Lecture 9

Last time

- $H \subset G$ normal if $\forall g \in G,\ gHg^{-1} = H$

- $G/H = \{ gH \mid g \in H \}$
  a set of equivalence classes
  for $a \sim b \iff a^{-1}b \in H$

Question: when G/H has a group structure?

It's tempting to say that G/H is a group with a product given by:

$$(aH)\cdot(bH) = (abH) \quad (*)$$

The problem is that this procedure is <u>NOT</u> well-defined in general.

Example: $G = S_3$, $H = \{1, (12)\}$

$$\begin{array}{ccccc} (123)H & \cdot & (132)H & = & H \\ \| & & & & \cancel{\|} \\ (13)H & \cdot & (132)H & = & (23)H \end{array}$$

← problem!

<u>Claim:</u> if $H \subset G$ is <u>normal</u> then G/H <u>has</u> a group structure given by the formula $(*)$

<u>proof</u> Need to check that the product (*) is well-defined.

In other words, need to check that

if $a_1 \sim b_1$, $a_2 \sim b_2$ $\Rightarrow$ $a_1 a_2 \sim b_1 b_2$

Indeed $b_1 = a_1 h_1$, $b_2 = a_2 h_2$

for some $h_1, h_2 \in H$

Then $b_1 b_2 = a_1 h_1 \cdot a_2 h_2 =$

$$= a_1 a_2 \cdot \overbrace{\underbrace{(a_2^{-1} h_1 a_2)}_{H} \cdot h_2}^{\text{in } H} \quad \checkmark$$

use that H - normal

Exercise: if formula (*) defines the group structure on G/H, then $H \subset G$ normal.

Upshot: $H \subset G$ subgroup

Can form G/H ⊸ <u>set</u>

becomes a <u>group</u> if $H \subset G$ normal

Example $G = S_3$, $H = A_3 = \{1, (123), (132)\}$

Then G/H ⊸ consists of <u>two</u> elements

" $\{H, (12)H\}$ $\quad \underline{H} \mapsto 1, \quad \underline{(12)H} \mapsto -1$

$\{\pm 1\}$ is iso. of groups

If $H \subset G$, then $\begin{array}{ccc} G & \twoheadrightarrow & G/H \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ g & \longmapsto & gH \end{array}$

normal

φ

surjective homomorphism

with kernel $= H$

Thm. if $\varphi : G \twoheadrightarrow G'$ ← surjective homom.

and $H = \ker \varphi$

⟸

1) $G/H \xrightarrow[\sim]{f} G'$

2)
$$\begin{tikzcd} g \in G \arrow[d, mapsto] & G \arrow[dl] \arrow[dr, "\varphi"] \arrow[d, phantom, "\Delta"] & \\ gH \in G/H \arrow[rr, "\sim"', "f"] & & G' \end{tikzcd}$$

← this diagram is commutative

In other words, φ "identifies" with

$G \twoheadrightarrow G/H$

proof

Let's construct a map $G/H \xrightarrow{f} G'$

Elements of G/H are cosets gH,

we defin $f(gH) := \varphi(g)$

φ

note that $\varphi(H) = \{1\}$

so f is well-defined

(does not depend on the choice of g)

By definitions:

(∗)

$$\begin{tikzcd} & G \arrow[dl] \arrow[dr, "\varphi"] \arrow[d, phantom, "\triangle"] & \\ G/H \arrow[rr, "f"'] & & G' \end{tikzcd}$$

← commutative

Remains to check that f ← isomorphism

① f ⊸ homomorphism: take aH, bH

Want: $$f(aH \cdot bH) \overset{???}{=} f(aH) \cdot f(bH)$$

$$\begin{array}{ccc} f(aH \cdot bH) & & f(aH)\cdot f(bH) \\ \| & & \| \\ f(abH) & & \varphi(a)\cdot\varphi(b) \\ \| & & \\ \varphi(ab) & & \end{array}$$

indeed equal ✓

② f ⊸ surjective follows from the fact that $(**)$ is commutative, is that clear?

③ f ⊸ bijective

enough to check that $\ker(f) = \{1_{G/H}\}$

Note now that $gH \overset{f}{\longmapsto} 1$ iff

$\varphi(g) = 1$ iff $g \in H$ i.e. $gH = H$ ✓

Back to cosets

arbitrary subgroup

Assume now that $H \subset G$.

We assume G finite

Define $[G:H] = \#(G/H)$

number of left cosets gH

this number is called index

Lemma. All left cosets of a group have the same number of elements

proof. enough to construct bijection

$aH \xrightarrow{\sim} H$

it is given by left multiplying by a^{-1}

inverse is the left multiplication by a

Corollary $|G| = |H| \cdot [G:H]$

order of G (sometimes denote by $\#G$)

size of one coset

number of cosets

Theorem (Lagrange's thm.)

Let $H \subset G$ subgroup. The order of H divides the order of G.

<u>Corollary.</u> The order of an element of a finite group divides the order of the group.

<u>proof.</u> Take $a \in G \to \langle a \rangle \subset G$.

Recall that $\text{ord}(a) = |\langle a \rangle|$ & divides $|G|$ by Lagrange's thm applied to $H = \langle a \rangle$

Corollary Suppose G has prime order.

$\Downarrow$

$$G \simeq \mathbb{Z}/p\mathbb{Z} \quad \text{or} \quad G = \{1\}$$

proof.

Assume that $G \neq \{1\}$. Take $a \in G$.

$\operatorname{ord}(a) > 1$, $\operatorname{ord}(a) \mid p \Rightarrow \operatorname{ord}(a) = p$

It follows that $\langle a \rangle = G$

is

proved $\mathbb{Z}/p\mathbb{Z}$ ✓

Proposition Let $G \supset H \supset K$ a subgroups

$$\Downarrow$$

$$[G:K] = [G:H] \cdot [H:K]$$

(for $K = \{1\}$ recover $|G| = [G:H] \cdot |H|$)

proof.

$$\left.\begin{aligned} |G| &= [G:H] \cdot |H| \\ |H| &= [H:K]\,|K| \end{aligned}\right\} \quad \begin{aligned} |G| = [G:H] \cdot \\ \cdot [H:K] \cdot |K| \end{aligned}$$

$$|G| = [G:K]\,|K|$$

$$[G:H] \cdot [H:K] \cdot \cancel{|K|} = [G:K] \cdot \cancel{|K|}$$

Exercise: $G_1 \supset G_2 \supset \ldots \supset G_n$

$$\Downarrow$$

$$[G_1 : G_n] = [G_1 : G_2] \cdot \ldots \cdot [G_{n-1} : G_n]$$

So, Lagrange's thm. tells us that

if $a \in G \Rightarrow \mathrm{ord}(a) \mid |G|$.

Is the converse true?

In general <u>NO!</u>,

take $(\mathbb{Z}/_{12}\mathbb{Z})^{\times}$, it has

order $= 4$ but no element

of order 4.

The converse is true for <u>prime</u> divisors

of $|G|$.

Theorem (Cauchy) ← nontrivial and important theorem!

(will combine all that we know to prove it)

G a finite group, $p \mid |G|$

prime

Then $\exists\, a \in G$ s.t. $\operatorname{ord}(a) = p$.

proof. We prove for G a commutative,

will deal with arbitrary G later.

Induction on $n = |G|$

Base: $n = p \Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z} \ni 1$ a element of order p ✓

proved

Induction step: take any $a \in G$, $a \neq 1$

Consider $H := \langle a \rangle \subset G$

normal as G - commutative

if $p \mid \mathrm{ord}(a) \Rightarrow a^{\frac{\mathrm{ord}(a)}{p}}$ has order p

if $p \nmid \mathrm{ord}(a) \Rightarrow p \mid |G/H|$

$\Downarrow$

(induction hypothesis)

can find $gH \in G/H$ s.t. $(gH)^p = H$

equality in G/H

Let m be the order of g.

We must have $(gH)^m = H \Rightarrow p \mid m$

So, $g^{\frac{m}{p}}$ element of order p. ✓