Announcements: CA office hours; Monday is a holiday; course feedback survey.

* <u>Set theory interlude:</u>

<u>Recall:</u> a map of sets $f: S \to T$ is
- <u>injective</u> if $\forall a,b \in S$, $f(a)=f(b) \Rightarrow a=b$. (or: $a\neq b \Rightarrow f(a)\neq f(b)$). Write $f: S \hookrightarrow T$
- <u>surjective</u> if $\forall c \in T\ \exists a \in S$ s.t. $f(a)=c$. Write $f: S \twoheadrightarrow T$.
- a bijection $f: S \xrightarrow{\sim} T$ if both hold.

* Say two sets S,T have the <u>same cardinality</u> if $\exists$ bijection $f: S\to T$, and write $|S|=|T|$.
If there exists an injection $f: S\hookrightarrow T$ then write $|S|\leq|T|$. This notation is legit thanks to the <u>Schröder-Bernstein theorem</u>:

‖ If there exist injective maps $f: S\hookrightarrow T$ and $g: T\hookrightarrow S$ then $|S|=|T|$.

(see Halmos Naive set theory p.88 for a proof; build a bijection $S\xrightarrow{\sim}T$ by using f on a subset of S and g^{-1} on the rest).

<u>Ex:</u> $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ all have the same cardinality, these are called <u>countably infinite</u>

e.g. construct a bijection $\mathbb{N}\to\mathbb{Z}$ by setting $f(n) = \begin{cases} n/2 & \text{if } n \text{ even} \\ -(n+1)/2 & \text{if } n \text{ odd.}\end{cases}$

for $\mathbb{Q}$, first understand how to enumerate $\mathbb{N}\times\mathbb{N}$ = pairs of integers.

* On the other hand, $\mathbb{R}$ is <u>uncountable</u>, using Cantor's diagonal argument:
No map $f: \mathbb{N}\to\mathbb{R}$ can be surjective, because:

write decimal or binary expansion of
$$\begin{aligned} f(0) &= a_{00}.a_{01}a_{02}a_{03}\ldots\ldots \\ f(1) &= a_{10}.a_{11}a_{12}a_{13}\ldots\ldots \\ f(2) &= a_{20}.a_{21}a_{22}a_{23}\ldots \\ f(3) &= a_{30}.a_{31}a_{32}a_{33}\ldots\ldots \end{aligned}$$

then let $y = b_0.b_1b_2b_3\ldots$ where we choose $b_j \neq a_{jj}$ for each j.
Looking at the j^{th} digit, $y\neq f(j)$ for all $j\in\mathbb{N}$, so f can't be surjective.

* The same argument shows there are arbitrarily large cardinals:
given a set S, let $\mathcal{P}(S) = \{\text{subsets of } S\}$ ("power set of S")

$$\begin{array}{c} \mathcal{P}(S) \\ \uparrow\cong \\ \{0,1\}^S = \{\text{maps } f: S\to\{0,1\}\} \end{array} \qquad \left(f\mapsto f^{-1}(1)\right) \quad A \mapsto \left(\mathbb{1}_A: x\mapsto \begin{cases}1 & \text{if } x\in A\\ 0 & \text{if } x\notin A\end{cases}\right)$$

If S is finite, $|S|=n$, then $|\mathcal{P}(S)|=2^n$. What if S is infinite?

<u>Thm:</u> ‖ if S is infinite then $|\mathcal{P}(S)|>|S|$.

This is just the diagonal argument again. Do you see how?

<u>Pf:</u> (Cantor): Given $f: S\to\mathcal{P}(S)$, let $A=\{x\in S \mid x\notin f(x)\}$. Assume $A=f(a)$ for some $a\in S$.
Then $a\in A$ iff $a\notin f(a)=A$, contradiction. So $A\notin f(S)$, $\nexists$ surjection. □

Back to groups: Recall:

Def^n: A group G = a set with an operation $G\times G \longrightarrow G$, $(a,b)\longmapsto a.b$ such that
(1) identity: $\exists\, e\in G$ st. $\forall a\in G$, $ae=ea=a$.
(2) inverse: $\forall a\in G\ \exists\, b(=a^{-1})\in G$ st. $ab=ba=e$.
(3) associativity: $\forall a,b,c\in G$, $(ab)c=a(bc)$.

Examples: numbers, matrices, permutations, ...

We didn't have time to discuss: Products of groups:

- Given two groups G, H, the product group is $G\times H=\{(g,h)\,/\,g\in G,\ h\in H\}$ with composition law $(g,h)\cdot(g',h')=(gg',hh')$.
- If G, H are finite, of order $m=|G|$ and $n=|H|$, then $G\times H$ is a finite group of order mn.
- Similarly for product of n groups:
  Ex: $\mathbb{Z}^n=\{(a_1,\dots,a_n)\,|\,a_i\in\mathbb{Z}\}$, $(a_1,\dots,a_n)+(b_1,\dots,b_n)=(a_1+b_1,\dots,a_n+b_n)$
  (similarly $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$ with componentwise addition)
- Given infinitely many groups $G_1, G_2, G_3, \dots$, there are two different notions:
  → the direct product $\prod_{i=1}^{\infty} G_i=\{(a_1,a_2,a_3,\dots)\,|\,a_i\in G_i\}$
  → the direct sum $\bigoplus_{i=1}^{\infty} G_i=\{(a_1,a_2,a_3,\dots)\,|\,a_i\in G_i,\ \text{all but finitely many are identity}\}$

Ex: consider $G_0=G_1=\dots=(\mathbb{R},+)$, denote $(a_0,a_1,a_2,\dots)$ by $\sum a_i x^i$.
then $\prod_{i=0}^{\infty}\mathbb{R}=\mathbb{R}[[x]]$ formal power series $\sum_{i=0}^{\infty} a_i x^i$ (w/ addition)
$\bigoplus_{i=0}^{\infty}\mathbb{R}=\mathbb{R}[x]$ polynomials $\sum_{\text{finite}} a_i x^i$.

★ Subgroups:

Def: 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.

Say H is a proper subgroup if $H\subsetneq G$

Examples:
- $(\mathbb{Z},+)\subset(\mathbb{Q},+)\subset(\mathbb{R},+)\subset(\mathbb{C},+)$
- $(\mathbb{Q}^*,\times)\subset(\mathbb{R}^*,\times)\subset(\mathbb{C}^*,\times)\supset(S^1,\times)$
- $\{e\}\subset G$ trivial subgroup
- $H_i\subset G_i \Rightarrow H_1\times\dots\times H_n\subset G_1\times\dots\times G_n$
- $\bigoplus G_i\subset\prod G_i$

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 $0 \le r < a_0$ (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 $H = \mathbb{Z}a_0$. $\square$

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

Observe: 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. $\square$

Similarly for more than two subgroups.

Now: 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 $\langle S \rangle = \{a_1 \dots a_k \mid a_i \in S \cup S^{-1} \ \forall 1 \le i \le k\}$

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).

Ex: $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a,b,c,d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$ can be generated by two elements! [exercise! fairly hard without hint].

Homomorphisms:

Def: Given two groups G, H, a homomorphism $\varphi: G \to H$ is a map which respects the composition law: $\forall a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b)$. (This implies $\varphi(e_G) = e_H$, and $\varphi(a^{-1}) = \varphi(a)^{-1}$).

Rmk: A pedantic way to state $\varphi(ab) = \varphi(a)\varphi(b)$ is by a commutative diagram

$$\begin{tikzcd} G \times G \arrow[r, "\varphi \times \varphi"] \arrow[d, "m_G"'] & H \times H \arrow[d, "m_H"] \\ G \arrow[r, "\varphi"'] & H \end{tikzcd}$$

"Commutative diagram" means

$$\begin{tikzcd} G \times G \arrow[dr, bend left] \arrow[dr, bend right] & \\ & H \end{tikzcd}$$

give the same map: it doesn't matter if we multiply first or apply φ first.

- an <u>isomorphism</u> is a bijective homomorphism (two isomorphic groups are "secretly the same")
- an <u>automorphism</u> is an isomorphism $G \to G$.

<u>Examples:</u> (isomorphisms)

- all groups of order 2 are isomorphic! $S_2 = (\{id, (1\,2)\}, \circ) \cong (\{\pm 1\}, \times) \simeq (\mathbb{Z}/2, +)$ because the table is always

m	e	x
e	e	x
x	x	e

- $(\mathbb{R}, +) \xrightarrow[\exp]{\sim} (\mathbb{R}_+, \times)$ $\quad (\mathbb{R}/\mathbb{Z}, +) \xrightarrow[\exp(2\pi i t)]{\sim} (S^1, \times)$
- $S_3 \cong$ symmetries of $\triangle$ (permutation of vertices).

<u>Examples:</u> (homomorphisms)

- $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$, $a \mapsto a \bmod n$ (remainder of Euclidean division by n).
- if $n|m$, $\mathbb{Z}/m \twoheadrightarrow \mathbb{Z}/n$ similarly (eg. $\underset{\text{last 2 digits}}{\mathbb{Z}/100} \to \underset{\text{last digit}}{\mathbb{Z}/10}$)
- determinant: $GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^*, \times)$
  $(\det(AB) = \det(A)\det(B))$.

<u>Definition:</u> + <u>Prop^n</u>

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

<u>Definition:</u>

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

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

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

<u>Def:</u> the <u>order</u> 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, 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 $\langle a \rangle = \{a^n \mid n = 0, .., k-1\}$ is isomorphic to $\mathbb{Z}/k$.

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

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

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. $1 + 1 \neq 0$.