Reminder: HW1 due tonight on Canvas; HW2 available on Canvas

Recall: A subgroup H of a group G is a non-empty subset $H \subset G$ which is closed under composition ($a, b \in H \Rightarrow ab \in H$) and inversion ($a \in H \Rightarrow a^{-1} \in H$). These conditions imply $e \in H$. So H (with same operation) is also a group.

Prop: if $H, H' \subset G$ are two subgroups, then $H \cap H'$ is also a subgroup.

Pf:
- $e \in H \cap H'$ so nonempty
- if $a, b \in H \cap H'$ then $ab \in H$ and $ab \in H'$, so $ab \in H \cap H'$.
- likewise for inverses. □

Similarly for more than two subgroups (even ∞ many). (However, $H \cup H'$ almost never a subgroup. Why?)

Subgroups of $\mathbb{Z}$: given $a \in \mathbb{Z}_{>0}$, $\mathbb{Z}a = \{ na \mid n \in \mathbb{Z} \} \subset \mathbb{Z}$ is a subgroup

Prop: All nontrivial subgroups of $(\mathbb{Z}, +)$ are of this form.

Proof: This follows from the Euclidean algorithm. Given a nontrivial subgroup $\{0\} \neq H \subset \mathbb{Z}$, there exists $a \in H$ such that $a > 0$. Let a_0 be the smallest positive element of H. Given any $b \in H$, $b = qa_0 + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < a_0$ (remainder). Since $b \in H$ and $qa_0 \in H$, $r \in H$. Since $r < a_0$, by def. of a_0, r must be zero. Hence $b \in \mathbb{Z}a_0$; so $H \subset \mathbb{Z}a_0$, and conversely $\mathbb{Z}a_0 \subset H$, so $H = \mathbb{Z}a_0$. □

So every subgroup of $\mathbb{Z}$ is generated by a single element a_0, in the following sense.

Q: Given a subset $S \subset G$ (nonempty), what is the smallest subgroup of G which contains S? This is denoted $\langle S \rangle$ and called the subgroup generated by S.

Answer: look at all subgroups of G which contain S (there's at least G itself!) and take their intersection: $\langle S \rangle = \bigcap_{\substack{S \subset H \subset G \\ \text{subgroup}}} H$.

More useful answer: $\langle S \rangle$ must contain all products of elements of S and their inverses, and these form a subgroup of G, so $\langle S \rangle = \{ a_1 \dots a_k \mid a_i \in S \cup S^{-1} \ \forall 1 \leq i \leq k \}$

Def: A group is cyclic if it is generated by a single element. (ex. $\mathbb{Z}$, $\mathbb{Z}/n$. These are in fact the only cyclic groups up to isomorphism).

Definition + Prop^{n}:
- The kernel of a homomorphism $\varphi: G \to H$ is $\mathrm{Ker}(\varphi) = \{ a \in G \mid \varphi(a) = e_H \}$.
- This is a subgroup of G. (check it contains e_G, products, inverses)
- φ is injective iff $\mathrm{Ker}(\varphi) = \{e_G\}$. (using: $\varphi(a) = \varphi(b) \Leftrightarrow a^{-1}b \in \mathrm{Ker}\,\varphi$)

Definition:
- The image of a group homomorphism $\varphi: G \to H$ is
$$\mathrm{Im}(\varphi) = \varphi(G) = \{ b \in H \mid \exists a \in G \text{ st. } \varphi(a) = b \}$$
- This is a subgroup of H. φ is surjective iff $\mathrm{Im}(\varphi) = H$.

Remark: if φ is injective, then G is isomorphic to the subgroup $\mathrm{Im}(\varphi) \subset H$. (the isomorphism is given by the map $G \to \mathrm{Im}(\varphi)$, $a \mapsto \varphi(a)$).

Example: Let $a \in G$ be any element in a group G, then the map $\varphi: \mathbb{Z} \to G$, $n \mapsto a^n$ is a homomorphism, with image $\langle a \rangle$ the subgroup generated by a.

Def: the order of $a \in G$ = smallest positive k such that $a^k = e$, if it exists. Else say a has infinite order.

⚠ do not confuse order of $a \in G$ with order of G ($= |G|$). Though, $\mathrm{order}(a) = |\langle a \rangle|$

If a has infinite order then powers of a are all distinct, $\varphi: n \mapsto a^n$ is injective, and $\langle a \rangle$ is isomorphic to $\mathbb{Z}$. If a has finite order k then $\ker(\varphi) = \mathbb{Z}k$, and $\langle a \rangle = \{ a^n \mid n = 0, \dots, k-1 \}$ is isomorphic to $\mathbb{Z}/k$.

(This completes the classification of cyclic groups, by the way).

Example: $\mathbb{Z}/6 \xrightarrow{\sim} \mathbb{Z}/2 \times \mathbb{Z}/3$ (observe: $(1,1) \in \mathbb{Z}/2 \times \mathbb{Z}/3$ has order 6, so generates).
$a \mapsto (a \bmod 2, a \bmod 3)$

Similarly, $\gcd(m,n) = 1 \Rightarrow \mathbb{Z}/m \times \mathbb{Z}/n \simeq \mathbb{Z}/mn$. But $\mathbb{Z}/2 \times \mathbb{Z}/2 \not\simeq \mathbb{Z}/4$
$x + x = 0 \ \forall x$ vs. $1 + 1 \neq 0$.

We will likely skip this proposition and come back to it later, when discussing group actions).

SKIP

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 $G \simeq \mathrm{Im}(\phi) \subset \mathrm{Perm}(G) \simeq S_{|G|}$. $\square$

An important question in group theory is the <u>classification of finite groups</u> 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!).

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

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

<u>Def</u>: An <u>equivalence relation</u> on a set S is a <u>binary relation</u> (ie. 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 $\begin{aligned} S &\longrightarrow S/\sim \\ a &\longmapsto [a]\end{aligned}$

<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 $\{0,..,n-1\}$ 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 $S = \bigsqcup_{t\in T} f^{-1}(t)$ $\quad f^{-1}(t) = \{a \in S \mid f(a)=t\}$
  if f not surjective, only consider $t \in f(S) \subset T$.
  and f factors through quotient: $S \twoheadrightarrow S/_\sim \hookrightarrow T$.
  $a \mapsto [a] \mapsto f(a)$
  (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:

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

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

Def^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, $b \in aK \Leftrightarrow \exists k \in K$ st. $b = ak \Leftrightarrow \exists k \in K$ st. $a^{-1}b = k \Leftrightarrow a^{-1}b \in K \Leftrightarrow a \sim b$. $\square$

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 $[k] = k + \mathbb{Z}\cdot n$ $(0 \le k \le n-1)$

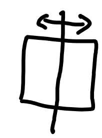
and we have a bijection $\mathbb{Z}/\mathbb{Z}n \cong \mathbb{Z}/n$, $[k] \mapsto k$. This gives a group law on the quotient! (addition of cosets $\Leftrightarrow$ addition mod n)

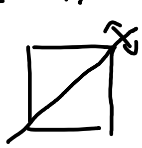
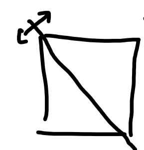
When a subgroup K is the kernel of a homomorphism $\varphi: G \twoheadrightarrow H$,
we get a bijection
$$G/K \cong H$$
$$aK \mapsto \varphi(a) \qquad (\text{recall } \varphi(b)=\varphi(a) \text{ iff } b\in aK).$$
and we can use this bijection to get a group structure on G/K, essentially
$(aK).(bK) = abK$. $\left(\xleftrightarrow[\text{via } \varphi]{} \ \varphi(a)\varphi(b) = \varphi(ab)\right)$.

Then $\begin{array}{l} G \twoheadrightarrow G/K \\ a \mapsto aK \end{array}$ is a group homomorphism.

For a general subgroup $K \subset G$, however, trying to make G/K a group by setting $(aK).(bK) = abK$ might not work. The obstacle to this is:

Assume $a \sim a'$ ($\Leftrightarrow aK = a'K \Leftrightarrow a^{-1}a' \in K$) and $b \sim b'$ ($\Leftrightarrow bK = b'K \Leftrightarrow b^{-1}b' \in K$).
Does it follow that $ab \sim a'b'$? ($\Leftrightarrow abK = a'b'K$?) (if not, our operation isn't well defined).

<u>Ex</u>: $G = D_4$ = symmetries of square, $H = \{e, h\}$ where h = horiz. flip 
Then $e \sim h$ (coset $eH = hH = \{e,h\}$), but setting r = rotation by $90°$ 

$h \circ r =$  vs. the coset of $e \circ r = r$ is $\{ r$, $r \circ h =$  $\}$

$\Rightarrow h \circ r \not\sim e \circ r$ even though $h \sim e$ (and $r \sim r$).

* <u>Right-cosets</u> vs. <u>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 means the two equivalence relations above agree.

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

<u>Theorem</u>: 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 $(aK).(bK) = abK$