Intergers modulo n

- The set $\{[0],[1],[2],...,[n-1]\}$ of the equivalence classes of $\equiv$ mod n is called the **integers modulo** n denoted by $\mathbb{Z}_n$.

- **Theorem**: Let $n \in \mathbb{Z}^+$.
  If $a \equiv a'\ mod\ n$, $b \equiv b'\ mod\ n$, then
  1. $a + b \equiv (a' + b')\ mod\ n$
  2. $ab \equiv a'b'\ mod\ n$
  3. $ac \equiv a'c\ mod\ n$ and c is relatively prime to n (i.e. $\gcd(c, n) = 1$), then $a \equiv a'\ mod\ n$.

- $(\mathbb{Z}_n, +)$ is a group.

- $(\mathbb{Z}_n, .)$?

Order of a Group

- The number of elements in a group G is called the order of G, denoted by $|G|$ or $o(G)$.

- Example:
  1. $(\mathbb{Z}_5, +)$ has order 5.
  2. $(\mathbb{Z}, +)$ has infinite order.

Order of an Element

- The order of an element, a, in a group G is the smallest positive integer n such that $a^n = e$.
- Example:
    1. Elements of $(\mathbb{Z}_5, +)$.

Remark:

1. If no such n exists, we say that a has infinite order.
2. The order of an element if denoted by $|a|$.
3. $|a|= |a^{-1}|\ \forall a \in G$.
4. $|ab|= |ba|\ \forall a, b \in G$.

Abelian Group

- If a group G has the property that

$$a * b = b * a \text{ for every} a, b \in G$$

  then G is called an **Abelian group**.

- Examples:

Exercise

- Show that the set $G = \{x + y\sqrt{3} : x, y \in \mathbb{Q}\}$ is a group under addition.

Exercise

- Symmetrices of a Square

Subgroups

- If a subset H of a group G is itself a group under the operation of G, then H is said to be a subgroup of G.
- Notation: $H \leq G$
- If H is a subgroup of G, but not equal to G then H is said to be a proper subgroup of G, denoted by $H < G$.
- The subgroup $\{e\}$ is called the trivial subgroup of G.

Exercise

- Is $(\mathbb{Z}_n, +)$ a subgroup of $(\mathbb{Z}, +)$? No

- Let H be a non-empty subset of a group G.
  $H \leq G$ if and only if $a, b \in H \implies ab^{-1} \in H$.

- Let H and K be two subgroups of a group G.
  Then $H \cap K$ is a subgroup of G.

- Let H and K be two subgroups of a group G.
  Then $H \cup K$ is a subgroup of $G \Leftrightarrow$ either $H \subseteq K$ or $K \subseteq H$.

Product of Two Subgroups:

- Let H and K be two subgroups of a group G. Then their product is defined as

$$HK = \{hk : h \in H, k \in K\}.$$

- **Theorem:**
  Let G be a group. Let H and K be subgroups of G.
  Then $HK \leq G \iff HK = KH$.

Cyclic Groups

- Let $a \in G$. Define $< a >= \{a^n : n \in \mathbb{Z}\}$
- $< a >$ is a subgroup of G.
- $< a >$ is called a cyclic subgroup generated by a.
- G is said to be cyclic if and only if $\exists a \in G$ such that $G =< a >$.
- Every cyclic group is Abelian.

Cyclic Groups: Examples

- Example 1: The set of integer $\mathbb{Z}$ under addition is cyclic.
- Example 2: $(\mathbb{Z}_8, +_8)$
- Example 3: $(\mathbb{Z}_5 \setminus \{0\}, *)$

Semi Group

- A non-empty set G with a binary operation $*$ is called a semi-group if

$$a * (b * c) = (a * b) * c \; \forall \; a, b, c \in G$$

- Remark: Every group is a semi-group. But the converse is not true.
- Example 1: $(\mathbb{Z}, *)$
- Example 2: $(\mathbb{Z}^+, +)$