MATH 433

Applied Algebra

Lecture 19:
Alternating group.
Abstract groups.

Sign of a permutation

Theorem 1 (i) Any permutation is a product of transpositions.
(ii) If $\pi = \tau_1\tau_2\ldots\tau_n = \tau_1'\tau_2'\ldots\tau_m'$, where τ_i, τ_j' are transpositions, then the numbers n and m are of the same parity.

A permutation π 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.

The **sign** $\operatorname{sgn}(\pi)$ of the permutation π is defined to be $+1$ if π is even, and -1 if π is odd.

Theorem 2 (i) $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$ for any $\pi, \sigma \in S(n)$.
(ii) $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$ for any $\pi \in S(n)$.
(iii) $\operatorname{sgn}(\mathrm{id}) = 1$.
(iv) $\operatorname{sgn}(\tau) = -1$ for any transposition τ.
(v) $\operatorname{sgn}(\sigma) = (-1)^{r-1}$ for any cycle σ 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 id is in $A(n)$.
(iii) For any permutation $\pi \in A(n)$, the inverse π^{-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**: id, $(1\ 2\ 3)$, and $(1\ 2)(3\ 4)$.

• The alternating group $A(5)$ has 60 elements of the following cycle shapes: 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 id). The additive notation is used only for commutative groups.

More examples

- Integers $\mathbb{Z}$ with addition.

(G1) $a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z}$

(G2) $(a + b) + c = a + (b + c)$

(G3) the identity element is 0 as $a + 0 = 0 + a = a$ and $0 \in \mathbb{Z}$

(G4) the inverse of $a \in \mathbb{Z}$ is $-a$ as $a + (-a) = (-a) + a = 0$ and $-a \in \mathbb{Z}$

(G5) $a + b = b + a$

More examples

- The set $\mathbb{Z}_n$ of congruence classes modulo n with addition.

(G1) $[a], [b] \in \mathbb{Z}_n \implies [a] + [b] = [a + b] \in \mathbb{Z}_n$

(G2) $([a] + [b]) + [c] = [a + b + c] = [a] + ([b] + [c])$

(G3) the identity element is [0] as $[a] + [0] = [0] + [a] = [a]$

(G4) the inverse of $[a]$ is $[-a]$ as $[a] + [-a] = [-a] + [a] = [0]$

(G5) $[a] + [b] = [a + b] = [b] + [a]$

More examples

- The set G_n of invertible congruence classes modulo n with multiplication.

A congruence class $[a]_n \in \mathbb{Z}_n$ belongs to G_n if $\gcd(a, n) = 1$.

(G1) $[a]_n, [b]_n \in G_n \implies \gcd(a, n) = \gcd(b, n) = 1$
$\implies \gcd(ab, n) = 1 \implies [a]_n[b]_n = [ab]_n \in G_n$

(G2) $([a][b])[c] = [abc] = [a]([b][c])$

(G3) the identity element is $[1]$ as $[a][1] = [1][a] = [a]$

(G4) the inverse of $[a]$ is $[a]^{-1}$ by definition of $[a]^{-1}$

(G5) $[a][b] = [ab] = [b][a]$

More examples

- Permutations $S(n)$ with composition ($=$ multiplication).

(G1) π and σ are bijective functions from the set $\{1, 2, \ldots, n\}$ to itself $\implies$ so is $\pi\sigma$

(G2) $(\pi\sigma)\tau$ and $\pi(\sigma\tau)$ applied to k, $1 \leq k \leq n$, both yield $\pi(\sigma(\tau(k)))$.

(G3) the identity element is id as $\pi\,\mathrm{id} = \mathrm{id}\,\pi = \pi$

(G4) the inverse of π is π^{-1} by definition of the inverse function

(G5) fails for $n \geq 3$ as $(1\ 2)(2\ 3) = (1\ 2\ 3)$ while $(2\ 3)(1\ 2) = (1\ 3\ 2)$.

More examples

- Even permutations $A(n)$ with multiplication.

(G1) π and σ are even permutations $\implies \pi\sigma$ is even

(G2) $(\pi\sigma)\tau = \pi(\sigma\tau)$ holds in $A(n)$ as it holds in a larger set $S(n)$

(G3) the identity element from $S(n)$, which is id, is an even permutation, hence it is the identity element in $A(n)$ as well

(G4) π is an even permutation $\implies \pi^{-1}$ is also even

(G5) fails for $n \geq 4$ as $(1\ 2\ 3)(2\ 3\ 4) = (1\ 2)(3\ 4)$ while $(2\ 3\ 4)(1\ 2\ 3) = (1\ 3)(2\ 4)$.

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, $(b^{-1}a^{-1})(ab) =$
$b^{-1}\big(a^{-1}(ab)\big) = b^{-1}\big((a^{-1}a)b\big) = b^{-1}(eb) = b^{-1}b = e$.

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