- **Bijection**:
  Function $f : X \to Y$ is bijection if f is both surjection(on to) and injection (one to one)
  Proposition:
  1. $f : X \to Y$ is bijection $\Leftrightarrow$
     $\exists g : Y \to X$ s.t. $g \circ f = id_x, f \circ g = id_y$ ($id_x \to$ identity)
  2. Composition Properties:
     ∘ Composition of two injective functions is injective.
     ∘ Composition of two surjective functions is surjective.
     ∘ Composition of two bijective functions is bijective.

- **Permutation:**
  Permutation on set X is a bijection $f : X \to X$
  If $X = \{1, 2, \ldots, n\}$ then, $S_n :=$ {all permutation on X} **Proposition:**
  1. if $f : X \to X$ is a permutation then $\exists f^{-1} : X \to X$ which is also permutation.
  2. composition of two permutation is again a permutation.

- **Group 5 Rules**:
  1. Closed under binary operation
  2. associative: (ab)c = a(bc)
  3. identity: $\exists e \in G, ea = ae = a \forall a \in G$
  4. inverse: $\forall a \in G, \exists! a^{-1} s.t. a^{-1} a = aa^{-1} = e$
  5. commutative $a, b \in G, ab = ba$.

  1,2: semigroup
  1,2,3: monoid
  1,2,3,4: group
  1,2,3,4,5: Abelian group

- **Equivalence Relation:**
  Operation   in Group G is equivalence if
  1. Reflective: $g \; g, \forall g \in G$
  2. Symmetry: $g \; g' \Rightarrow g' \; g, \forall g, g' \in G$
  3. transitive: $x \; y, y \; z \Rightarrow x \; z \forall x, y, z$

- **Subgroup**: H is a subgroup of G if
  - $H \subseteq G$
  - H is a group

  CHECK a SUBGROUP:
  - $H \subseteq G$ (subset)
  - $e \in H$ (non empty)
  - $\forall a, b \in H, ab \in H$ (closed)

- $\forall a \in H, a^{-1} \in H$

Proper subgroup: subgroup H that is not $H \neq G$

- **Order**:
  Order of a group: $|G|$ = # of elements in the group. If a group is infinite, then the order is ∞
  Order of an element: $g \in G, |g|$ = **smallest positive integer** n, $s.t.$ $x^n = e$
  Propositions:
  - Let $g \in G, |<g>| = |g|$
  - If H is a subgroup of G then $|H| \mid |G|$. If $x \in G$, then $|x| \mid |G|$
- $<x> := \{ x^n \mid n \in \mathbb{Z}\}$
- **Conjugate**: $x, g \in G$, conjugate of x by g: gxg^{-1}
  Conjugate class of x:= $\{gxg^{-1} \mid \forall g \in G\}$
- **ISOMORPHISMS of GROUP**: a function $f : G \to G'$ is called isomorphism if:
  1. $f(xy) = f(x)f(y)$
  2. f is one to one (injective)
  3. f is onto (surjective)

  We use $G \cong G'$ (group isomorphisim) to show that $\exists f : G \to G'$ that is isomorphic. Then $|G| = |G'|$. **Propositions:**
  - Suppose $G \cong G'$ Then G is abelian $\Leftrightarrow$ G' is abelian. (which implies that abelian group and non abelian group is not isomorphic)
  - if G and G' are cyclic and $|G| = |G'|$ then $G \cong G'$
  - Let $G = (Z_n, +_n) = \{[0], [1] \cdots, [n-1]\}$, $G' = (Z_n, +_n) = (\{0, 1, 2, \cdots, n-1\}, +_n)$ Then $G \cong G'$ and the isomorphisim can be take $[x]_n \to x$
- **Cyclic**: $\exists a \in G$, $s.t.$ $<a> = G$ such a is called a generator.
- **Center of Group**:
  Center of a Group $G : Z(G) := \{Z \in G | gz = zg, \ \forall g \in G\}$
  Proposition:
  1. $Z(G)$ is asubgroup of G.
  2. If G is abelian, then $Z(G) = G$
- **External direct product of Groups:**
  Group G, H, Define $G \times H := \{(x, y) \mid x \in G, y \in H\}$
  $(x_1, y_1)(x_2, y_2) = (x_1 x_2, y_1 y_2)$
  Proposition:
  1. $e_{G\times H} = (e_G, e_H)$
  2. $(x, y)^{-1} = (x^{-1}, y^{-1})$
  3. $|(x, y)| = LCM(|x|, |y|)$

- **Internal product of groups:**
  Group G has subgroup H, K. Defind $HK := \{xy | x \in H, y \in K\}$
  NOTE: HK is not always a subgroup.
  Proposition:

  1. H, K are subgroup of G.
     Suppose $x^{-1}yx \in K, \forall x \in H, y \in K$ Then HK is a subgroup of G.
     Corollary: H, K are subgroup of abelien group G, then HK is a subgroup of G.

- **Group Homomorphisms:**
  $f : G \to G'$ if $f(xy) = f(x)f(y) \forall x, y \in G$
  Compared to isomorphism, we don't need bijection.

- **Kernal and Image:**
  $f : G \to G'$, Define:
  Kerf $:= \{g \in G \mid f(g) = e'_G\}$
  Imf $:= \{y \in G' \mid \exists x \in G, s.t.\ f(x) = y\} \equiv \{f(x) \mid x \in G\}$
  Lemma:
  $f : G \to G'$ be a group homomorphism.

  1. $f(e_G) = e_{G'}$
  2. $f(a^n) = (f(a))^n, \forall n > 0, n \in \mathbb{Z}$
  3. $f(a^{-1}) = (f(a))^{-1}$
  4. From 2,3 we can conclude: $f(a^n) = (f(a))^n$

  Proposition:

  1. $f : G \to G'$ be group homomorphism:
     - kerf is a subgroup of G
     - Imf is a subgroup of G'
  2. If $G =< a >$ i.e. G is a cyclic group. Then, it is enough to define homomorphism $f : G \to G'$ on a and extend to all a^n.
  3. $f : G \to G'$ be a group homomorphism, then $|f(a)| \mid |a|$

- **Left Coset and Right Coset:**
  Definition:
  Let G be a group , let H be a subgroup of G.
  Left coset of H in G: $aH := \{ah \mid h \in G\}$
  Right coset of H in G: $Ha := \{ha \mid h \in G\}$ **Proposition:**

  - $aH = H$ iff $a \in H$
  - $$\begin{aligned} aH = bH \quad &\Leftrightarrow \quad a \in bH \\ &\Leftrightarrow \quad b \in aH \\ &\Leftrightarrow \quad a^{-1}b \in H \\ &\Leftrightarrow \quad b^{-1}a \in H \end{aligned}$$
  - $aH \cup bH = \emptyset$ or $aH = bH$.
    Only two posibilities. When it is $\emptyset$, properties above fails. When it is not $\emptyset$ the only posibility is that $aH = bH$ and above properties holds.

- $G = \sqcup aH$ (disjoint union of left cosets.)
  Taking elements inside the set H won't generate new cosets. Only taking elements outside the set would generate new cosets.
- $H < G, |aH| = |H|, \forall a \in G$

Definition: $H < G$, $[G : H] :=$ # of left cosets of H in G
Properties: $|G| = [G : H] \cdot |H| \Leftrightarrow [G : H] = |G|/|H|$
In general, $aH \neq Ha$, sometimes they are the same.

- **Normal Subgroup:**
  Definition: $H < G, H$ is normal subgroup $\Leftrightarrow H \triangleleft G$ if $aH = Ha, \forall a \in G$.
  Theorem: $H < G$, the following are equivalent:
  - $H \triangleleft G$
  - $aH = Ha, \forall a \in G$
  - $aHa^{-1} \subseteq H, \forall a \in G$
  - $aHa^{-1} = H, \forall a \in G$

  Prop: If G is an abelian group, then every subgroup of G is normal.