

LECTURE 12  
(Friday OCT. 25, 2019)

— When  $G$  is cyclic they're the only ones!

★) EX Subgroups of  $(\mathbb{Z}, +)$ ? Examples:  $\langle N \rangle = N\mathbb{Z}$

Any subgroup  $H \leq \mathbb{Z}$  is of this form:  $H = N\mathbb{Z}$ .

Why? May assume  $H \neq \{0\}$ .

↑  
unique if  $\geq 0$ .

By (3) it contains a positive number.

Let  $N :=$  smallest positive integer  $\in H$

(well-ordering principle...)

CLAIM:  $H = N\mathbb{Z}$

$\supseteq$ : immediate.  $Nn = \overbrace{N + \dots + N}^n \in H$  by (1).

$\subseteq$ :  $a \in H$  arbitrary. Division w. remainder: and (3) if  $n < 0$ .  
... and if  $n = 0$ ?

$$\begin{array}{c} a \\ H \end{array} = \begin{array}{c} qN \\ H \end{array} + r, \quad 0 \leq r < N.$$

Deduce  $r = a - qN$  belongs to  $H$ .

Since  $r < N$  and  $N$  minimal,  $r$  cannot

be  $> 0$ . Thus  $r = 0$ , meaning

$$a = qN \in N\mathbb{Z}. \quad \checkmark$$

EX (cf. HW)

$$M\mathbb{Z} \cap N\mathbb{Z} = \text{LCM} \cdot \mathbb{Z}$$

$$M\mathbb{Z} + N\mathbb{Z} = \text{GCD} \cdot \mathbb{Z}$$

Theorem. Let  $(G, *)$  be a cyclic group.  
 Then every subgroup  $H \leq G$  is also cyclic.

PROOF. When  $|G| = \infty$  we know  $G$  is "isomorphic" to  $\mathbb{Z}$ ,  
 and this boils down to the previous ex.

— assume  $|G| < \infty$ .

Say  $G = \langle a \rangle$ . May assume  $H \neq \{e\}$ .

Let  $m :=$  smallest positive integer  
 for which  $a^m \in H$ .

1st one  
 in  $H$ .  
 $\downarrow$

CLAIM:  $H = \langle a^m \rangle$ .  $G = \{e, a, \dots, a^m, \dots\}$ .

$\supseteq$ : Obvious — using axioms (1)–(3) of course..

$\subseteq$ :  $b \in H$ . Write  $b = a^n$  some  $n \in \mathbb{Z}$ .

Div. Alg.:  $n = qm + r$ ,  $0 \leq r < m$ .

$$\begin{array}{ccc} \Downarrow & & \\ a^n = (a^m)^q * a^r & & \\ \nearrow & \Uparrow & \\ H & & H \end{array}$$

$$\Downarrow a^r \in H.$$

As above,  $r$  cannot be  $> 0$   
 since  $r < m$  and  $m$  minimal.

Ergo  $r = 0$  and  
 $b = a^n = (a^m)^q \in \langle a^m \rangle \quad \square$

say  $G = \langle a \rangle$ .

Theorem.  $(G, *)$  finite cyclic group,  $N = |G|$ .

(1) If  $H \leq G$  is a subgroup, then  $|H|$  divides  $|G|$ .

[eventually we'll show this for all finite  $G$ , "LAGRANGE"]

(2) Conversely  $\forall d|N$  there's a unique subgroup  $H \leq G$

with  $|H| = d$ .

[This part fails in general for arbitrary finite  $G$ .]

— Namely  $H = \langle a^{\frac{N}{d}} \rangle$ .

PROOF(1): Know  $H$  is cyclic, so  $H = \langle a^n \rangle$  some  $n$   
— where  $G = \langle a \rangle$ . Then:

$$(\star) \quad |H| = \text{ord}(a^n) = \frac{\text{ord}(a)}{\text{GCD}(n, \text{ord}(a))} = \frac{|G|}{\text{GCD}(n, |G|)}$$

shows  $|G| = |H| \cdot \text{GCD}(n, |G|)$ .

PROOF(2): By  $(\star)$  with  $n = \frac{N}{d}$ , we see  $|\langle a^{\frac{N}{d}} \rangle| = d$

(so  $\langle a^{\frac{N}{d}} \rangle$  is an example of such a group  
 $\Rightarrow$  existence.)

Uniqueness: It's the only one. For suppose  $H = \langle a^n \rangle$  has  
 $|H| = d = \frac{N}{\text{GCD}(n, N)}$ . Then  $\frac{N}{d} = \text{GCD}(n, N)$  divides  $n$ ,

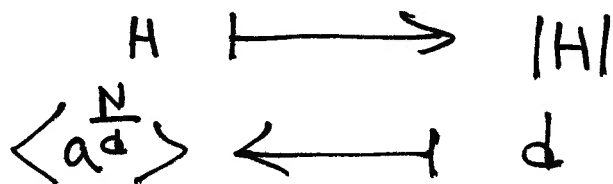
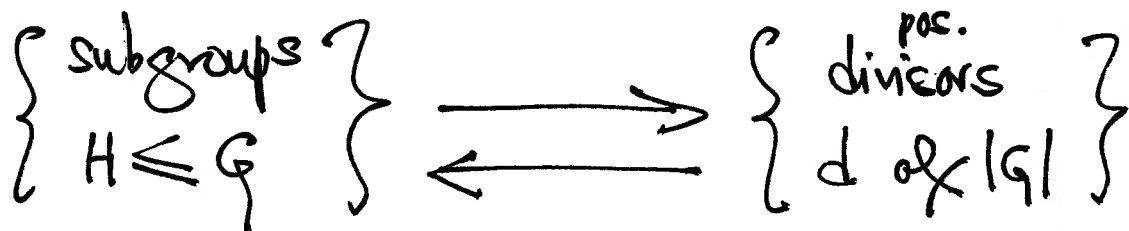
so certainly  $a^n \in \langle a^{\frac{N}{d}} \rangle$ . Thus  $H \subseteq \langle a^{\frac{N}{d}} \rangle$ .

— which must be  $=$  since same size  $\square$

say  $G = \langle a \rangle$ .

(pick generator  $a \in G$ )

Corollary  $(G, *)$  finite cyclic group of size  $N = |G|$ .  
Then there's a one-to-one correspondence:



Ex. How many subgroups of  $\mathbb{Z}_{100}$ ? (Have  $a = [1]$ )

$100 = 2^2 \cdot 5^2$  has  $(2+1) \cdot (2+1) = 9$  divisors.

For instance, the one of size 5 is

$$\langle [20] \rangle = \{ [0], [20], [40], [60], [80] \}.$$