

## Cyclic Groups:

Def: A subgroup  $H$  of  $G$  is a subset of  $G$  which is still a group using the operation  $*$  of  $G$ .

Notation: we write  $H \leq G$

If  $H = \{e\}$  we call  $H$  trivial. If  $H \neq G$  we call  $H$  proper.  $H \leq G$

A subgroup is cyclic if it is of the form

$$H = \{a^k \mid k \in \mathbb{Z}\} = \{e, a, a^{-1}, a^2, a^{-2}, a^3, a^{-3}, \dots\}$$

Notation:  $H = \langle a \rangle$

$H$  is the subgroup generated by  $a$  and  $a$  is a generator for  $H$ .

A group  $G$  is cyclic if  $G = \langle a \rangle$  for some  $a \in G$ .

Ex:  $H = \{3k \mid k \in \mathbb{Z}\}$  is the subgroup of  $\mathbb{Z}$  generated by 3

Ex:  $H = \{(1234), (13)(24), (4321), e\}$   
is the cyclic subgroup of  $S_4$  gen. by  $(1234)$ .

Ex:  $H = \{(1234), (13)(24), (4321), e,$   
 $(12)(34), (23)(14), (24)(13)\} \leq S_4$

is not a cyclic subgroup. **Why not?**

**Q: What do subgroups of  $\mathbb{Z}$  look like??**

**Properties of cyclic groups:**

Prop: If  $G$  is cyclic, then  $G$  is abelian.

Theorem: Every subgroup of a cyclic group is cyclic.

Proof:

$$G = \langle a \rangle, \quad H = \{a^{m_1}, \dots, a^{m_r}\} \leq G.$$

Let  $m = \gcd(m_1, m_2, \dots, m_r)$ .

Then  $m = k_1 m_1 + \dots + k_r m_r$  for some  $k_1, \dots, k_r \in \mathbb{Z}$ .

Thus

$$a^m = (a^{m_1})^{k_1} (a^{m_2})^{k_2} \dots (a^{m_r})^{k_r} \in H. \text{ Hence } \langle a^m \rangle \leq H.$$

Also  $m | m_j \forall 1 \leq j \leq r$  so  $\exists n_j \in \mathbb{Z}$  with  $m_j = n_j m$ .

Thus

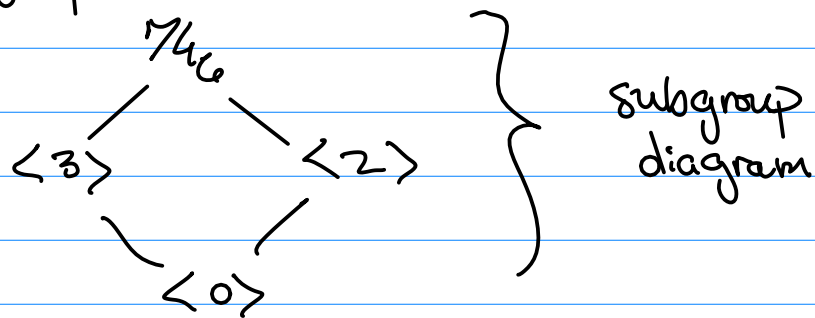
$$a^{m_j} = (a^m)^{n_j} \in \langle a^m \rangle \quad \therefore H \leq \langle a^m \rangle.$$

Consequently  $H = \langle a^m \rangle$  is cyclic.  $\square$

Ex: The subgroups of  $\mathbb{Z}_6$  are

$$\begin{aligned} \langle 0 \rangle &= \{0\} & \langle 3 \rangle &= \{0, 3\} \\ \langle 1 \rangle &= \mathbb{Z}_6 & \langle 4 \rangle &= \{0, 2, 4\} \\ \langle 2 \rangle &= \{0, 2, 4\} & \langle 5 \rangle &= \mathbb{Z}_6 \end{aligned}$$

Five subgroups



Theorem:  $\langle a^m \rangle$  generates  $G = \langle a \rangle \iff$

$\gcd(m, n) = 1$  where  $|G| = n$ .

Proof:

If  $\langle a^m \rangle = G$ , then  $a = (a^m)^k$  for some  $k$ .

Therefore  $a^{mk-1} = e$ , so that  $mk-1 = nj$  for some  $j$ . Thus  $\gcd(m, n) = 1$ . Conversely,

if  $\gcd(m, n) = 1$  then  $mk - nj = 1$  for some  $m, n$

and therefore  $a = a^{mk-nj} = a^{mk} = (a^m)^n \in \langle a^m \rangle$ .

It follows that  $G = \langle a^m \rangle$ .

$\square$

Theorem: If  $G$  is a cyclic group, then

$$G \cong \mathbb{Z} \quad \text{or} \quad G \cong \mathbb{Z}_n \quad \text{for some } n.$$

Proof:

Let  $G = \langle a \rangle$  for some  $a \in G$ .

Case I: If  $|G| = \infty$ , define

$$f: \mathbb{Z} \rightarrow G, \quad f(k) = a^k$$

This is surjective and satisfies  $f(j+k) = f(j)f(k)$   
If  $f(j) = f(k)$  then  $a^{k-j} = 1$ . If  $k-j \neq 0$ , then  
this means  $a$  has finite order  $\Rightarrow \Leftarrow$ . Thus  $k-j=0$

so  $f$  is injective. Thus it is an isomorphism.

Case II: If  $|G| = n < \infty$  define

$$f: \mathbb{Z}_n \rightarrow G, \quad f(k) = a^k$$

This is surjective and satisfies  $f(j+k) = f(j)f(k)$

Since  $|\mathbb{Z}_n| = |G|$  this automatically makes  $f$  injective too

Hence  $f$  is an isomorphism

□



