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 $H \leqslant \mathbb{Z}$ is of this form: $H = N\mathbb{Z}$.

unique if $\geqslant 0$.

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

By (3) it contains a positive number.

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

(well—ordering principle...)

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

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

and (3) if $n<0$.

... and if $n=0$?

$\subseteq$: $a \in H$ arbitrary. Division w. remainder:

$$\underset{H}{\underset{\cap}{a}} = q\underset{H}{\underset{\cap}{N}} + r, \quad 0 \leqslant r < N.$$

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

Since $r < N$ and N minimal, r cannot be >0. Thus $r = 0$, meaning

$a = qN \in N\mathbb{Z}$. ✓

EX (cf. HW)

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

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

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

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.: $n = qm + r, \quad 0 \leqslant r < m.$

$$\Downarrow$$

$$\underset{\substack{\cup\\ H}}{a^n} = (\underset{\substack{\cup\\ H}}{a^m})^q * a^r$$

$$\Downarrow$$

$$a^r \in H.$$

– 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 $G = \langle a \rangle$.

<u>Theorem</u>. $(G,*)$ finite <u>cyclic</u> group, $N = |G|$.

(1) If $H \leqslant G$ is a subgroup, then $|H|$ <u>divides</u> $|G|$.

[eventually we'll show this for <u>all</u> finite G; "LAGRANGE"]

(2) Conversely $\forall d | N$ there's a <u>unique</u> subgroup $H \leqslant G$ with $|H| = d$.

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

[This part <u>fails</u> in general for arbitrary finite G.]

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

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

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

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

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

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

$$\left\{ \begin{matrix} \text{subgroups} \\ H \leq G \end{matrix} \right\} \rightleftarrows \left\{ \begin{matrix} \text{pos. divisors} \\ d \text{ of } |G| \end{matrix} \right\}$$

$$H \longmapsto |H|$$

$$\langle a^{\frac{N}{d}} \rangle \longleftarrow d$$

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

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

For instance, the one of size 5 is

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