Last time: a subgroup $K \subset G$ determines an equivalence relation on G, $a \sim b \iff a^{-1}b \in K$ whose equivalence classes are the (left) cosets of K, $aK = \{ah \mid h \in K\} \subset G$. ($a \sim b \iff b \in aK$).

- The quotient $G/K :=$ the set of cosets
- The index of the subgroup H is the number of cosets, $(G:K) = |G/K|$.

When G is a finite group, since each coset has $|aK| = |K|$ ($\begin{matrix} K \xrightarrow{\sim} aK \\ h \mapsto ah \end{matrix}$ bijection) the partition $G = \bigsqcup_{aK \in G/K} aK$ implies: $\boxed{|G| = |G/K| \cdot |K|}$

(Lagrange's theorem)

Corollary: If K is a subgroup of a finite group G, then $|K|$ divides $|G|$.

Corollary: $\forall a \in G$ finite group, the order of a divides $|G|$.

↳ recall this is the smallest $n > 0$ st. $a^n = e$ & also the order of the subgroup $\langle a \rangle$.

Corollary: If $|G| = p$ is prime, then $G \simeq \mathbb{Z}/p$.

(indeed, take $a \in G$ st. $a \neq e$, then a has order p hence $\langle a \rangle = G$, $G = \{e, a, \dots, a^{p-1}\}$, and $G \xrightarrow{\sim} \mathbb{Z}/p$ by mapping $a^k \longmapsto k \bmod p$.)

---

* Right-cosets vs. left-cosets: similarly to the left cosets $aK = \{ak \mid k \in K\}$ ($a \sim b \iff a^{-1}b \in K$) we define right cosets $Ka = \{ka \mid k \in K\}$, which correspond to $a \sim b \iff ba^{-1} \in K$

Rmk: none of these are subgroups of G! (except for K itself) (they don't contain e!).

Also denote $aKa^{-1} = \{aka^{-1} \mid k \in K\}$ (this one is a subgroup).

Def: $K \subset G$ is a normal subgroup if $\forall a \in G$, $aK = Ka$ ("left cosets = right cosets") or equivalently, $\forall a \in G$, $aKa^{-1} = K$.

↳ this means the two equivalence relations above agree.

Examples:
- any subgroup of an abelian group is normal. ($a + K = K + a$ ✓).
- in D_4, the subgroup $H = \{e, h\}$ is not normal. $\left(\begin{matrix} rH = \{r, rh\} \\ \neq Hr = \{r, hr\} \end{matrix}\right)$

  ↑ horiz. reflection

Theorem: Given a group G and a subgroup $K \subset G$, the following are equivalent:
(1) there exists a group homomorphism $\varphi: G \to H$ (some other group) with $\ker(\varphi) = K$
(2) K is a normal subgroup.
(3) G/K has a group structure given by $(aK)\cdot(bK) = abK$

<u>Proof:</u> (1) ⇒ (2) suppose $\exists \varphi: G \to H$ homomorphism with $\ker(\varphi) = K$.

Then $\forall a,b \in G$, $\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a)^{-1}\varphi(b) = e \Leftrightarrow \varphi(a^{-1}b) = e \Leftrightarrow a^{-1}b \in K \Leftrightarrow b \in aK$

but also $\varphi(a) = \varphi(b) \Leftrightarrow \varphi(b)\varphi(a)^{-1} = e \Leftrightarrow \varphi(ba^{-1}) = e \Leftrightarrow ba^{-1} \in K \Leftrightarrow b \in Ka$.

So $aK = Ka \ \forall a \in G$, K is normal.

(2) ⇒ (3): assume K is normal, and define an operation on G/K by $aK \cdot bK = abK$.

- We need to check this is well-defined, ie. $aK = a'K$ & $bK = b'K \overset{?}{\Rightarrow} abK = a'b'K$.

  Equivalently: $a^{-1}a' \in K$, $b^{-1}b' \in K \overset{?}{\Rightarrow} (ab)^{-1}(a'b') \in K$. Using K normal $\Rightarrow b^{-1}Kb = K$;

  $$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = \underbrace{b^{-1}\underbrace{a^{-1}a'}_{\in K}b}_{\in b^{-1}Kb = K}\underbrace{b^{-1}b'}_{\in K} \in K \checkmark.$$

- It clearly satisfies group axioms: $eK \cdot aK = eaK = aK$, similarly other axioms follow from the definition of the operation + the fact that G is a group.

(3) ⇒ (1) Now, $G \twoheadrightarrow G/K$, $a \mapsto aK$ is clearly a homomorphism with kernel $= K$. □

<u>Remark:</u> If $\varphi: G \to H$ is a group homomorphism, then $K \subset G$ is a normal subgroup, and φ factors as

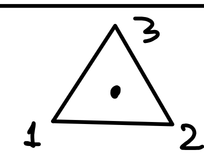
$$\begin{array}{ccccccc} G & \xrightarrow{\text{quotient}} & G/K & \xrightarrow{\bar\varphi} & \operatorname{Im}\varphi & \overset{\text{incl.}}{\hookrightarrow} & H \\ a & \longmapsto & aK & \longmapsto & \varphi(a) & & \end{array}$$

$\bar\varphi$ is well def$^{\text{d}}$ $(aK = a'K \Rightarrow \varphi(a) = \varphi(a'))$;

and a homomorphism because $\bar\varphi(aK \cdot bK) = \bar\varphi(abK) = \varphi(ab) = \varphi(a)\varphi(b) = \bar\varphi(aK)\bar\varphi(bK)$.

$\bar\varphi$ is injective $(\bar\varphi(aK) = e_H \Leftrightarrow a \in K \Leftrightarrow aK = K)$, surjective, so isomorphism!

<u>Hence:</u> $G/\ker(\varphi) \simeq \operatorname{Im}(\varphi) \subset H$. (with isom. given by $\bar\varphi$).

<u>Example:</u> S_3 = permutations of $\{1,2,3\}$ = symmetries of  contains

- e = identity, does nothing, order 1.
- three <u>transpositions</u> which swap two elements: $(1\ 2)$ $(2\ 3)$, $(1\ 3)$
  ↔ reflections of the triangle ; order 2

  <u>cycle notation:</u> $(a\ b\ c\ d)$
- two <u>3-cycles</u> $(1\ 2\ 3)$ and $(1\ 3\ 2)$
  ↔ rotations by $\pm 120°$. These have order 3.

<u>Subgroups of S_3:</u>

have order 1, 2, 3 or 6

necess. cyclic

- $\{e\}$ trivial
- $\{e, (1\ 2)\}$ and two others $(\simeq \mathbb{Z}/2)$.
- $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ subgroup of rotations $(\simeq \mathbb{Z}/3)$
- all of S_3.

$\{e\}$ and S_3 are obviously normal subgroups.

$H = \{e, (1\,2)\}$ is not normal - its conjugate $(1\,2\,3)\,H\,(1\,2\,3)^{-1} = \{e, (2\,3)\} \neq H$.

rotate then swap $(1\,2)$ then rotate $\Leftrightarrow$ swap $(2\,3)$.

$K = \{e, (123), (132)\} \simeq \mathbb{Z}/3$ is normal

It's the kernel of $S_3 \xrightarrow{\text{sign}} \{\pm 1\} \simeq \mathbb{Z}/2$ rotations $\mapsto +1$, reflections $\mapsto -1$

Def: Say a group G is simple if it has no normal subgroups other than G and $\{e\}$.

We use normal subgroups $K \subset G$ to view G as built from hopefully simpler groups K and G/K. Simple groups are then the basic building blocks.

Notation: a sequence of groups & homomorphisms $\cdots \to G_{i-1} \xrightarrow{\varphi_{i-1}} G_i \xrightarrow{\varphi_i} G_{i+1} \to \cdots$ is an exact sequence if $\forall i$, $\mathrm{Im}(\varphi_{i-1}) = \mathrm{Ker}(\varphi_i)$.

This means $\varphi_i(x) = e \Leftrightarrow \exists a \in G_{i-1}$ s.t. $x = \varphi_{i-1}(a)$.

In particular, $\varphi_i \circ \varphi_{i-1} =$ trivial hom. $(x \mapsto e \ \forall x \in G_{i-1})$ $\quad (\Leftrightarrow \mathrm{Im}(\varphi_{i-1}) \subset \mathrm{Ker}(\varphi_i))$

A short exact sequence is the simplest case, $\{e\} \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to \{e\}$

often denoted 1 for multiplicative groups, 0 additive

- φ injective homomorphism
- ψ surjective homomorphism
- $\mathrm{Im}\,\varphi = \mathrm{Ker}\,\psi$.

Such an exact seq. exists iff B contains a normal subgroup K isomorphic to A, and s.t. the quotient group B/K is isomorphic to C.

(the prototype short exact seq. is $1 \to K \xrightarrow[\text{inclusion}]{} B \xrightarrow[\text{quotient}]{} B/K \to 1$).

Example: for any groups A and C, $\{e\} \to A \to A \times C \to C \to \{e\}$

$a \mapsto (a, e)$

$(a, c) \mapsto c$

Example: $0 \to \mathbb{Z}/2 \to \mathbb{Z}/6 \to \mathbb{Z}/3 \to 0$ and $0 \to \mathbb{Z}/3 \to \mathbb{Z}/6 \to \mathbb{Z}/2 \to 0$

$n \mapsto 3n$, $\quad m \mapsto m \bmod 3$ $\qquad n \mapsto 2n$, $\quad m \mapsto m \bmod 2$

Example: there exists an exact seq. $\{e\} \to \mathbb{Z}/3 \to S_3 \xrightarrow{\text{sign}} \mathbb{Z}/2 \to \{e\}$.

$n \mapsto (123)^n$

but not $\{e\} \to \mathbb{Z}/2 \to S_3 \to \mathbb{Z}/3 \to \{e\}$ (no normal subgroup of order 2!)

More about S_n:

- A <u>cycle</u> $\sigma = (a_1\, a_2 \dots a_k) \in S_n$ is a permutation mapping $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\dots$, $a_k \mapsto a_1$ and all other elements to themselves.
  ↳ distinct elements of $\{1..n\}$

- <u>Prop:</u> any permutation can be expressed as a product of disjoint cycles, uniquely up to reordering the factors (disjoint cycles commute so order doesn't matter)

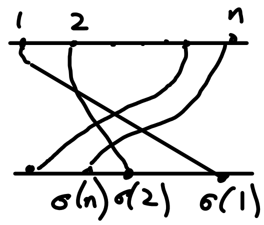
<u>Ex:</u> $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} = (1\,3\,6)(2\,5)$ ↳ same for other elements not in the previous cycles.
↳ successive images of 1 under σ until returns to 1

- A k-cycle can be written as a product of $(k-1)$ <u>transpositions</u> (= 2-cycles):
  $(a_1\, a_2 \dots a_k) = (a_1\, a_2) \circ (a_2\, a_3) \circ \dots \circ (a_{k-1}\, a_k)$.

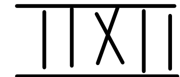
<u>So:</u> S_n is generated by transpositions. $(i\ j)$ $1 \le i < j \le n$.

In fact it is generated by $(1\,2), (2\,3), \dots, (n-1\ n)$.
Either directly (show $(i\ j)$ can be expressed in terms of these specific transpositions), or ...

<u>Idea:</u> draw σ as



, slice into a stack of



$(i\ i{+}1)$.

[see also: <u>bubble sort</u> algorithm]

- Permutations are <u>odd</u> or <u>even</u> depending on length of expression of σ as a product of transpositions ($\Leftrightarrow$ parity of $\#\{(i,j) \mid 1 \le i < j \le n,\ \sigma(j) > \sigma(i)\}$)

  Even permutations form a normal subgroup A_n = <u>alternating group</u> $\subset S_n$.
  [this is nontrivial! proof by induction].
  $1 \to A_n \to S_n \to \mathbb{Z}/2 \to 1$.

★ <u>Fact:</u> even though $A_3 \simeq \mathbb{Z}/3$, and A_4 has a normal subgroup $\simeq \mathbb{Z}/2 \times \mathbb{Z}/2$, for $n \ge 5$ A_n is <u>simple</u>!

Advertisement for Galois theory. (Math 123).

(This fact is used to prove that there is no general formula for solving polynomial equations of degree ≥ 5! The quadratic formula has a $\pm\sqrt{\ }$, and the sign is there because over $\mathbb{C}$ there's not a consistent choice of $\sqrt{\ }$ of all complex numbers – ambiguity is in $\mathbb{Z}/2 \simeq S_2$ permuting the two roots. The Cardano formula for cubics has $\sqrt[3]{\dots + \sqrt{\dots}}$ in it. The $\mathbb{Z}/2$ & $\mathbb{Z}/3$ ambiguities in choosing these roots combine to an S_3 permuting the roots. Similarly, the formula for roots of a deg. 5 equation should have a built-in S_5 symmetry – but any expression involving $\sqrt[k]{\dots}$ will have symmetry group built from cyclic $\mathbb{Z}/k$'s. This can't be S_5 since A_5 is simple.)

★ Did you know: $\mathrm{Aut}(S_n) \cong S_n$ <u>except</u> for $n=2$ ($\mathrm{Aut}(S_2) = \{id\}$) and $n=6$!
(autom's given by conjugation). ($\mathrm{Aut}(S_6) \supsetneq S_6$).