MATH 433

Applied Algebra

# Lecture 19:
# Alternating group.
# Abstract groups.

# Sign of a permutation

**Theorem 1** For any $n \geq 2$ there exists a unique function $\mathrm{sgn} : S(n) \to \{-1, 1\}$ such that

- $\mathrm{sgn}(\pi\sigma) = \mathrm{sgn}(\pi)\,\mathrm{sgn}(\sigma)$ for all $\pi, \sigma \in S(n)$,
- $\mathrm{sgn}(\tau) = -1$ for any transposition $\tau$ in $S(n)$.

A permutation $\pi$ is called **even** if it is a product of an even number of transpositions, and **odd** if it is a product of an odd number of transpositions. It turns out that $\pi$ is even if $\mathrm{sgn}(\pi) = 1$ and odd if $\mathrm{sgn}(\pi) = -1$.

**Theorem 2 (i)** $\mathrm{sgn}(\pi\sigma) = \mathrm{sgn}(\pi)\,\mathrm{sgn}(\sigma)$ for any $\pi, \sigma \in S(n)$.
**(ii)** $\mathrm{sgn}(\pi^{-1}) = \mathrm{sgn}(\pi)$ for any $\pi \in S(n)$.
**(iii)** $\mathrm{sgn}(\mathrm{id}) = 1$.
**(iv)** $\mathrm{sgn}(\tau) = -1$ for any transposition $\tau$.
**(v)** $\mathrm{sgn}(\sigma) = (-1)^{r-1}$ for any cycle $\sigma$ of length $r$.

# Alternating group

Given an integer $n \geq 2$, the **alternating group** on $n$ symbols, denoted $A_n$ or $A(n)$, is the set of all even permutations in the symmetric group $S(n)$.

**Theorem (i)** For any two permutations $\pi, \sigma \in A(n)$, the product $\pi\sigma$ is also in $A(n)$.
**(ii)** The identity function $\mathrm{id}$ is in $A(n)$.
**(iii)** For any permutation $\pi \in A(n)$, the inverse $\pi^{-1}$ is in $A(n)$.

In other words, the product of even permutations is even, the identity function is an even permutation, and the inverse of an even permutation is even.

**Theorem** The alternating group $A(n)$ has $n!/2$ elements.

*Proof:* Consider the function $F : A(n) \to S(n) \setminus A(n)$ given by $F(\pi) = (1\ 2)\pi$. One can observe that $F$ is bijective. It follows that the sets $A(n)$ and $S(n) \setminus A(n)$ have the same number of elements.

*Examples.* • The alternating group $A(3)$ has 3 elements: the identity function and two cycles of length 3, $(1\ 2\ 3)$ and $(1\ 3\ 2)$.

• The alternating group $A(4)$ has 12 elements of the following **cycle shapes**: $\mathrm{id}$, $(1\ 2\ 3)$, and $(1\ 2)(3\ 4)$.

• The alternating group $A(5)$ has 60 elements of the following cycle shapes: $\mathrm{id}$, $(1\ 2\ 3)$, $(1\ 2)(3\ 4)$, and $(1\ 2\ 3\ 4\ 5)$.

# 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 examples.* • Real numbers $\mathbb{R}$ with addition.

(G1) $x, y \in \mathbb{R} \implies x + y \in \mathbb{R}$

(G2) $(x + y) + z = x + (y + z)$

(G3) the identity element is 0 as $x + 0 = 0 + x = x$

(G4) the inverse of $x$ is $-x$ as $x + (-x) = (-x) + x = 0$

(G5) $x + y = y + x$

• Nonzero real numbers $\mathbb{R} \setminus \{0\}$ with multiplication.

(G1) $x \neq 0$ and $y \neq 0 \implies xy \neq 0$

(G2) $(xy)z = x(yz)$

(G3) the identity element is 1 as $x1 = 1x = x$

(G4) the inverse of $x$ is $x^{-1}$ as $xx^{-1} = x^{-1}x = 1$

(G5) $xy = yx$

The two basic examples give rise to two kinds of notation for a general group $(G, *)$.

**Multiplicative notation:** We think of the group operation $*$ as some kind of multiplication, namely,

- $a * b$ is denoted $ab$,
- the identity element is denoted 1,
- the inverse of $g$ is denoted $g^{-1}$.

**Additive notation:** We think of the group operation $*$ as some kind of addition, namely,

- $a * b$ is denoted $a + b$,
- the identity element is denoted 0,
- the inverse of $g$ is denoted $-g$.

*Remark.* Default notation is multiplicative (but the identity element may be denoted $e$ or $\mathrm{id}$ or $1_G$). The additive notation is used only for commutative groups.