Group Theory
5th class

$\mathbb{Z}_n$: The integers modulo n

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\} \qquad |\mathbb{Z}_n| = n$$

$(\mathbb{Z}_n, +, \cdot)$ is a ring (in fact, a commutative ring)

* $(\mathbb{Z}_n, +, 0)$ is a group (in fact, comm. group)
* $(\mathbb{Z}_n, \cdot, 1)$ is a monoid (in fact, comm. monoid)
* multiplication distributes through sums.

$\mathbb{Z}_n^\times = \{\text{units in } \mathbb{Z}_n\} = \{a \in \mathbb{Z}_n : \exists b \in \mathbb{Z}_n \text{ s.t. } ab = 1\}$

units $=$ invertible elements in $\mathbb{Z}_n$

* $(\mathbb{Z}_n^\times, \cdot, 1)$ is a (commutative) group
* $|\mathbb{Z}_n^\times| = \varphi(n) = \{1 \le k < n : \gcd(n,k) = 1\}$

Thm (Euler) $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \Rightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

eg: $\varphi(p) = p\left(1 - \frac{1}{p}\right) = p - 1$

$\varphi(p^r) = p^r\left(1 - \frac{1}{p}\right) = p^r - p^{r-1}$

Def An element $a \in \mathbb{Z}_n$ is a zero-divisor if $\exists\, 0 \neq b \in \mathbb{Z}_n$ st. $ab = 0$

Eg

* $\mathbb{Z}_3 = \{0, 1, 2\}$ — 0 is a zero-divisor; $1 \,\&\, 2$ are not zero-divisors (but they are invertible)

  $\mathbb{Z}_3^\times = \{1, 2\}$
* $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ — $0, 2$ are zero-divisors (check: $2 \cdot 2 = 0 \pmod 4$); $1, 3$ are not zero-divisors (in fact, they are units)

  $\mathbb{Z}_4^\times = \{1, 3\}$

  $(1^{-1} = 1,\ 3^{-1} = 3)$ since $3 \cdot 3 = 9 \equiv 1 \pmod 4$

Remark In any comm. ring (such as $\mathbb{Z}_3$)

$$\boxed{a \text{ unit} \Rightarrow a \text{ \underline{not} a zero-divisor}}$$

reason: Suppose . $\exists b$ st $ab=1$ (a unit)

. $\exists c \neq 0$ st $ac=0$ (a zero-divisor)

Then:

$$\left.\begin{array}{l} abc = (ab)\cdot c = 1\cdot c = c \\ \overset{\text{comm.}}{\|} \\ bac \underset{\text{assoc}}{=} b(ac) = b\cdot 0 = 0 \end{array}\right) \Rightarrow c=0$$

Easy remark 1 (the identity element in $\mathbb{Z}_n$) is <u>always</u> invertible (or, a unit)

Another example $(\mathbb{Z}, +, \cdot)$ is also a ring

- $\mathbb{Z}^{\times} = \{1, -1\}$ $\quad \begin{cases} 1\cdot 1 = +1 = 1 \\ (-1)(-1) = +1 = 1 \end{cases}$
- zero divisors of $\mathbb{Z}$: $\{0\}$
- All integers $\neq 0$ or ± 1 are neither invertible, nor zero-divisors

---

Prop Every element in $\mathbb{Z}_n$ is either invertible, or a zero-divisor.

Proof Let $[a] \in \mathbb{Z}_n$, with $0 \le a \le n-1$. Then:

(1) $a=0 \to a$ is a zero-divisor

(2) if $\gcd(a,n)=1$, then a is invertible

(3) if $a \neq 0$, and $\gcd(a,n) \neq 1$, then $\gcd(a,n)=d$, where $0<d<n$ & $d \neq 1$

Note: $d \mid a \longrightarrow a = d\cdot q$

$d \mid n \longrightarrow n = d\cdot r$ $\quad r \neq n$, so $[r] \neq 0$

$\to [a]$ is a zero divisor

$\therefore [a]\cdot[r] = [ar] = [dqr] = [drq] = [n\cdot q] = [0]$

Subgroups

Let $(G, *, e)$ be a group

Def A subset $H \subseteq G$ is called a <u>subgroup</u> if $(H, *)$ is a group.

$$\begin{tikzcd} G \times G \arrow[r, "*"] & G \\ H \times H \arrow[u, phantom, "\cup"] \arrow[ur, "*"] \arrow[r, dashed, "*"'] & H \arrow[u, phantom, "\cup"] \end{tikzcd}$$

<u>Examples</u>

(1) - $\{e\}$ is a subgroup of G (the <u>Trivial</u> subgroup)
- G is a subgroup of G (obviously)

(2) (a) Is ϕ a subgroup of G? No, by (b)

(b) Is ϕ ever a group? No, since a group must have an identity (e), and so, it cannot be empty!

(3) $G = \mathbb{Z}$ has subgroups $\{0\}$ and $n\mathbb{Z}$, for some $n \in \mathbb{Z}$, $n > 0$.
(In fact, these are <u>all</u> the subgroups of $\mathbb{Z}$.)

(4) $G = \mathbb{Z}_3 \longrightarrow$ has subgroups $\{0\}$, G

subsets of G: ϕ, $\{0,1\}$, $\{0,2\}$, $\{1,2\}$, $\{0\}$, $\{1\}$, $\{2\}$, $\{0,1,2\}$

$G = \mathbb{Z}_4$ Subgroups: $\{0\}$, $\{0,1,2,3\}$, $\{0,2\}$

subsets: $\cancel{\phi}$, 0, $\cancel{1}$, $\cancel{2}$, $\cancel{3}$, $\cancel{01}$, 02, $\cancel{03}$, $\cancel{12}$, $\cancel{13}$, $\cancel{23}$, $\cancel{012}$, $\cancel{013}$, $\cancel{023}$, $\cancel{123}$, 1230

(5) $\mathbb{Z}^\times \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$ a chain of subgroups $(* = \cdot)$

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ $(* = +)$

Visualize subgroup condition on Cayley table:

$G = \mathbb{Z}_4 = \{0,1,2,3\}$
$* = +$
$e = 0$

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

subgroup $\{0, 2\}$

0	2
2	0

Prop A non-empty subset $H \subseteq G$ is a subgroup of G if and only if

(i) $ab \in H$ for all $a, b \in H$

(ii) $a^{-1} \in H$ for all $a \in H$

Proof ($\Rightarrow$) Clearly, H subgroup $\Rightarrow$ (i) & (ii) hold

($\Leftarrow$)
- $(a,b) \longmapsto ab$ is a binary oper. on H (by (i))
- This operation is associative (since it is assoc. on G)

- Since $H \neq \emptyset$, $\exists\, a \in H$, so $a^{-1} \in H$ (by (ii))
  Hence $e = a \cdot a^{-1} \in H$ (by (i))
  But $e \cdot a = a \cdot e = a$ $\forall a \in G$, and so for $\forall a \in H$
  $\therefore$ e is an identity for H
- All elements in H have an inverse by (ii) and the fact that e is also the identity of H $\boxed{}$

Cor $\Big($A subset $\emptyset \neq H \subseteq G$ is a subgroup$\Big) \Leftrightarrow \Big(ab^{-1} \in H, \ \forall a, b \in H\Big)$ (*)

Proof ($\Rightarrow$) Clear, since $a, b \in H \Rightarrow b^{-1} \in H \Rightarrow ab^{-1} \in H$ ✓

($\Leftarrow$) • $a \in H \underset{\text{take } b=a \text{ in } (*)}{\Longrightarrow} \underset{\overset{\shortparallel}{e}}{a \cdot a^{-1}} \in H \Rightarrow e \in H$

- $a \in H \underset{\text{take } b=a \text{ \& } a=e \text{ in } (*)}{\Longrightarrow} \underset{\overset{\shortparallel}{a^{-1}}}{e \cdot a^{-1}} \in H \Rightarrow a^{-1} \in H$
- $a, b \in H \underset{\text{take } b=b^{-1} \text{ in } (*)}{\Longrightarrow} \underset{\overset{\shortparallel}{ab}}{a(b^{-1})^{-1}} \in H \Rightarrow ab \in H$

$\blacksquare$

Cyclic groups

Let $(G, \cdot)$ be a group (with $\cancel{*} = \cdot$, $e = 1$)

For $a \in G$, write
$$a^2 = a \cdot a$$
$$a^3 = a \cdot a \cdot a = a^2 \cdot a$$
$$a^4 = a \cdot a \cdot a \cdot a = a^3 \cdot a = a^2 \cdot a^2$$

also $a^{-2} = a^{-1} \cdot a^{-1} = (a^2)^{-1}$ [Check: $a^2 (a^{-2}) = (a \cdot a)(a^{-1} \cdot a^{-1}) = a \cdot (a a^{-1}) a^{-1} = a \cdot e \cdot a^{-1} = 1$]

in general, we write (for $n \in \mathbb{Z}$)

$$a^n = \begin{cases} \underbrace{a \cdots a}_{n} & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ \underbrace{a^{-1} \cdots a^{-1}}_{-n} & \text{if } n < 0 \end{cases}$$

Then $\boxed{a^n \cdot a^m = a^{n+m}}$

Def $\langle a \rangle = \{ x \in G : x = a^n \text{ for some } n \in \mathbb{Z} \}$

note: $\langle a \rangle$ is a subgroup of G, since:
$$a^n \cdot a^{-m} = a^{n-m} \in \langle a \rangle, \quad \forall n, m \in \mathbb{Z}$$
— and then use Corollary above

Def $\langle a \rangle$ is called the cyclic subgroup generated by a.

Def G is a ***cyclic group*** if $G = \langle a \rangle$ for some $a \in G$. (a is called a ***generator*** of G)

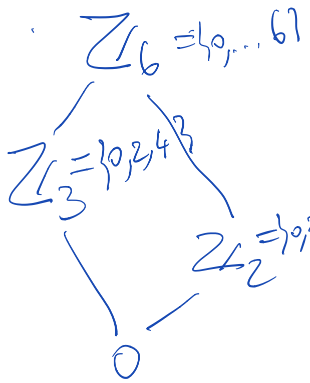
Eg: (1) $G = \mathbb{Z}$ is a cyclic group, generated by 1

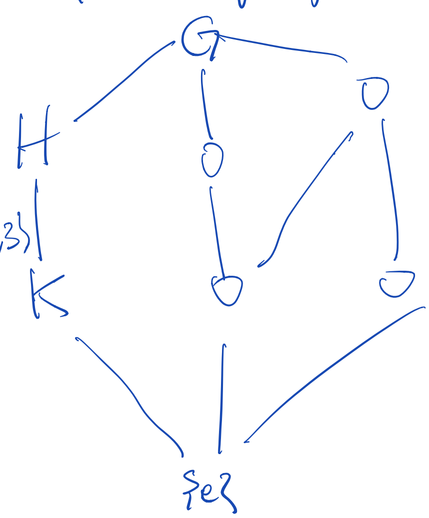
$$\langle 1 \rangle = \{ \underbrace{1 + \cdots + 1}_{n} : n \in \mathbb{Z} \} = \{ n : n \in \mathbb{Z} \} = \mathbb{Z}$$

(2) $\underset{\langle [1] \rangle}{\overset{\shortparallel}{\mathbb{Z}_n}}$ is a cyclic group of order n

---

Lattice of subgroups





eg