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

- Real numbers $\mathbb{R}$ with addition.
- Nonzero real numbers $\mathbb{R}$ with multiplication.
- Integers $\mathbb{Z}$ with addition.
- Congruence classes modulo n with addition.
- Invertible congruence classes modulo n with multiplication.
- Symmetric group $S(n)$: permutations of $\{1, 2, \ldots, n\}$ with composition.
- Alternating group $A(n)$: even permutations of $\{1, 2, \ldots, n\}$ with composition.

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.
- The inverse element is unique.
- $(ab)^{-1} = b^{-1}a^{-1}$.
- $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}$.
- **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, $ba = ca \implies b = c$.

- If $hg = g$ or $gh = g$ for some $g \in G$, then h is the identity element.
- $gh = e \iff hg = e \iff h = g^{-1}$.

Cayley table

A binary operation on a finite set can be given by a **Cayley table** (i.e., “multiplication” table):

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The Cayley table is convenient to check commutativity of the operation (the table should be symmetric relative to the diagonal), cancellation properties (left cancellation holds if each row contains all elements, right cancellation holds if each column contains all elements), existence of the identity element, and existence of the inverse.

However this table is not convenient to check associativity of the operation.

Problem. The following is a partially completed Cayley table for a certain commutative group:

$*$	a	b	c	d
a	b			c
b			c	
c				a
d		d		

Complete the table.

Solution:

$*$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

$*$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

This is the Cayley table of the group $(G_8, \cdot)$ of invertible congruence classes modulo 8 with mutiplication. Namely, $a = [3]_8$, $b = [1]_8$, $c = [5]_8$ and $d = [7]_8$.

Theorem If a group is not commutative, then it has at least 5 elements.

Idea of the proof: Let g and h be two elements of the group that do not commute: $gh \neq hg$. Let 1 denote the unit element. Then the following elements are all distinct: $1, g, h, gh, hg$.

Theorem If a group is not commutative, then it has at least 6 elements.

Idea of the proof: In addition to $1, g, h, gh, hg$, the sixth element is g^{-1} or ghg^{-1}. One first checks that g^{-1} is different from all 5 elements except, possibly, g. Further, ghg^{-1} is different from all 5 elements except, possibly, hg. Finally, the equalities $g^{-1} = g$ and $ghg^{-1} = hg$ cannot hold simultaneously as otherwise we would get $ghg = hg$, which would imply $g = 1$, a contradiction.