# Midterm Review



## Set Theory

Set Theory

Functions: bijectivity $\longleftrightarrow$ invertibility $\quad f: X \to Y \quad g: Y \to X$

injectivity + surjectivity $\quad \begin{cases} f \circ g = id_Y \\ g \circ f = id_X \end{cases}$

(one-to-one) (onto)

For a homomorphism $f: G \to G'$.

$f$ injective $\longleftrightarrow \ker(f) = \{1\}$. trivial

- Use inverse to prove bijectivity
- Use Kernel to prove injectivity

# Equivalence Relation

Equivalence Relations:

- Definition: $\left\{ \begin{array}{l} \text{reflexive} \\ \text{symmetric} \\ \text{transitive} \end{array} \right.$

- Equivalence classes:

The distinct ones form a partition of the set.

$[a] \cap [b] = \varnothing$ or $[a] = [b]$.

- Quotient Space.

  The set of all distinct equivalence classes.

- Equivalence classes on $X \longleftrightarrow$ Partitions of $X$.

- Typical Examples of equivalence relations on a group $G$:

  - $x \sim y$ if $y^{-1}x \in H$.

    this construction leads to cosets.

  - $x \sim y$ if $y = g x g^{-1}$ for some $g$.

    this construction leads to conjugacy classes.

# Groups

**Groups**: Definition (associativity, identity, inverse).

Important Examples: $(\mathbb{Z},+)$, $S_n$, $A_n$, $K_4$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{R}^\times$, $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$.

Basic concepts:

- order of Group.
- Subgroups (closure, identity, inverse)
  - Subgroups of cyclic groups → (Examples: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$)
  - cyclic subgroups

    ⇓

    order of an element in a group.

    $|g| = |\langle g\rangle|$.

    Alternatively,

    $|g| = \min\{k\in\mathbb{Z} \mid k>0,\ g^k=1\}$ if the set is nonempty.

    $|g| = \infty$ if the above set is empty.

$$\boxed{\text{If } |g|=n, \text{ then } g^k=1 \Leftrightarrow n\mid k.}$$

Applications to numbers:

- greatest common divisor of $a, b$.

  $g\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z}$.
- relatively prime: $\gcd(a,b)=1$.

  i.e., $a\mathbb{Z}+b\mathbb{Z}=\mathbb{Z}$.

  In particular, $1 = ak+bl$ for some $k, l\in\mathbb{Z}$.

  $\Updownarrow$

  $\gcd(a,b)=1$

## Homomorphisms

$f: G \to G'$. $\gcd(a,b)=1$

**Homomorphisms**: . Definition ($f(ab)=f(a)f(b)$).

· Properties: $f(1)=1'$, $f(g)^{-1}=f(g^{-1})$

· $\ker(f)=\{g\in G \mid f(g)=1'\}$ $\longrightarrow$ normal subgroups

· $\mathrm{Im}(f)=G' \Leftrightarrow$ surjectivity of $f$.

special case: Isomorphisms.

Isomorphic groups. $G \cong G'$

First Isomorphism Theorem

**Automorphisms**: $\mathrm{Aut}(G)$. the group of all automorphisms on $G$.

It has a normal subgroup $\mathrm{Inn}(G)$.

Also there's a homomorphism

$$\Phi: G \longrightarrow \mathrm{Aut}(G)$$
$$g \longmapsto \phi_g$$

$\ker(\Phi)=Z(G)$, $\mathrm{Im}(\Phi)=\mathrm{Inn}(G)$

Examples:

$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

$\mathrm{Aut}(\mathbb{Z}) \cong \{\pm 1\}$.

$\mathrm{Aut}(S_3) \cong S_3$.

## Quotient of Groups

Quotient of Groups: $aH=bH \Leftrightarrow a\in bH \Leftrightarrow b^{-1}a\in H$

- Cosets. left cosets & right cosets

  (they coincide for a normal subgroup)

  Lagrange theorem: $[G:H]\cdot|H|=|G|$.

  Its corollaries: $\begin{cases} \cdot\ |H| \text{ divides } |G| \\ \cdot\ |g| \text{ divides } |G| \end{cases}$

  $[G:K]=[G:H]\cdot[H:K] \qquad G\supseteq H\supseteq K$

- Quotient group: $G/N$. ← N needs to be a normal subgroup.

  $aN.bN=abN$

  $\pi: G\to G/N$ is a surjective homomorphism.

  $g\mapsto gN$

  Example: $\mathbb{Z}/n\mathbb{Z}$. units. $(\mathbb{Z}/n\mathbb{Z})^\times$. group of units

  $$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})\cong(\mathbb{Z}/n\mathbb{Z})^\times.$$

  Applications to numbers: Fermat's Little Theorem

- First Isomorphism Theorem:

  $f: G\to G'$ homomorphism

  $$\boxed{G/\ker(f)\cong \mathrm{Im}(f).}$$

## Product

Products: $G \times G'$. what're the elements?
what's the composition?

$G = H \times K$ if $f: H \times K \longrightarrow G$ is an isomorphism.
$(h,k) \longmapsto hk$

thm. $G = H \times K \iff$ • $H$ & $K$ are normal subgroups of $G$
• $H \cap K = \{1\}$
• $HK = G$

Example. $C_m \times C_n \cong C_{mn}$ if $\gcd(m,n) = 1$.
(Chinese Remainder Theorem)

## Symmetric Groups

$S_n$: symmetric groups.

- cycles and cycle decomposition.
- Computational results:
  - $\sigma (a_1 \ a_2 \dots a_k) \sigma^{-1} = (\sigma(a_1) \ \dots\dots \ \sigma(a_k))$.
  - $(a_1 \ a_2 \dots a_n) = (a_1 \ a_n)(a_1 \ a_{n-1}) \dots\dots (a_1 \ a_3)(a_1 \ a_2)$
- signature function & parity of a permutation

$\mathrm{sgn}(\sigma) \in \{\pm 1\}$. $\quad$ $\mathrm{sgn}: S_n \longrightarrow \{\pm 1\}$ is a surjective homomorphism $(n > 1)$.

- $A_n = \ker(\mathrm{sgn})$. alternating group.

  $A_n$ consists of all <u>even permutations</u> (i.e., $\mathrm{sgn}(\sigma) = +1$)

  $[S_n : A_n] = 2$. $(n > 1)$

  $A_n \triangleleft S_n$.

- $A_n$ is simple for $n \geq 5$.

$A_2 = \{id\}$ simple.

$A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$ simple.

$A_4$ is not simple. $A_4$ has proper normal subgroup $\{id, (12)(34), (13)(24), (14)(23)\}$