- **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 $X = \{1, 2, \dots, n\}$ then, $S_n := \{\text{all permutation on } X\}$ **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 $\sim$ in Group G is equivalence if

  1. Reflective: $g \sim g, \forall g \in G$
  2. Symmetry: $g \sim g' \Rightarrow g' \sim g, \forall g, g' \in G$
  3. transitive: $x \sim y, y \sim z \Rightarrow x \sim z \forall x, y, z$

- **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)

  $G \cong G'$ (group isomorphisim): $\exists f : G \to G'$ 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 a subgroup of G.
  2. If G is abelian, then $Z(G) = G$

- **External direct product of Groups:**
  Group G, H, Define $G \times H := \{(x, y) \mid x \in G, y \in H\}$
  $(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$
  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 $a \in H$
  - $$\begin{aligned} aH = bH &\Leftrightarrow a \in bH \\ &\Leftrightarrow b \in aH \\ &\Leftrightarrow a^{-1}b \in H \\ &\Leftrightarrow b^{-1}a \in H \end{aligned}$$
  - $aH \cup bH = \emptyset$ 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.
- **Symmetric Group:**
  Definition: transposition is an element $\tau_{ij} = (ij)$ (permutation of length 2)
  Prop: Every permutation seauence $b \in S_n$ can be written as a product of transpositions.
  - Step 1: write the permutation in disjoint cycles.
  - Step 2: write each cycle as a product of transpositions.

  Example: $(1346)(13)(14)(16) = (3461) \Rightarrow (16)(14)(13) = (1346)$
- **Sign of permutation:** Definition: the sign of permutation σ is the parity of the number of transpositions in any decompositions.
  To conclude: length of cycle is even $\Rightarrow$ parity odd; length of cycle is odd $\Rightarrow$ parity even.
  Prop: even$\cdot$ even = even; even$\cdot$odd = odd; odd$\cdot$even = odd; odd$\cdot$odd = even
- **Quotient Group:**
  $H \triangleleft G$ then $G/H = \{aH \mid a \in G\}$.
  G/H is a group under operation: $(aH)(bH) = abH$. identity: $e_{G/H} = eH = H$. inverse: $(aH)^{-1} = a^{-1}H$
- **Isomorphism Theorem:**
  1. Let $f : G \to G'$ be a group homomorphism. Then $G/kerf \cong imf$
     - Let $H < G$, let $i : H \to G$ be $i(x) = x$.
       Then, 1. i is a gorup homomorphism.
       2. i is one to one.
       3. $ker(i) = e$
       4. $im(i) = H$.

- Let $H \triangleleft G$. Let $\pi : G \to G/H$ be given as $\Pi(x) = xH$
  Then, 1. π is a group homomorphism.
  2. $ker(\pi) = H$
  3. π is onto
  4. $Im(\pi) = G/H$.
- **Theorem:** $f : G \to G'$, f is a group homomorphism.
  (a) $ker(f) \triangleleft G$
  (b) $G/kerf$ is a group.
  (c) $Imf \leq G'$, Imf is a subgroup.
  (d) $f : G \to G'$ becomes:
  $G \xrightarrow{\pi} G/kerf \overset{\overline{f}}{\longleftrightarrow} Imf \overset{i'}{\longleftarrow} G'$, where $\overline{f}(a \cdot kerf) = f(a)$
  Then $f = i'\overline{f}\pi$, i.e. any f can be write in composition of $i\overline{f}\pi$

2. Let $H, N < G$, suppose $N \triangleleft G$, then $(H \cdot N)/N \cong H/(H \cup N)$
   Proof Steps:
   (a) HN is a subgroup of G
   Proof. – Show $HN \subseteq G$
   $x \in HN \Rightarrow x = yz, y \in H, z \in N$
   $y \in H, H \subseteq G \Rightarrow y \in G$
   $z \in N, N \subseteq G \Rightarrow z \in G$
   Since G is a group, G is closed under operation. Therefore, $x = yz \in G$
   - Show $e \in HN$
     Since $e = e \cdot e$ and H, N are groups, then $e \in H, e \in N$. Therefore, $e \in HN$
   - Closed under operation.
     Claim:$a, b \in HN$, **WTS:** $ab \in HN$
     By assumption $\exists h \in H, n \in N, a = hn$
     By assumption $\exists h' \in H, n' \in N, b = h'n'$
     Then $ab = hnh'n'$.
     $nh' \in Nh'$
     Since $N \triangleleft G \Rightarrow nh' \in h'N$
     Therefore, $\exists \hat{n} \in N$ s.t. $nh' = h'\hat{n}$
     Then,$ab = hnh'n' = hh'\hat{n}n'$.
     Since $hh' \in H, \hat{n}n' \in N$, $ab \in HN$.
   - Closed under inversion.
     Claim:$a \in HN$, **WTS:** $a^{-1} \in HN$
     By assumption $\exists h \in H, n \in N, a = hn$
     Then $a^{-1} = n^{-1}h^{-1}$
     Since $n^{-1} \in N$, then $n^{-1}h^{-1} \in Nh^{-1}$
     Since N is a normal subgroup of G and $h^{-1} \in G$, then $n^{-1}h^{-1} \in h^{-1}N$.
     Then $\exists \hat{n} \in N$ s.t. $n^{-1}h^{-1} = h^{-1}\hat{n}$
     Since $h \in H$ and H is a group, $h^{-1} \in H$
     $\Rightarrow a^{-1} = h^{-1}\hat{n}$ where $h^{-1} \in H, \hat{n} \in N$
     Therefore, $a^{-1} \in HN$

   □

   (b) N is normal subgroup in HN

Proof.

- Show $N \subseteq HN$

  If $x \in N \Rightarrow \exists n \in N,\ s.t.\ x = en$

  Since H is a group, then $e \in H$. Therefore, $x \in HN$

  Therefore, $\Rightarrow N \subseteq HN$

- Show $e \in N$: Trivial since N is already a group by definition.
- Show N closed under operation: Trivial since N is already a group by definition.
- Show N closed under inverse: Trivial since N is already a group by definition.

$\square$

(c) HN/N is a group: This is a quotient group by definition.

(d) $H \cap N \leq H$: Skipped In Class (trivial)

(e) $H \cap N \triangleleft H$: Skipped In Class

(f) $HN/N \cong H/(N \cap H)$

Proof. We define an homomorphism $f : H \to HN/N, f(h) = hN$:

$$\begin{cases} H & \xrightarrow{i} & HN \\ x \xrightarrow{f} HN/N & \xleftarrow{\pi} & HN \end{cases}$$

Then $kerf = \{x \in H \mid f(x) = e_{HN/N}\}$
$= \{x \in H \mid xN = N\}$
$= \{x \in H \mid x \in N\}$
$= H \cap N$

Use theoem A for f: $H/kerf \cong Imf$.

Then, $H/(H \cap N) \cong HN/N$ $\square$

3. Let $K, H \triangleleft G$ (normal subgroup), suppose $K \subset H$. Then, $(G/K)\ /\ (H/K) \cong G/H$