Groups

**Definition**: A set $G$ with a binary operation $\circ$ is called a group if

1. $x \circ y \in G$ if $x, y \in G$  
2. $x \circ (y \circ z) = (x \circ y) \circ z$ for any $x, y, z \in G$  
3. $\exists e \in G$ s.t. $x \circ e = e \circ x = x$ for all $x \in G$  
4. $x \in G \Rightarrow \exists x^{-1} \in G$ s.t. $x \circ x^{-1} = x^{-1} \circ x = e$

- $e$ is called the identity element of $G$  
- $x^{-1}$ is called the inverse of $x$

**Exercise**: Show that the identity element is unique.

**Show that for each $x$, the inverse of $x$ is unique.**

e.g. $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$
(general linear group) \( \text{GL}_n(\mathbb{R}) = \{ \text{invertible n \times n real matrices} \} \)

(symmetric group) \( S_n = \{ \sigma : \{1, \ldots, n\} \rightarrow \{1, \ldots, n\} : \sigma \text{ is bijective} \} \)

(dihedral group) \( D_n = \{ 1, x, x^2, \ldots, x^{n-1}, y : x^n = y^2 = (xy)^2 = 1 \} \)
\[ = \langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle \]
\[ = \text{Set of reflections and rotations of the regular n-gon.} \]

**Def (Subgroup)** Let \( (G, \circ) \) be a group and \( H \subseteq G \).
If \( (H, \circ) \) is a group, then we call \( H \) a subgroup of \( G \) and denote by \( H \leq G \).

**Def (Abelian group)** A commutative group \( (G, \circ) \)
(i.e. \( x \circ y = y \circ x \) for all \( x, y \in G \)) is called an abelian group.

**e.g.** \( (\mathbb{C}, +) \) is an abelian group and
\[ \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \]
\[ \mathbb{Z}_n : = \{ 1, x, x^2, \ldots, x^{n-1} : x^n = 1 \} \]
\[ \mathbb{Z}_n \subseteq D_n \]

**Def (cyclic group)** A cyclic group is a group
generated by a single element, i.e. \((G, 0)\) is cyclic if
\[ G = \langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \} \]
for some \(x \in G\).

**Def (Order)** The order of a group \(G\) is the cardinality of \(G\) and denoted by \(|G|\). If \(x \in G\), the order of \(x\) is the order \(\langle x \rangle\) and denoted by \(|x|\).

**Prop (Subgroup Test)** \(H \leq (G, 0)\). \(H\) is a subgroup if
1. \(e \in H\)
2. \(xy^{-1} \in H\) for \(x, y \in H\)

**Prop** If \(G\) is a cyclic group, then all subgroups of \(G\) are cyclic.
If \(|G| = n\), the order of \(\langle x^m \rangle\) is \(n / \gcd(m, n)\).

**Thm (Lagrange)** Let \(G\) be the finite group order \(n\) and \(x \in G\) order \(m\). Then \(m \mid n\).
Thm (Sylow) Let $G$ be the finite group order $n = p^k m$ where $p$ is prime and $p \nmid m$. Then there exists a subgroup $H \leq G$ of order $p^i$ for $1 \leq i \leq k$.

Def (homomorphism) Let $(G, \circ)$, $(H, \ast)$ be groups. $\varphi : G \to H$ is a homomorphism if $\varphi(x \circ y) = \varphi(x) \ast \varphi(y)$

A homomorphism $\varphi$ is called an isomorphism if $\varphi$ is bijective.

Exercise $\varphi : G \to H$ homomorphism. Show that

1) $\varphi(e_G) = e_H$
2) $|x| = |\varphi(x)|$
3) $\varphi(x^{-1}) = \varphi(x)^{-1}$
4) $|\varphi(G)| | H |$, $|\varphi(G)| | |G|$
5) $G' \leq G \Rightarrow \varphi(G') \leq H$
6) $\ker \varphi \leq G$

Goal: Classify group up to isomorphism
Theorem: Suppose $G$ is an abelian group of finite order. $G \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n}$, where $p_1, \ldots, p_n$ (not necessarily distinct) prime numbers.

Example: $x \in G$, $y \in H$ \quad 1x1 = m \quad 1y1 = n$
$(x, y) \in G \times H \quad \gcd (x, y) = 1 = \text{lcm} (x, y)$
$
\mathbb{Z}_m \times \mathbb{Z}_n = \mathbb{Z}_{mn}$ \quad if \quad $\gcd (m, n) = 1$

Example: How many abelian groups have order $12$?

$12 = 2 \cdot 2 \cdot 3$
$= 2^2 \cdot 3$

$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ \quad or \quad $\mathbb{Z}_2^2 \times \mathbb{Z}_3$

(\cong \mathbb{Z}_2 \times \mathbb{Z}_6) \quad (\cong \mathbb{Z}_{12})$

Rings

Definition: A ring $(R, +, \cdot)$ is a set with two binary operations such that
1) \((R,+)\) is an abelian group w/ id \(0\), and inverse \(-x\) for \(x\)

2) \((R,\cdot)\) is associative

3) \(x \cdot (y+z) = xy+xz\) \((z+y) \cdot z = xz+yz\)

If \((R,\cdot)\) has multiplicative identity, it is denoted by \(1 \in R\) and \(R\) is called a ring w/ unity.

If \((R,\cdot)\) is commutative, \(R\) is called a commutative ring.

**Def** Let \((R,+,\cdot)\) be a ring w/ unity \(1\). Then an element \(x \in G\) w/ \(x^{-1} \in G\) s.t. \(x \cdot x^{-1} = x^{-1} \cdot x = 1\) is called a unit of \(R\).

An element \(x \in G\) w/ non-zero \(y \in G\) s.t. \(xy = 0\) or \(yx = 0\) is called zero-divisor.

**Def** A commutative ring w/ unity and no zero divisors is called an integral domain.

**Def** A field \((F,+,\cdot)\) is a ring s.t. \((R\setminus \{0\},\cdot)\) is an abelian group.