

Proposition: (subgroups of  $\mathbb{Z}$ ) Let  $H \subseteq \mathbb{Z}$ .

Then  $H$  is cyclic, and either

$$H = \langle n \rangle \text{ where}$$

$n \in \mathbb{N}$  is the smallest natural number in  $H$  or  $H = \{0\}$ .

proof: Suppose  $H \neq \{0\}$ . Then  $\exists m \in \mathbb{Z}$ ,

$m \in H$  and  $m \neq 0$ . Since  $H \subseteq \mathbb{Z}$ ,

$\exists -m \in H$ . Therefore, we may

assume that  $H \cap \mathbb{N} \neq \emptyset$ .

By the Well-Order Principle,

$\exists n \in H \cap \mathbb{N}$  such that

$\forall m \in H \cap \mathbb{N}, n \in \mathbb{N}$ ,

Then since  $H \subseteq \mathbb{Z}$  and  $n \in H$ ,

$\langle ns \rangle \subseteq H$ . Now suppose

$\exists k \in H, k \notin \langle ns \rangle$ .

Then by the division algorithm,

$\exists q, r \in \mathbb{Z}, 0 \leq r < n$ ,

with

$$k = nq + r.$$

Since  $k \in H$  and  $nq \in \langle ns \rangle \subseteq H$ ,

we know

$$k - nq \in H$$

Note  $nq \in \langle n \rangle$  since

$$nq = \underbrace{n + n + n + \dots + n}_{q \text{ times}} \quad \text{if } q > 0$$

$$\text{or } -nq = \underbrace{-n - n - n - \dots - n}_{q \text{ times}} \quad \text{if } q < 0.$$

But

$$r = k - nq \in H.$$

We assumed that  $n$  was the smallest positive integer in  $H$ , and since  $0 \leq r < n$ , we must have

$r=0$ . Therefore,  $k=nq \in \langle n \rangle$ ,

so  $H = \langle n \rangle$ .

□

**Observation:** If  $n \in \mathbb{N}$ , then in  $\mathbb{Z}$ ,

$$\langle n \rangle = n\mathbb{Z} . \text{ So by}$$

the previous proposition,

every subgroup of  $\mathbb{Z}$  is

of the form  $n\mathbb{Z}$  for

$$n \in \mathbb{N} \cup \{0\} -$$

Proposition: (subgroups of  $\mathbb{Z}_n$ ) Let

$H \subseteq \mathbb{Z}_n$ . Let  $d \in \{1, 2, \dots, n-1\}$

be the smallest positive integer

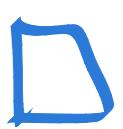
such that  $[d] \in H$ . Then

either  $H = \langle d \rangle$  or no

such  $d$  exists, in which case,

$$H = \{[0]\}.$$

proof: Identical to that for  $\mathbb{Z}$ , with  
a bit more care taken with  
the modulus-



Corollary: (Subgroups of cyclic groups)

Every subgroup of a cyclic group is cyclic.

Proof: Let  $G$  be a cyclic group.

Suppose  $H \subseteq G$ . Let

$$\varphi : G \rightarrow \{\mathbb{Z}, \mathbb{Z}_{|G|}\}$$

be an isomorphism

( $\varphi : G \rightarrow \mathbb{Z}$  if  $|G| = \infty$  and

$\varphi : G \rightarrow \mathbb{Z}_{|G|}$  if  $|G| < \infty$ ) .

Then  $\varphi(H) \subseteq \varphi(G)$ ,

since

$\mathcal{Q}(H)$  1)  $e_6 \in H$ , so  
nonempty

$0 = \varphi(e_6) \in \varphi(H)$  if  $|G| = \infty$

$[0] = \varphi(e_6) \in \varphi(H)$  if  $|G| < \infty$ .

$\mathcal{Q}(H)$   
is closed  
under " $+$ " 2) If  $x, y \in \mathcal{Q}(H)$ , then  
 $\exists a, b \in H, x = \varphi(a),$   
 $y = \varphi(b)$ . Then

$$x + y = \varphi(a) + \varphi(b)$$

$$x + y = \varphi(a \cdot b) \in \varphi(H)$$

Inverses  
of elements  
in  $\mathcal{Q}(H)$   
are in  $\mathcal{Q}(H)$  3) If  $x \in \mathcal{Q}(H)$ ,  $x = \varphi(a)$  for  
 $a \in H$ , then  $\bar{a} \in H$  since  $H \subseteq G$ ,  
and  $x^{-1} = \varphi(a)^{-1} = \varphi(\bar{a}) \in \varphi(H)$

By the subgroup test,

$$\varphi(H) \subseteq \varphi(G).$$

Every subgroup of  $\mathbb{Z}$  or  $\mathbb{Q}_\lambda$

is cyclic, so  $\exists x \in \varphi(H)$ ,

$$\varphi(H) = \langle x \rangle. \text{ Applying } \varphi^{-1},$$

$$H = \langle \varphi^{-1}(x) \rangle.$$

Note:  $\forall z, y \in \varphi(G),$

$$\varphi^{-1}(z+y) = \varphi^{-1}(\varphi(a)+\varphi(b))$$

for some  $a, b \in G$ .

Since  $\varphi$  is an isomorphism,

$$\varphi^{-1}(z+y) = \varphi^{-1}(\varphi(a) + \varphi(b))$$

$$\varphi^{-1}(z+y) = \varphi^{-1}(\varphi(a \cdot b))$$

$$\varphi^{-1}(z+y) = a \cdot b$$

$$\varphi^{-1}(z+y) = \varphi^{-1}(z) \cdot \varphi^{-1}(y) \quad \checkmark$$

Therefore,  $\varphi^{-1}$  is an isomorphism

onto  $G$ , so

$$H = \varphi^{-1}(\varphi(H)) = \varphi^{-1}(\langle x \rangle)$$

$$\text{But } \varphi^{-1}(\langle x \rangle) = \{ \varphi^{-1}(nx) \mid n \in \mathbb{Z} \}$$

$$= \{ (\varphi^{-1}(x))^n \mid n \in \mathbb{Z} \}$$



Corollary: (generators of  $\mathbb{Z}_n$ ) Let

$x \in \{1, 2, \dots, n-1\}$ . Then

$\langle [x] \rangle = \mathbb{Z}_n$  if and only

if  $\gcd(x, n) = 1$ . In

particular, if  $n$  is prime,

every nonzero element is a

generator of  $\mathbb{Z}_p$ !

Proof:  $\Rightarrow$  If  $\langle [x] \rangle = \mathbb{Z}_n$ ,

then  $[1] \in \langle [x] \rangle$ .

If this is so, then

$\exists m \in \mathbb{N}$ ,

$$[1] = n [x] .$$

Unravelling,

$$1 \equiv mx \pmod{n} ,$$

so  $\exists l \in \mathbb{Z}$ ,

$$1 - mx \equiv ln \quad , \text{ and}$$

$$1 \equiv ln + mx$$

$$\Rightarrow \gcd(n, x) = 1 .$$

$\Leftarrow$  Suppose  $\gcd(n, x) = 1$ .

Then  $\exists l, m \in \mathbb{Z}$ ,

$$1 \equiv ln + mx .$$

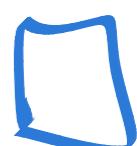
Then

$$(-mx \equiv l \pmod{n})$$

$$\Rightarrow l \equiv mx \pmod{n}$$

$$\Rightarrow [l] = m[x]$$

$$\Rightarrow [l] \in \langle [x] \rangle$$



Note: the only generators of  $\mathbb{Z}$   
are  $\lambda = 1$  and  $\lambda = -1$ .