Set Theory

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

$\begin{cases} f \circ g = id_Y \\ g \circ f = id_X \end{cases}$

injectivity + surjectivity
(one-to-one) (onto)

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

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

Equivalence Relations: · Definition: $\begin{cases} \text{reflexive} \\ \text{symmetric} \\ \text{transitive} \end{cases}$

· 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 $y = gxg^{-1}$ for some g.
  this construction leads to conjugacy classes.

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 $\to$ (Examples: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$)
  - cyclic subgroups
    $\Downarrow$
    order of an element in a group.

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

$\begin{cases} |g| = \min\{k \in \mathbb{Z} \mid k > 0,\ g^k = 1\} & \text{if the set is nonempty.} \\ |g| = \infty & \text{if the above set is empty.} \end{cases}$

> If $|g| = n$,
> then $g^k = 1 \iff n \mid k$.

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**: $f: G \to G'$.
- Definition ($f(ab) = f(a)f(b)$).
- Properties: $f(1) = 1'$, $f(g)^{-1} = f(g^{-1})$
- $\ker(f) = \{g \in G \mid f(g) = 1'\}$ $\to$ normal subgroups
- $\operatorname{Im}(f) = G' \iff$ surjectivity of f.

special case: Isomorphisms.
Isomorphic groups. $G \cong G'$ (First Isomorphism Theorem)

Automorphisms: $\operatorname{Aut}(G)$, the group of all automorphisms on G.
It has a normal subgroup $\operatorname{Inn}(G)$.
Also there's a homomorphism
$\Phi: G \longrightarrow \operatorname{Aut}(G)$
$g \longmapsto \phi_g$
$\ker(\Phi) = Z(G)$, $\operatorname{Im}(\Phi) = \operatorname{Inn}(G)$

Examples:
$\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
$\operatorname{Aut}(\mathbb{Z}) \cong \{\pm 1\}$.
$\operatorname{Aut}(S_3) \cong S_3$.

· **Quotient of Groups:** $aH = bH \iff a \in bH \iff b^{-1}a \in H$
- 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. $\leftarrow$ N needs to be a normal subgroup.
  $aN \cdot bN = abN$
  $\pi: G \longrightarrow G/N$ is a surjective homomorphism.
  $g \longmapsto gN$

Example: $\mathbb{Z}/n\mathbb{Z}$. units. $(\mathbb{Z}/n\mathbb{Z})^\times$, group of units.
$\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
Applications to numbers: Fermat's Little Theorem

- First Isomorphism Theorem:
  $f: G \to G'$ homomorphism
  $$G/\ker(f) \cong \operatorname{Im}(f).$$

· **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. $G = H \times K \iff \begin{cases} \cdot\ H \,\&\, K \text{ are normal subgroups of } G \\ \cdot\ H \cap K = \{1\} \\ \cdot\ HK = G \end{cases}$

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

· S_n: symmetric groups.
- cycles and cycle decomposition.
- Computational results:
  - $\sigma(a_1\ a_2 \dots a_k)\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k))$.
  - $(a_1\ a_2 \dots a_n) = (a_1\ a_n)(a_1\ a_{n-1}) \dots (a_1\ a_3)(a_1\ a_2)$
- signature function & parity of a permutation
  $\operatorname{sgn}(\sigma) \in \{\pm 1\}$. $\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}$ is a surjective homomorphism $(n > 1)$.
- $A_n = \ker(\operatorname{sgn})$, alternating group.
  A_n consists of all even permutations (i.e., $\operatorname{sgn}(\sigma) = +1$)
  $[S_n : A_n] = 2$. $(n > 1)$
  $A_n \lhd S_n$.
- 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 $\{id, (12)(34), (13)(24), (14)(23)\}$