Lecture 13:

called subgroup generated by g.

Last time: Recall $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, \overset{\overset{e}{\|}}{1}, g, g^{2}, \dots\}$

Thm: • $\langle g \rangle$ is the smallest subgroup that contains $g \in G$.

Def: A cyclic group is a group G that has an element $g \in G$ st. $\langle g \rangle = G$.

Theorem Every cyclic group is isomorphic to one of the following groups.

- $\mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$, $n > 0$
- $\mathbb{Z}$.

equivalently
$C_n = \{1, x, \dots, x^{n-1}\}$.

proof: Assume G is cyclic. Let $g \in G$ be such that $\langle g \rangle = G$.

then every element of G is of the form g^k for some k.

Case 1: $\dots, g^{-2}, g^{-1}, e, g, g^{2}, \dots$ are all distinct. Then, we claim $G \cong (\mathbb{Z}, +)$

Let $\varphi : \mathbb{Z} \to G$ be given by
$\varphi(k) = g^{k}$.

- φ is injective because g^k are all distinct.
- φ is surjective because every element of G is of the form g^k for some k, (since $\langle g \rangle = G$).

φ is a homomorphism since.

$$\varphi(k_1+k_2) = g^{k_1+k_2} = g^{k_1}\cdot g^{k_2}$$
$$= \varphi(k_1)\cdot\varphi(k_2).$$

Hence $\varphi : \mathbb{Z} \to G$ is an isomorphism.

<u>case 2:</u> $\ldots g^{-2}, g^{-1}, 1, g, g^2, \ldots$
are not all distinct. Let $|g|$ be the smallest positive number such that

$g^{|g|} = 1$. So

$G = \langle g \rangle = \{1, g, g^2, \ldots, g^{|g|-1}\}$

Let $\varphi : \mathbb{Z}/_{|g|\mathbb{Z}} \to G$ be given by $n = |g|$

$$\varphi(\bar{k}) = g^k$$

- <u>φ is well defined</u>: Let $n = |g|$

If $k_1 = k_2 + cn$, then

$$\varphi(k_1) = \varphi(k_2 + cn) = g^{k_2+cn} = g^{k_2}(g^n)^c$$
$$= g^{k_2} = \varphi(k_2)$$

- φ is a homomorphism: $\varphi(\bar{k}_1 + \bar{k}_2) = g^{k_1+k_2} = g^{k_1}\cdot g^{k_2} = \varphi(\bar{k}_1)\cdot\varphi(\bar{k}_2)$.
- φ is surjective since $G = \langle g \rangle$
- φ is injective: Let $\varphi(\bar{k}_1) = \varphi(\bar{k}_2)$

then $g^{k_1} = g^{k_2}$, so $g^{k_1-k_2} = 1$.

~~since~~ Then $n \mid k_1 - k_2$ because otherwise,

$k_1 - k_2 = cn + r$, $n > r > 0$, and

$1 = g^{k_1-k_2} = \underbrace{(g^n)^c}_{1} \cdot g^r$ so $g^r = 1$, but $|g| = n$ was smallest positive number st $g^n = 1$. and $r < n$, so $r = 0$

hence $n \mid k_1 - k_2$
thus $\bar{k}_1 = \bar{k}_2 \in \mathbb{Z}/_{n\mathbb{Z}}$

Thus φ is injective.

□

Definition: The smallest $n \in \mathbb{N}$, $n \geq 1$ s.t $g^n = e$ is called the order of g and is denoted by $|g|$.

Remark: In proof above, we showed that:

Lemma: If $g^k = 1$, then $|g| \mid k$.

proof: write $n = |g|$.

$k = cn + r \qquad n > r \geq 0$.

If $g^k = 1$, then

$$1 = g^k = g^{cn+r} = \underbrace{(g^n)^c}_{1} \cdot g^r$$

So $g^r = 1$. Since n was minimal, then $r = 0$ and hence $n = |g| \mid k$. $\square$

Ex: In D_6, $|r| = 3$ $\quad |r^2| = 3$ $\quad \langle r^2 \rangle = \{1, r^2, r^4 = r\}$

$|s| = 2$

<u>Theorem</u>: A subgroup of a cyclic group is a cyclic group.

<u>proof</u>: Let G be a cyclic group generated by $a \in G$. $G = \langle a \rangle$

Let $H \leq G$ be a subgroup.

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

If $H \neq \{e\}$, then look at the smallest positive n s.t. $a^n \in H$.

We claim that $H = \langle a^n \rangle$.

We want to show every $b \in H$ is a power of a^n. Let $b = a^m \in H$.
$\uparrow$ since $b \in G$.

Division algorithm: $\exists!\ q, r$ with $0 \leq r < n$

s.t. $m = q \cdot n + r$
q: quotient, r: remainder.

So $\exists\ q, r$ s.t. $a^m = (a^n)^q \cdot a^r$.

but since $a^m \in H$, and $a^n \in H$,

we have $a^m (a^n)^{-q} = a^r \in H$.

But n was minimal s.t $a^r \in H$ so, since $0 \leq r < n$,
we must have $r = 0$, and thus: $b = a^m = (a^n)^q$. $\square$