

Lecture 10:

Last time: A subgroup H of a group $(G, *)$ is a subset $H \subset G$ that is a group with the binary operation $*$: $H \times H \rightarrow H$ induced by $*$.
↳ assuming it's a binary operation on H .

Lemma: $H \subset G$ is a subgroup if:

- (1) H is closed under $*$
- (2) $e \in H$
- (3) H is closed under taking inverses.

Definition: $C_n = \{1, x, x^2, x^3, \dots, x^{n-1}\}$

$$x^a \cdot x^b = x^{a+b \pmod{n}}$$

(C_n, \cdot) is called the cyclic group.

We have already seen this group.

$$(C_n, \cdot) \cong (U_n, \cdot) \cong (\mathbb{Z}/n\mathbb{Z}, +)$$

↑
 $\{e^{i2\pi k/n} \mid k \in \mathbb{Z}\} \subset \mathbb{C}$

these groups are isomorphic.

In other words, (C_n, \cdot) is multiplicative version of $\mathbb{Z}/n\mathbb{Z}$.

Ex: Subgroups of C_{12} : $1, x, x^2, \dots, x^{11}$
 x^{12}

• $\{1\}$ is a subgroup.

• If $x^a \in H$, H subgroup, then $(x^a)^k \in H$ for all $k \in \mathbb{Z}$.

Definition: For $g \in G$ a group.

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

is called the subgroup generated by g in G .

Why is it a subgroup?

(1) closed: $g^a \cdot g^b = g^{a+b}$

(2) $e = g^0 \in \langle g \rangle$

(3) $(g^a)^{-1} = g^{-a}$

↳ or
"cyclic subgroup"
generated by g .

continuing with subgroups of $C_{12} = \{1, x, x^2, \dots, x^{11}\}$.

$$\langle x^2 \rangle = \{x^2, x^4, x^6, x^8, x^{10}, 1\}$$

$$\langle x \rangle = C_{12}$$

$$\langle x^3 \rangle = \{x^3, x^6, x^9, 1\}$$

$$\langle x^4 \rangle = \{x^4, x^8, 1\}$$

$$\langle x^5 \rangle = \{x^5, x^{10}, x^3, x^8, x, \dots\} = C_{12}$$

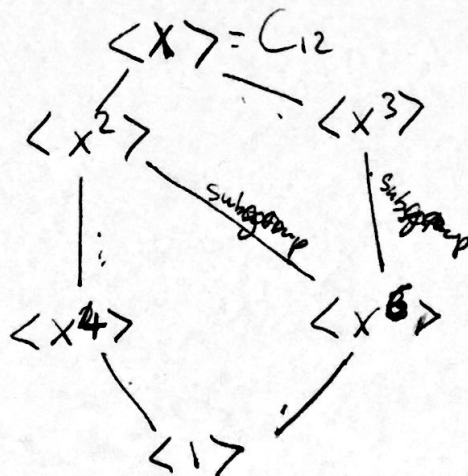
⋮

Subgroups of C_{12} :

$$\langle 1 \rangle, \langle x \rangle, \langle x^2 \rangle, \langle x^3 \rangle, \langle x^4 \rangle, \langle x^6 \rangle$$

How are these C_{12} contained in each other?

"lattice of subgroups"



↑ Bigger

↓ Smaller