Lecture 12:

Recall some definitions:

Def: For $g \in G$, G a group

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \}$$

is called the subgroup generated by g.

Def: A cyclic group is a group such that $G = \langle g \rangle$.

Proposition: A cyclic group is a group of the form $(C_n, \cdot)$, where

$$C_n = \{1, x, x^2, \dots, x^{n-1}\}$$

(i.e. isomorphic to $(C_n, \cdot)$), or a group isomorphic to $\mathbb{Z}$.

proved on page 2.

Also recall: $(C_n, \cdot) \cong (\mathbb{Z}/n\mathbb{Z}, +)$

Theorem: $\langle g \rangle$ is the smallest subgroup of G that contains g, in the sense that if $H \leq G$ and $g \in H$, then $H \supset \langle g \rangle$.

ex: In D_6,
$\langle s \rangle = \{1, s\}$
$\langle r \rangle = \{1, r, r^2\}$
$\langle sr \rangle = \{1, sr\}$
$(srsr = 1)$

exercise: check $\langle g \rangle$ is a subgroup.

proof: Let H be a subgroup s.t. $g \in H$. Since H is closed under the group operation, $g \cdot g = g^2 \in H$, and $\underbrace{g \cdots g}_{k} = g^k \in H$ for all $k > 0$, $g^0 = e \in H$.

On the other hand, H is also closed under taking inverses, so $g^{-1}, g^{-2}, \dots \in H$ also.
Hence $g^k \in H$ for all $k \in \mathbb{Z}$. Thus $\langle g \rangle \subset H$. $\square$

proof of proposition:

Assume $g \in G$ s.t. $G = \langle g \rangle$.

Let $C_n = \{1, x, x^2, \dots, x^{n-1}\}$.

where $n = |G|$ the size of the group G.

Let $\varphi : C_n \to G$ be defined by

$$\varphi(x^k) = g^k . \qquad k_2, k_1 \in \{0, 1, \dots, n-1\}$$

• φ is injective: If $\varphi(x^{k_1}) = \varphi(x^{k_2})$

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

But then $k_1 = k_2$ because if $0 < k_1 - k_2 < n$,

then $\{1, g, \dots, \underbrace{g^{k_1 - k_2}}_{e}, \dots\}$,

has $< n$ elements. so $x^{k_1} = x^{k_2}$.

• φ is surjective: Let $g^k \in G$,
$k \in \{0, 1, \dots, n-1\}$ $(n = |G|)$

then $\varphi(x^k) = g^k$.

• φ is a homomorphism:

$$\varphi(x^{k_1}) . \varphi(x^{k_2}) = g^{k_1} . g^{k_2}$$
$$= g^{k_1 + k_2} .$$
$$= g^{k_1 + k_2 \pmod n}$$
since $g^n = e$
$$= \varphi(x^{k_1 + k_2 \pmod n}).$$

Def: The smallest $n \in \mathbb{N}$ s.t. $g^n = e$ is called the order of $g \in G$.
Denoted $|g|$.

Theorem: A subgroup of a cyclic group is a cyclic group.

proof: 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 $b = a^m \in H$.
since $b \in G$.

Division algorithm: $\exists!\, q, r$ with $0 \leq r < n$
s.t. $m = q \cdot n + r$
quotient (q), remainder (r).

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