Lecture 13: Examples of groups.
Abstract groups

Definition. A group is a set $G$, together with a binary operation $\ast$, that satisfies the following axioms:

(G1: closure)
for all elements $g$ and $h$ of $G$, $g \ast h$ is an element of $G$;

(G2: associativity)
$(g \ast h) \ast k = g \ast (h \ast k)$ 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 $e \ast g = g \ast e = g$ 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 $g \ast h = h \ast g = e$.

The group $(G, \ast)$ is said to be commutative (or Abelian) if it satisfies an additional axiom:

(G5: commutativity) $g \ast h = h \ast g$ 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 \((G, \ast)\).

**Multiplicative notation:** We think of the group operation \(\ast\) as some kind of multiplication, namely,

- \(a \ast b\) 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 \(\ast\) as some kind of addition, namely,

- \(a \ast b\) 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 \(\text{id}\)). 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) $[a][b] = [ab] = [b][a]$
• Permutations $S(n)$ with composition ($=$ multiplication).

(G1) $\pi$ and $\sigma$ 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 $\pi \text{id} = \text{id} \pi = \pi$

(G4) the inverse of $\pi$ is $\pi^{-1}$ 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) $\pi$ and $\sigma$ 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 $\text{id}$, is an even permutation, hence it is the identity element in $A(n)$ as well

  (G4) $\pi$ 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 $(2\ 3\ 4)(1\ 2\ 3) = (1\ 3)(2\ 4)$. 
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 $(G, \ast)$, where $G = \{e\}$ and $e \ast e = e$.
  Verification of all axioms is straightforward.

• Positive real numbers with the operation $x \ast y = 2xy$.

  (G1) $x, y > 0 \implies 2xy > 0$
  (G2) $(x \ast y) \ast z = x \ast (y \ast z) = 4xyz$
  (G3) the identity element is $\frac{1}{2}$ as $x \ast e = x$ means $2ex = x$
  (G4) the inverse of $x$ is $\frac{1}{4x}$ as $x \ast y = \frac{1}{2}$ means $4xy = 1$
  (G5) $x \ast y = y \ast x = 2xy$
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 $A \ast B = A \cup B$. 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 $h_1 = h_1 e = h_1(gh_2) = (h_1 g)h_2 = e h_2 = h_2$.

• $(ab)^{-1} = b^{-1} a^{-1}$.
We need to show that $(ab)(b^{-1} a^{-1}) = (b^{-1} a^{-1})(ab) = e$. Indeed, $(ab)(b^{-1} a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$. Similarly, $(b^{-1} a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$.

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