Last time: Lagrange's Thm

G group, H subgroup. Constructed coset spaces:

$$G/H = \{gH \mid g \in G\}, \qquad H\backslash G = \{Hg \mid g \in G\}$$

* realized left (right) cosets as equivalence classes for equivalence relations $\equiv_L$, $\equiv_R$.
* Saw: $|G| = [G:H] \cdot |H|$, where $[G:H] \overset{def}{=} |G/H|$

Corollaries: (G finite) for any $H < G$, $\#H$, $[G:H] \mid \#G$.

↑ size = order of G.

② for any $g \in G$, $\text{order}(g) \mid \#G$: $\text{order}(g) = \#\langle g \rangle$

③ $g^{\#G} = e$: $g^k = e$ iff $\text{order}(g) \mid k$.

Question: What is hG if $h \in H$? Answer: Clearly $hG \subseteq G$.
Conversely, for any $g \in G$, $g = h(h^{-1}g) \in hG$.

In particular, $G/G = \{eG\} = \{G\}$

Special case: $G = (\mathbb{Z}/m\mathbb{Z})^\times$, order of this group denoted $\phi(m)$ ("Euler function")

Conclude: if $[a] \in G$ then $[a]^{\phi(m)} = [1]$.

usually written $a^{\phi(m)} \equiv 1 \ (m)$ if $\gcd(a,m) = 1$ ("Euler's thm")

In particular, if $m = p$ is prime, saw $\phi(p) = p-1$ (every non-zero class in $\mathbb{Z}/p\mathbb{Z}$ is invertible)

get "Fermat's little thm": if $p \nmid a$, $a^{p-1} \equiv 1 \ (p)$

or (for any a) $a^p \equiv a \ (p)$

Corollary toward classification of groups:

Lem Prop: Let G be a group of prime order p. Then $G \cong C_p$

Proof: Let $g \in G$, $g \neq e$. Consider the subgp $\langle g \rangle = H$.

By Lagrange's Thm, $\#H \mid p = \#G$, so $\#H \in \{1, p\}$.

But $H \neq \{e\}$ (contains g) so $\#H > 1$. Conclude that $\#H = p$, $H = G$, and G is cyclic.

Note: At order p^2 have at least C_{p^2}, $C_p \times C_p$.
(we'll see later that no others)

Today: Normal subgroups, Quotient groups

We'll answer question "which $H < G$ are kernels of homomorphisms?"

Start by examining Kernels.

Observation: Let $f \in \mathrm{Hom}(G, H)$, $g \in G$. Then $gKer(f)g^{-1} = Ker(f)$

Pf: If $n \in Ker(f)$, then $f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)f(g^{-1}) = e$
($f(n) = e$)

so $gKer(f)g^{-1} \subseteq Ker(f)$

Conversely, for any $g \in G$ have $g^{-1}Ker(f)g \subseteq Ker(f)$ $\quad (g = (g^{-1})^{-1})$

mult. on left by g, on right by g^{-1}, get

$$Ker(f) \subseteq gKer(f)g^{-1}$$

Def: Call $N < G$ normal if for all $g \in G$, $gNg^{-1} = N$.

Note: from pf above, enough to check $gNg^{-1} \subseteq N$ for all $g \in G$.

Notation: write $N \triangleleft G$ if N is normal

Examples: $\{e\}$, G itself, any subgp of an abelian gp

$A_n \triangleleft S_n$. (Kernel of sgn: $S_n \to \{\pm 1\}$)

Remark: Given $H < G$, $\not\exists$ $H \trianglelefteq H$, in fact there is a largest subgp of G in which H is normal (see HW)

Claim: Intersection of any family of normal subgps is normal

Pf: Say $\mathcal{N}$ is a non-empty set of " ". Let $H = \bigcap \mathcal{N}$, Let $g \in G$, $h \in H$. Consider ghg^{-1}!

For any $N \in \mathcal{N}$, $h \in N$, $N \trianglelefteq G$ so $ghg^{-1} \in N$. It follows that $ghg^{-1} \in H$. ∎

Construction: The normal closure of $S \subseteq G$ is the subgp

$$\langle S \rangle^N = \bigcap \{ N \mid \begin{matrix} N \trianglelefteq G \\ S \subseteq N \end{matrix} \}$$

(necessarily contains $\langle S \rangle$)

Non-example: $\{ id, (12) \} \subseteq S_n$, $n \geq 3$. Then for $\sigma \in S_n$,

$$\sigma \{ id, (12) \} \sigma^{-1} = \{ \sigma \circ id \circ \sigma^{-1}, \sigma(12)\sigma^{-1} \} = \{ id, (\sigma(1)\ \sigma(2)) \} \neq \{ id, (12) \}$$

so long as σ maps one of 1,2 to 3.

so $\{ id, (12) \}$ not normal in S_n.

Quotient groups

Lemma: $N \trianglelefteq G$ iff $\equiv_R (N)$ is the same as $\equiv_L (N)$.

(we then write $\equiv (N)$)

Pf: The notions of congruence are same iff $gN = Ng$ for all g (same equivalence classes)

$\Updownarrow$

$gNg^{-1} = N$

Lemma: $N \trianglelefteq G$ iff $\cdot \equiv_R \cdot (N)$ (equiv. $\cdot \equiv_L \cdot (N)$) respects $;, ^{-1}$ (gp operation)

Pf: Suppose $N \trianglelefteq G$.

Let $g \equiv_R g' (N)$, $h \equiv_R h' (N)$. This means ① $g'g^{-1} \in N$ ② $h'h^{-1} \in N$

compare gh, $g'h'$:

$$(g'h') \cdot (gh)^{-1} = g' \underbrace{h' h^{-1}}_{②\ N} g^{-1} = \underbrace{(g'g^{-1})}_{①\ N} \underbrace{g(h'h^{-1})g^{-1}}_{N\ (N \text{ is normal})} \in N$$

similarly, $g^{-1}, (g')^{-1}$: $g^{-1}(g'^{-1})^{-1} = g^{-1}g' = g^{-1}g'g^{-1}g \in N$.

($\underbrace{\quad}_{①\ N}$: N normal)

(for the level of sets, $(gN)\cdot(hN) = ghN$, $(gN)^{-1} = g^{-1}N$)

(converse left as exercise)

Construction: The quotient group G/N is the group with underlying set G/N, and operation $gN \cdot hN = gh \cdot N$

Lemma $\Leftrightarrow$ the operation is well-defined

Prop: $(G/N, \cdot)$ is a group, the map ("quotient map") $q : G \to G/N$, $q(g) = gN$ is a surjective group homomorphism, and

$$\ker q = N$$

Pf: That the operation on G/N is well-defined gave us

$$q(gh) = ghN = gN\,hN = q(g) \cdot q(h)$$

The map is evidently surjective (every coset has representatives = elements)

group axioms:

for $x, y, z \in G/N$ let g, h, k be coset rep's:

$x = q(g) = gN$

$y = q(h) = hN$

$z = q(k) = kN$.

then: ① $(xy)\cdot z = (q(g)\,q(h))\,q(k) = q((gh)\cdot k) =$ (q respects $\cdot$ in G)

$= q(g(hk)) = x(yz)$

(assoc law of G)

② $q(e)\cdot x = q(e)\cdot q(g) = q(e\cdot g) = q(g) = x$ so $q(e) = N \in G/N$ is a left identity

③ $q(g^{-1})\cdot x = q(g^{-1})\,q(g) = q(g^{-1}g) = q(e)$ so $g^{-1}N$ is inverse to gN.

(c.f. discussion of $\mathbb{Z}/n\mathbb{Z}$)

$\ker(q) = \{g \in G \mid q(g) = N\} = \{g \in G \mid gN = N\} = N$

($N = e_{G/N}$; if $gN = N$ then $g\cdot e \in N$ so $g \in N$)

Summary: Given a normal subgp N, constructed a group G/N (endowed G/N with group structure)

Idea of gp theory: "assemble G from N, G/N"