Last time:

Lagrange's theorem (among other things)

If G is a finite group and $H < G$ then

$|H| \mid |G|$ (defined $[G:H] = \frac{|G|}{|H|}$)

"the index of H in G"

Corollary: if $g \in G$, G finite

then $o(g) \mid |G|$

$o(g) =$ min pos. n s.t. $g^n = e$

Pf: $\langle g \rangle = \{ g^i \mid i \in \mathbb{Z} \} < G$ and $|\langle g \rangle| = n$

$= \{ g^0, g^1, \ldots, g^{n-1} \}$ $n = o(g)$

Today: Quotients and equiv. relations

If S a set, $\sim$ an equiv relation

can define $S/\sim$ "quotient of S by $\sim$"

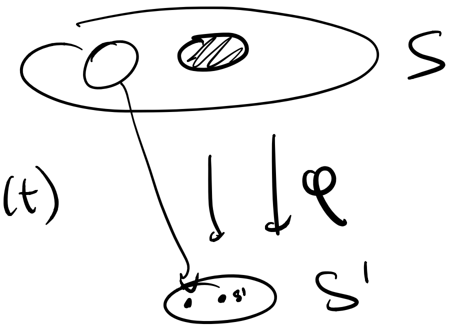
= the set of equivalence classes.

Notation $[s] = \{ t \in S \mid t \sim s \}$

In fact equiv. relations are "the same" as surjective functions $S \longrightarrow S'$

for us — these concepts (eq. rel) $\longleftrightarrow$ (surj map) carry same info.

$s/t \quad \frac{s}{t}$



$s \sim t$ iff $\varphi(s) = \varphi(t)$

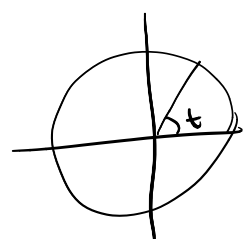
$S \longrightarrow S/\sim$

---

example

surj map

$$\boxed{\begin{aligned} \mathbb{R} &\longrightarrow S^1 \\ t &\longmapsto e^{it} \end{aligned}}$$



equiv. rel.

$\mathbb{R}/\sim \qquad r \sim r + 2\pi n$ any n.

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$

$\overline{i} = \{i + nk \mid k \in \mathbb{Z}\}$

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$i \longmapsto \bar{i}$$

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

Q: Given a group G, and an eq. rel $\sim$, when is $G/\sim$ a group?

> Notation $H < G$ subgrp
> $N \triangleleft G$ normal subgroup.

Prop Suppose $\sim$ is an eq. rel on group G, and suppose the rule $[g][h] = [gh]$ is well defined ~~& makes $G/\sim$ into a group~~. then it makes $G/\sim$ into a group and

~~Then~~ $\exists\, N \triangleleft G$ s.t. $a \sim b$ iff $aN = bN$

Conversely, if $N \triangleleft G$, and we define $a \sim b \Leftrightarrow aN = bN$ then $G/\sim$ is group as above.

Pf: Suppose $\sim$ an equiv rel s.t. $G/\sim$ is a group as above.
set $N = [e]$

Claim $N < G$

if $g, h \in N$ $\quad gh \in N \iff gh \in [e]$

$\iff [gh] = [e]$

but, if gp. well defined $\quad [gh] = [g][h]$

$h, g \in [e]$ $\quad = [e][e] = [e]$

$gh \in [e] = N.$

well dfnd:

if $[g] = [g']$ $\quad [gh] = [g'h']$

$[h] = [h']$

Show: $[a]^{-1} = [a^{-1}] = \{b \in G \mid b \sim a^{-1}\}$

potential elmt in quot gp.

$\shortparallel$

$\boxed{\{b \in G \mid b \sim a\}}^{-1}$

inverse in quotient group

$\boxed{G/\sim}$ is a group

$[a][a^{-1}] = [aa^{-1}] = [e] \overset{?}{=}$ id in $G/\sim$?

$[a][e] = [ae] = [a]$ ✓

$\Rightarrow [e] = e$ in $G/\sim$ ✓

$[a^{-1}] = [a]^{-1}$ in $G/\sim$

if $a \in N = [e]$

$$[a^{-1}] = [a]^{-1} = [e]^{-1} = [e^{-1}] = [e] = N$$

$$a^{-1} \in N$$

$N \triangleleft G$? if $a \in N$ $b \in G$

want to show: $bab^{-1} \in N$

$$[bab^{-1}] = [b][a][b^{-1}] = [b][e][b^{-1}]$$
$$= [bb^{-1}] = [e] = N$$

$\Rightarrow bab^{-1} \in N.$

Now $a \sim b \iff [a] = [b] \iff [a][b]^{-1} = [e]$

$\iff [ab^{-1}] = [e]$

$\iff ab^{-1} \in N$ $ab^{-1} = n$

$\Updownarrow$

$\iff a \in Nb$ $\Leftarrow a = nb$

$\shortparallel$

bN

$\iff aN = bN.$

so eq. rel is defined by

$a \sim b \iff aN = bN$

Conversely

if $N \trianglelefteq G$, define $a \sim b$ if $aN = bN$

$[a] = aN$

then $[a][b] = [ab]$ $aNbN = abN$

defines a group.

check well defined:

$a \sim a'$, $b \sim b'$ then $[ab] = [a'b']$

$a \sim a' \Leftrightarrow a' = an$ $n, m \in N$

$b \sim b' \Leftrightarrow b' = bm$

$a'b' = anbm$

$nb \in Nb = bN$

$\Rightarrow nb = bn'$ some $n' \in N$

$a'b' = anbm = abn'm \sim ab$

$[ab] = [a'b']$ well defined.

$\Rightarrow$ it's a group!