation group. Namely, $R_\alpha R_\beta = R_{\alpha+\beta}$, $R_\alpha^{-1} = R_{-\alpha}$, and $R_0 = \mathrm{id}$.

The group of rotations is a subgroup of the group of all symmetries of the circle (the other symmetries are reflections).

Group of automorphisms

Definition. Any isomorphism of a group G onto itself is called an **automorphism** of G.

Automorphisms are "symmetries" of the group as an algebraic structure. All automorphisms of a given group G form a transformation group denoted $\mathrm{Aut}(G)$.

Example. • Conjugation.

Take any $g \in G$ and define a map $i_g : G \to G$ by $i_g(x) = gxg^{-1}$. Then $i_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1}$ $= (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$. Hence i_g is a homomorphism. Further, $i_g(i_h(x)) = i_g(hxh^{-1})$ $= g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = i_{gh}(x)$. Hence $i_g \circ i_h = i_{gh}$ for all $g, h \in G$. In particular, $i_g \circ i_{g^{-1}} = i_{g^{-1}} \circ i_g = i_e = \mathrm{id}_G$. Therefore $i_{g^{-1}} = (i_g)^{-1}$ so that i_g is bijective.

Automorphisms of the form i_g are called **inner**. They form a group $\mathrm{Inn}(G)$, which is a normal subgroup of $\mathrm{Aut}(G)$.

Group action

Definition. An **action** ϕ of a group G on a set X (denoted $\phi : G \curvearrowright X$) is a function $\phi : G \times X \to X$ such that

- $\phi(gh, x) = \phi(g, \phi(h, x))$ for all $g, h \in G$ and $x \in M$;
- $\phi(e, x) = x$ for all $x \in X$.

Typically, the element $\phi(g, x)$ is denoted gx. Then the above conditions can be rewritten as $g(hx) = (gh)x$ and $ex = x$.

The action ϕ can (and should) be regarded as a collection of transformations $T_g : X \to X$, $g \in G$, given by $T_g(x) = \phi(g, x)$. It follows from the definition that $T_g T_h = T_{gh}$, $T_{g^{-1}} = T_g^{-1}$, and $T_e = \mathrm{id}_X$. Hence $\{T_g\}_{g \in G}$ is a transformation group and $g \mapsto T_g$ is a homomorphism of the group G to the symmetric group S_X.

The group actions can be used to represent a given group as a transformation group or to parametrize a transformation group by an abstract group.

Examples of group actions

- Trivial action

Any group G acts on any nonempty set X; the action $\phi : G \curvearrowright X$ is given by $\phi(g, x) = x$.

- Scalar multiplication

The multiplicative group $\mathbb{R} \setminus \{0\}$ acts on any vector space V; the action $\phi : \mathbb{R} \setminus \{0\} \curvearrowright V$ is given by $\phi(\lambda, \mathbf{v}) = \lambda\mathbf{v}$.

- Natural action of a transformation group

G is a subgroup of S_X (all permutations of the set X); the action $\phi : G \curvearrowright X$ is given by $\phi(f, x) = f(x)$.

- Koopman representation

G is a subgroup of S_X; it acts on the vector space $\mathcal{F}(X, \mathbb{R})$ of functions $f : X \to \mathbb{R}$ by change of the variable. The action $\phi : G \curvearrowright \mathcal{F}(X, \mathbb{R})$ is given by $\phi(g, f) = f \circ g^{-1}$. Note that $(f \circ g_1^{-1}) \circ g_2^{-1} = f \circ (g_2 g_1)^{-1}$.

Examples of group actions

- Left adjoint action

Any group G acts on itself; the action $\phi : G \curvearrowright G$ is given by $\phi(g, x) = gx$.

- Right adjoint action

Any group G acts on itself; the action $\phi : G \curvearrowright G$ is given by $\phi(g, x) = xg^{-1}$. Note that $(xg_1^{-1})g_2^{-1} = x(g_2 g_1)^{-1}$.

- Conjugation

Any group G acts on itself; the action $\phi : G \curvearrowright G$ is given by $\phi(g, x) = gxg^{-1}$. This action is by automorphisms.

- Action on cosets of a subgroup

Any group G acts on the factor space G/H by a subgroup H (where H need not be normal); the action $\phi : G \curvearrowright G/H$ is given by $\phi(g, xH) = (gx)H$.

An action of the additive group $\mathbb{R}$ is called a **flow**.

Example. Consider an autonomous system of n ordinary differential equations of the first order

$$\begin{cases} \dot{x}_1 = g_1(x_1, x_2, \dots, x_n), \\ \dot{x}_2 = g_2(x_1, x_2, \dots, x_n), \\ \cdots\cdots\cdots \\ \dot{x}_n = g_n(x_1, x_2, \dots, x_n), \end{cases}$$

where $g_1, g_2, \dots, g_n$ are differentiable functions defined in a domain $D \subset \mathbb{R}^n$. In vector form, $\dot{\mathbf{v}} = G(\mathbf{v})$, where $G : D \to \mathbb{R}^n$ is a vector field. Assume that for any $\mathbf{x} \in D$ the initial value problem $\dot{\mathbf{v}} = G(\mathbf{v})$, $\mathbf{v}(0) = \mathbf{x}$ has a unique solution $\mathbf{v}_{\mathbf{x}}(t)$, $t \in \mathbb{R}$. For any $t \in \mathbb{R}$ and $\mathbf{x} \in D$ let $F_t(\mathbf{x}) = \mathbf{v}_{\mathbf{x}}(t)$. Then the maps $F_t : D \to D$, $t \in \mathbb{R}$ describe evolution of a dynamical system governed by the ODEs.

Since the system of ODEs is autonomous, it follows that $F_t F_s = F_{t+s}$ for all $t, s \in \mathbb{R}$ so that $\phi(t, \mathbf{x}) = F_t(\mathbf{x})$ is a flow on D.

Orbits

Suppose $\phi : G \curvearrowright X$ is a group action. Consider a relation $\sim$ on the set X such that $x \sim y$ if and only if $x = gy$ for some $g \in G$.

Proposition The relation $\sim$ is an equivalence relation.

The equivalence class of a point $x \in X$ consists of all points of the form gx, $g \in G$. It is called the **orbit** of x under the action ϕ and denoted Gx or $\mathrm{Orb}_\phi(x)$.

The term "orbit" is motivated by the flows that describe celestial motions.

The action $\phi : G \curvearrowright X$ is called **transitive** if the entire set X forms a single orbit. For example, the adjoint actions of the group G on itself (both left and right) are transitive.

The extreme opposite of a transitive action is the trivial action, for which every point of X is a separate orbit.

Suppose $\phi : G \curvearrowright X$ is a group action.

Given an element $g \in G$, let $\mathrm{Fix}(g) = \{x \in X \mid gx = x\}$. Elements of $\mathrm{Fix}(g)$ are called **fixed points** of g (with respect to the action ϕ).

Given a point $x \in X$, let $\mathrm{Stab}(x) = \{g \in G \mid gx = x\}$. Then $\mathrm{Stab}(x)$ is a subgroup of G called the **stabilizer** (or **isotropy group**) of x.

The action ϕ is called **faithful** if $T_g \neq T_h$ whenever $g \neq h$, where $T_g(x) = gx$. In other words, each element of G acts on X in a distinct way. In the case of a faithful action, the groups G and $\{T_g\}_{g \in G}$ are isomorphic. The action ϕ is called **free** if $\mathrm{Stab}(x) = \{e\}$ for all $x \in X$. It is called **totally non-free** if $\mathrm{Stab}(x) \neq \mathrm{Stab}(y)$ whenever $x \neq y$.

Theorem (Cayley) The left adjoint action of any group G is free and hence faithful. Consequently, any group is isomorphic to a transformation group.