MATH 433

Applied Algebra

Lecture 14:
Further examples of groups.
Semigroups.

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 $g, h \in G$.

Examples

- Real numbers $\mathbb{R}$ with addition.
- Nonzero real numbers $\mathbb{R}$ with multiplication.
- Integers $\mathbb{Z}$ with addition.
- Congruence classes modulo n with addition.
- Invertible congruence classes modulo n with multiplication.
- Symmetric group $S(n)$: permutations of $\{1, 2, \ldots, n\}$ with composition.
- Alternating group $A(n)$: even permutations of $\{1, 2, \ldots, n\}$ with composition.
- Any vector space V with addition.

Matrix groups

A group is called **linear** if its elements are $n \times n$ matrices and the group operation is matrix multiplication.

- **General linear group** $GL(n, \mathbb{R})$ consists of all $n \times n$ matrices that are invertible (i.e., with nonzero determinant).

The identity element is $I = \mathrm{diag}(1, 1, \ldots, 1)$.

- **Special linear group** $SL(n, \mathbb{R})$ consists of all $n \times n$ matrices with determinant 1.

Closed under multiplication since $\det(AB) = \det(A)\det(B)$. Also, $\det(A^{-1}) = (\det(A))^{-1}$.

- **Orthogonal group** $O(n, \mathbb{R})$ consists of all orthogonal $n \times n$ matrices $(A^T A = AA^T = I)$.

- **Special orthogonal group** $SO(n, \mathbb{R})$ consists of all orthogonal $n \times n$ matrices with determinant 1.

$SO(n, \mathbb{R}) = O(n, \mathbb{R}) \cap SL(n, \mathbb{R})$.

Groups of symmetries

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

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.

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.

Basic properties of groups

- The identity element is unique.
- The inverse element is unique.
- $(ab)^{-1} = b^{-1}a^{-1}$.
- $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}$.
- **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, $ba = ca \implies b = c$.

- If $ba = a$ or $ab = a$ for some $a \in G$, then b is the identity element.
- $gh = e \iff hg = e \iff h = g^{-1}$.

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

Semigroups

Definition. A **semigroup** is a nonempty set S, together with a binary operation $*$, that satisfies the following axioms:

(S1: closure)
for all elements g and h of S, $g * h$ is an element of S;

(S2: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in S$.

The semigroup $(S, *)$ is said to be a **monoid** if it satisfies an additional axiom:

(S3: existence of identity) there exists an element $e \in S$ such that $e * g = g * e = g$ for all $g \in S$.

Additional useful properties of semigroups:

(S4: cancellation) $g * h_1 = g * h_2$ implies $h_1 = h_2$ and $h_1 * g = h_2 * g$ implies $h_1 = h_2$ for all $g, h_1, h_2 \in S$.

(S5: commutativity) $g * h = h * g$ for all $g, h \in S$.

Examples of semigroups

- Real numbers $\mathbb{R}$ with multiplication (commutative monoid).
- Positive integers with addition (commutative semigroup with cancellation).
- Positive integers with multiplication (commutative monoid with cancellation).
- Given a set X, all functions $f : X \to X$ with composition (monoid).
- All $n \times n$ matrices with multiplication (monoid).
- Invertible $n \times n$ matrices with integer entries, with multiplication (monoid with cancellation).
- All subsets of a set X with the operation $A * B = A \cup B$ (commutative monoid).
- Positive integers with the operation $a * b = \max(a, b)$ (commutative monoid).

Examples of semigroups

• Given a finite alphabet X, the set X^* of all finite words in X with the operation of concatenation.

If $w_1 = a_1 a_2 \dots a_n$ and $w_2 = b_1 b_2 \dots b_k$, then $w_1 w_2 = a_1 a_2 \dots a_n b_1 b_2 \dots b_k$. This is a monoid with cancellation. The identity element is the empty word.

• The set $S(X)$ of all automaton transformations over an alphabet X with composition.

Any transducer automaton with the input/output alphabet X generates a transformation $f : X^* \to X^*$ by the rule $f(\text{input-word}) = \text{output-word}$. It turns out that the composition of two transformations generated by finite state automata is also generated by a finite state automaton.

Theorem Any finite semigroup with cancellation is actually a group.