MATH 433

Applied Algebra

Lecture 21:
Basic properties of groups.
Cayley table.
Transformation groups.

Abstract groups

Definition. A **group** is a set G, together with a binary operation $*$, that satisfies the following axioms:

(G1: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G2: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G3: existence of identity)
there exists an element $e \in G$, called the **identity** (or **unit**) of G, such that $e * g = g * e = g$ for all $g \in G$;

(G4: existence of inverse)
for every $g \in G$ there exists an element $h \in G$, called the **inverse** of g, such that $g * h = h * g = e$.

The group $(G, *)$ is said to be **commutative** (or **Abelian**) if it satisfies an additional axiom:

(G5: commutativity) $g * h = h * g$ for all $g, h \in G$.

Basic properties of groups

- The identity element is unique.

Assume that e_1 and e_2 are identity elements. Then $e_1 = e_1 e_2 = e_2$.

- The inverse element is unique.

Assume that h_1 and h_2 are inverses of an element g. Then $h_1 = h_1 e = h_1(gh_2) = (h_1 g)h_2 = eh_2 = h_2$.

- $(ab)^{-1} = b^{-1}a^{-1}$.

We need to show that $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$.
Indeed, $(ab)(b^{-1}a^{-1}) = \big((ab)b^{-1}\big)a^{-1} = \big(a(bb^{-1})\big)a^{-1}$ $= (ae)a^{-1} = aa^{-1} = e$. Similarly, $(b^{-1}a^{-1})(ab) =$ $b^{-1}\big(a^{-1}(ab)\big) = b^{-1}\big((a^{-1}a)b\big) = b^{-1}(eb) = b^{-1}b = e$.

- $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}$.

Basic properties of groups

- **Cancellation properties**: $ab = ac \implies b = c$ and $ba = ca \implies b = c$ for all $a, b, c \in G$.

Indeed, $ab = ac \implies a^{-1}(ab) = a^{-1}(ac)$
$\implies (a^{-1}a)b = (a^{-1}a)c \implies eb = ec \implies b = c$.
Similarly, $ba = ca \implies (ba)a^{-1} = (ca)a^{-1}$
$\implies b(aa^{-1}) = c(aa^{-1}) \implies be = ce \implies b = c$.

- If $hg = g$ or $gh = g$ for some $g \in G$, then h is the identity element.

Indeed, $hg = g \implies hg = eg$. By right cancellation, $h = e$.
Likewise, $gh = g \implies gh = ge$. By left cancellation, $h = e$.

- $gh = e \iff hg = e \iff h = g^{-1}$.

$$gh = e \iff gh = gg^{-1} \iff h = g^{-1} \iff hg = g^{-1}g \iff hg = e$$

Cayley table

A binary operation on a finite set can be given by a **Cayley table** (i.e., "multiplication" table):

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The Cayley table is convenient to check commutativity of the operation (the table should be symmetric relative to the diagonal), cancellation properties (left cancellation holds if each row contains all elements, right cancellation holds if each column contains all elements), existence of the identity element, and existence of the inverse.

However this table is not convenient to check associativity of the operation.

Problem. The following is a partially completed Cayley table for a certain commutative group:

$*$	a	b	c	d
a	b			c
b			c	
c				a
d		d		

Complete the table.

Solution:

$*$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

Transformation groups

Definition. A **transformation group** is a group of bijective transformations of a set X with the operation of composition.

Examples.

- Symmetric group $S(n)$: all permutations of $\{1, 2, \dots, n\}$.
- Alternating group $A(n)$: even permutations of $\{1, 2, \dots, n\}$.
- $\mathrm{Homeo}(\mathbb{R})$: 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 $\mathrm{Homeo}(\mathbb{R})$ (i.e., 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**).

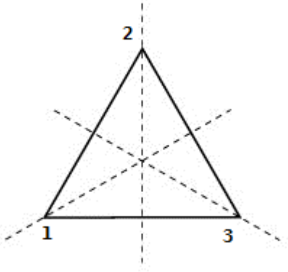
Groups of symmetries

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.