MATH 433

Applied Algebra

Lecture 22:
Transformation groups (continued).
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 $g, h \in G$.

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 $\{1, 2, \ldots, n\}$.
- Alternating group $A(n)$: even permutations of $\{1, 2, \ldots, n\}$.
- $\mathrm{Homeo}(\mathbb{R})$: 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**).

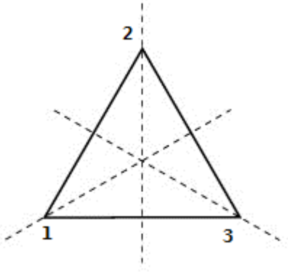
Groups of symmetries

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.

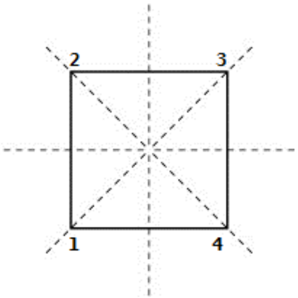
Example. • The **dihedral group** $D(n)$ is the group of symmetries of a regular n-gon. It consists of $2n$ elements: n reflections, $n-1$ rotations by angles $2\pi k/n$, $k = 1, 2, \ldots, n-1$, and the identity function.



Equlateral triangle

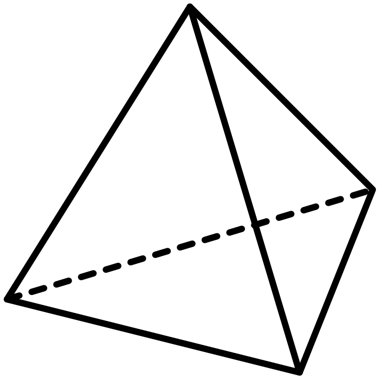
Any symmetry of a polygon maps vertices to vertices. Therefore it induces a permutation on the set of vertices. Moreover, the symmetry is uniquely recovered from the permutation.

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



Square

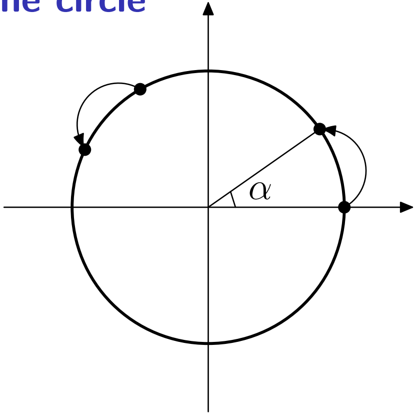
In the case of the square, not every permutation of vertices comes from a symmetry of the square. The reason is that a symmetry must map adjacent vertices to adjacent vertices.



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 part (a **subgroup**) of the group of all symmetries of the circle (the other symmetries are reflections).

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 $(A^T = A^{-1})$.

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

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

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 $g \in S$.

Optional 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

- Clearly, any group is also a semigroup and a monoid.

- Real numbers $\mathbb{R}$ with multiplication (commutative monoid).

- Positive integers with addition (commutative semigroup with cancellation).

- Positive integers with multiplication (commutative monoid with cancellation).

- $\mathbb{Z}_n$, congruence classes modulo n, with multiplication (commutative monoid).

- Given a nonempty set X, all functions $f : X \to X$ with composition (monoid).

- All injective functions $f : X \to X$ with composition (monoid with left cancellation: $g \circ f_1 = g \circ f_2 \implies f_1 = f_2$).

- All surjective functions $f : X \to X$ with composition (monoid with right cancellation: $f_1 \circ g = f_2 \circ g \implies f_1 = f_2$).

Examples of semigroups

- All $n \times n$ matrices with multiplication (monoid).
- All $n \times n$ matrices with integer entries, with multiplication (monoid).
- Invertible $n \times n$ matrices, with multiplication (group).
- Invertible $n \times n$ matrices with integer entries, with multiplication (monoid with cancellation).
- All subsets of a set X with the operation of union (commutative monoid).
- All subsets of a set X with the operation of intersection (commutative monoid).
- Positive integers with the operation $a * b = \max(a, b)$ (commutative monoid).
- Positive integers with the operation $a * b = \min(a, b)$ (commutative semigroup).

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 can also be generated by a finite state automaton.

Powers of an element in a semigroup

Suppose S is a semigroup. Let us use multiplicative notation for the operation on S. The **powers** of an element $g \in S$ are defined inductively:

$$g^1 = g \text{ and } g^{k+1} = g^k g \text{ for every integer } k \geq 1.$$

Theorem Let g be an element of a semigroup G and $r, s \in \mathbb{Z}$, $r, s > 0$. Then **(i)** $g^r g^s = g^{r+s}$, **(ii)** $(g^r)^s = g^{rs}$.

Proof: Both formulas are proved by induction on s.
(i) The base case $s = 1$ follows from the definition: $g^r g^1 = g^r g = g^{r+1}$. The induction step relies on associativity. Assume that $g^r g^s = g^{r+s}$ for some value of s (and all r). Then $g^r g^{s+1} = g^r(g^s g) = (g^r g^s)g = g^{r+s}g = g^{r+(s+1)}$.
(ii) The base case $s = 1$ is trivial: $(g^r)^1 = g^r = g^{r \cdot 1}$. The induction step relies on (i), which has already been proved. Assume that $(g^r)^s = g^{rs}$ for some value of s and all r. Then $(g^r)^{s+1} = (g^r)^s g^r = g^{rs} g^r = g^{rs+r} = g^{r(s+1)}$.

Theorem Any finite semigroup with cancellation is, in fact, a group.

Lemma If S is a finite semigroup with cancellation, then for any $s \in S$ there exists an integer $k \geq 2$ such that $s^k = s$.

Proof: Since S is finite, the sequence $s, s^2, s^3, \ldots$ contains repetitions, i.e., $s^k = s^m$ for some $k > m \geq 1$. If $m = 1$ then we are done. If $m > 1$ then $s^{m-1}s^{k-m+1} = s^{m-1}s$, which implies $s^{k-m+1} = s$.

Proof of the theorem: Take any $s \in S$. By Lemma, we have $s^k = s$ for some $k \geq 2$. Then $e = s^{k-1}$ is the identity element. Indeed, for any $g \in S$ we have $s^k g = sg$ or, equivalently, $s(eg) = sg$. After cancellation, $eg = g$. Similarly, $ge = g$ for all $g \in S$. Finally, for any $g \in S$ there is $n \geq 2$ such that $g^n = g = ge$. Then $g^{n-1} = e$, which implies that $g^{n-2} = g^{-1}$.