Last time, we talked about the partition of a group G into (left) cosets of a subgroup $H \subset G$, $aH = \{ah \mid h \in H\} \subset G$.

- The cosets are the equivalence classes for $a \sim b \Leftrightarrow a^{-1}b \in H$
- The quotient $G/H :=$ the set of cosets
- The <u>index</u> of the subgroup H is the number of cosets, $(G:H) = |G/H|$.

When G is a finite group, since each coset has $|aH| = |H|$ $\left(\begin{array}{l} H \xrightarrow{\sim} aH \text{ bijection} \\ h \mapsto ah \end{array}\right)$
the partition $G = \bigsqcup_{aH \in G/H} aH$ implies: $\boxed{|G| = |G/H| \cdot |H|}$

(<u>Lagrange's theorem</u>)

<u>Corollary</u>: If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

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

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

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

(indeed, take $a \in G$ s.t. $a \neq e$, 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 $a^k \mapsto k \bmod p$.)

Recall we also define right cosets $Ha = \{ha \mid h \in H\}$ ← equiv classes for $a \sim b \Leftrightarrow ba^{-1} \in H$.
and conjugate subgroups $aHa^{-1} = \{aha^{-1} \mid h \in H\}$.

<u>Def</u>: $K \subset G$ is a <u>normal subgroup</u> 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.

<u>Theorem</u>: Given a group G and a subgroup $K \subset G$, there exists a group homomorphism $\varphi: G \to H$ (some other group) with $\ker(\varphi) = K$ if and only if K is a normal subgroup.

(Then G/K has a group structure given by $(aK)\cdot(bK) = abK$ and we can take φ to be the quotient map $G \twoheadrightarrow G/K$.)

<u>Proof</u>:

$\Rightarrow$ 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.

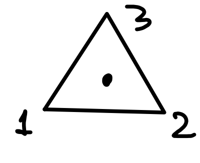
$\Leftarrow$ assume K is normal, and define an operation on G/K by $aK \cdot bK = abK$.

- 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: $eK . aK = eaK = aK$, similarly other axioms follow from the definition of the operation + the fact that G is a group.
- Now, $G \twoheadrightarrow G/K$, $a \mapsto aK$ is clearly a homomorphism with kernel $= K$. $\square$

<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: $(1\ 2)$ $(2\ 3)$, $(1\ 3)$ → <u>cycle notation</u>: $(a\ b\ c\ d)$

  $\leftrightarrow$ reflections of the triangle ; order 2
- two <u>3-cycles</u> $(1\ 2\ 3)$ and $(1\ 3\ 2)$

  $\leftrightarrow$ rotations by $\pm 120°$. These have order 3.

<u>Subgroups of S_3</u>: have order 1, 2, 3 or 6 (2, 3: 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 <u>not</u> 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 $(2\ 3)$.

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

It's the kernel of $S_3 \overset{\text{sign}}{\twoheadrightarrow} \{\pm 1\} \simeq \mathbb{Z}/2$

rotations $\mapsto +1$
reflections $\mapsto -1$

(= determinant of corresponding 2x2 matrix = does it preserve/reverse orientation).

<u>Def</u>: Say a group G is <u>simple</u> 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.

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

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

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

often denoted 1 for multiplicative groups, 0 additive

- φ <u>injective</u> homomorphism
- ψ <u>surjective</u> 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 $1 \to K \xrightarrow[\text{inclusion}]{} B \xrightarrow[\text{quotient}]{} B/K \to 1$).

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

$a \mapsto (a,e)$

$(a,c) \mapsto c$

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

$n \mapsto 3n$ $\qquad$ $n \mapsto 2n$

$m \mapsto m \bmod 3$ $\qquad$ $m \mapsto m \bmod 2$

<u>Example:</u> 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 <u>not</u> $\{e\} \to \mathbb{Z}/2 \to S_3 \to \mathbb{Z}/3 \to \{e\}$ (no normal subgroup of order 2 !)

<u>More about S_n:</u>

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

- <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)

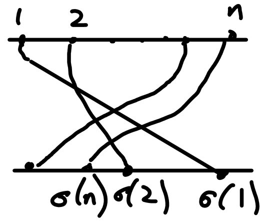
<u>Ex:</u> $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} = (1\,3\,6)(2\,5)$ ↳ same for other elements not in the previous cycles.

↳ successive images of 1 under σ until returns to 1

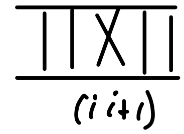
- A k-cycle can be written as a product of $(k-1)$ <u>transpositions</u> ($=$ 2-cycles):
$$(a_1\, a_2 \dots a_k) = (a_1\, a_2)\circ(a_2\, a_3)\circ\dots\circ(a_{k-1}\, a_k).$$

<u>So:</u> S_n is generated by transpositions $(i\ j)$ $1\le i<j\le n$.
In fact it is generated by $(1\,2), (2\,3), \dots, (n{-}1\ n)$.

(<u>Idea</u>: draw σ as



, slice into a stack of



).

[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>!

(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.)

Advertisement for Galois theory (Math 123).

★ 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). ($\mathrm{Aut}(S_6)\supsetneq S_6$).

★ We've talked about the <u>center</u> $Z(G)=\{z\in G \mid az=za\ \forall a\in G\}$.
Since elements of the center commute with everyone, they commute w/ each other, so $Z(G)$ is abelian! Also, $aZ(G)a^{-1}=Z(G)$, so $Z(G)$ is a normal subgroup of G.

★ Another interesting object is the <u>commutator subgroup</u> $C(G)=[G,G]=\left\{\prod_{i=1}^{k}[a_i,b_i] \;/\; a_i,b_i\in G\right\}$
where $[a,b]:=aba^{-1}b^{-1}$ (the "commutator" of a & b, $=e$ iff $ab=ba$).

This is a normal subgroup because $g^{-1}\prod_{i=1}^{k}[a_i,b_i]\,g = \prod_{i=1}^{k}[g^{-1}a_ig,\ g^{-1}b_ig]$.

$\Rightarrow g^{-1}C(G)g = C(G). \quad \forall g \in G.$

The quotient $G/[G,G]$ is called the abelianization of G.

Since $[G,G]$ contains all commutators $[a,b]$, quotienting makes $[a,b]=e$ in the quotient group, ie. $ab=ba \ \forall a,b \in G/[G,G]$.
Since $[G,G]$ is generated by commutators, it is the smallest subgroup of G with that property. The abelianization is the largest abelian group onto which G admits a surjective homomorphism.

* The free group F_n on n generators $a_1, \dots, a_n$.

Elements are all reduced words $a_{i_1}^{m_1} \dots a_{i_k}^{m_k}$ — $k \geq 0$ (empty word is e), $i_1 \dots i_k \in \{1..n\}$, $i_j \neq i_{j+1}$, $m_1 \dots m_k \in \mathbb{Z} \setminus \{0\}$

(non reduced words: reduce by:
- if $i_j = i_{j+1}$, combine $a_i^m a_i^{m'} \rightsquigarrow a_i^{m+m'}$
- if an exponent is zero, remove a_i^0).

Repeat until word is reduced.

- This is the "largest" group with n generators, all others are $\simeq$ quotients of F_n.
  If G is generated by $g_1, \dots, g_n \in G$, define a homomorphism
  $F_n \twoheadrightarrow G$ by $\prod a_{i_j}^{m_j} \mapsto \prod g_{i_j}^{m_j}$. $(\star)$
- A finitely generated group is said to be finitely presented if the kernel of $(\star)$ is the smallest normal subgroup of F_n containing some finite subset $\{r_1, \dots, r_k\} \subset F_n$ ($\hookrightarrow$ words in the generators), (ie. the subgroup generated by r_j's and their conjugates $x^{-1}r_jx$).

  Write $G \cong \langle \underbrace{a_1, \dots, a_n}_{\text{generators}} \mid \underbrace{r_1, \dots, r_k}_{\text{relations}} \rangle$, then $G \cong F_n / \langle \text{conj's of } r_1 \dots r_k \rangle$

  Ex: $\mathbb{Z}^n \cong \langle a_1, \dots, a_n \mid a_i a_j a_i^{-1} a_j^{-1} \ \forall i,j \rangle$.

  Ex: $S_3 \cong \langle t_1, t_2 \mid t_1^2, t_2^2, (t_1t_2)^3 \rangle$