A cool group!

Elliptic curve

\{(x,y) \text{ s.t. } y^2 = x^3 + ax + b \} \cup \{\infty\}

Last time. Fix \( \phi : G \to L \) a group homomorphism

We defined \( \text{Im}(\phi) = \{g \in L \mid \exists g' \in G : \phi(g') = g\} \)

\( \ker(\phi) = \{g \in G \mid \phi(g) = e_L\} \triangleleft G \)

Thm. Fix \( \phi : G \to L \) suppose \( K \leq G \) is a subgroup s.t. \( K \triangleleft \ker(\phi) \).

Then \( \exists ! \varphi : G/K \to L \) s.t. \( \varphi \circ \pi = \phi \) (\( \phi \) factors through \( G/K \))

\[
\begin{array}{ccc}
G & \xrightarrow{\phi} & L \\
\downarrow{\pi} & & \downarrow{\varphi} \\
G/K & \xrightarrow{\exists ! \varphi} & \\
\end{array}
\]

Moreover, when \( K \triangleleft G \), \( \varphi \) is a gp-hom.
Let's study subgroups of an arbitrary $G$.

To show $\phi: G \to \text{Im}(\phi)$ is surjective:

$\phi(g) = \phi(\text{Im}(\phi)) = e \Rightarrow \exists g \in G$ such that $\phi(g) = e$.

This is a homomorphism by the Universal Property.

$L: \text{ker}(\phi) \to \text{Im}(\phi)$ is an isomorphism.

To show $L$ is injective, it suffices to show $\ker(L) = 1$.

$L(g) = \phi(g) = e \Rightarrow g \in \ker(L)$.

The closed arrow is the unique $\phi$.

This is the hypothesis of the theorem.

But here is the cool thing.

But what does it mean for $\ker(\phi) = K$?

It means this diagram commutes.

$L: K \to \text{Im}(\phi)$, $\phi$.
Fix \( g \in G \). Then consider the set \( \{ g, g^2, \ldots \} = \langle g \rangle = \{ g^a : a \in \mathbb{Z} \} \).

**Defn.** We let \( \langle g \rangle = \{ g^a : a \in \mathbb{Z} \} \) and call it the **subgp of** \( G \) **generated by** \( g \).

**Prop.** Given \( g \in G \), \( \exists \) isomorphism:

\[
\langle g \rangle \cong \mathbb{Z} / \langle n \rangle \mathbb{Z}
\]

for some \( n \geq 0 \).

**Prf.** The map \( \phi : \mathbb{Z} \to G \) is a gp hom.

\[
a \mapsto g^a
\]

**Note:** \( \text{Im} (\phi_g) = \{ g^a : a \in \mathbb{Z} \} = \langle g \rangle \).

On the other hand, by the 1st isomorphism thm,

\[
\text{im}(\phi_g) \cong \mathbb{Z} / \ker(\phi_g)
\]

but by the hom any subgroup of the int is \( \equiv n \mathbb{Z} \) for some \( n \). So \( \ker(\phi) = n \mathbb{Z} \). \( \square \)

This number \( n \) is a **p. cool invariant of** \( g \in G \).

**Prop.** Fix \( g \in G \) and some finite \( n > 0 \). \( \implies \)

(1) \( \langle g \rangle \cong \mathbb{Z} / n \mathbb{Z} \)

(2) \( n \) is the smallest positive int s.t. \( g^n = e \).

(3) \( \ker(\phi_g) = n \mathbb{Z} \) with \( \phi_g \) as above

**Ex.** In HW you showed if \( |G| = \infty \) and \( \langle g \rangle \) is a subgroup then \( |H| \) divides \( |G| \).

\( \implies \langle \langle g \rangle \rangle \) divides \( |G| \).

**Ex.** \( G = S_3 \), \( |G| = 6 \). \( \exists \ g \in G \) s.t. \( |g| = 4 \).

**Defn.** Let \( G \) be a gp. If \( \exists \ g \in G \) s.t. \( \langle g \rangle = G \), \( G \) is called **cyclic**.

**Cor.** Cyclic groups are isomorphic to \( \mathbb{Z} / n \mathbb{Z} \) for some \( n > 0 \).

**Cor.** Let \( G \) be a group of order \( p \) where \( p \) is prime. Then \( G \) is iso. to any other gp of order \( p \).

**Prf.** Choose \( g \in G \) s.t. \( g \neq e \). \( \langle \langle g \rangle \rangle \cong \mathbb{Z} / \{ 1, 2 \} \mathbb{Z} \).

On the other hand \( |\langle g \rangle| \) divides \( |G| \).

\[
|\langle g \rangle| = p
\]

\( \implies \langle g \rangle = G \implies \mathbb{Z} / p \mathbb{Z} \cong G \). \( \square \)

**Exs.** Try to prove this:

\[
g \text{ has an inverse } g^{-1} \in \langle g \rangle \]

\( g^{-1} = g^a \) so let \( n = a + c \).

\[
bcg^{-1}g = e \rightarrow g^b = e \rightarrow g^{ab} = e
\]

Then \( a + g^a \) is a bijection.

ohh nice.

**Defn.** If such \( n > 0 \), \( n \) is called the **order of** \( g \).

If \( \langle g \rangle \cong \mathbb{Z} / n \mathbb{Z} \cong \mathbb{Z} \), the order of \( g \) is called **infinite**.

The order of \( g = \text{size of } \langle g \rangle \).