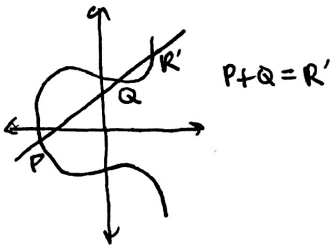
Sep 18

A cool group!

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

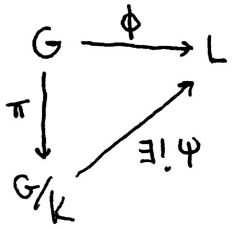


Last time. Fix $\phi: G \to L$ a group homomorphism

we defined $\mathrm{Im}(\phi) = \{\ell \in L \mid \ell = \phi(g) \text{ for some } g \in G\} \subset L$ (subgrp)

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

Thm. Fix $\phi: G \to L$ & suppose $K \subset G$ is a subgroup s.t. $K \subset \ker(\phi)$.
Then $\exists!\ \Psi: G/K \to L$ s.t. $\Psi \circ \pi = \phi$ (ϕ factors through G/K)

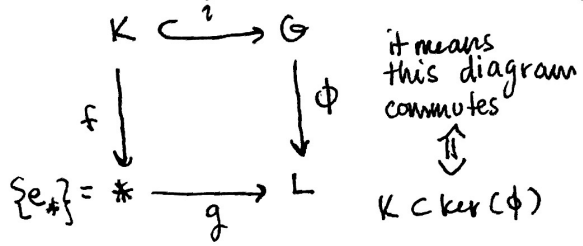


Moreover, when $K \lhd G$, Ψ is a gp. hom.

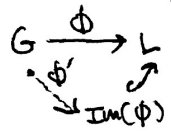
Thm (Universal property of quotient gps) ← a weaker form of the above thm

Suppose $K \lhd G$. Fix a gp. hom. $\phi: G \to L$ and assume $\ker(\phi) \supset K$
Then $\exists!$ gp hom $\varphi: G/K \to L$ s.t. $\phi = \varphi \circ \pi$

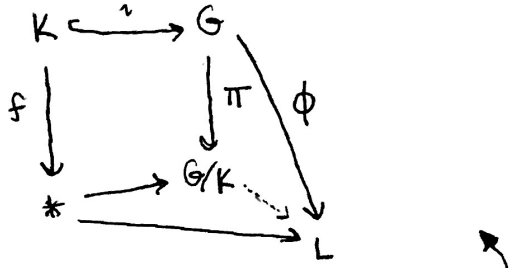
what does it mean for $\ker(\phi) \supset K$?



Rmk. Note that both ϕ and φ factor through $\mathrm{Im}(\phi)$



But here is the cool thing.



This is the hypothesis of the thm
The dased arrow is the unique φ

Thm. Fix $\phi: G \to L$. Then the gp. hom. ← "First isomorphism thm" stated but not proved last time. Analogous to rank-nullity

$$G/\ker(\phi) \longrightarrow \mathrm{Im}(\phi)$$

is an isomorphism.

Pf. This is a homomorphism by the Universal Property
↑ $\varphi(g\ker\phi) = \phi(g)$
To show ~~bijection~~ injection it suffices to show $\ker(\varphi) = \{e_{G/\ker\phi}\} = \{\ker\phi\}$

$\ker(\varphi) = \{g\ker\phi \text{ s.t. } \varphi(g\ker\phi) = e_L\}$

$= \{g\ker\phi \text{ s.t. } \phi(g) = e_L\}$

$= \{\ker\phi\}$

To show $\varphi: G/\ker\phi \to \mathrm{Im}(\phi)$ is surjective:

$\ell \in \mathrm{Im}(\varphi) \iff \exists\, g \in G \text{ s.t. } \phi(g) = \ell$

$\Rightarrow \varphi(g\ker\phi) := \phi(g) = \ell$

Math applications

Let's study subgroups of an arbitrary G.

Fix $g \in G$. Then consider the set $\{\ldots g^{-1}, g, g^2, \ldots\} = \{g^a\}_{a \in \mathbb{Z}}$

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

Propn. Given $g \in G$, $\exists$ isomorphism

$$\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

for some $n \geq 0$.

Pf. the fxn $\phi_g : \mathbb{Z} \to G$ 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 isophism thm,

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

but by the hw any subgroup of the ints is $= n\mathbb{Z}$ for some n. So $\ker \phi = n\mathbb{Z}$ □

ohh nice.

Exs. Try to prove this
let $\phi : \langle g \rangle \to \mathbb{Z}/n\mathbb{Z}$
$g \mapsto n$
g has an inverse $g^{-1} \in \langle g \rangle$
$g^{-1} = g^a$ so let $n = a+1$?
bc $g^{-1}g = e \Rightarrow g^a g = e \Rightarrow g^{a+1} = e$
then $a \mapsto g^a$ is a bijection

This number n is a p. cool invariant of $g \in G$.

Propn. Fix $g \in G$ and some finite integer $n > 0$. TFAE:

(1) $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$
(2) n is the smallest positive int s.t. $g^n = e_G$
(3) $\ker(\phi_g) = n\mathbb{Z}$ with ϕ_g as above

→ **Defn.** If such $n > 0$, n is called the order of g
→ If $\langle g \rangle \cong \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$, the order of g is called infinite.
→ The order of g = size of $\langle g \rangle$

Ex. In HW you showed if $|G| < \infty$ and $H \subset G$ is a subgroup then $|H|$ divides $|G|$
$\Rightarrow |\langle g \rangle|$ divides $|G|$.

Ex. $G = S_3$, $|G| = 3! = 6$. $\nexists$ $g \in G$ 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 $n \geq 0$.

Cor. Let G be a group of order p where p is prime. then G is iso. to any other gp of order p.

Pf. Choose $g \in G$ s.t. $g \neq e_G$. ($|\langle g \rangle| \geq 2$) (b/c $\{e_G, g\} \subset \langle g \rangle$)
On the other hand $|\langle g \rangle|$ divides $|G|$
so $|\langle g \rangle| = p$
$\Rightarrow \langle g \rangle = G \Rightarrow \mathbb{Z}/p\mathbb{Z} \cong G$ □

Excs prove it.
$|\langle g \rangle|$ divides p $\forall g \in G$
so $|\langle g \rangle|$ is either 1 or p
If $|\langle g \rangle| = 1$ then $|g| = 1$ $\forall g \in G$
If $|\langle g \rangle| = p$ then g generates G
but this can't happen bc nontrivial subgroups have order ≥ 2
Thus g gens G g' gens G_2 $|G_2| = p$
isomism: $g^a \leftrightarrow g'^a$