MATH 415

Modern Algebra I

Lecture 5: Examples and properties of groups.

Groups

Definition. A **group** is a binary structure $(G, *)$ that satisfies the following axioms:

(G0: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G1: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G2: 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 $g \in G$;

(G3: 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:

(G4: 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.

(G0) $a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z}$

(G1) $(a + b) + c = a + (b + c)$

(G2) the identity element is 0 as $a + 0 = 0 + a = a$ and $0 \in \mathbb{Z}$

(G3) the inverse of $a \in \mathbb{Z}$ is $-a$ as $a + (-a) = (-a) + a = 0$ and $-a \in \mathbb{Z}$

(G4) $a + b = b + a$

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 $-g$.

Remarks. Default notation is multiplicative (but the identity element may be denoted e or id or 1_G). The additive notation may be used only for commutative groups.

Example: addition modulo n

Given a natural number n, let
$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$.
A binary operation $+_n$ (**addition modulo** n) on $\mathbb{Z}_n$ is defined for any $x, y \in \mathbb{Z}_n$ by

$$x +_n y = \begin{cases} x + y & \text{if } x + y < n, \\ x + y - n & \text{if } x + y \geq n. \end{cases}$$

Now let n be a positive real number and $\mathbb{R}_n = [0, n)$. The binary operation $+_n$ on $\mathbb{R}_n$ is defined by the same formula as above.

Theorem Each $(\mathbb{Z}_n, +_n)$ and each $(\mathbb{R}_n, +_n)$ is a group. All groups $(\mathbb{R}_n, +_n)$ are isomorphic.

Example: invertible functions

- Symmetric group $S(X)$: all bijective functions $\pi : X \to X$ with composition ($=$ multiplication).

(G0) π and σ are bijective functions from the set X to itself $\implies$ so is $\pi\sigma$

(G1) $(\pi\sigma)\tau$ and $\pi(\sigma\tau)$ applied to $x \in X$ both yield $\pi(\sigma(\tau(x)))$

(G2) the identity element is the identity function id_X as $\pi\,\mathrm{id}_X = \mathrm{id}_X\,\pi = \pi$

(G3) the inverse function π^{-1} satisfies $\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}_X$ (conversely, if $\pi\sigma = \sigma\pi = \mathrm{id}_X$, then $\sigma = \pi^{-1}$)

(G4) fails if the set has more than 2 elements

Example: set theory

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

(G0) $A, B \subseteq X \implies A \triangle B \subseteq X$.

(G1) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ 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)

(G2) the identity element is the empty set $\emptyset$ since $A \triangle \emptyset = \emptyset \triangle A = A$ for any set A

(G3) the inverse of a set $A \subseteq X$ is A itself: $A \triangle A = \emptyset$

(G4) $A \triangle B = B \triangle A = (A \cup B) \setminus (A \cap B)$

Example: 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)”.

(G0) $\text{“true XOR false”} = \text{“false XOR true”} = \text{“true”}$,
$\text{“true XOR true”} = \text{“false XOR false”} = \text{“false”}$

(G1) “$(x \ \mathrm{XOR} \ y) \ \mathrm{XOR} \ z$”=“$x \ \mathrm{XOR} \ (y \ \mathrm{XOR} \ z)$”

(G2) the identity element is “false”

(G3) the inverse of $x \in \mathcal{L}$ is x itself

(G4) “$x \ \mathrm{XOR} \ y$”=“$y \ \mathrm{XOR} \ x$”

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 $x * y = 2xy$.

(G0) $x, y > 0 \implies 2xy > 0$
(G1) $(x * y) * z = x * (y * z) = 4xyz$
(G2) the identity element is $\frac{1}{2}$ as $x * e = x$ means $2ex = x$
(G3) the inverse of x is $\frac{1}{4x}$ as $x * y = \frac{1}{2}$ means $4xy = 1$
(G4) $x * y = y * x = 2xy$

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.

- Irrational numbers with addition.

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

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

Basic properties of groups

- **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, $ba = ca \implies (ba)a^{-1} = (ca)a^{-1}$
$\implies b(aa^{-1}) = c(aa^{-1}) \implies be = ce \implies b = c$.

- If $hg = g$ or $gh = g$ for some $g \in G$, then h is the identity element.

Indeed, $hg = g \implies hg = eg$. By right cancellation, $h = e$.
Likewise, $gh = g \implies gh = ge$. By left cancellation, $h = e$.

- $gh = e \iff hg = e \iff h = g^{-1}$.

$$gh = e \iff gh = gg^{-1} \iff h = g^{-1} \iff hg = g^{-1}g \iff hg = e$$