Announcements: • HW 1 due (before midnight Eastern time).
• HW 2 posted

Last time, we discussed
- subgroups ($H \subset G$ subset which is also a group for the same operation)
- homomorphisms ($\varphi : G \to H$ s.t. $\varphi(ab) = \varphi(a)\varphi(b)$).

Proposition: Every finite group G is isomorphic to a subgroup of the symmetric group S_n for some n. (In fact we can take $n = |G|$).

(this is not actually helpful for classifying finite groups; instead it says subgroups of S_n are hard to classify in general).

Proof: define a map $\phi : G \longrightarrow \mathrm{Perm}(G)$ = permutations of G (bijections $G \to G$) by $\phi(g) = m_g$, where m_g is left multiplication by g, $m_g : G \to G$, $x \mapsto gx$

(Check: Why is m_g a permutation?)

- The fact that ϕ is a homomorphism follows from associativity:

$$\phi(gh) = m_{gh} : x \mapsto (gh)x$$
$$\phi(g) \circ \phi(h) = m_g \circ m_h : x \mapsto g(hx)$$
same

- If $g \neq g'$ then $m_g(e) = g \neq g' = m_{g'}(e)$, so $\phi(g) \neq \phi(g')$.

Hence ϕ is injective, and $G \simeq \mathrm{Im}(\phi) \subset \mathrm{Perm}(G) \simeq S_{|G|}$. □

An important question in group theory is the classification of finite groups up to isomorphism. This becomes increasingly difficult as $|G|$ increases. The beginning:

- every group of order 2 is isomorphic to $\mathbb{Z}/2$ (by writing the table of the composition law ...).
- similarly, every group of order 3 is $\simeq \mathbb{Z}/3$.
- for order 4, we know $\mathbb{Z}/4$ and $\mathbb{Z}/2 \times \mathbb{Z}/2$.
  (these are different: every nonzero element of $\mathbb{Z}/2 \times \mathbb{Z}/2$ has order 2, while $\mathbb{Z}/4$ has an element of order 4).

In fact these are the only two groups of order 4 up to iso.

(Classification completed in the 1980s, taking thousands of pages. We'll learn some of the key tools & concepts in the class, but certainly won't tackle the complete classification!).

Aside: equivalence relations and partitions (cf. Artin §2.7 ; also Halmos Set theory)

An equivalence relation on a set S is a way to declare certain elements equivalent to each other ("$a \sim b$"), yielding a smaller set of equivalence classes ("$S/\sim$") (the quotient of S by $\sim$).

Def: An <u>equivalence relation</u> on a set S is a <u>binary relation</u> (ie. a map $\sim : S\times S \to \underset{\text{false, true}}{\{0,1\}}$, or equivalently a subset of $S\times S$; write $a\sim b$ iff (a,b) are in this subset) which is

1) <u>reflexive</u>: $\forall a\in S,\ a\sim a$
2) <u>symmetric</u>: $\forall a,b\in S,\ a\sim b \Rightarrow b\sim a$
3) <u>transitive</u>: $\forall a,b,c\in S$, if $a\sim b$ and $b\sim c$ then $a\sim c$.

- The <u>equivalence class</u> of $a\in S$ is $\{a'\in S \mid a\sim a'\}$ (sometimes denoted $[a]$).
  (by transitivity, the elements of $[a]$ are all equivalent to each other.)
- The equivalence classes form a <u>partition</u> of S, ie. these are mutually disjoint subsets of S whose union is S.
- The <u>quotient</u> of S by $\sim$ is the set of equivalence classes: $S/\!\sim\ = \{[a] \mid a\in S\}\subset \mathcal{P}(S)$.
  This comes with a <u>surjective</u> map $\begin{aligned} S &\to S/\!\sim \\ a &\mapsto [a]\end{aligned}$

<u>Example</u>:
- $S=\mathbb{Z}$, given $n\in\mathbb{Z}_{>0}$, set $a\sim b$ iff n divides $b-a$.
  This is congruence mod n; check it is an equivalence relation.
  There are n equivalence classes
  $[0]=\{\dots,-n,0,n,2n,\dots\}=\mathbb{Z}n$
  $[1]=\{\dots,1-n,1,1+n,1+2n,\dots\}$
  $\dots$
  $[n-1]$
  The quotient is naturally in bijection with $\mathbb{Z}/n$: $\begin{aligned}\mathbb{Z} &\twoheadrightarrow \mathbb{Z}/\!\sim\ \cong \mathbb{Z}/n.\\ a &\mapsto [a]\end{aligned}$
  (we defined $\mathbb{Z}/n$ as $\{0,\dots,n-1\}$ only to avoid the language of equivalence classes) but it makes more sense to redefine it as the quotient set.
- given a map $f: S\to T$, set $a\sim b$ iff $f(a)=f(b)$.
  This is an equivalence relation; the partition into equivalence classes is $S=\bigsqcup_{t\in T} f^{-1}(t)$
  $f^{-1}(t) = \{a\in S \mid f(a)=t\}$
  $t\in T$: if f not surjective, only consider $t\in f(S)\subset T$.
  and f factors through quotient: $\begin{aligned} S &\twoheadrightarrow S/\!\sim\ \hookrightarrow T.\\ a &\mapsto [a] \mapsto f(a)\end{aligned}$
  (if f surjective then $S/\!\sim\ \cong T$)

Using this construction: equivalence relation on S $\Longleftrightarrow$ partition of S into disjoint subsets
$\Longleftrightarrow$ surjective map from S to another set T (up to composition with a bijection $T\xrightarrow{\sim}T'$).

Back to groups: assume we have a surjective group homomorphism $\varphi: G \to H$.

Recall the kernel $K = \mathrm{Ker}(\varphi) = \{a \in G \mid \varphi(a) = e_H\}$ is a subgroup of G.

Let's look at the partition of G induced by φ:

$$\varphi(a) = \varphi(b) \iff \varphi(a)^{-1}\varphi(b) = e_H \iff a^{-1}b \in K$$

let $k = a^{-1}b$, then $b = ak$ $\iff b \in aK = \{ak \mid k \in K\}$.

Def$^{\underline{n}}$ + Proposition: Given any subgroup K of a group G,

- $aK = \{ak \mid k \in K\} \subset G$ is called the (left) coset of $K \subset G$ containing a.
- The relation $a \sim b \Leftrightarrow a^{-1}b \in K$ is an equivalence relation on G, whose equivalence classes are the left cosets.
- The quotient (the set of left cosets) is denoted by G/K.

  We have a partition $G = \bigsqcup_{aK \in G/K} aK$.

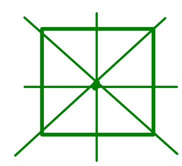
Proof:
- $a^{-1}a = e \in K$, so $a \sim a$ $\forall a \in G$.
- if $a \sim b$ then $a^{-1}b \in K$, hence $(a^{-1}b)^{-1} = b^{-1}a \in K$, hence $b \sim a$.
- if $a \sim b$ and $b \sim c$ then $a^{-1}b \in K$, $b^{-1}c \in K$, so $(a^{-1}b)(b^{-1}c) \in K$, $a \sim c$.

Also, $b \in aK \iff \exists k \in K$ s.t. $b = ak \iff \exists k \in K$ s.t. $a^{-1}b = k \iff a^{-1}b \in K \iff a \sim b$. $\square$

Example: $\varphi: \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$, $a \mapsto a \bmod n$ has kernel $\mathbb{Z}\cdot n \subset \mathbb{Z}$: the cosets are $[k] = k + \mathbb{Z}\cdot n$ $(0 \le k \le n-1)$

and we have a bijection $\mathbb{Z}/\mathbb{Z}n \cong \mathbb{Z}/n$, $[k] \mapsto k$. This gives a group law on the quotient! (addition of cosets $\Leftrightarrow$ addition mod n).

Breakout room exploration: let D_4 = symmetries of the square. (with composition)



After taking a moment to introduce yourselves to each other,

- Let $K \subset D_4$ the 4-element subgroup generated by horizontal reflection & vertical reflection?
  $h(x,y) = (-x,y)$ $\quad$ $v(x,y) = (x,-y)$

  What are the left cosets of K?

- Do products of elements in two cosets aK, bK all belong to same coset (abK?)
- What about the subgroup $H = \{e, h\}$?

  Eg. let r = rotation by $90°$. What is rH?

  Do products of two elements of rH all live in a single coset? ($rH \cdot rH = r^2H$??).

When a subgroup K is the kernel of a homomorphism $\varphi: G \twoheadrightarrow H$,

we get a bijection $G/K \cong H$

$aK \mapsto \varphi(a)$ (recall $\varphi(b)=\varphi(a)$ iff $b \in aK$).

and we can use this bijection to get a group structure on G/K, essentially

$(aK).(bK) = abK$. Then $G \twoheadrightarrow G/K$, $a \mapsto aK$ is a group homomorphism.

($\xleftrightarrow[\text{via } \varphi]{}$ $\varphi(a)\varphi(b) = \varphi(ab)$).

But this doesn't necessarily work for all subgroups $K \subset G$! E.g. it fails for $\{e,h\} \subset D_4$.

* <u>Right-cosets vs. left-cosets</u>: similarly to the left cosets $aK = \{ak \,/\, k \in K\}$ ($a \sim b \Leftrightarrow a^{-1}b \in K$)

we define <u>right cosets</u> $Ka = \{ka \,/\, k \in K\}$, which correspond to $a \sim b \Leftrightarrow ba^{-1} \in K$

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

Also denote $aKa^{-1} = \{aka^{-1} \,/\, k \in K\}$ (this one <u>is</u> a subgroup).

<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 mean 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 $(aK).(bK) = abK$ and we can take φ to be the quotient map $G \twoheadrightarrow G/K$.)

<u>Proof</u> (likely <u>next time</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>Examples</u>:
- any subgroup of an abelian group is normal. ($a+K = K+a$ ✓).
- in D_4, the subgroup $\{e,h\}$ is not normal.
  (h = horiz. reflection)

  the subgroup generated by horizontal & vertical reflection is normal.
  (and the quotient is $\simeq \mathbb{Z}/2$).
- in any group G, the <u>center</u> $Z(G) = \{z \in G \mid az = za \ \forall a \in G\}$
  (elements that commute with <u>all</u> other elements) is a normal subgroup.

  <u>Exercise</u>: check it's a subgroup.
  Clearly, $a^{-1}Z(G)a = Z(G)$, in fact $a^{-1}za = z \quad \forall z \in Z(G)$.
  This is stronger than being normal, which only requires $a^{-1}za$ to be equal to some element of the subgroup (not necessarily $= z$).

<u>Next time</u>:
- Lagrange's Theorem (H subgroup $\subset G$ finite group $\Rightarrow |H|$ divides $|G|$)
- proof of theorem on normal subgroups & kernels.
- short exact sequences
- example: subgroups of S_3
- more about permutations