Cyclic Subgroups

↑ Subgroup generated by 1 element

Ex | $3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, \ldots\}$

$\mathbb{Z}$ is a cyclic group (generated by 1)

Ex | $H = \{2^n \mid n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Q}^*$ (non-zero rationals with mult.)

If $a = 2^m, b = 2^n \in H \Rightarrow ab^{-1} = 2^m 2^{-n} = 2^{m-n} \in H$

(By Prop 3.31)

H is a subgroup.

Theorem 4.3. *Let G be a group and a be any element in G. Then the set*

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G that contains a.

Proofs:

- $e \in \langle a \rangle$ since $a^0 = e \in \langle a \rangle$
- If $g, h \in \langle a \rangle \Rightarrow g = a^m, h = a^n \Rightarrow g \cdot h = a^m \cdot a^n = a^{m+n} \in \langle a \rangle$
- $g = a^n \in \langle a \rangle \Rightarrow g^{-1} = a^{-n} \in \langle a \rangle$

$\therefore \langle a \rangle$ is a subgroup of G

Now any subgroup H of G containing a must contain all powers of a (by closure) $\therefore$ H contains $\langle a \rangle$ $\therefore$ $\langle a \rangle$ is the smallest of G containing a.

■

$G = \langle a \rangle$ — the cyclic subgroup generated by a

↑ generator.

If $a \in G$ the order of a is the smallest positive $n \in \mathbb{N}$ s.t. $a^n = e$, write this as $|a| = n$

If there is no such integer $\Rightarrow |a| = \infty$

- If $|G| = |a| < \infty$ and G is a cyclic group $\Rightarrow G = \langle a \rangle$

Ex] A cyclic group may have multiple gens.

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

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

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

- $\mathbb{Z}$, $\mathbb{Z}_n$ are cyclic

Ex] $U(9)$ the group of units mod 9 with mult.

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

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

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

Ex) Not every Group is cyclic, consider Symetries of an equilatral triangle.

$\circ$	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

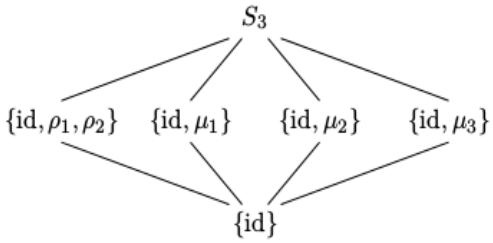

Figure 4.8: Subgroups of S_3

Theorem 4.9 Every cyclic group is abelian.

Proof:

Let $G = \langle a \rangle$ be cyclic, If $g, h \in G$ we have $g = a^r, b = a^s$

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

Theorem 4.10 Every subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle a \rangle$ be cyclic, Suppose H is a subgroup of G

- If $H = \{e\} \Rightarrow H$ cyclic
- Now Suppose $g \in H$, $g \neq e \Rightarrow g = a^n$ for $n \in \mathbb{Z}$ (we may assume $n > 0$)

$\therefore$ Consider the set of a^n, $n > 0$ (which is non-empty).
So 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 $h = a^m$ generates H. Suppose that $h' \in H$ (show that $h' = h^l, l \in \mathbb{Z}$)

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

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

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

$\Rightarrow h^1 = a^k = a^{mq+r} = (a^m)^q \cdot a^r = h^q \cdot a^r$

$a^r = a^k h^{-q}$ since $a^k \in H$, $h^{-q} \in H \Rightarrow a^r \in H$

but m is the smallest s.t. $a^m \in H \Rightarrow r = 0$

$\hookrightarrow h^1 = h^q$ for any $h^1 \in H$

$\Rightarrow H = \langle h \rangle$ ∎

Corrollary 1

The subroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$

↑ All cyclic subgroups.

Propcsition 4.12

Let G ba a cyclic group of order n and suppose $a = \langle a \rangle$

Then $a^k = e$ if and only if $n \mid k$ (i.e. $k = ln$ $l \in \mathbb{N}$)

Proof:

suppose $a^k = e$. by division alg $k = nq + r$, $0 \le r < n$

$\therefore \quad e = a^k = a^{nq} \cdot a^r = a^r \Rightarrow a^k = a^{nq}$ whenever $a^k = e$

if $n \mid k \Rightarrow k = ns \quad a^k = a^{ns} = e$ ∎

Theorem 4.13 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

wish to find smallest $m \in \mathbb{Z}$ s.t. $e = b^m - a^{km}$

by the previous proposition this is the smallest m s.t.

$n \mid km$

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

$d = \gcd(n,k) \Rightarrow \frac{n}{d}, \frac{k}{d}$ are relatively prime.

$\Rightarrow$ if $\frac{n}{d} \mid m\left(\frac{k}{d}\right)$ then $\frac{n}{d} \mid m$

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

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

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

$1 \cdot 9 = 9$	$2 \cdot 9 = 2$	$3 \cdot 9 = 11$
$4 \cdot 9 = 4$	$5 \cdot 9 = 13$	$6 \cdot 9 = 6$
$7 \cdot 9 = 15$	$8 \cdot 9 = 8$	$9 \cdot 9 = 1$
$10 \cdot 9 = 10$	$11 \cdot 9 = 3$	$12 \cdot 9 = 12$
$13 \cdot 9 = 5$	$14 \cdot 9 = 14$	$15 \cdot 9 = 7.$