MATH 433

Applied Algebra

Lecture 20:
Abstract groups (continued).

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: numbers

- Real numbers $\mathbb{R}$ with addition.

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

- 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) $a + b = b + a$

Examples: modular arithmetic

- 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) $[a] + [b] = [a+b] = [b] + [a]$

Examples: modular arithmetic

- 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) $[a][b] = [ab] = [b][a]$

Examples: permutations

• Symmetric group $S(n)$: all permutations on n elements 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 permutation π^{-1} satisfies $\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}$ (conversely, if $\pi\sigma = \sigma\pi = \mathrm{id}$, then $\sigma = \pi^{-1}$)

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

Examples: permutations

• Alternating group $A(n)$: even permutations on n elements with composition (= 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 $\implies$ π^{-1} is also even

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

Examples: set theory

- All subsets of a set X with the operation of symmetric difference: $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

(G1) $A, B \subset X \implies A \triangle B \subset X$.

(G2) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ consists of those elements of X that belong to an odd number of sets A, B, C (either to just one of them or to all three)

(G3) the identity element is the empty set $\emptyset$ since $A \triangle \emptyset = \emptyset \triangle A = A$ for any set A

(G4) the inverse of a set $A \subset X$ is A itself: $A \triangle A = \emptyset$

(G5) $A \triangle B = B \triangle A = (A \cup B) \setminus (A \cap B)$

Examples: logic

- Binary logic $\mathcal{L} = \{\text{"true"}, \text{"false"}\}$ with the operation XOR (eXclusive OR): "x XOR y" means "either x or y (but not both)".

(G1) "true XOR false" = "false XOR true" = "true",
"true XOR true" = "false XOR false" = "false"

(G2) "(x XOR y) XOR z" = "x XOR (y XOR z)"

(G3) the identity element is "false"

(G4) the inverse of $x \in \mathcal{L}$ is x itself

(G5) "x XOR y" = "y XOR x"

More examples

- Any vector space V with addition.

Those axioms of the vector space that involve only addition are exactly axioms of the commutative group.

- Trivial group $(G, *)$, where $G = \{e\}$ and $e * e = e$.

Verification of all axioms is straightforward.

- Positive real numbers with the operation $x * y = 2xy$.

(G1) $x, y > 0 \implies 2xy > 0$
(G2) $(x * y) * z = x * (y * z) = 4xyz$
(G3) the identity element is $\frac{1}{2}$ as $x * e = x$ means $2ex = x$
(G4) the inverse of x is $\frac{1}{4x}$ as $x * y = \frac{1}{2}$ means $4xy = 1$
(G5) $x * y = y * x = 2xy$

Counterexamples

- Real numbers $\mathbb{R}$ with multiplication.

0 has no inverse.

- Positive integers with addition.

No identity element.

- Nonnegative integers with addition.

No inverse element for positive numbers.

- Odd permutations with multiplication.

The set is not closed under the operation.

- Integers with subtraction.

The operation is not associative: $(a-b)-c = a-(b-c)$ only if $c = 0$.

- All subsets of a set X with the operation $A * B = A \cup B$.

The operation is associative and commutative, the empty set is the identity element. However there is no inverse for a nonempty set.

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

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