

(Chapter 4) Cyclic Groups

$\mathbb{Z}, \mathbb{Z}_n$  are groups under addition & addition modulo  $n$ , respectively, and are examples of cyclic groups.

(§ 4.1) Cyclic Subgroups and Groups.

Some examples:

1)  $3 \in \mathbb{Z}$ . Then all multiples of 3 give the set

$$3\mathbb{Z} = \{ \dots, -6, -3, 0, 3, 6, \dots \}$$

Prop. 3.31

$3\mathbb{Z} \leq \mathbb{Z}$ , since  $\forall g, h \in 3\mathbb{Z}, g = 3k, h = 3l$  and

$$h^{-1} = -3l \quad (\text{as } 3l + (-3l) = 0) \Rightarrow (3k) + (-3l) =$$

$$3(k-l) \in 3\mathbb{Z}. \quad \text{Note: every element in } 3\mathbb{Z} \text{ is}$$

"generated" by 3.

2)  $H = \{ 2^n, n \in \mathbb{Z} \} \leq \mathbb{R}^*$  since  $\forall g = 2^n, h = 2^m$

$$\text{with } h^{-1} = (2^m)^{-1} = 2^{-m}, gh^{-1} = 2^n 2^{-m} = 2^{n-m} \in H.$$

look at  $H$ : every element is "generated" by 2.

3) Consider group  $G$  and  $a \in G$ . (abstractly)

Q: What is the smallest subgroup of  $G$  that contains  $a$ ?

It must also contain identity, then all powers of  $a$  (closure!), inverse  $a^{-1}$ , all powers of  $a^{-1}$ . Thus:

$$\{ \dots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots \}$$

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

notation (angle brackets)

(generated by  $a$ )

Thm. 4.3  $\langle a \rangle = \{ a^k, k \in \mathbb{Z} \} \leq G$  and

( $G$ -group,  $a \in G$ )  $\langle a \rangle$  is the smallest subgroup of  $G$  containing  $a$ . ( $\Rightarrow \langle a \rangle \neq \emptyset$ )

Proof:  $a^0 \in \langle a \rangle$  and  $e = a^0$  is the identity:

$\forall a^k, a^k a^0 = a^0 a^k = a^k$ . Take  $g, h \in \langle a \rangle$ , s.t.

$g = a^k, h = a^l$ . Then since  $h^{-1} = (a^l)^{-1} = a^{-l} \in \langle a \rangle$

and  $gh^{-1} = a^k a^{-l} = a^{k-l} \in \langle a \rangle \Rightarrow \langle a \rangle \leq G$ .  
by Subgroup test

$\langle a \rangle$  is the smallest, as if any other subgroup of  $G$ ,  $H$ , contains  $a$ , by closure, it must contain all the powers of  $a \Rightarrow \langle a \rangle \subset H$ .  $\square$

Note: if we have addition on  $G$ , then  $\langle a \rangle$  looks like  $\langle a \rangle = \{ ka, k \in \mathbb{Z} \} \leq G$ .

Earlier:  $3\mathbb{Z} = \langle 3 \rangle \leq \mathbb{Z}$ ,  $\langle 2 \rangle = \{ 2^n, n \in \mathbb{Z} \} \leq \mathbb{R}^*$ ,  $\langle a \rangle \leq G$ . They all are examples of cyclic subgroups.

Def: For  $a \in G$  (group),  $\langle a \rangle = \{ a^k, k \in \mathbb{Z} \}$  is the cyclic subgroup of  $G$  generated by  $a$ .

Def: If a group  $G = \langle a \rangle$  for some  $a \in G$ , then  $G$  is a cyclic group,  $a$  is called a generator of  $G$ .

Def: Order of  $a \in G$  is the smallest  $n \in \mathbb{N}$  s.t.  $a^n = e$  (or  $na = e$ ). We write  $|a| = n$ . ( $n > 0$ )  
If there is no such  $n$ ,  $|a| = \infty$  (the order of  $a$  is infinite).

Recall:  $|G| = \#$  elements in  $G$  (order of a group)

More Examples:

1)  $(\mathbb{Z}, +)$  is cyclic. (infinite)

$\mathbb{Z} = \langle 1 \rangle = \{ k \cdot 1, k \in \mathbb{Z} \} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$   
Also,  $\mathbb{Z} = \langle -1 \rangle = \{ k(-1), k \in \mathbb{Z} \}$  (1 & -1 are inverses)

$\mathbb{Z}$  has 2 generators. Note: no other integers can generate the entire  $\mathbb{Z}$ , we only get cyclic subgroups of  $\mathbb{Z}$  (ex:  $3\mathbb{Z}$ )

Remark:  $|1| = |-1| = \infty$  since there is no  $n \in \mathbb{N}$ , s.t.  $n \cdot (\pm 1) = 0$  (identity of  $\mathbb{Z}$ )

2)  $\mathbb{Z}_n$  is a cyclic group. (finite, of order n) Under addition mod n

$\mathbb{Z}_n = \{ 0, 1, 2, \dots, n-1 \}$ . Generators? 1 and n-1

for sure.  $\mathbb{Z}_n$  may have more generators, depending on n (later!) inverses

Consider  $\mathbb{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}$

Note: if  $\langle a \rangle = G \Rightarrow \langle a^{-1} \rangle = G$

$\langle 1 \rangle = \{ 1, 1+1, 1+1+1, 1+1+1+1, \dots \}$   
 $= \{ 1, 2, 3, 4, 5, 0 \} = \mathbb{Z}_6$

$\langle 2 \rangle = \{ 2, 2+2, 2+2+2, \dots \} = \{ 2, 4, 0 \} \neq \mathbb{Z}_6$

$\langle 3 \rangle = \{ 3, 3+3, \dots \} = \{ 3, 0 \} \neq \mathbb{Z}_6$

$\langle 4 \rangle = \{ 4, 2, 0 \} = \langle 2 \rangle \neq \mathbb{Z}_6$

$\langle 0 \rangle = \{ 0 \} \neq \mathbb{Z}_6$

$\langle 5 \rangle = \langle 6-1 \rangle = \{ 5, 5+5, 5+5+5, \dots \}$   
 $= \{ 5, 4, 3, 2, 1, 0 \} = \mathbb{Z}_6$

So,  $\mathbb{Z}_6$  has only 2 generators, 1 and 5  
(Note  $|1| = 6, |5| = 6$   
 $6 \cdot 1 = 0 \pmod{6}, 6 \cdot 5 = 30 \equiv 0 \pmod{6}$ )

If we consider  $\mathbb{Z}_8 = \{0, 1, 2, \dots, 7\}$ , then

$\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$ , i.e., 1, 3, 5, 7 are generators of  $\mathbb{Z}_8$ .

E.g.,  $\langle 3 \rangle = \{3, 3+3, 3+3+3, \dots\} = \{3, 6, 1, 4, 7, 2, 5, 0\} = \mathbb{Z}_8$

$\langle 2 \rangle = \{0, 2, 4, 6\} \neq \mathbb{Z}_8$ .

3) Consider  $U(9)$ , the group of units of  $\mathbb{Z}_9$

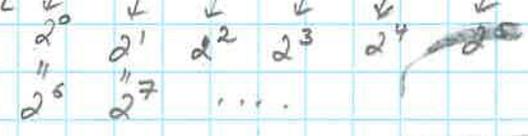
$U(9) = \{1, 2, 4, 5, 7, 8\}$

recall: these are coprime w/ 9  $\Rightarrow$  they all have multiplicative inverses modulo 9:

$8^{-1} \equiv 8 \pmod{9}$  as  $8 \cdot 8 = 64 \equiv 1 \pmod{9}$   
 $1^{-1} = 1 \pmod{9}$   
 $5 \cdot 2 = 10 \equiv 1 \pmod{9}$  etc, etc.  
 $4 \cdot 7 = 28 \equiv 1 \pmod{9}$

$\langle 1 \rangle = \{1\} \neq U(9)$

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



$|2| = 6$

So,  $U(9)$  is cyclic with 2 being a generator.

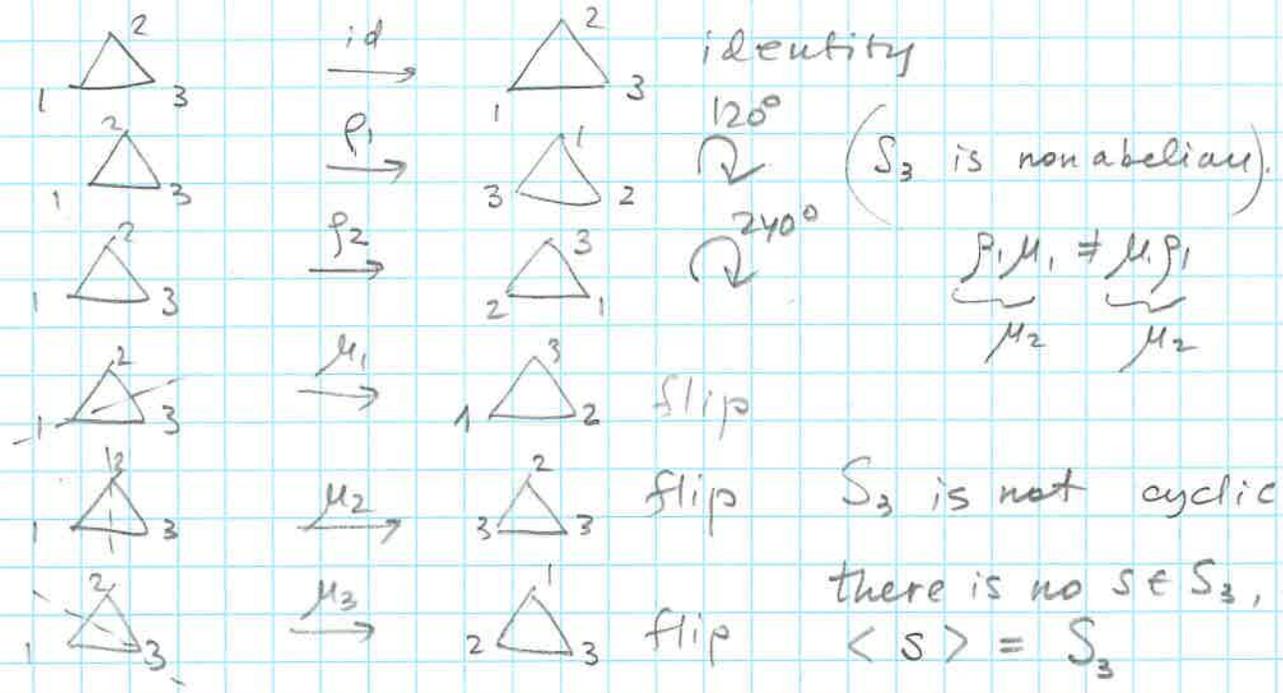
Others?  $\langle 4 \rangle = \{1, 4, 7\}$ . Check other elements!

Are there any other generators?

4) Not every group is a cyclic group.

Ex. 4.7  $S_3 = \{id, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\} (= D_3)$

the symmetry group of an equilateral triangle.



Subgroups of  $S_3$ :  $\{id\}$ ,  $\{id, \mu_1\}$ ,  $\{id, \mu_2\}$ ,  $\{id, \mu_3\}$ ,  $\{id, \rho_1, \rho_2\}$  are all cyclic!

(See Fig. 3.5 in § 3.1)

$\{id\} = \langle id \rangle$   
 $\{id, \mu_i\} = \langle \mu_i \rangle$   
 $\{id, \rho_1, \rho_2\} = \langle \rho_1 \rangle = \langle \rho_2 \rangle$

Remark:  $D_4$  is not a cyclic group either.

(But, clearly, the subgroup of all rotations  $\{R_0, R_{90}, R_{180}, R_{270}\} = \langle R_{90} \rangle$  is cyclic!

Thm. (4.9) Every cyclic group is abelian.

Proof: If  $G = \langle a \rangle$ , then  $\forall g, h \in G$ ,

$g = a^m, h = a^n$  for some  $m, n \in \mathbb{Z}$ . Then

$gh = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = hg.$  □

## Subgroups of Cyclic Groups

(6)

- Thm. (4.10) Every subgroup of a cyclic group is cyclic.

Proof: Let  $G = \langle a \rangle$  and  $H \leq G$ .

If  $H = \{e\} \Rightarrow H$  is cyclic.

If  $H \neq \{e\}$  (non-trivial) then there is  $a^n \in H$  for some integer  $n > 0$ . Why? Since  $G = \langle a \rangle$

$\Rightarrow \forall h \in H, h = a^n, n \in \mathbb{Z}$ . Since  $H \leq G \Rightarrow h^{-1} \in H$ ,  $h = a^{-n}$ . Either  $n > 0$  or  $-n > 0$ .

So, from above, we assume that  $H$  contains some positive powers of  $a$ , i.e.  $a^n, n > 0$ . We can also pick  $m$  to be the smallest power of  $a$ ,  $m > 0$  (such  $a^m \in H$ ) ( $m$  exists by WOP). We now claim that  $h = a^m$

is a generator for the subgroup  $H$ , that is,  $\forall g \in H$ ,  $g$  is a power of  $a^m$ . Since  $g \in H \Rightarrow g = a^k, k \in \mathbb{Z}$ , and by the division algorithm,  $\exists q, r$  (integers)

s.t.  $k = mq + r, 0 \leq r < m$ ; therefore,

$$g = a^k = a^{mq+r} = \underbrace{(a^m)^q}_h a^r = h^q a^r \Rightarrow a^r = \underbrace{a^k}_{\text{in } H} \underbrace{h^{-q}}_{\text{in } H} \Rightarrow$$

$a^r \in H$ . Since  $0 \leq r < m$  and  $m$  is the

smallest power of  $a$  in  $H$ , then  $r$  must be 0.

Thus,  $g = a^k = h^q \underbrace{a^0}_e = (a^m)^q$ , i.e. any  $g \in H$

is a power of  $a^m$ . Hence,  $H = \langle a^m \rangle$  (cyclic)  $\square$

- Corollary (4.11)  $n\mathbb{Z}, n = 0, 1, 2, \dots$  form cyclic subgroups of  $\mathbb{Z}$

• Proposition: If  $G = \langle a \rangle$  and  $|a| = n$ , then  
 $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ . ( $\Rightarrow a^n = e$  or  $na = e$ )

Proof: Indeed, the elements  $e, a, \dots, a^{n-1}$  are in  $\langle a \rangle$ .

Now suppose that  $a^k$  is an arbitrary member of  $\langle a \rangle$ . then  $a^k = a^{nq+r} = (a^n)^q a^r = e a^r = a^r$ .

(by division alg.,  $k = nq + r$ ,  $0 \leq r < n$ )  $\rightarrow |a| = n$

Since  $0 \leq r < n \Rightarrow a^r = a^k \in \langle a \rangle$ . Thus,  $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$  if  $|a| = n$ .  $\square$

• Corollary:  $|\langle a \rangle| = |a|$   
# elements in  $\langle a \rangle$       order of  $a$  ( $\Rightarrow$  clear why we use the same notation for  $|G|$  &  $|a|$ )

• Proposition (4.12) Let  $G$  be a cyclic group,  $|G| = n$ , and suppose  $G = \langle a \rangle$  for some  $a \in G$ .

Then  $a^k = e \Leftrightarrow n | k$ . ( $k \in \mathbb{Z}$ )  
( $ka = e$ )

Proof: read! (using the division algorithm.)

• Corollary:  $G = \langle a \rangle$ ,  $|G| = n$ . Then  $a^k = e \Leftrightarrow |a| | k$ .  
(recall  $|\langle a \rangle| = |a|$ )  $\Rightarrow n | k \Rightarrow |a| | k$

• Theorem (4.13) Let  $G = \langle a \rangle$  (cyclic),  $|G| = n$ .

If  $b = a^k$ , then  $|b| = \frac{n}{\gcd(k, n)}$ .  
( $b = ka$ )

Proof: Let  $|b| = m$ , that is,  $m$  is the smallest positive integer s.t.  $b^m = e$ . What is  $m$ ? Since  $b = a^k$

$\Rightarrow (a^k)^m = a^{km} = e$ . Let  $d = \gcd(k, n)$ . By Prop. 4.12,

$n | km \Rightarrow \frac{n}{d} | \frac{km}{d}$ . Also, since  $d | k$ ,  $d | n$ , and  $\exists r, s$

s.t.  $rk + sn = d \Rightarrow r(\frac{k}{d}) + s(\frac{n}{d}) = 1 \Rightarrow \frac{k}{d}$  &  $\frac{n}{d}$  are

relatively prime! Then, since  $\frac{n}{d} \mid \left(\frac{k}{d}\right)m$   
 then  $\frac{n}{d} \mid m \Rightarrow$  the smallest such  $m = \frac{n}{d} = \frac{n}{\gcd(k,n)}$   
 ( $m \geq \frac{n}{d}$ )

• Corollary (4.14) The generators of  $\mathbb{Z}_n$  are  $r \in \mathbb{Z}$ ,  $1 \leq r < n$  s.t.  $\gcd(r, n) = 1$ .  
 ( $r, n$  are coprime) □

Why? Let  $\langle r \rangle = \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ ,  $1 \leq r < n$ .

Then  $|r| = n$ . Also, since  $\langle 1 \rangle = \mathbb{Z}_n$ , then  
 $r = r \cdot 1 \Rightarrow |r| = \frac{n}{\gcd(r, n)} = n \Leftrightarrow \gcd(r, n) = 1$ .  
 $k=r$  generator Thm. 4.13

• Examples:

1)  $\mathbb{Z}_6 = \{0, 1, \dots, 5\} = \langle 1 \rangle = \langle 5 \rangle$

2)  $\mathbb{Z}_9 = \{0, 1, 2, \dots, 8\} = \langle 1 \rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 8 \rangle$ .

3)  $\mathbb{Z}_{12}: |3| = |3 \cdot 1| = \frac{12}{\gcd(3, 12)} = \frac{12}{3} = 4$  (Check:  $4 \cdot 3 = 12 \equiv 0 \pmod{12}$ )  
order of 3 → generator

4) Suppose  $G$  is a finite group and  $g \in G$ .

What are the possibilities for  $|g|$  if  $g^6 = e$ ?

Recall  $|g| \mid 6$ . Then  $|g| = 1, 2, 3, 6$ .

5) Ex. 4.15 in text

• Fundamental Theorem of Cyclic Groups.

If  $|\langle a \rangle| = n$  then the subgroups of  $\langle a \rangle$  are the cyclic groups  $\langle a^{n/k} \rangle$  of order  $k$ , where  $k$  varies over all positive divisors of  $n$ .

$\langle \frac{n}{k} a \rangle$  for  $(\oplus)$

Example:  $G = \langle a \rangle$ ,  $|G| = |\langle a \rangle| = 30$ .

Then the subgroups of  $G$  are:  $\langle a^{30/k} \rangle$  of order  $k$  for each  $k = 1, 2, 3, 5, 6, 10, 15, 30$ , i.e.

$k=30$   $\langle a \rangle = \{e, a, a^2, \dots, a^{29}\}$  order 30

$k=15$   $\langle a^2 \rangle = \{e, a^2, a^4, \dots, a^{28}\}$  order 15

$k=10$   $\langle a^3 \rangle = \{e, a^3, a^6, \dots, a^{27}\}$  order 10

$k=6$   $\langle a^5 \rangle = \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\}$  order 6

$k=5$   $\langle a^6 \rangle = \{e, a^6, a^{12}, a^{18}, a^{24}\}$  order 5

$k=3$   $\langle a^{10} \rangle = \{e, a^{10}, a^{20}\}$  order 3

$k=2$   $\langle a^{15} \rangle = \{e, a^{15}\}$  order 2

$k=1$   $\langle a^{30} \rangle = \{e\}$  order 1

$\mathbb{Z}_{30}$ :	$k=1$ :	$\langle 30/1 \rangle = \langle 30 \rangle = \langle 0 \rangle = \{0\}$	order 1
"	$k=2$ :	$\langle 30/2 \rangle = \langle 15 \rangle = \{15, 0\}$	order 2
"	$k=3$ :	$\langle 30/3 \rangle = \langle 10 \rangle = \{10, 20, 0\}$	order 3
$\langle 1 \rangle$	$k=5$ :	$\langle 30/5 \rangle = \langle 6 \rangle = \{6, 12, 18, 24, 0\}$	order 5
	$k=6$ :	$\langle 30/6 \rangle = \langle 5 \rangle = \{5, 10, 15, 20, 25, 0\}$	order 6
	$k=10$ :	$\langle 30/10 \rangle = \langle 3 \rangle = \{3, 6, 9, \dots, 27, 0\}$	order 10
	$k=15$ :	$\langle 30/15 \rangle = \langle 2 \rangle = \{2, 4, 6, \dots, 28, 0\}$	order 15
	$k=30$ :	$\langle 30/30 \rangle = \langle 1 \rangle = \{1, 2, \dots, 29, 0\} = \mathbb{Z}_{30}$	order 30

Q: How many subgroups does  $\mathbb{Z}_{18}$  have?

divisors of 18: 1, 2, 3, 6, 9, 18  $\Rightarrow 6$

Of order 6? one:  $\langle 18/6 \rangle = \langle 3 \rangle = \{3, 6, 9, 12, 15, 0\}$