

- **Bijection:**

Function $f : X \rightarrow Y$ is bijection if f is both surjection(on to) and injection (one to one)

Proposition:

1. $f : X \rightarrow Y$ is bijection \Leftrightarrow
 $\exists g : Y \rightarrow X$ s.t. $g \circ f = id_x, f \circ g = id_y$ ($id_x \rightarrow$ 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 $f : X \rightarrow X$

If $X = \{1, 2, \dots, n\}$ then, $S_n := \{\text{all permutation on } X\}$ **Proposition:**

1. if $f : X \rightarrow X$ is a permutation then $\exists f^{-1} : X \rightarrow X$ 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: $\forall a \in G, \exists ! a^{-1} \text{ s.t. } a^{-1}a = aa^{-1} = e$
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 $H = G$

- **Order:**

Order of a group: $|G| = \#$ of elements in the group. If a group is infinite, then the order is ∞

Order of an element: $g \in G, |g| = \text{smallest positive integer } n, \text{ s.t. } x^n = e$

Propositions:

- Let $g \in G, |\langle g \rangle| = |g|$
- If H is a subgroup of G then $|H| \mid |G|$. If $x \in G$, then $|x| \mid |G|$

- $\langle x \rangle := \{x^n \mid n \in \mathbb{Z}\}$

- **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 $f : G \rightarrow G'$ 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 isomorphism): $\exists f : G \rightarrow G'$ 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 $G = (Z_n, +_n) = \{[0], [1], \dots, [n-1]\}$, $G' = (Z_n, +_n) = (\{0, 1, 2, \dots, n-1\}, +_n)$ Then $G \cong G'$ and the isomorphism can be take $[x]_n \rightarrow x$

- **Cyclic:** $\exists a \in G, \text{ s.t. } \langle a \rangle = G$ such a is called a generator.

- **Center of Group:**

Center of a Group $G : Z(G) := \{Z \in G \mid gz = zg, \forall g \in G\}$

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. $|(x, y)| = \text{LCM}(|x|, |y|)$

- **Internal product of groups:**

Group G has subgroup H, K . Define $HK := \{xy | x \in H, y \in K\}$

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 abelian group G , then HK is a subgroup of G .

- **Group Homomorphisms:**

$f : G \rightarrow G'$ if $f(xy) = f(x)f(y) \forall x, y \in G$

Compared to isomorphism, we don't need bijection.

- **Kernal and Image:**

$f : G \rightarrow G'$, Define:

$\text{Kerf} := \{g \in G \mid f(g) = e_{G'}\}$

$\text{Imf} := \{y \in G' \mid \exists x \in G, s.t. f(x) = y\} \equiv \{f(x) \mid x \in G\}$

Lemma:

$f : G \rightarrow G'$ 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. $f : G \rightarrow G'$ be group homomorphism:
 - kerf is a subgroup of G
 - Imf is a subgroup of G'
2. If $G = \langle a \rangle$ i.e. G is a cyclic group. Then, it is enough to define homomorphism $f : G \rightarrow G'$ on a and extend to all a^n .
3. $f : G \rightarrow G'$ 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 : $aH := \{ah \mid h \in H\}$

Right coset of H in G : $Ha := \{ha \mid h \in H\}$ **Proposition:**

- $aH = H$ iff $a \in H$
- $aH = bH \iff a \in bH$
- $\iff b \in aH$
- $\iff a^{-1}b \in H$
- $\iff b^{-1}a \in H$
- $aH \cup bH = \emptyset$ or $aH = bH$.

Only two possibilities. When it is \emptyset , properties above fails. When it is not \emptyset the only possibility 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 sequence $b \in S_n$ 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 $f : G \rightarrow G'$ be a group homomorphism. Then $G/\ker f \cong \text{im} f$

- Let $H < G$, let $i : H \rightarrow G$ be $i(x) = x$.
Then, 1. i is a group homomorphism.
- 2. i is one to one.
- 3. $\ker(i) = e$
- 4. $\text{im}(i) = H$.

- Let $H \triangleleft G$. Let $\pi : G \rightarrow G/H$ be given as $\Pi(x) = xH$
Then, 1. π is a group homomorphism.
2. $\ker(\pi) = H$
3. π is onto
4. $\text{Im}(\pi) = G/H$.
- **Theorem:** $f : G \rightarrow G'$, f is a group homomorphism.
 - (a) $\ker(f) \triangleleft G$
 - (b) $G/\ker f$ is a group.
 - (c) $\text{Im} f \leq G'$, $\text{Im} f$ is a subgroup.
 - (d) $f : G \rightarrow G'$ becomes:

$$G \xrightarrow{\pi} G/\ker f \xrightarrow{\bar{f}} \text{Im} f \xrightarrow{i'} G', \text{ where } \bar{f}(a \cdot \ker f) = f(a)$$
 Then $f = i' \bar{f} \pi$, i.e. any f can be write in composition of $i' \bar{f} \pi$
- 2. Let $H, N < G$, suppose $N \triangleleft G$, then $(H \cdot N)/N \cong H/(H \cap N)$
- 3. Let $K, H \triangleleft G$ (normal subgroup), suppose $K \subset H$. Then, $(G/K) / (H/K) \cong G/H$