Cyclic Groups Cont.

$G = \langle a \rangle \qquad a \in G$

$\uparrow$ cyclic subgroup generated by a

If $a^n = e$ is the smallest such $n \Rightarrow |a| = n$

if no such n exists $\Rightarrow |a| = \infty$

If $|G| = |a| < \infty \Rightarrow$ G is a cyclic group generated by a

$\Rightarrow G = \langle a \rangle$

Ex] A cyclic group can have multiple generators

$\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$

$\{1, 2, 3, 4, 5, 0\} \qquad \{5, 4, 3, 2, 1, 0\}$

$\langle 2 \rangle = \{2, 4, 0\}$ is a proper subgroup

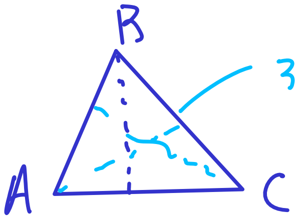
Ex] $U(9)$ = the group of units with mult modulo 9

$U(9) = \{1, 2, 4, 5, 7, 8\}$

$U(9) = \langle 2 \rangle$

$2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 7, \quad 2^5 = 5, \quad 2^6 = 1$

Ex] Not every Group is cyclic, consider Symetries of an equilateral triangle $= S_3$



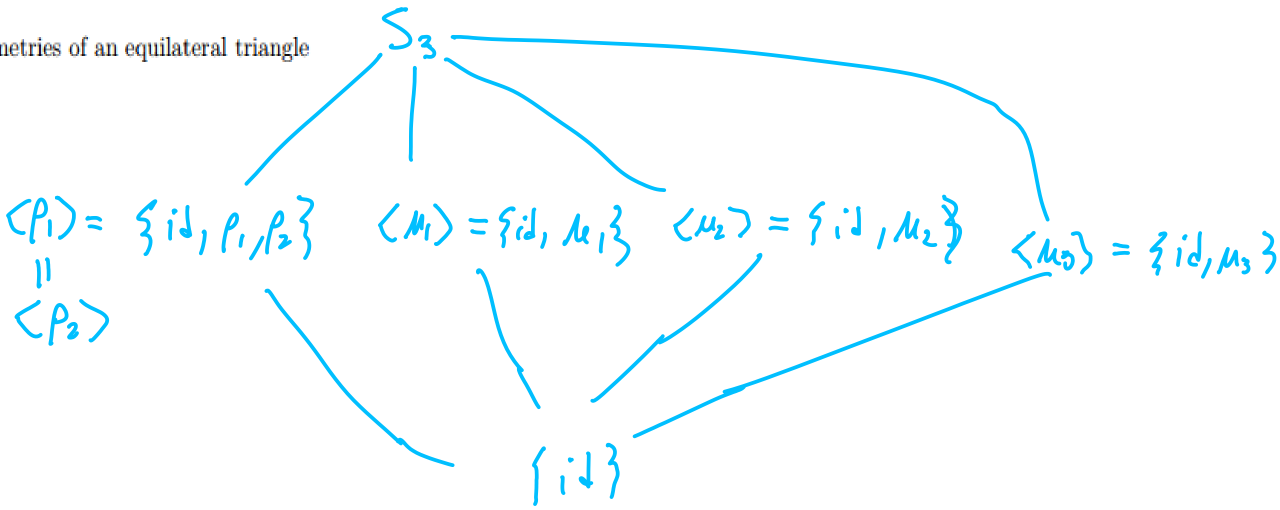
3 reflections
2 rotations

$\mu_1, \mu_2, \mu_3 =$ reflections

$\rho_1, \rho_2 =$ rotations.

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Table 3.7: Symmetries of an equilateral triangle



Thm.] Every cyclic group is abelian.

Proof:

Let $G = \langle a \rangle$ be cyclic.

If $g, h \in G \Rightarrow g = a^r, h = a^s$

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg. \quad \blacksquare$$

Thm.] Every subgroup of a cyclic group is cyclic.

<u>Proof:</u> Let $G = \langle a \rangle$ by cyclic, suppose H is a subgroup of G.

- If $H = \{\underset{\text{identity}}{e}\} \Rightarrow H$ is cyclic
- If H is strictly larger than $\{e\} \Rightarrow \exists\, g \in H$ s.t $g \neq e$

$\Rightarrow g = a^n$ for some $n \in \mathbb{Z}$ (we may assume $n > 0$)

consider the set of all a^n, $n > 0$ s.t $a^n \in H$
(which is non-empty)

By the principle of well ordering we may chose an $m \in \mathbb{N}$ that is the smallest m for which $a^m \in H$

Now show that $h = a^m$ generates H.

Suppose $h' \in H$, [idea: show $h' = h^l$ for some $l \in \mathbb{Z}$]

$h' = a^k$ for some $k > 0$ $(k \geq m)$

By the division alg. $\exists\, q, r \in \mathbb{Z}$ s.t.

$$k = mq + r \quad \text{where} \quad 0 \leq r < m$$

$$h' = a^k = a^{mq+r} = a^{mq} \cdot a^r = (a^m)^q a^r = h^q \cdot a^r$$

$h^{-q} a^k = a^r$. Since $a^k \in H$, $h^{-q} \in H$

$\Rightarrow a^r \in H$

$\Rightarrow r = 0$ Since m is the least non-zero integer s.t $a^m \in H$.

$k = mq$

$h' = a^k = a^{mq} = h^q$ $\therefore h' \in \langle h \rangle$. ∎

$\boxed{\text{corrallary}}$

The subgroups of $(\mathbb{Z},+)$ are exactly

$\langle n\rangle = n\mathbb{Z} = \{\ldots, -n, 0, n, 2n, 3n, \ldots\}$ for $n = 0, 1, 2, \ldots$

Remember $\boxed{|G| = |a| \text{ if } a \text{ generates } G}$

Prop Let $G = \langle a\rangle$ be a cyclic group, $|G| = n$.
Then $a^k = e$, $k > 0$, if and only if $n \mid k$ i.e. $k = ln$ for $l \in \mathbb{N}$

Proof:

Suppose $a^k = e$. By division alg. $k = nq + r$, $0 \le \underline{r < n}$

$\therefore e = a^k = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$

Since $r < n$ and $|a| = |G| = n$

$\Rightarrow r = 0$

$\therefore a^k = (a^n)^q \quad \therefore k = nq$

$\Rightarrow$ if $k = ln \Rightarrow a^k = a^{ln} = (a^n)^l = e$.

$\blacksquare$

Theorem Let G be a cyclic group of order n
$G = \langle a\rangle$. If $b = a^k$ then $|b| = \frac{n}{d}$ where
$d = \gcd(k, n)$.

Proof:

Want the smallest $m > 0$ s.t. $e = b^m = a^{km}$

By previous prop. this is the smallest m s.t.

$n \mid km$

equivalently $\frac{n}{d} \mid m\frac{k}{d}$ where $d = \gcd(n,k)$

Since d is gcd of n, k

$\Rightarrow$ [$\frac{n}{d}$ and $\frac{k}{d}$ are relatively prime

$\therefore \frac{n}{d} \nmid \frac{k}{d}$ Aside]

$\Rightarrow$ $\therefore$ if $\frac{n}{d} \mid m\frac{k}{d} \Rightarrow \frac{n}{d} \mid m$

$\therefore$ smallest choice for $m = \frac{n}{d}$.

Cor] The generators of $\mathbb{Z}_n$ are $r \in \mathbb{Z}$ s.t. $1 \leq r < n$ and $\gcd(r,n) = 1$.

Ex] $\mathbb{Z}_{16} = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 15 \rangle$

The Multiplicative Group of Complex numbers

$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

$i^2 = -1$

$z = a + bi$, $w = c + di$

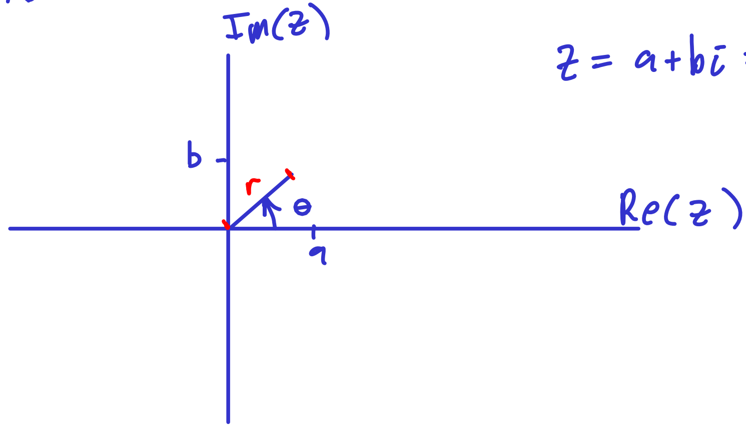
$z \cdot w = (ac - db) + (ad + bc)i$

$z \neq 0$

$z^{-1} = \dfrac{a - bi}{a^2 + b^2}$

$|z| = \sqrt{a^2+b^2}$

$z = a+bi = \mathrm{Re}(z) + \mathrm{Im}(z)i$



$z = a + ib$, $z = r(\cos(\theta) + i \sin\theta)$